UNIVERSIDADE PRESBITERIANA MACKENZIE

JOSÉ ANTONIO CORRALES TORRES

UM MÉTODO DE CLASSIFICAÇÃO EM GRUPOS DE INFORMAÇÕES VISANDO SUA SEGURANÇA

São Paulo
2008

JOSÉ ANTONIO CORRALES TORRES

UM MÉTODO DE CLASSIFICAÇÃO EM GRUPOS DE INFORMAÇÕES VISANDO SUA SEGURANÇA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Presbiteriana Mackenzie como parte dos requisitos para a obtenção do Título de Mestre em Engenharia Elétrica.

Orientador: Prof. Dr. Nizam Omar

São Paulo
2008

C823m Corrales Torres, José Antonio.
Um método de classificação em grupos de informações visando sua segurança / José Antonio Corrales Torres – 2008.
153 f. : il. ; 30 cm.

Dissertação (Mestrado em Engenharia Elétrica) - Universidade Presbiteriana Mackenzie, São Paulo, 2008.
Bibliografia: f. 144-153.

1. Informações. 2. Segurança. 3. Classificação das informações. 4. Redes neurais. 5. Redes de Kohonen. 6. Mapas auto-organizáveis. I. Título.

CDD 006.32

JOSÉ ANTONIO CORRALES TORRES

UM MÉTODO DE CLASSIFICAÇÃO EM GRUPOS DE INFORMAÇÕES VISANDO SUA SEGURANÇA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Engenharia Elétrica da Universidade Presbiteriana Mackenzie como parte dos requisitos para a obtenção do Título de Mestre em Engenharia Elétrica.

Aprovado em: São Paulo, de de 2.008

BANCA EXAMINADORA

Prof. Dr. Nizam Omar - Orientador
Universidade Presbiteriana Mackenzie

Prof[a]. Dr[a]. Maria Inês Lopes Brosso
Universidade Presbiteriana Mackenzie

Prof. Dr. Alessandro Anzaloni
Instituto Tecnológico da Aeronáutica

À memória do meu pai José, à minha mãe Maruja, à minha amada esposa Cristina e aos meus queridos filhos Alethea e Juan Carlos, pelo amor e carinho incondicional e o pleno apoio em todos os momentos.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus que me presenteou as condições necessárias para realizar meus maiores sonhos.

Aos professores do programa de pós-graduação em Engenharia Elétrica da Universidade Presbiteriana Mackenzie, que além da competência técnica, da sabedoria e do conhecimento, também transmitiram prazer pela docência.

Ao Prof. Dr.Nizam Omar pela gentileza de suas sugestões e orientações, sempre oportunas e precisas.

À Prof[a]. Dr[a]. Pollyana Notargiacomo Mustaro pelo auxilio em muitas oportunidades que a ela recorri.

Aos meus pais pelos extraordinários e diligentes esforços para proporcionar minha base ética e moral.

Aos meus filhos, pela inesgotável fonte de amor, motivação, alegria e felicidade.

À minha esposa Cristina, por sua compreensão, dedicação e apoio à nossa família, que permitiu minha maior dedicação a este programa.

Aos amigos alcançados neste programa de pós-graduação, sempre presentes, que muitas vezes, em detrimento do próprio interesse, estiveram disponíveis e foram incansáveis em auxiliar-me. Destaque ao Patric, Fabiano, Eric e Joaquim.

Ao Fábio Alves, pela sua amizade, companheirismo e contribuição para o desenvolvimento deste estudo.

“Um livro deve ser o machado que quebra o mar gelado em nós mesmos”
(Franz Kafka)

Para minha Família e meus Amigos

"Porque Me fizeste este pedido, e não pediste longa vida, nem riqueza, nem a morte de teus inimigos, mas sim inteligência para praticar a justiça, vou satisfazer o teu desejo; dou-te um coração tão sábio e inteligente, como nunca houve igual antes de ti, nem haverá depois. Dou-te, além disso, o que não Me pediste: riquezas e glória, de tal modo que não haverá nenhum rei que te iguale durante toda a tua vida. E se andares nos Meus caminhos e observares os Meus preceitos e mandamentos como o fez David, teu pai, conceder-te-ei longa vida"
1 Reis 3, 11-14

RESUMO

Na sociedade contemporânea, a informação e o conhecimento assumiram a importância de representar os ativos de maior valor, num cenário em que o espaço e o tempo, devido à tecnologia voltada à mobilidade, perderam a relevância e tornaram-se mais vulneráveis. Surgiram novos procedimentos e mecanismos destinados à segurança. A classificação das informações é o requisito fundamental para direcionar as medidas, o nível de proteção e o custo. Atualmente o processo é manual, restrito ao entendimento de algumas pessoas e sujeito a imperfeições. Este estudo propõe um método para classificar as informações, quanto à sua confidencialidade, em grupos gerados por uma Rede Neural Artificial. O desenvolvimento deste método foi pautado por estudos em metodologias destinadas à segurança das informações, ao gerenciamento de risco de negócio e tecnológico, metodologias para classificação e estruturas de controle. A implementação usou a Rede Neural, baseada nos Mapas Auto-Organizáveis (*SOM*) de Kohonen, devido à sua acentuada especialização no tratamento de grupos. O estudo de caso objetivou a implementação e contemplou as informações das universidades, em razão da diversidade de suas propriedades (administrativa, pedagógica e pesquisa científica). A análise dos resultados obtidos permitiu observar a semelhança dos elementos que compõe os grupos gerados pelo treinamento da Rede Neural, complementado por cálculos que utilizam os pesos iniciais. Mostrou-se a viabilidade da aplicação do método proposto para uma organização.

Palavras-chave: informações, segurança, classificação das informações, redes neurais, redes de Kohonen, mapas auto-organizáveis.

ABSTRACT

In the contemporary society, information and knowledge grew in importance and have become the most valuable assets, space and time are less relevant and more vulnerable due to the increasing mobile technology. New procedures and processes were created towards security. The information classification is the primary requirement to adjust rules and procedures, the protection level and cost. The current process is manual, restricted by the knowledge of few people and subject to imperfections. This study suggests a method to classify the information, regarding its confidentiality, using groups generated by an Artificial Neural Network. The development of this method was supported by studies of methodologies applied to information protection, to the technology and business risk management, classification methodologies and control structures. The implementation made use of a Neural Network, based on the Self-Organization Maps (SOM) of Kohonen, due to its heavy specialization on groups handling. The study case objective was the implementation and it considered the information from universities, due to their various properties (administrative, pedagogic and scientific research). The analysis of the results indicated the similarity among the elements that composed the groups generated by the training of the Neural Network, complemented by calculations using the original weights. The viability of the application of the considered method to an organization was confirmed.

Index Terms: information, security, information classification, artificial neural networks, Kohonen's net, self-organization maps.

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

CAPÍTULO 1 – INTRODUÇÃO

1.1 – Problema e Motivação

As últimas décadas têm sido marcadas pela abrangência e importância das inovações tecnológicas e pela fugacidade de seu uso, criando um ciclo de vida dos produtos de curta duração. Dentre os principais efeitos decorrentes da ampliação do uso e da dependência de recursos tecnológicos nas atividades cotidianas da sociedade, se observa a crescente importância e valor das informações (Stallings, 2005).

Em face do avanço das inovações tecnológicas, as concepções de espaço e de tempo perderam a relevância, de forma que o virtual usa novos espaços e novas velocidades, problematizando e reinventando o mundo (Lévy, 1997). Como conseqüência, grande parte dos ativos perdeu a tangibilidade e passou a ser representado por informação e conhecimento.

O novo ambiente tem fronteiras sutis, fragilidade do controle e facilidade de dissimular a identidade dos usuários. Permite o desenvolvimento e a disseminação de ameaças ao seu conteúdo, assim como pode atender a interesses ilícitos (Lévy, 1997).

A reação da sociedade manifestou-se através da criação de estruturas de controle e o desenvolvimento de mecanismos para o gerenciamento de riscos, o que permitiria nortear as medidas de segurança para proteger todos os ativos e, principalmente, as informações (NIST, 2004b). Paralelamente, foram criados dispositivos de segurança física e lógica com a finalidade de aprimorar a segurança no trânsito e guarda dos dados.

Os estudos voltados à implementação de segurança ressaltam a importância de classificar as informações quanto a sua demanda pela preservação de sigilo, como pode ser observado nas estruturas de trabalho, como o *Control Objectives for Information and Related Technology* - Cobit 4.1 (*ITGI*, 2007) ou padrões de segurança da informação, como a ABNT NBR ISO/IEC NBR 17799 (*ISO*, 2005). Contudo, hoje em dia, a classificação dos níveis de confidencialidade se dá pelo senso comum de um grupo de usuários,

que baseado em sua experiência, estabelece uma categoria de sigilo de maior conveniência. Esta categorização determinará a escolha dos dispositivos e dos procedimentos de proteção à informação (NIST, 2004b).

Os recursos atuais não afiançam a uniforme e adequada categorização da informação, cuja imprecisão provocará danos consideráveis. Se os níveis de confidencialidade e integridade forem determinados em proporções superiores à sua real demanda, onerará os custos computacionais e de segurança desnecessariamente. Caso contrário, permitirá a exposição de dados imprudentemente, com conseqüências danosas nas atividades relacionadas às informações classificadas. Portanto, a assertividade na classificação, atrelada ao eficiente gerenciamento dos dispositivos de segurança, estabelecem uma relação satisfatória e econômica.

A escassez de recursos financeiros disponíveis para inversão em segurança associada à diversidade de ofertas de serviços e dispositivos para esse fim, compele ao refinamento de separar o conhecimento, informações ou dados que efetivamente representem valor para as organizações, de maneira a preservar o patrimônio e a acurácia dos investimentos (Schneier, 2001).

Entretanto, o levantamento realizado em artigos acadêmicos, disponíveis em sites de universidades nacionais e estrangeiras, e junto a profissionais envolvidos com segurança de sistemas de informação, em indústrias, bancos, consultorias e universidades brasileiras, apresentou a ausência de métodos e recursos que desempenhem satisfatoriamente a classificação das informações com base em rotinas automáticas, uniformes e evolutivas. De maneira geral, a motivação deste estudo está representado em na Figura 1-1, desenvolvida pelo autor.

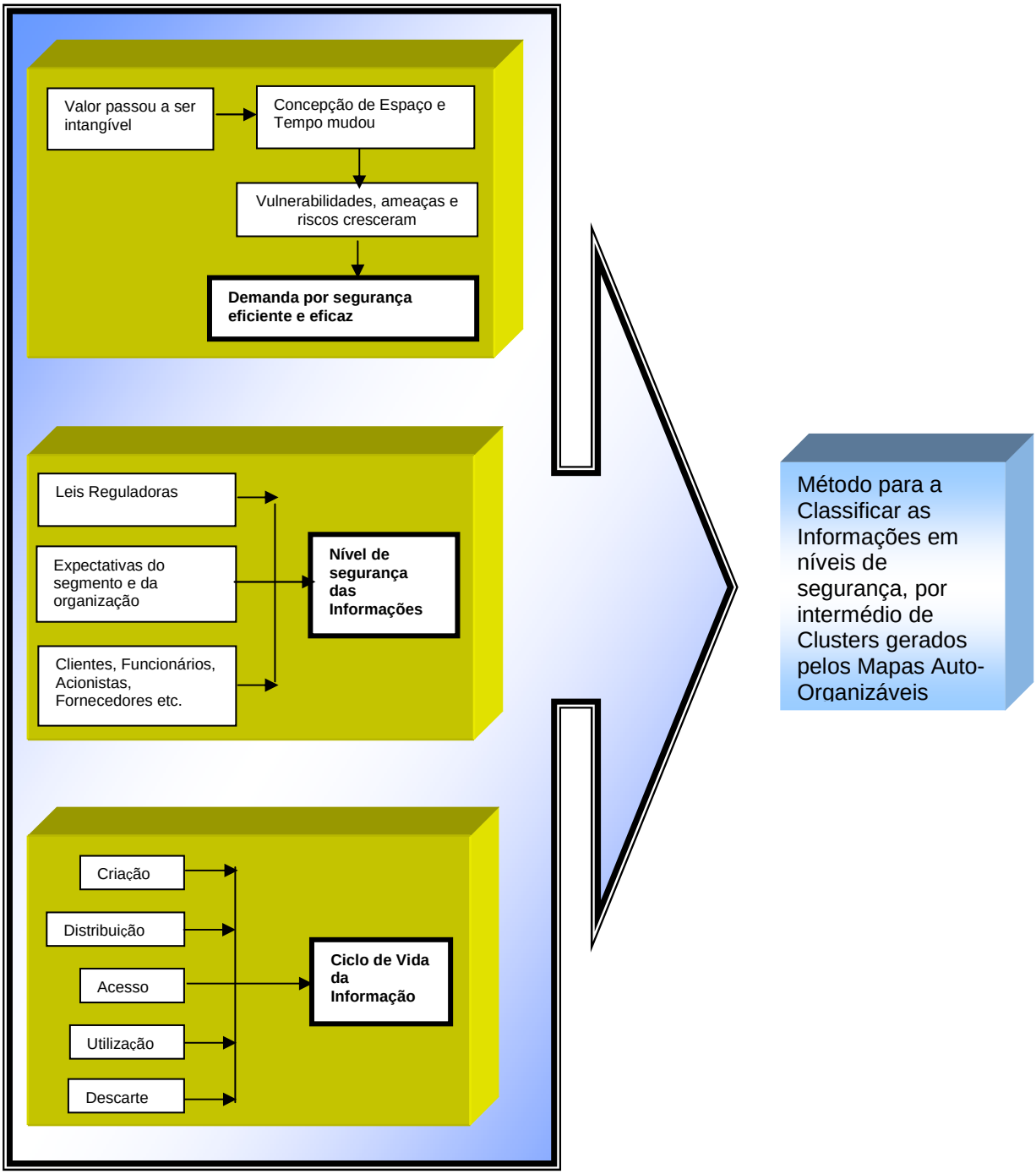

Figura 1-1: Motivação

1.2 - Objetivos

O objetivo deste estudo é mostrar um método que reduza a incidência de erro no processo de classificação das informações, de maneira a proporcionar a melhor relação entre os custos (financeiros, operacionais,

desempenho etc.) e a adequada segurança e proteção dos ativos representados pela informação e conhecimento.

A proposta é um estudo destinado ao desenvolvimento de um método de classificação das informações que seja baseado em conhecimento e experiências anteriores e seja uniforme, sistemático e assertivo.

Visa apresentar uma alternativa para classificar as informações, que considerará a necessidade de sigilo e integridade, baseado em um sistema de rede neural de inteligência artificial, não supervisionada, desenvolvido por Teuvo Kohonen, denominado *Self Organization Maps* (*SOM*).

1.3 – Metodologia Utilizada

O desenvolvimento deste trabalho considerou que Método é um procedimento regular, explícito e passível de ser repetido para alcançar um objetivo material ou conceitual. Método científico é um conjunto de procedimentos por meio dos quais são propostos os problemas científicos e, a seguir, são colocadas à prova as hipóteses científicas (Bunge, 1974).

As etapas destinadas ao desenvolvimento do método proposto estão baseadas no conhecimento do problema, na busca de dados e instrumentos relacionados, na proposição de uma solução baseada nos levantamentos realizados, na implementação e análise dos resultados alcançados. Estas etapas assemelham-se ao método denominado por Bunge como teoria da investigação (Lakatos e Marconi, 1995).

Os métodos de pesquisa apresentados por Lakatos e Marconi (1995) podem ser resumidos em método indutivo, que parte de observações particulares para fazer generalizações e o método dedutivo, que parte de observações gerais e chega a conclusões particulares. Algumas características distinguem os métodos indutivos e dedutivos, conforme apresenta o Quadro 1-1.

Quadro 1-1: Características dos Métodos Dedutivo e Indutivo

DEDUTIVO	INDUTIVO
• Se todas as premissas são verdadeiras, a conclusão deve ser verdadeira.	• Se todas as premissas são verdadeiras, a conclusão é provavelmente verdadeira, mas não necessariamente verdadeira.
• Toda a informação ou conteúdo factual da conclusão já estava, pelo menos implicitamente, nas premissas.	• A conclusão encerra informação que não estava, nem implicitamente, nas premissas.

Fonte: Salmon (1979)

No estudo realizado, a identificação do problema partiu da observação a respeito da evolução de perdas ocasionadas por falhas de segurança na infra-estrutura de TI e nos sistemas de informação, com impacto relevante nos produtos, processos e atividades das organizações. Em semelhante proporção houve a evolução da oferta de dispositivos de segurança, contudo sem atenuar de forma eficaz e eficiente os efeitos das ameaças diante das vulnerabilidades.

Posteriormente, visou identificar a perspectiva do problema constatado diante de um cenário tecnologicamente evolutivo e contextualizado pelo gerenciamento de riscos em diversos segmentos de atividades. Adicionalmente o trabalho apresenta alguns mecanismos de controle e segurança de maior destaque.

O levantamento realizado visou o conhecimento de estruturas de controle e segurança destinadas às organizações, independente do seu segmento de atuação, com objetivo de obter referência dos critérios e padrões que poderão ser aplicados no estudo.

Foram realizados estudos de metodologias destinadas à preservação da segurança das informações. Estas foram desenvolvidas por entidades que possuem abrangência internacional e por entidades do governo norte americano que detêm responsabilidade por direcionar os procedimentos de controle e segurança das informações tratadas no âmbito das instituições federais. A aplicação destas metodologias tem auxiliado grande parte das organizações que mantêm interesse pela preservação do sigilo, integridade e

disponibilidade das informações, entretanto, sem alcançar a acurácia de proteção para cada tipo específico de informação.

As principais fontes relativas às metodologias analisadas que estudam e atuam neste campo, encontram-se relacionadas no Quadro 1-2.

Quadro 1-2: Fontes de Pesquisa

Entidade	Atuação	Abordagem
National Institute of Standards and Technology (NIST)	Fundada em 1901, é uma agência federal do Departamento de Comércio dos USA, cuja missão inclui a promoção de padrões de segurança em tecnologia.	• Gerenciamento de riscos; • Associação do Risco Técnico com o Risco de Negócio; • Controles Técnicos.
"International Organization for Standardization" e "International Electro technical Commission" (ISO/IEC)	Centralizada em Genebra, Estabelece padrões aplicáveis a empresas púbicas e privadas, com objetivo de interligá-las através da regulamentação e compatibilidade técnicas dos seus produtos, métodos de produção e serviços, segurança e qualidade.	• Padrão de Segurança das Informações.
US Department of Justice (DoJ)	Fazer cumprir a lei e defender os interesses dos USA; para garantir a segurança pública contra as ameaças externa e interna; proporcionar a liderança federal na prevenção e controle da criminalidade; prover punição aos culpados de comportamento ilícito; e de garantir a justa e imparcial administração da justiça para os americanos.	• Metodologia para a Classificação das Informações.
IT Governance Institute (ITGI)	Criada em 1998, para assegurar a efetividade dos processos de TI, visa assegurar o cumprimento das metas corporativas, maximizar investimentos tecnológicos e administrar adequadamente os recursos de TI, relacionando riscos e oportunidades.	• Estrutura de Controle denominado Cobit, cuja aplicação é voltada para a governança de TI.
Bank for International Settlements. (BIS)	Estabelecido desde 1930, sua atuação é caracterizada como o Banco Central Mundial, assim, além de promover a cooperação financeira e monetária internacional, norteia as exigências de controle e segurança.	• Classificação dos Riscos de Negócio; • Gerenciamento de risco voltado às atividades de negócio.

Fonte: Autor

O estudo dos riscos apresentados pelo BIS foi desenvolvido objetivando alcançar os aspectos financeiros, todavia são aplicáveis a todas as atividades de negócio, em qualquer segmento.

Considere-se que os sistemas de informação e a infra-estrutura de TI atende essencialmente aos interesses das atividades primárias das organizações. Nesse contexto, qualquer falha de segurança que permita o sucesso de uma ameaça causará invariavelmente impacto às organizações, por meio de demandas legais, perdas financeiras, desconforto aos clientes, funcionários etc.

Portanto, o estudo apresentado pelo BIS auxiliou a elaboração da classificação dos riscos, decorrentes de falhas de controle no ambiente computacional, que causam impacto nas atividades de negócio. Esta mesma abordagem é apresentada pelo NIST na descrição do Risco Técnico, onde destaca a importância da integração do risco técnico (infra-estrutura de TI) e do risco de negócio.

Os processos e as etapas destinadas à classificação das informações foram subsidiados no modelo desenvolvido pelo Departamento de Defesa dos Estados Unidos da América, cujo principal objetivo é auxiliar a proteção das informações do governo federal e, por conseguinte, proteger o cidadão americano. Também foram aplicadas, no desenvolvimento do modelo proposto, as diretrizes para a classificação especificadas pelo NIST.

Após o entendimento do problema e sua contextualização, iniciou-se o estudo de alternativas de Redes Neurais de Inteligência Artificial com foco na implementação parcial do modelo. Nesta fase, além do *SOM* de Kohonen, também foram analisados as Redes Bayesianas e Sistemas Especialistas. A rede neural selecionada foi o *SOM*, devido a sua apropriada característica ao tratamento de clusters, através do software *Matlab*.

O Estudo de Caso visa representar a aplicação dos levantamentos realizados em um segmento de atividade que contemple características diversificadas em seus processos e atividades e, preferencialmente, não apresente estruturas pré-estabelecidas de segurança, como seriam as empresas que atuam em segmentos de reconhecida exposição ao risco de ameaças perenes (exemplo: bancos).

Uma vez selecionado o segmento de atuação destinado ao desenvolvimento do Estudo de Caso, é necessário identificar suas rotinas e atividades de maior importância para proceder ao conhecimento das Categorias de Risco próprios ao segmento escolhido. Com base nos fluxos operacionais, por onde transitam e são armazenadas as informações, e nos agentes de maior relevância (funcionários, clientes, acionistas, governo etc.), inicia-se a seleção de um grupo de informações destinadas ao treinamento da rede neural. Deve ser representativa, de maneira que alcance o maior número de produtos, processos, atividades e agentes envolvidos.

A correlação entre as Categorias de Risco e as Informações Selecionadas será estabelecida por um grupo de profissionais que desempenham funções afetas ao controle, segurança ou ocupações afins. A tabela de correlação preenchida representará os dados de entrada para o treinamento da rede neural. Esta desenvolvida em *Matlab* formulará o agrupamento em clusters que mostrarão a categorização que determinará o nível de segurança e proteção requerido.

Os resultados alcançados serão analisados e passíveis de apresentação a um profissional especialista em controle e segurança de TI, para emissão de parecer a fim de subsidiar a conclusão do trabalho.

Os trabalhos futuros serão extraídos do corpo deste trabalho, como forma complementar a este estudo iniciado.

1.4 – Organização do Trabalho

A seguir será descrito um resumo dos próximos capítulos que apresentam o contexto do problema tratado neste trabalho, a fundamentação teórica e a proposta de uma alternativa de solução.

O segundo capítulo apresentará a “Importância da segurança das informações” e descreverá o papel que a informação e o conhecimento está assumindo no contexto contemporâneo, ao ponto de representar os ativos de maior valor que transitam e são armazenados no formato digital. Este novo formato de riqueza atende as circunstâncias atuais, cuja dimensão de tempo e

espaço deixaram de impor limites e restrições para a execução de trabalhos em qualquer segmento de atividade. Neste capítulo também serão mostrados os estudos destinados à análise dos riscos correspondentes, os quais serão responsáveis por direcionar as medidas de proteção e segurança.

O capítulo três, “Tecnologias de Segurança e Classificação das Informações”, tem como objetivo mostrar os principais mecanismos de segurança destinados à proteção das informações. Apresenta os conceitos e procedimentos necessários para a classificação das informações, bem como o processo implementado pelo Departamento de Justiça do governo norte americano para esta finalidade. Também mostra um estudo de Redes Neurais.

O quarto capítulo, “Proposta de um Modelo de Informações” visará justificar a solução apresentada neste trabalho e as etapas necessárias para seu o desenvolvimento com o uso de uma rede neural.

A aplicação experimental deste trabalho será descrita no capítulo cinco, “Estudo de Caso para Informações Acadêmicas”, onde serão exibidos os mecanismos selecionados para o estudo de caso e a visualização dos resultados.

O último capítulo, “Resultados e Conclusões”, expõe a análise dos resultados alcançados, as conclusões obtidas e os próximos trabalhos que serão desenvolvidos após a conclusão deste estudo de caso.

CAPÍTULO 2 - IMPORTÂNCIA DA SEGURANÇA DAS INFORMAÇÕES

Este capítulo visa apresentar a importância das informações e do conhecimento num contexto de transformação de valores, da sua forma de representação, uma vez que o dinamismo e a profundidade da inovação tecnológica têm modificado os processos, produtos e serviços que envolvem as corporações, universidades, governos, organizações não governamentais e os hábitos cotidianos da população de forma geral.

Nesta nova realidade, parte dos bens é representada por artigos tangíveis, tais como imóveis, automóveis, moedas etc., porém há acentuado crescimento na participação do patrimônio constituído por ativos intangíveis como o valor de uma marca, o conhecimento adquirido, o dinheiro representado por informações, dentre outros. Em contraposição às benesses ofertadas pelo progresso, observa-se o surgimento crescente e diversificado de novas ameaças com a finalidade de subtração de riqueza.

2.1 Transformação dos valores tangíveis em informações

A partir de meados do século passado, a evolução tecnológica desencadeou profundas alterações no comportamento da sociedade e principalmente na geração de riqueza, pela criação de novos segmentos e destruição de outros, por outro lado também produziu oportunidades para ascensão social.

Essas alterações provocaram mudanças nos conceitos de “Valor”, uma vez que outrora havia um vínculo direto entre a materialidade e a representação do valor. Estas mudanças podem ser observadas na história que deu origem ao dinheiro representado em papel-moeda até sua transformação em código binário, que transita por impulso elétrico ou por ondas de rádio a velocidades crescentes e dimensões físicas irrestritas.

2.1.1 Virtual e Real

O desastre social observado no final dos anos 90, causadas pelas crises do México, Rússia e Sudoeste Asiático teve correlação com a liberdade e a facilidade tecnológica de transferência de capitais entre os países, aos simples comandos, realizados pelos investidores, em seus computadores (Cassen, 1999).

A título de exemplo, foram comparadas as duas modalidades econômicas, (real e virtual). No âmbito da “Economia Virtual”, o Citibank, em uma única operação especulativa sobre divisas, obteve resultado equivalente a quase o dobro do lucro de um semestre obtido pelo grupo automobilístico francês Peugeot-PSA.

No banco, há 350 pessoas empregadas como operadores numa sala de negócios; na Peugeot, são 140 mil trabalhadores. Há uma parte significativa dos 21 trilhões de dólares investida em especulação sobre moedas ou divisas. Aproximadamente US$ 1,8 bilhão mudam de titularidade a cada dia, além de mudar de divisa (Cassen, 1999).

Este contexto tecnológico, político, econômico e financeiro implicou em profundas alterações na sociedade no que tange as ameaças, vulnerabilidades, controles e gerenciamento de risco, para corporações, universidades e interesses pessoais conectados mundialmente e hoje fortemente expostos a atos criminosos e terroristas, praticados por meio de recursos tecnológicos.

A compreensão do processo de virtualização da economia requer a análise de um contexto teórico de caráter multidisciplinar, com ênfase nas ciências sociais, econômicas e na pesquisa das novas tecnologias de informação parte do conceito de virtual Lévy (1997). A palavra virtual tem origem no latim medieval *virtualis*, derivado por sua vez de *virtus*, força, potência. Na filosofia escolástica, é virtual o que existe em potência e não em ato. O virtual tende a atualizar-se, sem ter passado, no entanto, à concretização efetiva ou formal. Em termos filosóficos, o virtual não se opõe ao real, mas ao atual.

Para Lévy (1997) há uma falsa oposição entre o real e o virtual. Freqüentemente, a palavra virtual tem sido usada para significar a pura e simples ausência de existência, a 'realidade' supondo uma efetuação material, uma presença tangível. O autor enfatiza as concepções de espaço e de tempo (o desprendimento do aqui e agora), de forma que o virtual usa novos espaços e novas velocidades, problematizando e reinventando o mundo. No virtual, os limites de espaço e tempo não são relevantes e há um compartilhamento de maior amplitude, criando circunstâncias em que não há uma clara separação entre o ambiente público e o privado, das informações próprias das informações comuns, do que é subjetivo e do que é objetivo.

O ambiente virtual é caracterizado pela sutileza das fronteiras, fragilidade do controle e facilidade de dissimular a identidade dos usuários. Permite o desenvolvimento e a disseminação de ameaças ao seu conteúdo e também o uso para atender aos interesses operacionais e estratégicos do crime organizado, o que compreende ações ilícitas suportadas em eficiente fluxo de informações e na operação de atividades econômicas diversificadas, tais como construção civil, transporte de carga, esporte, *show business* etc. A legitimação desses recursos financeiros, de origem criminosa, também utiliza as condições propiciadas pelo ambiente virtual para executar a lavagem "eletrônica" e tornar regular e legitimo o produto ilícito.

Para Lévy (1997) a virtualização da economia é fortemente dependente de dois ativos primordiais e particulares: informação e o conhecimento. São considerados dessa maneira em razão de sua importância para a produção de riquezas; particulares porque se diferem de outros bens pela sua característica de compartilhamento, uma vez que sua cessão não implica em sua perda e o seu consumo não decorre na sua destruição.

Uma boa metáfora da chamada globalização vista pelas lentes das novas ferramentas de comunicação, é dada pelo jornalista Clóvis Rossi: A notícia do assassinato do presidente norte-americano Abraham Lincoln, em 1865, levou 13 dias para cruzar o Atlântico e chegar à Europa. A recente queda da Bolsa de Valores de Hong Kong levou 13 segundos para cair como um raio sobre São Paulo, Tóquio, Nova York, Tel Aviv, Buenos Aires e Frankfurt.

De acordo com Dantas (1996), o ordenamento institucional vem sendo objeto de profundas reformas, para possibilitar a apropriação do valor da informação, privatizando-a e retirando dela seu caráter social. A invenção do circuito integrado (chip), na década de 40, viabilizou, definitivamente, a digitalização da informação. A partir daí, tornou-se possível reduzir todo tipo de informação em uma seqüência de zeros e uns. Texto, som e imagens se transformam em bits.

2.1.2 Dinheiro na sociedade

Em 15 de agosto de 1971, o presidente norte-americano Richard Nixon decretou a extinção do sistema monetário que impunha ao dólar americano o lastro equivalente em ouro. A desvinculação do dinheiro de uma base de sustentação real se deveu ao superávit das reservas de dólar (US$ 300 bilhões), frente às reservas em ouro (US$ 14 bilhões) nos cofres do governo norte-americano.

Para Kurtzman (1995) a proposta de Nixon tirou da moeda os valores subjacentes e tornou o dinheiro (que representava um símbolo de riqueza reconhecidamente tangível) em uma abstração deturpada. Em que pesem as decorrências no âmbito macro econômico, o Ato do governo americano retirou qualquer limitação da capacidade de emissão, o autor entende que este ato representaria o início de um processo que determinará a queda da importância do dinheiro tradicional.

Este fato é determinante para o início de uma nova era, onde muitos autores passaram a tratar da transmutação do dinheiro em impulso eletrônico, ou apenas uma combinação do código binário que viaja em extraordinária velocidade entre uma vasta diversidade de dispositivos eletrônicos, interligando as Corporações de diversos segmentos e portes, onde a maioria das localidades mundiais se tornou acessível.

Ainda de acordo com Kurtzman (1995), o dinheiro eletrônico propiciou a criação de um novo ambiente que inclui redes que integram todos os mercados do mundo: ações, bônus, futuros, moedas, taxas de juros, opções etc. Este novo ambiente recebeu a denominação de “Economia Virtual”, baseada em

dinheiro eletrônico e passou a dividir o mundo econômico em duas partes. A “Economia Real”, na qual os produtos são fabricados, serviços são prestados e pesquisas são realizadas etc., por outro lado, a “Economia Virtual” é baseada em ultratecnologia e responde por uma movimentação na ordem de trilhões de dólares americanos diários, entre diversas redes, sem controle adequado e com pouca regulamentação governamental.

2.1.3 Perspectiva do Dinheiro

A partir dos anos 90, a inovação dos recursos tecnológicos vem transformando os hábitos de significativa parcela dos cidadãos que realizam transações de qualquer ordem, sejam aquisições, empréstimos, aluguéis etc., cuja liquidação é feita por meio de transferência de dinheiro.

Intrinsecamente, o dinheiro representa valor, contudo, os processos e os recursos tecnológicos estão transformando a mesma representação de valor em pura informação. Especificamente, há uma referência direta no valor que passou da representação das notas e moedas (físico) para o formato digital (invisível, volátil, intangível) (Exame VIP, 2007).

O Conselho de Pagamentos Europeu considera que a União Européia efetua 360 bilhões de transações em dinheiro a um custo superior a €50 bilhões (US$65 bilhões) por ano. A bandeira de cartões de crédito Visa estima que o dispêndio em pequenos itens seja da ordem de US$ 1,3 Trilhão por ano.

Gradativamente foram criadas alternativas para sobrepor desconfortos do papel-moeda. O primeiro produto data da década de 50 e deu origem ao que hoje conhecemos por Cartão de Crédito. Evidente que, à época, não geravam informações, mas eram de plástico e, por isso, muito práticos. Sua evolução continuou e propiciou o crescimento do comércio internacional (Exame VIP, 2007).

Atualmente, a importância maior recai sobre a disponibilidade de recursos financeiros das pessoas, empresas, universidades ou entidades para

saldar seus compromissos. A essa disponibilidade é atribuído o nome de crédito, e sobre o qual passará a fundamentar-se o dinheiro eletrônico.

A utilização de dinheiro eletrônico apresenta forte tendência de crescimento, uma vez que em alguns países são oferecidos descontos mediante pagamentos efetuados por dinheiro eletrônico. Como conseqüência, há estimativa que o papel-moeda possa extinguir-se dentro de 15 anos (*The Economist*, 2007). Ainda assim, permanecerão nichos para sua utilização, dentre estes restará a população que não possui acesso aos bancos, *Smart Cards* ou companhias telefônicas.

As companhias telefônicas foram relacionadas junto aos bancos, em razão da tendência dessas empresas intermediarem transações monetárias entre os cidadãos, principalmente por meio de telefones celulares, equipados com chips, que permitem armazenar créditos e efetuar pagamentos de maneira rápida e segura. Estes produtos estão implantados em alguns países asiáticos e africanos. As operadoras de telefones celulares anunciam novos serviços que permitirão realizar transferências de recursos financeiros entre paises, mesmo que o emissor e o receptor não possuam uma conta bancária.

Será necessário analisar todos os impactos decorrentes desse novo cenário, uma vez que a ampliação de transações eletrônicas, permite visualizar o fluxo de informação com abrangência jamais imaginada, como os dados de valores, datas, produtos adquiridos, estabelecimentos, freqüência de compras etc., cujo rastreamento permite descrever os hábitos e perfil das pessoas e empresas. Assim, poderá caracterizar-se a perda gradual de privacidade e acarretará novos incômodos aos cidadãos.

2.2 Contexto da Informação

Negroponte (2001), em seu artigo sobre Civilização Digital, destaca o desenvolvimento econômico de países que efetuaram inversões de capital na tecnologia disponível e observa a aproximação da economia digital aos consumidores.

O autor cita a profundidade das alterações observadas nas atividades que se tornaram possíveis a partir da conjugação das inovações tecnológicas e, por decorrência desses fatos, afirma que brevemente haverá um volume maior de “coisas” conectadas à rede mundial de computadores, em detrimento da conectividade entre as pessoas.

Destaca a mudança nos fatores geográficos que serão submetidos às demarcações digitais, deixaram de ser local para tornarem-se universais. Haverá aproximação dos habitantes do campo às vantagens e a qualidade do mundo urbano. Finalmente, Negroponte prevê que o processo educacional passará a produzir alterações palpáveis e será importante objeto de transformações.

A transformação da sociedade contemporânea, que abrange aspectos geográficos, econômicos e tecnológicos, em grande parte é motivada pela concorrência globalizada. Como principal resultado, observa-se o desenvolvimento de nações, regiões, setores, empresas e até indivíduos.

Segundo Cassiolato e Lastres (2000), as condições fundamentais para este cenário da economia globalizada são propiciadas por amplos processos de inovação, relacionados ao desenvolvimento e à transferência do conhecimento, seja este tácito ou explícito, por intermédio das estruturas eficientes de Tecnologia da Informação (TI).

Cassiolato e Lastres (2000) descrevem o processo de inovação como dependente do desenvolvimento tecnológico e sua difusão pela interação entre organizações e segmentos distintos de toda sociedade, empresas públicas e privadas e as entidades envolvidas em pesquisa científica. A inovação resulta em maior velocidade no desenvolvimento e na transferência do conhecimento. Em seu artigo, os autores mencionam as quatro tendências identificadas pela União Européia quanto ao processo inovativo:

- Redução do tempo para o lançamento de novos produtos, a aplicação comercial do novo conhecimento e o ciclo de vida dos produtos;
- O rápido desenvolvimento e uso amplo de TI e comunicações;

- A integração de diferentes tecnologias, baseadas em diferentes disciplinas científicas e;
- Maior participação dos centros produtores do conhecimento, dada a crescente necessidade do processo inovativo se apoiar em avanços científicos.

A evolução dos processos tecnológicos viabilizou o acesso à informação por um contingente maior de pessoas, que compõem um grupo diferenciado e heterogêneo voltado à informação e ao aprendizado, com acesso a tecnologias convergentes, que tratam de forma simplificada as informações em diversos formatos (textual, sonoro, gráfico, visual etc.), em entidades ou objetos, que são disponibilizados de acordo com a necessidade particular de um individuo ou grupo.

Apesar da alteração do perfil dos usuários, a rapidez do desenvolvimento e a substituição de tecnologias desafiam as habilidades dos leigos e dos profissionais da informação em termos do seu entendimento, domínio e gerenciamento efetivo; assim como se reconhece a importância das habilidades de criação, busca, análise e interpretação da informação, de forma que as necessidades se tornam cada vez mais complexas e dependentes de múltiplas fontes.

A integração das diversas tecnologias, o desenvolvimento dos sistemas de informação, a aceleração do processo de inovação e a produção de conhecimento têm motivado e fortalecido a sociedade globalizada que é pautada pelo dinamismo e a velocidade das decisões que envolvem a migração de capital e a transferência das atividades produtivas de um país para outro. Além da transferência física de uma fábrica, os valiosos conteúdos informativos transitam por intermédio de seus executivos (conhecimento) e pelas redes de comunicação eletrônica. Valorizada como recurso, atualmente a informação define a competitividade de pessoas, grupos, produtos, serviços e atividades.

A gestão integral dos recursos de informação nas organizações inclui diversas disciplinas, porém destaca o contexto político, ético, social e legal. Este estudo representa as situações e políticas que englobam as atividades

humanas em geral e de informação em particular, incluindo o direito à privacidade, à não-segregação informativa, à liberdade de informação, à segurança de dados, dentre outros.

2.3 Segurança das Informações

De acordo com Stallings (2005), antes do uso extensivo do processamento eletrônico de dados, a segurança de informações era feita principalmente por meios físicos e administrativos. Atualmente as medidas de segurança são necessárias para proteger os dados durante sua transmissão e na sua guarda. Também deve garantir sua autenticidade.

A necessidade de segurança da informação nas organizações tem sofrido duas importantes mudanças nas últimas décadas. Com a introdução do computador a necessidade de ferramentas automatizadas para proteger arquivos e outras informações tornou-se evidente. Em especial para os sistemas compartilhados, que estão disponíveis a partir de redes telefônicas ou de dados. A segunda mudança foi a introdução dos sistemas distribuídos, por meio das redes e dos recursos de comunicação para transportar dados entre o terminal do usuário e o computador central e também entre computadores.

Na visão de Stallings (2005), a tecnologia para as aplicações de segurança de rede e de computadores está fundamentada na criptografia. Por essa razão, o gerenciamento de segurança se concentra na geração, distribuição e no armazenamento de chaves de criptografia. A este processo é adicionado o monitoramento de controle de acesso às redes de computadores e, ao acesso às informações de gerenciamento de rede.

Segundo Gollmann (1999), segurança computacional trata a prevenção e detecção de ações não autorizadas a um sistema computacional. Garfinkel e Spafford (1996) definem que um sistema é seguro caso este se comporte de acordo com o esperado. A diferença entre as duas definições está no modo de medir a segurança. A primeira visão mede a ausência de ataques ou o sucesso das ações danosas aos sistemas computacionais, enquanto Garfinkel e Spafford relacionam a segurança com a capacidade do sistema garantir a continuidade dos serviços após um ataque.

A necessidade de proteção deve ser definida a partir das possíveis ameaças que uma organização pode sofrer e dos riscos decorrentes. Portanto, cada organização tem, por obrigação, que estabelecer o que pode ser permitido em termos de segurança. O principal recurso que estabelece a diretriz sobre o grau de segurança que a organização deseja alcançar é a política de segurança. Esta também determina como cada parte do sistema deve funcionar e ser utilizada, os direitos e deveres de cada elemento que utiliza o sistema, e como e quais os ativos devem ser protegidos.

De acordo com Ferraiolo *et al.* (2003) o controle de acesso visa determinar os direitos do usuário sobre determinado recurso, o período permitido para exercer seus direito e de que forma poderá fazê-lo. Assim, o controle de acesso se tornou uma das principais soluções para segurança computacional e para mitigar os riscos relacionados à informação. Os objetivos de segurança da informação podem ser categorizados em Confidencialidade, Integridade e Disponibilidade, cuja descrição, a definição de perda e impactos estão descritos no Quadro 2-1.

Quadro 2-1: Descrição Perda e Impacto dos Objetivos de Segurança

Objetivo de Segurança	Descrição	Definição de Perda	Impacto
Confidencialidade	Guarda segura e privada da informação, inclui qualquer situação (de segredo de estado a um memorando) e tipo de informação (financeira, de segurança etc.).	Sua perda implica na divulgação não autorizada da informação.	Pode resultar em desrespeito de privacidade, constrangimento, ações legais etc.
Integridade	Proteção da informação, quanto à alteração imprópria, por pessoas ou grupos não autorizados.	Sua perda implica na destruição ou modificação, não autorizada, da informação.	Pode gerar a imprecisão dos dados, fraude, decisões incorretas e afeta a disponibilidade e a confidencialidade.
Disponibilidade	Garante que a informação é disponível para uso quando é requisitada.	Sua perda ocasiona a interrupção de acesso ou uso da informação e dos sistemas de informação.	Pode resultar na perda de funcionalidade e eficiência operacional da organização.

Fonte: Descrição (Ferraiolo et al., 2003); Definição de Perda. (NIST,2004 b) e; Impacto (NIST, 2002).

Stallings (2005), adiciona aos objetivos de segurança citados, um quarto objetivo dedicado a Autenticidade, que define a exigência de um host ou um serviço que seja capaz de verificar e validar a identidade de um usuário.

A preservação dos objetivos de segurança é assegurada pela autorização e a autenticação dos usuários, desde que a validação mantenha a dependência entre ambos.

Autenticação é o processo que determina a legitimidade da reivindicação de uma identificação do usuário, portanto comprova que o usuário é realmente quem diz ser. Uma das formas mais comuns de autenticação é o uso de senhas, contudo o uso de equipamentos biométricos (utilizam características do ser humano para identificação, tais como: impressão digital, íris, voz, veias da palma da mão etc.), *smart cards* etc. vêm apresentando maior eficácia e eficiência. O principal requisito de autenticação é reconhecer algo que seja do conhecimento exclusivo do usuário, ou algo que o usuário tenha ou algo que represente uma característica física do usuário. Atualmente, é comum a sobreposição de recursos de autenticação (senha, cartão e outros etc).

Autorização é o ato de determinar se um usuário, seja uma pessoa, um grupo de pessoas ou um sistema computacional, têm o direito de executar determinada tarefa, tal como leitura ou alteração do conteúdo de um arquivo ou execução de um programa. Geralmente os usuários encontram-se divididos em diferentes grupos com características de direitos distintos (Kuong, 1974).

Autenticidade e autorização são sempre empregadas em conjunto, pois um usuário deve ser autenticado antes de poder executar tarefas que ele esteja autorizado a executar (Kuong, 1974).

2.3.1 Requerimentos de Segurança de TI

Na literatura sobre segurança em sistemas de informação, a norma NBR ISO/IEC 17799 (*ISO*, 2005), derivada da norma inglesa BS7799, e a estrutura de trabalho para governança corporativa em Tecnologia da Informação denominado *Control Objective for Information and Related Technology* (Cobit)

são unânimes em determinar a importância de classificar as informações na exata medida da necessidade em manter a restrição de acesso para um grupo específico de pessoas, a fim de assegurar sua condição de confidencialidade. Atualmente, os critérios aplicados para a classificação são subjetivos e dependem do conhecimento tácito das pessoas que detêm essa responsabilidade, normalmente baseados na experiência e na realidade vivida por cada um deles.

Estas circunstâncias não afiançam o uniforme e adequado atributo originado na classificação da informação, que pode incorrer em inexatidão, com efeitos danosos aos proprietários e usuários. Caso o nível de confidencialidade seja determinado em proporções superiores à sua real demanda, pressupõe a redução do desempenho do processamento devido ao uso de recursos de segurança desnecessários e também ao encarecimento dos custos. Se o nível determinado for inferior à sua real necessidade, permitirá a exposição de dados, cuja conseqüência é a evolução dos riscos nas diversas atividades relacionadas às informações classificadas. A assertividade na classificação das informações, atrelada a um eficiente processo de definição dos dispositivos de segurança, estabelece uma relação satisfatória e econômica na implementação de uma política corporativa de segurança.

O critério adotado para a classificação obedece à importância e a necessidade que cada informação demonstra para a preservação do sigilo em todo o ciclo de maturação, permitindo que sua classificação seja revista de acordo com sua propriedade. Isto significa que o modelo apresentado poderá tratar situações pré-estabelecidas que levem à nova classificação, quando decorrente da concretização de determinados eventos ou datas previstas, de maneira que será possível identificar e alterar a classificação do maior nível de confidencialidade para a condição de informação pública.

Para o NIST (2002), os requerimentos de segurança são baseados em padrões sistemáticos, evolutivos e que identificam as vulnerabilidades dos ativos (pessoas, hardware, software, informação), dos processos e das informações associados aos sistemas de TI distribuídos nas áreas de segurança Gerencial, Operacional e Técnica.

A identificação das vulnerabilidades que envolvem as informações pode atender aos critérios de segurança em TI, estabelecido por cada organização. Os critérios são sugeridos no Quadro 2-2.

Quadro 2-2: Critérios de Segurança

Área de Segurança	Critérios de Segurança
Gerenciamento da Segurança	• Definição de responsabilidades • Suporte contínuo • Capacidade de resposta a incidentes • Revisões periódicas dos controles e segurança • Segurança pessoal e competência para investigar • Avaliação de risco • Treinamento de segurança e aspectos técnicos • Segregação de funções • Sistema de autorização e re-autorização • Sistema ou aplicação do plano de segurança
Segurança Operacional	• Controle sobre o ar-condicionado • Controle para assegurar a qualidade do fornecimento de energia • Acesso e disponibilidade dos dados nas suas respectivas mídias • *Label* e distribuição externa das informações • Facilidade de proteção • Controle de unidade • Controle de temperatura • Estações de trabalho, laptops e PC *stand alone*

Fonte: NIST (2002)

Os controles são necessários para tratar os aspectos de segurança, abrangem métodos técnicos e não-técnicos. Controles técnicos são salvaguarda do que está incorporado nos computadores hardware, software ou firmware (ex. mecanismos de controle de acesso, identificação e autenticação, criptografia, software para identificar intrusão)

Controles não técnicos são aqueles gerenciais e operacionais, tal qual as políticas de segurança, os procedimentos operacionais, os pessoais, os físicos e a segurança de ambiente.

De acordo com o NIST (2002), as Categorias de Controle descrevem a característica de sua aplicação e podem ser divididos em controles:

- Preventivo: inibe tentativas de violação da política de segurança, controle de acesso etc. e;
- Detectivo: alerta as violações ou tentativas que afetam às políticas de segurança, controles de trilhas de auditoria etc.

2.4 Administração de Risco

As alterações originadas pelo processo de mudança sistemática e profunda provocam, na mesma intensidade, a alteração das variáveis que afetam os controles de proteção contra ameaças e ataques. O estudo da administração de risco destina-se a direcionar as ações que visam restabelecer o controle e a proteção esperados.

2.4.1 A Evolução do Estudo do Risco

Em toda a sua existência, o ser humano sempre conviveu com o risco. A partir da determinação de correr riscos a humanidade conquistou novas terras, alcançou tratamentos que prolongam vidas, evoluiu em pesquisas e até conquistou o espaço sideral. O risco é um fator limitador, mas é também propulsor da ousadia que levou o homem às conquistas substanciais. Estudar a evolução do risco significa conhecer um pouco da trajetória da história do homem, cuja concepção moderna do risco teria suas raízes no sistema de numeração indo-arábico que alcançou o Ocidente há cerca de oitocentos anos (Bernstein, 1997). Mas o estudo sério do risco começou no Renascimento, quando as pessoas se libertaram das restrições do passado e desafiaram abertamente as crenças consagradas.

O estudo do risco, na forma com é visto hoje, teve início no século XVII com o desenvolvimento do cálculo das probabilidades (Toranzos, 1969). Os seus iniciadores foram os matemáticos italianos e franceses, particularmente Fermat e Pascal, que iniciaram os estudos do cálculo de probabilidades tratando de resolver problemas de jogos de azar propostos pelo Cavaleiro de Méré:

> “Em 1654, época em que o Renascimento estava em pleno alvorecer, o cavaleiro de Méré, um nobre francês com gosto pelo jogo e pela matemática, desafiou o famoso matemático francês Blaize Pascal a

> decifrar um enigma. A pergunta era como dividir as apostas de um jogo de azar entre dois jogadores, que foi interrompido quando um deles estava vencendo. O enigma confundira os matemáticos desde sua formulação, duzentos anos antes, pelo monge Luca Paccioli. Este foi o homem que trouxe a contabilidade das partidas dobradas à atenção dos homens de negócios da época – e ensinou as tabuadas de multiplicação a Leonardo da Vinci. Pascal pediu ajuda a Pierre de Fermat, advogado que também era brilhante matemático. O resultado de sua colaboração foi pura dinamite intelectual. O que poderia parecer uma versão do século XVII do jogo da Busca Trivial levou à descoberta da teoria das probabilidades, o núcleo matemático do conceito de risco (Bernstein,1997)".

A solução do enigma de Paccioli permitiu que, pela primeira vez, as pessoas tomassem decisões e previssem o futuro com ajuda dos números. Nos mundos medieval e antigo, ou mesmo nas sociedades pré-escrita e camponesas, os indivíduos conseguiam tomar decisões, defender seus interesses e praticar o comércio, mas sem uma compreensão real do risco ou da natureza da tomada de decisões. Atualmente, as pessoas dependem da superstição e da tradição menos que no passado, não por serem mais racionais, mas porque a compreensão do risco permite tomar decisões de modo racional (Bernstein,1977).

Com o passar do tempo, a teoria da probabilidade passou a ser instrumento poderoso para a interpretação e aplicação das informações, dando origem a técnicas quantitativas de administração do risco. Por volta de 1715 surgiram as tabelas de expectativa de vida.

Cem anos após a descoberta dos pilares da teoria da probabilidade, produto do encontro entre Pascal e Fermat, foi que Thomas Bayes, um dissidente Pastor, demonstrou matematicamente ser possível tomar melhores decisões ao se mesclar novas e velhas informações. Trata-se do Teorema de Bayes, que focaliza as situações em que é possível contar com julgamentos intuitivos seguros sobre a probabilidade de algum evento e de que maneira podemos alterá-los com o desenrolar dos eventos reais.

Para Bernstein, todas as ferramentas atualmente usadas na administração do risco resultam das evoluções ocorridas entre 1654 e 1760. No entanto cita duas exceções: A descoberta da chamada regressão à média, por Francis Galton em 1875, que versa sobre a expectativa de que as coisas voltarão “à normalidade”, após a tomada de uma decisão. Outra exceção foi a demonstração matemática que a diversificação do investimento leva a redução de riscos, por uma ferramenta desenvolvida por Harry Markowitz, ganhador do Prêmio Nobel em 1952, então um jovem estudante de doutorado em pesquisa operacional na Universidade de Chicago. Essa revelação desencadeou o movimento intelectual que revolucionou Wall Street, as finanças corporativas e as decisões empresariais em todo o mundo; seus efeitos até hoje se fazem sentir.

2.4.2 Gerenciamento do Risco

As origens da palavra risco remontam ao latin resecare (“cortar separando”). O significado teve origem na noção de perigo que os navegantes tinham ao passar por rochas perigosas e pontiagudas (Jorion, 1999). Deriva também do italiano antigo risicare (“ousar”), sentido em que o risco é uma opção e não um destino.

A história do risco trata das ações que ousamos tomar e dependem de nível de liberdade de opção ao qual estamos subordinados (Bernstein, 1997). Gitman (1997) considera risco como a possibilidade de que os resultados realizados possam diferir daqueles esperados, portanto, para efeito de inversão de investimentos, quanto maior o risco envolvido, há expectativa de taxas de retorno mais altas. Risco pode ser definido como a volatilidade de resultados inesperados, normalmente relacionada ao valor de ativos ou passivos de interesse (Jorion, 1999).

No estudo do risco é importante distinguir risco de incerteza. Risco se aplica a resultados que possam ser estimados pela experiência ou por dados estatísticos. A incerteza está presente quando o resultado não pode ser previsto. Portanto, a incerteza está presente em toda análise e deve testar suas

suposições de risco através da análise de sensibilidade e avaliação do impacto da mudança (Marshall, 2002). Há eventos que parecem fortuitos, mas não são.

Também é importante distinguir os fatos aleatórios dos resultados que apresentem a relação de causa e efeito. Ao correr risco, se aposta em um resultado, que será conseqüência de uma decisão tomada.

> "A essência da administração do risco está em maximizar as áreas onde temos certo controle sobre o resultado, enquanto minimizamos as áreas onde não temos absolutamente nenhum controle sobre o resultado e onde o vínculo entre efeito e causa está oculto de nós." (Bernstein, 1997).

Para Jorion (1999), os negócios das empresas estão relacionados à administração de riscos, uma vez que aquela com maior competência tem êxito, outras não. Embora algumas aceitem os riscos financeiros incorridos de forma passiva, outras se esforçam por ter vantagem competitiva, expondo-se a riscos de maneira estratégica. Porém, em ambas esses riscos devem ser monitorados cuidadosamente, visto que podem acarretar grandes perdas. O autor recorre à citação de Walter Wriston, ex-presidente do Citcorp "tudo na vida é administração de risco, não sua eliminação". Para Gitman (1997), as pessoas racionais estão sempre assumindo riscos e os administradores de empresas devem entender a relevância do risco e do retorno para suas atividades diárias.

2.4.3 Gerenciamento de Risco no ambiente de TI

Em termos de estratégia organizacional, risco é a possibilidade de ocorrência de um determinado evento hostil que possa reduzir o valor dos seus ativos (Blakley, 2002). Este evento hostil, ou risco, representa um custo, mesmo quando envolve a segurança das informações, pode ser quantificado (Farahmand, 2003). Estes custos refletem tanto o impacto financeiro causado por ataques às informações, quanto pelos gastos na aquisição e implementação de recursos de segurança.

Tal mensuração é possível pelo gerenciamento de risco que essencialmente atua em torno da decisão de quanto poderá ser gasto na segurança do ambiente de TI e, se os gastos justificarão os benefícios obtidos

(*ITGI*, 2007). Por isso, segurança das informações é uma disciplina norteada pelo gerenciamento de risco.

O gerenciamento de risco permite balancear os custos operacionais e econômicos das medidas de proteção e alcançar ganhos na missão de capacitar a proteção dos sistemas de TI e das informações. Este processo é aplicável a outras atividades operacionais e de negócio das organizações (NIST, 2002).

Devido ao atual ambiente de competição, as organizações não têm mecanismo de controle que levem a certeza da totalidade de suas vulnerabilidades ou sobre a eficiência de suas medidas de segurança. O gerenciamento de risco busca substituir esta incerteza pela quantificação da probabilidade de perigo, pela estimativa das possíveis conseqüências e o peso dos custos de proteção contra esses perigos (Geer *et al.*, 2003). Ainda destacam três realizações que impulsionaram as organizações em direção ao gerenciamento de risco:

- A fragilidade do ativo da informação: A maioria das organizações tem o sucesso altamente dependente das informações. Todas as ocorrências de falha de segurança, corrupção ou destruição intensifica a preocupação sobre essa dependência. A magnitude da segurança da informação e da necessidade de proteção contra as ameaças tem se expandido;
- Indisponibilidade de métricas consistentes de segurança: Como resultado há dificuldade em determinar opções satisfatórias, efetivas de segurança, conseqüentemente não é possível mensurar as despesas necessárias em segurança;
- Justificativa do custo: O clima atual da economia e a concorrência por aplicação em recursos registrada nos orçamentos de TI demonstra a pouca disponibilidade financeira para inversão em segurança. A relação entre custo e benefício, o retorno de investimento passou a desempenhar um papel de destaque para obter recursos financeiros destinados a segurança.

Diversos Órgãos Reguladores têm imposto a adoção de mecanismos para o gerenciamento seguro dos riscos. Por exemplo, o Acordo de Capital da Basiléia II requer aos bancos uma alocação de reserva de capital financeiro para cobrir os riscos de crédito, mercado e operacional, o que inclui a segurança das informações (BIS, 2004).

O gerenciamento de risco aplicado aos Sistemas de Informação é tratado pelo *National Institute of Standards and Technology – Technology Administration* (*NIST*), órgão do governo americano responsável pela segurança computacional e gerenciamento de TI das organizações públicas.

De acordo com o NIST (2002) o gerenciamento de risco para os sistemas de TI é composto essencialmente pelos processos de: Análise de Risco (identificação, avaliação e impactos); Mitigação do Risco (priorização, implementação e manutenção das medidas de proteção) e Avaliação do Risco (contínua revisão dos processos chaves para implementar o gerenciamento de risco).

Destaca a importância de designar uma autoridade e um sistema destinado ao tratamento do risco residual, o que compreende o nível de aceitação ou a decisão de implementação de controles de segurança que favorecem a eliminação ou a redução dos riscos residuais.

2.4.3.1 Análise de Risco de Sistemas de TI

Na maioria das organizações as redes locais continuam se expandindo e atualizando, os componentes são trocados e os softwares aplicativos são substituídos e atualizados em novas versões. Adicionalmente, as mudanças de pessoas e das políticas de segurança ocorrem rotineiramente. O conjunto de mudanças cria novos riscos que demandam avaliações constantes e evolutivas.

Risco é a função que apresenta a *Probabilidade* das *Ameaças* exercerem sua potencialidade sobre as *Vulnerabilidades*, que resultam em *Impacto* adverso. A probabilidade considera a conjugação das ameaças, as vulnerabilidades e os controles. Os impactos referem-se à magnitude dos

eventuais danos. A metodologia de avaliação de risco para sistemas de TI compreende nove etapas (NIST, 2002) representadas na Figura 2-1.

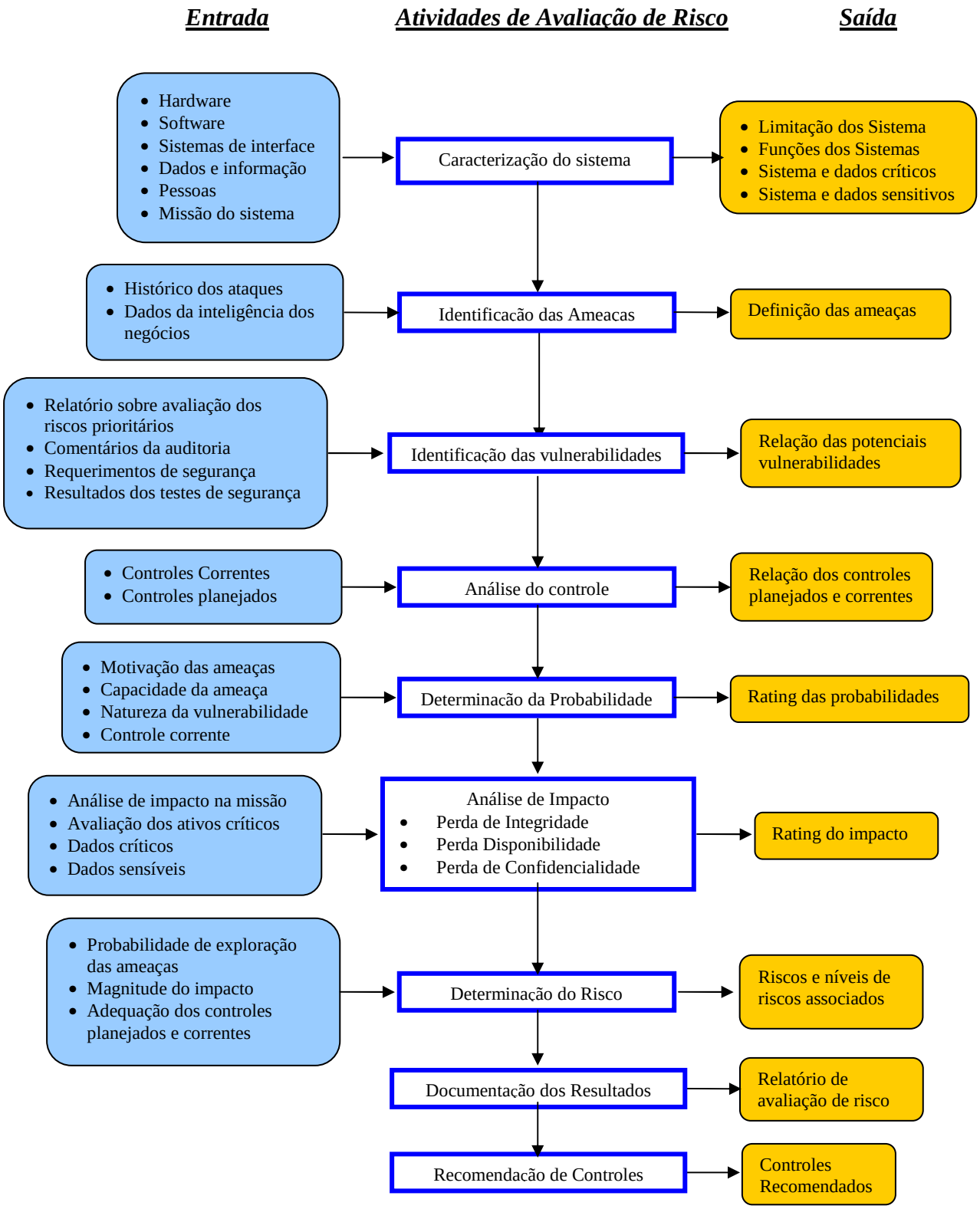

Figura 2-1: Etapas do Gerenciamento de Risco

A identificação dos riscos dos sistemas de TI requer o entendimento do ambiente onde ocorre o processamento, tipicamente colhendo informações sobre: Hardware, Software, Interface, Dados e Informações, Sistemas e Dados críticos e sensíveis (NIST, 2002).

Também é necessário obter dados sobre o ambiente operacional dos sistemas de TI, ou seja: Requerimentos Funcionais; Usuários e Provedores (inclusive o suporte técnico); Políticas de Segurança; Arquitetura dos Sistemas e Topologia da rede local; Proteção do *storage*; Fluxo das informações; Controles Técnicos e Operacionais e respectivo gerenciamento e Segurança física do ambiente (NIST, 2002).

Após a identificação e a análise dos possíveis impactos nas organizações, a determinação do risco para uma ameaça envolve:

- Probabilidade que a ameaça se concretize;
- Magnitude do impacto anteriormente constatado, caso se concretize a ação da ameaça em uma determinada vulnerabilidade;
- A adequação ou a aderência dos controles de segurança para reduzir ou eliminar o risco.

Independentemente dos mecanismos automáticos e dos processos que cada organização adota para a determinação da Probabilidade, é preciso que considerem:

- Ameaça: origem, motivação e competência;
- Natureza da vulnerabilidade e;
- Existência e efetividade dos controles.

2.4.3.2 Análise de Impacto

A determinação do impacto resultante do sucesso de uma ameaça sobre a vulnerabilidade deve considerar: Missão do sistema; Criticidade do sistema e dos dados; Sensitividade do sistema e dos dados. Além disso, pode

ser baseado em avaliações quantitativas e qualitativas da criticidade e sensitividade dos seus ativos.

A criticidade se relaciona com a representatividade de um determinado sistema de informação diante do contexto ou do fluxo operacional onde se situa, portanto tal análise está voltada à atividade operacional ou de negócio.

Segundo o NIST (2002), a sensitividade de um sistema de informação e dos dados pode ser determinada pelo nível de proteção necessário para preservar os objetivos de segurança. O impacto decorrente da diminuição ou perda dos objetivos de controle está descrito no Quadro 2-1 (Descrição da Perda e Impacto dos Objetivos de Segurança).

A análise de impacto necessita de uma avaliação que apresente aos gestores indicativos destinados à mensuração de eventuais danos ocasionados pelas ameaças. Os mecanismos habitualmente recomendados são as avaliações Quantitativas e Qualitativas.

A avaliação qualitativa dos impactos prioriza os riscos e a identificação das áreas para tratar as vulnerabilidades, com a desvantagem de não apresentar uma medida da magnitude dos impactos. Por essa razão, a análise da relação de Custo X Benefício das recomendações de implementação de controle são imprecisas (NIST, 2002).

Por outro lado, a vantagem da análise de impacto quantitativa apresenta a medida numérica da magnitude do impacto, o que facilita a análise da relação de Custo X Benefício na implementação de controles. Por vezes, a medida pode não ser suficientemente clara e requerer a complementação de uma análise qualitativa. Abaixo, algumas considerações observadas pelo NIST (2002):

- Estimativa da freqüência em que as ameaças ocorrem;
- Estimativa dos custos no caso que cada ameaça se concretize frente às vulnerabilidades;

- O fator estimado do impacto decorrente da efetivação de uma ameaça.

A análise de impacto demanda o conhecimento da criticidade e sensibilidade das informações. Para tanto, um o NIST elaborou um estudo destinado a categorizar as informações.

O NIST (2004 b), destaca que a Categorização da Segurança para as informações e os respectivos sistemas é baseada no potencial impacto às organizações sobre sua missão, proteção dos seus ativos, responsabilidades legais, manutenção de suas funções diárias e proteção das pessoas. Portanto, a avaliação de impacto requer a Categorização das Informações, dos Sistemas e da Análise dos Requerimentos Funcionais de Segurança.

A Categorização considera o tipo especifico de cada informação, uma vez que esta pode ser pessoal, médica, financeira, investigativa, sensível a cláusulas contratuais, de segurança etc. Este tipos são definidos por cada organização ou por circunstâncias especificadas exigidas pela lei, por órgãos reguladores, pelas políticas internas, pelo segmento econômico etc (NIST, 2004 b).

A Análise dos Requerimentos inclui os recursos e os sistemas de segurança do ambiente (políticas de segurança e arquitetura de segurança) e requerimentos funcionais de segurança. Também abrange a análise das leis e regulamentos.

Esta análise considera que a segurança da informação não se limita a confidencialidade, pois há sistemas que embora determinem baixo nível de requerimento de confidencialidade, demandam destacado nível de integridade e disponibilidade.

O NIST (2004 b), define níveis de impacto potencial para os objetivos de segurança, porém destaca que a aplicação destes deve ser associado ao contexto de cada organização. De acordo com o Quadro 2-3.

Quadro 2-3: Níveis de Impacto

Nível de Impacto	Descrição
Baixo	A perda dos objetivos de segurança pode causar efeitos **limitados** na operação, nos ativos corporativos ou individuais.
Moderado	A perda dos objetivos de segurança pode causar efeitos **sérios** na operação, nos ativos corporativos ou individuais. Ex. Degradação da capacidade de executar sua missão, com extensão e duração que afetem o desempenho de suas atividades primárias e reduza a efetividade de suas funções.
Alto	A perda dos objetivos de segurança pode causar efeitos **severos ou catastrófico** na operação, nos ativos corporativos ou individuais.

Fonte: NIST (2004 b)

Categorização de Segurança Aplicada aos Tipos de Informação.

A categorização da segurança está associada aos usuários e aos sistemas de informação (eletrônicas e não-eletrônicas), requer a determinação do *impacto potencial* para cada objetivo de segurança associado com o tipo particular de informação.

Os sistemas de segurança (ex. roteamento da rede local, senha de arquivos, gerenciamento das chaves criptográficas etc.) devem proteger, ao nível compatível, as informações de maior criticidade ou sensibilidade, desde o processamento, armazenamento ou transferência da informação, assegurando o atendimento dos objetivos de segurança (NIST, 2004 b).

O potencial impacto, quando definido como “Não Aplicável” (NA), somente é destinado para o objetivo de segurança confidencialidade. O tipo da informação, quanto à categoria de segurança pode ser expresso conforme segue:

Tipo da informação = {(**confidencialidade**, *impacto*), (**integridade**, *impacto*), (**disponibilidade**, *impacto*)},

Exemplos:

Informação pública = {(confidencialidade, *NA*), (integridade, *moderada*), (disponibilidade, *moderada*)}.

Informação investigativa = {(confidencialidade, *alto*), (integridade, *moderada*), (disponibilidade, *moderada*)}.

Informação administrativa = {(confidencialidade, *alto*), (integridade, *baixo*), (disponibilidade, *baixo*)}.

Categorização de Segurança Aplicada aos Sistemas de Informação.

A definição da categoria de segurança do sistema de informação requer análise e consideração das categorias de segurança de todos os tipos de informação residentes no sistema de informação. Para o sistema de informação, o valor do impacto potencial determinado para o respectivo objetivo de segurança, pode ser aquele de maior valor dentre aquelas que haviam sido determinadas para cada tipo de informação.

O sistema de informação é composto por programas e informações para realizar suas funções e sua missão. Este sistema deve estar preparado para a pior situação possível.

De forma geral, a Categoria de Segurança de sistemas de informação atende a expresso:

Sistemas de Informação = {(**confidencialidade**, *impacto*), (**integridade**, *impacto*), (**disponibilidade**, *impacto*)},

Exemplo:

Informações sobre contratos = {(confidencialidade, *moderado*), (integridade, *moderado*), (disponibilidade, *baixo*)}

Informação administrativa = {(confidencialidade, *baixo*), (integridade, *baixo*), (disponibilidade, *baixo*)}.

O resultado da categorização deste exemplo de sistema de informação é:

Sistema de aquisições = {(confidencialidade, *moderado*), (integridade, *moderado*), (disponibilidade, *baixo*)}

De forma sintetizada a definição do impacto potencial para cada objetivo de segurança está apresentado no Quadro 2-4:

Quadro 2-4: Definição dos Impactos aos Objetivos de Segurança

Objetivos de Segurança	Impacto Potencial		
	Baixo	**Moderado**	**Alto**
Confidencialidade: preserva as restrições autorizadas para o acesso às informações e sua divulgação, incluindo aspectos de proteção à privacidade pessoal e propriedade da informação.	A divulgação não autorizada da informação pode causar efeito adverso **Limitado** na operação, nos ativos das organizações e também individuais.	A divulgação não autorizada da informação pode o causar **Sérios** efeitos adversos na operação, nos ativos das organizações e também individuais.	A divulgação não autorizada da informação pode causar efeito adverso **Severo** ou **Catastrófico** na operação, nos ativos das organizações e também individuais.
Integridade: Guarda contra alteração ou destruição imprópria e inclui assegurar o não-repúdio e a autenticação.	A modificação ou destruição não autorizada da informação pode causar efeito adverso **Limitado** na operação, nos ativos das organizações e também individuais.	A modificação ou destruição não autorizada da informação pode causar efeito adverso **Sérios** na operação, nos ativos das organizações e também individuais.	A modificação ou destruição não autorizada da informação pode causar efeito adverso **Severo** ou **Catastrófico** na operação, nos ativos das organizações e também individuais.
Disponibilidade: assegura a tempestividade e realização do acesso e utilização da informação.	A descontinuidade do acesso ou uso da informação ou do sistema de informação pode causar efeito adverso **Limitado** na operação, nos ativos das organizações e também individuais.	A descontinuidade do acesso ou uso da informação ou do sistema de informação pode causar efeito adverso **Sério** na operação, nos ativos das organizações e também individuais.	A descontinuidade do acesso ou uso da informação ou do sistema de informação pode causar efeito adverso **Severo** ou **Catastrófico** na operação, nos ativos das organizações e também individuais.

Fonte: NIST (2004 b)

O Quadro 2-4 fornece subsídio para a melhor interpretação dos impactos atrelados a cada objetivo de segurança, o que representa uma etapa necessária para a definição da Categorização de Segurança das informações e dos sistemas de informação.

Os controles são importantes no tratamento dos riscos, em razão de apresentarem o nível de exposição das vulnerabilidades conhecidas a um conjunto de ameaças. Primeiramente, é preciso que os controles existam e sejam adequados à expectativa definida, posteriormente requer que seja observado seu efetivo cumprimento, de forma que atenda ao objetivo proposto.

Os controles recomendados pelo NIST (2002) para a identificação, mitigação, redução ou eliminação dos riscos que envolvem os sistemas de TI,

são concernentes à legislação e regulamentação, política organizacional, impacto operacional e segurança.

2.4.3.3 Mitigação de Risco de TI

A mitigação do risco é o segundo processo do gerenciamento do risco, envolve a priorização, análise e a implementação dos controles apropriados para a redução do risco, conforme recomendado no processo de avaliação de risco.

A eliminação total do risco é usualmente impraticável ou próximo do impossível. A responsabilidade pertence à alta gerência funcional e gestora de negócios sobre a abordagem de menor custo e implementação dos controles mais apropriados para reduzir o impacto do risco, aos recursos ou a missão das organizações, a um nível aceitável.

Mitigação de risco é a metodologia sistemática usada para reduzi-lo. O Quadro 2-5 apresenta das opções para sua realização.

Quadro 2-5: Níveis de Impacto

Opção de Mitigação	Descrição
Assunção do risco	Aceitação do risco potencial e continuar a operação dos sistemas de TI ou a implementação de controle para a redução do risco ao nível aceitável.
Evitar o risco	Através da eliminação da causa ou da conseqüência do risco.
Limitação do risco	Por meio da implementação de controles para minimizar o impacto das ameaças agindo sobre as vulnerabilidades.
Planejamento dos riscos	Por meio da implementação e manutenção dos controles.
Pesquisa e reconhecimento	A redução dos riscos pode ser alcançada pelo reconhecimento das vulnerabilidades ou falhas e pela pesquisa dos controles destinada à correção destes.
Transferência de risco	É a compensação das perdas através de mecanismos de compensação das perdas, tal qual a aquisição de seguros.

Fonte: NIST (2002)

As organizações podem analisar a extensão de risco à medida que os controles são implementados e reduzem a probabilidade das vulnerabilidades em produzirem impactos. Novos controles ou o incremento daqueles existentes podem mitigar os riscos por meio da:

- Eliminação das vulnerabilidades e reduzir as conseqüências;
- Adição de controles para reduzir a capacidade e motivação das ameaças e redução da magnitude dos impactos;
- Limitando a extensão das vulnerabilidades ou modificando a relação entre os sistemas de TI e a missão das organizações.

2.4.4 Tipos de risco

Há muitas tipologias de risco que atendem a diversas finalidades, contudo o segmento financeiro tem se destacado no desenvolvimento e na implementação de trabalhos destinados à identificação dos riscos, sua classificação e administração como mecanismo de alavancagem dos seus resultados. Por isso, este estudo terá como base a classificação do Comitê de Supervisão Bancária da Basiléia contida no documento *Core Principles for Effective Banking Supervision* (*Basel Core Principles*) (BIS, 1997), acrescida de conceitos de outros autores igualmente reconhecidos.

O BIS (1997), descreve os seguintes tipos de risco: de crédito, do país, de transferência, de mercado, de taxa de juros, de liquidez, legal, reputacional e operacional. Subsidiariamente acrescenta-se a essa tipologia o risco estratégico, da forma descrita por Marshall (2002). Estes riscos são essencialmente aplicados às atividades de negócio e de amplitude macro econômico e estratégico.

- O risco país pode ser conceituado como aquele associado ao ambiente econômico, social e político do país de origem do tomador do recurso. (BIS, 1997). Por exemplo, a possibilidade de perda devido à restrição à saída de recursos do país em decorrência de decisões de governo soberano;
- O risco de taxa de juros está relacionado com a exposição da condição financeira de uma empresa aos movimentos adversos nas taxas de juros. Este risco afeta as organizações que oferecem crédito, bem como aquelas que demandam. (BIS, 1997);
- O risco reputacional advém de falhas operacionais, falhas de conformidade a leis relevantes e regulamentos, ou outras fontes. Risco reputacional é

particularmente danoso, visto que a natureza da maioria dos negócios requer a confiança da comunidade que interage nas suas atividades. (BIS, 1997);

- O risco estratégico é conseqüência de decisão malsucedida ou ineficaz que fracasse em alcançar o retorno pretendido (Marshall, 2002).

Para Jorion (1999), as empresas estão expostas a três tipos de risco: riscos operacionais são aqueles assumidos voluntariamente, a fim de criar vantagem competitiva e valorizar a empresa perante seus acionistas; riscos estratégicos resultam de mudanças fundamentais no cenário econômico ou político, como, por exemplo, foi a extinção da União Soviética no final de década de 1980, que proporcionou declínio gradual nos gastos com armas, afetando diretamente esse setor industrial; riscos financeiros estão ligados a possíveis perdas nos mercados financeiros, devidas às oscilações de variáveis financeiras como taxas de juro e de câmbio. A exposição a riscos financeiros pode ser otimizada cautelosamente, para que as empresas possam concentrar-se no que fazem melhor, que é administrar suas exposições a riscos operacionais.

A seguir, os tipos de risco serão detalhados a partir da ampliação da visão de Jorion, BIS e outros autores.

2.4.4.1 Risco de Mercado

O Risco de Mercado surge de mudanças nos preços (ou volatilidades) de ativos e passivos financeiros. São mensurados pelas mudanças no valor das posições em aberto ou nos ganhos (Jorion, 1999). Também pode ser conceituado como a possível perda, em posições dentro ou fora de balanços, que surgem a partir de movimentos em preços de mercado. Um elemento específico do risco de mercado é o risco cambial, que decorre de posições em moeda diferente da moeda local (BIS, 1997). Exemplo: aquisição de obrigação em dólar, mas com recebimento da receita em reais gera exposição ao risco cambial decorrente da flutuação da cotação negociada entre as moedas.

2.4.4.2. Risco de Crédito

Surgem quando as contrapartes não desejam ou não são capazes de cumprir suas obrigações contratuais. São mensurados pelo custo de reposição de fluxos de caixa, caso a outra parte fique inadimplente (Jorion, 1999). De acordo como o BIS, o risco de crédito relaciona-se com a possibilidade de inadimplência de uma contraparte em atuar de acordo com uma disposição contratual. Segundo Caquette *et al.* (1999), o risco de crédito é o efeito de um contrato financeiro entre o provedor de fundos e o usuário desses fundos.

2.4.4.3 Risco de Liquidez

Surge quando uma transação não pode ser conduzida pelos preços de mercado prevalecentes, devido a uma atividade insuficiente de mercado (risco de liquidez mercado-produto), ou quando há impossibilidade de cumprir as obrigações relativas aos fluxos de caixa, o que pode forçar a liquidação antecipada de contratos, transformando perdas escriturais em perdas reais (risco de liquidez de fluxo de caixa-obtenção de recursos) (Jorion, 1999);

O risco de liquidez advém da habilidade das organizações para adequar suas obrigações ou para consolidar o aumento dos ativos. (BIS, 1997). Exemplo: a possibilidade de uma transação não ser concretizada ao preço esperado devido a insuficiente atividade do mercado.

2.4.4.4. Risco Legal

Surge quando uma contraparte não possui autoridade legal ou regulatória para se envolver em uma transação (Jorion, 1999). O risco legal está relacionado com a desvalorização de ativos ou de valorização de passivos com intensidade inesperada devido a pareceres ou documentos legais inadequados ou incorretos. (BACEN, 2000).

2.4.4.5 Risco Operacional

O risco operacional está diretamente relacionado às atividades computacionais e de sistemas de informação de todas as organizações, pois as vulnerabilidades, ameaças, controles e impactos são tratadas sob a abordagem

deste tipo de risco. Portanto, é de fundamental importância que este estudo considere a abrangência destes elementos e a compreensão do risco operacional, pois suas características serão aplicadas na qualificação das informações selecionadas.

Risco operacional não é um tema pacífico na literatura. Isto acontece porque, segundo Crouhy *et al.*, (2001), não há uma clara distinção entre o risco operacional e as incertezas corriqueiras enfrentadas pelas organizações nas suas atividades diárias. Contudo, outros autores e autoridades reguladoras buscaram conceituar e tipificar esse risco. Duarte Jr. (1996), relaciona o risco operacional a possíveis perdas como resultado de sistemas ou controles inadequados, falhas de gerenciamento e erros humanos. Ainda de acordo com Duarte, o risco operacional, risco de crédito, risco de mercado e risco legal são os quatro grandes grupos de risco.

Para Jorion (1999), o risco operacional refere-se às perdas potenciais resultantes de sistemas inadequados, má administração, controles defeituosos ou falha humana, a qual inclui o risco de execução, correspondente a situações em que as operações não são executadas, resultando, às vezes, em atrasos onerosos ou em penalidades. Também inclui fraude e risco tecnológico, o qual se refere à necessidade de proteger os sistemas contra violações. Outros exemplos são as falhas de sistema, prejuízos oriundos de desastres naturais ou acidentes envolvendo pessoas importantes.

Segundo IOSCO (1998), risco operacional compreende o risco de perdas decorrentes de operações impróprias de processamento de transações ou sistemas de gerenciamento.

De acordo com BIS (2004), o risco operacional é definido como o risco de perdas resultantes de processos internos falhos ou inadequados, pessoas e sistemas, ou eventos externos. O conceito enumera fatores de risco: processos, pessoas, sistemas e eventos externos. Segundo Marshall (2002), “existe um componente aleatório no fator”. Em outras palavras, é possível que os fatores sejam gerenciados, mas não totalmente controlados. Outra

característica dos fatores de risco é que podem ser intrínsecos a produtos e processos específicos ou extrínsecos à empresa.

O Quadro 2-6 apresenta fatores de risco e categorias de eventos de perda. Tais categorias guardam relação com os tipos de eventos presentes em BIS (2001, 2003).

Quadro 2-6: Fatores de Risco e Eventos de Perda

Fatores	Categorias de Eventos de Perda
• Pessoas	• Fraudes Internas
	• Fraudes Externas
• Sistemas	• Práticas empregatícias e segurança no trabalho
	• Perdas ligadas a clientes, produtos e práticas de negócio
• Processos	• Danos a ativos físicos
	• Interrupção de negócios e falhas em sistemas tecnológicos
• Eventos Externos	• Falhas de execução, de distribuição ou de processos gerenciais

Fonte: Adaptado de Pereira (2004)

Pereira (2004), observou que a categorização dos eventos de perda auxilia na identificação dos fatores de riscos, o que permite sistematizar o entendimento das causas de risco operacional dentro da instituição.

Outra classificação, por sete tipos de evento de perda para o risco operacional, está apresentada no Quadro 2-7. As categorias estão descritas até o nível dois (terceira coluna). Essa classificação está baseada nos estudos relacionados ao tratamento regulatório do risco operacional feitos pelo Comitê da Basiléia.

Quadro 2-7: Descrição dos Tipos de Eventos de Risco Operacional

Categoria de tipo de evento	Definição	Categoria (nível 2): alguns exemplos
Fraudes internas	• Perdas devidas a atos com intenção de defraudar a instituição, violar regulamentos, a lei ou política interna (exclui discriminação), que envolvam ao menos uma parte interna.	Atividade não autorizada, roubo ou fraude.
Fraude externa	• Perdas devidas a atos com a intenção de defraudar a instituição, violar regulamentos, lei ou política interna (exclui discriminação), que sejam cometidos por uma terceira parte.	Roubo e fraude, segurança de sistemas.
Práticas empregatícias e segurança no ambiente de trabalho	• Perdas devidas a atos inconsistentes com as condições empregatícias. Violações de acordos sanitários ou de segurança trabalhista ou perdas com danos de acidentes de trabalho ou de ações de discriminação de qualquer tipo (inclui assédio sexual).	Relações trabalhistas, ações na justiça do trabalho, segurança no ambiente de trabalho, diversidade.
Clientes, produtos e práticas de negócio	• Perdas oriundas de falhas em cumprir obrigações com clientes ou perdas por causa de desenhos/estruturas de produtos.	Prática de negócio imprópria, falha em produtos, falhas em conselhos ou consultorias etc.
Danos a ativos físicos	• Perdas oriundas de danos a ativos físicos.	Desastres e outros eventos.
Interrupção de negócios e falhas nos sistemas	• Perdas devidas a qualquer interrupção do negócio ou falhas em sistemas.	Sistemas.
Execução, entrega e gestão de processos	• Perdas oriundas de falha no processamento de transações, ou gestão de processos, de relações com parceiros comerciais e *vendors*.	Captura de Transações, Execução e Manutenção, Monitoramento e reporte, Admissão de cliente e documentação, Gestão da conta de usuários e cliente, Parceiros de Negócio, Fornecedores e *vendors*.

Fonte: Adaptado pelo Autor BIS (2001)

2.4.4.6 Risco Técnico

De uma forma geral o NIST trata a infra-estrutura aplicada ao funcionamento dos recursos técnicos de TI (sistemas aplicativos, instalações, informações e tecnologia), bem como os processos e atividades que utilizam os recursos com a finalidade de assegurar os requerimentos de negócio

distribuídos em: Requerimento de Qualidade (Qualidade, Custo e Entrega), Requerimento de Credibilidade (Eficácia e Eficiência, Credibilidade dos reportes financeiros e *Compliance* com as normas internas, leis e regulamentações) e requerimentos de segurança.

Com o objetivo de mitigar os riscos técnicos e maximizar sua efetividade nos sistemas de TI, o *NIST* sugere a adoção de controles específicos, contudo seu desenvolvimento e implementação requerem conjugar aspectos técnicos, gerenciais e operacionais, uma vez que os controles de segurança usados apropriadamente, podem prevenir, limitar ou deter as ameaças e seus danos à organização.

Controles Técnicos de Segurança

Os controles técnicos são configurados para proteger os dados, informações e sistemas de TI sensitivos e críticos contra vários tipos de ameaças e podem envolver desde medidas simples até complexas, tais como arquitetura, engenharia e pacotes de segurança com a mescla de hardware e software, firmware. Todas funcionam em conjunto, uma vez que os controles técnicos abrangem a maioria das categorias.

Os controles técnicos são: Suporte (voltados a TI), Prevenção (previne falhas de segurança) e Detecção e Recuperação (detecta e recupera falhas de segurança). Estes controles técnicos e a maneira pela qual se relacionam estão apresentados na Figura 2-2 (NIST, 2002) e descritos no Quadro 2-8.

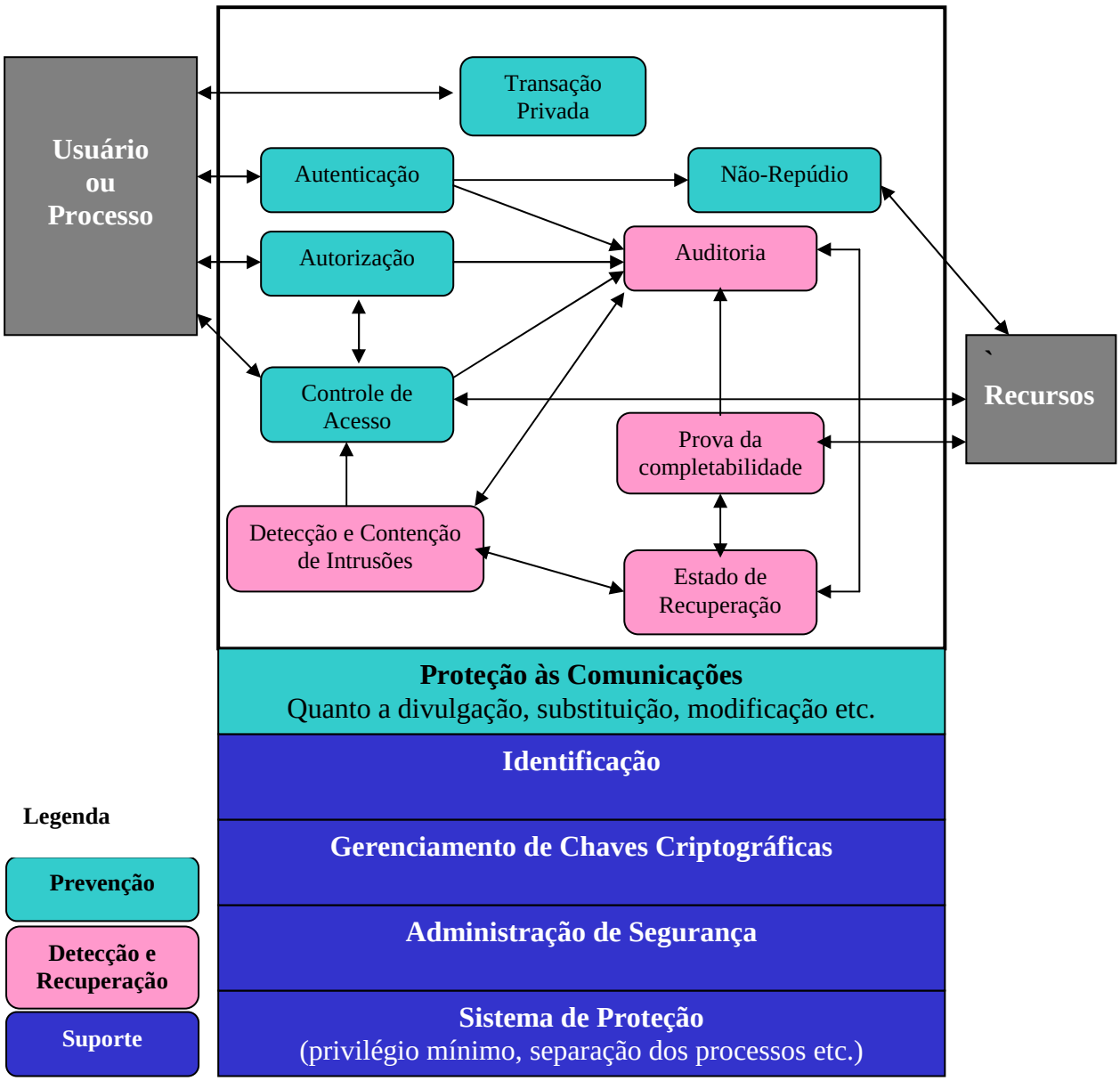

Figura 2-2: Controles Técnicos de Segurança

Os controles técnicos de Suporte, Prevenção e Detecção e Recuperação encontram-se relacionados, junto às respectivas descrições no Quadro 2-8.

Quadro 2-8: Controles Técnicos de Suporte, Prevenção e Recuperação

Controle Técnico	Descrição
Suporte	• Identificação: Usuários, processos e recursos de informação; • Gestão das chaves criptográficas: geração, distribuição, armazenamento e manutenção; • Administração de segurança: configuração de acordo com a necessidade especifica do ambiente operativo. Os sistemas de segurança são voltados aos sistemas operacionais e aplicativos; • Sistemas de proteção: representa a qualidade de implementação do processo e dos sistemas de segurança.
Prevenção	• Autenticação; • Autorização; • Controle de Acesso: visa à integridade e confidencialidade dos dados, através do cumprimento de uma política de segurança, cuja efetividade e poder depende da precisão das configurações do software e da segurança de hardware; • Não repúdio: visa à confiabilidade do sistema na habilidade de assegurar que as informações enviadas e recebidas não são passíveis de negação. Este mecanismo é preventivo e corretivo; • Comunicações protegidas: visa à preservação dos objetivos de segurança, na medida que transitam informações por canais seguros; • Transações privadas: trata sobre a manutenção da privacidade das pessoas e das organizações.
Detecção e Recuperação	• Auditoria: atua sobre eventos relevantes, monitorando anormalidades dos sistemas de TI, após a detecção e recuperação de incidentes motivados por fragilidades de segurança; • Detecção e contenção de Intrusões: objetiva a detecção e resposta tempestiva de falhas de segurança; • Prova de Completabilidade: visa assegurar a integridade dos sistemas através da identificação de irregularidades, eventuais exposições e ameaças. Este controle não estabelece políticas, mas detecta violações e auxilia a determinar a ação corretiva mais apropriada; • Restabelecer o estado de segurança: habilita o sistema a retornar para o estado que é dado como seguro, após a ocorrência de um incidente de segurança; • Detecção e erradicação de vírus: esta atividade destina-se a preservação da integridade dos dados e a segurança do sistema.

Fonte: Adaptado do NIST (2002)

Os controles de detecção e recuperação são aplicados para alertar violações ou mesmo as tentativas que venham a ferir a política de segurança o que inclui trilhas de auditoria, métodos de detecção de intrusão e checagens lógicas e físicas. Os controles de recuperação podem ser usados para re-estabelecer as atividades computacionais interrompidas. São necessárias para complementar as medidas técnicas de suporte e prevenção.

O gerenciamento sobre os controles de segurança trata sobre o acompanhamento e avaliação dos resultados alcançados, que subsidiarão o

direcionamento das ações destinadas a mitigação dos riscos identificados. O Quadro 2-9 apresenta os tipos de gerenciamento e as ações.

Quadro 2-9: Gerenciamento dos Controles de Segurança

Gerenciamento	Descrição das Ações
Preventivo	• Designação de responsabilidades; • Desenvolvimento e manutenção dos planos dos sistemas de segurança; • Implementação dos controles de segurança pessoais; • Conduta segura e treinamento técnico para garantir que os usuários se mantenham atentos à aderência das regras e suas responsabilidades quanto à proteção dos ativos.
Detectivo:	• Revisão periódica dos controles; • Auditoria periódica de desempenho dos controles; • Avaliação perene da identificação e avaliação dos riscos; • Atuação sobre os riscos residuais pelos gestores de TI.
Recuperação	• Prover continuidade do suporte e desenvolvimento, teste e manutenção do plano de continuidade da operação diante de emergências e desastres; • Definir competência para responder a incidentes, de forma que reconheçam, reportem e respondam a incidentes.

Fonte: Adaptado do NIST (2002)

A operação dos controles de segurança permite a avaliar e redefinir os parâmetros de proteção e os procedimentos voltados aos ativos e recursos de TI presentes nas organizações.

Os controles operacionais são utilizados para corrigir deficiências operacionais e impedir a ação de potenciais ameaças, através da consistência e uniformidade da segurança das operações. É necessário que os procedimentos e métodos para a implementação desses controles sejam claramente definidos e divulgados adequadamente.

Os controles operacionais incluem aspectos preventivos (segurança física e lógica, recursos computacionais, infra-estrutura e contingência), assim como os detectivos (monitoramento de segurança física e ambiental).

Ameaças e Vulnerabilidades

O perene processo de identificação das vulnerabilidades existentes no ambiente operacional, nos sistemas de informação e dos recursos TI,

associado ao monitoramento e entendimento das novas e evolutivas ameaças conduzem a maior eficácia dos controles e do sistema de segurança. Com essa finalidade o NIST descreve no Quadro 2-10 as possíveis origens, motivações e ações mais freqüentes.

Quadro 2-10: Ameaças humanas: Origem, Motivação e Ações

Origem da Ameaça	Motivação	Ações
Hacker e Cracker	Desafio; Ego; Rebelião.	• Hacking; • Engenharia social; • Quebra do sistema de proteção de Intrusões; • Acesso desautorizado aos sistemas.
Crime computacional	Destruição da informação; Divulgação ilegal da informação; Ganho financeiro; Alteração ilegal de dados.	• Crime computacional; • Ato fraudulento; • Suborno; • Trapaça; • Sistema de intrusão.
Terrorismo	Blackmail; Destruição; Explosão; Vingança.	• Bombas terroristas; • Informações de guerra; • Ataque aos sistemas de informação; • Sistemas de falsificação.
Espionagem industrial (empresas, governos etc.)	Vantagem competitiva; Espionagem econômica.	• Exploração econômica; • Roubo de informação; • Intrusão à privacidade pessoal; • Engenharia social; • Penetração nos sistemas; • Acesso não autorizado aos sistemas.
Ações internas (treinamento insuficiente, descontentamento, maldade, negligência, desonestidade ou funcionários demissionários)	Curiosidade; Ego; Inteligência; Ganho monetário; Vingança; Erros não intencionais e omissões (erros de sistemas e falhas de infra-estrutura).	• Assalto ou ataque por funcionários; • *Blackmail;* • Pesquisa sobre a propriedade das informações; • *Abuse computer;* • Fraude e roubo; • Suborno; • Input de informações falsas ou corrompidas; • Interceptação; • Códigos maliciosos; • Venda de informações pessoais; • Erros de sistemas; • Intrusão nos sistemas; • Sabotagem nos sistemas; • Acesso não autorizado aos sistemas.

Fonte: Adaptado do NIST (2002)

O Quadro 2-11 apresenta alguns exemplos de vulnerabilidades essencialmente técnicas atreladas a origens de ameaças, que podem resultar em ações efetivas, prejudiciais aos recursos técnicos.

Quadro 2-11: Vulnerabilidades e Ameaças

Vulnerabilidade	Origem da Ameaça	Ações de ameaças
Acesso aos sistemas por funcionários em via de desligamento.	Funcionários terminais.	Acessos externos a rede local da companhia e acesso aos dados proprietários.
A configuração de firewall permite a Telnet e os usuários guest se encontram habilitados.	Usuários não autorizados (hackers, crackers, funcionários terminais, terroristas, criminosos cibernéticos etc.).	Uso de telnet para conexão de acesso aos sistemas através de usuários *guest*.
O fornecedor identifica falhas no desenho dos sistemas de segurança. Com isso, as novas correções não são necessariamente implementadas no seu sistema.	Usuários não autorizados (hachers, funcionários descontentes, criminosos cibernéticos, terroristas).	Obtenção de acesso não autorizado aos sistemas com dados sensitivos, com base no conhecimento das vulnerabilidades existentes.
O data center usa sprinklers com água para combater incêndio, recursos de proteção de equipamentos contra danos provocados pela água estão fora do local apropriado.	Fogo e negligência pessoal.	Acionar os sprinklers do Data Center.

Fonte: Adaptado do NIST (2002)

Nos exemplos acima foram identificadas as possíveis vulnerabilidades relacionadas a natureza dos sistemas de TI. É possível aplicar uma sistemática semelhante nas fases do Ciclo de Vida do Desenvolvimento dos Sistemas de Informação (SDLC). Segundo o NIST, neste caso, teríamos:

- Nas etapas anteriores ao desenho do sistema, a pesquisa por vulnerabilidades concentra-se nas políticas de segurança, planejamento dos procedimentos, na definição dos requerimentos dos sistemas, dos fornecedores e da análise da segurança dos produtos que serão adquiridos;
- Nos sistemas em funcionamento, as vulnerabilidades são afetas às informações Por isso, devem ser analisados os sistemas de segurança, controles, recursos técnicos e procedimentos destinados a proteção.

O NIST declara a importância de integrar os aspectos de segurança no SDLC e para tanto descreve as etapas que auxiliam essa integração, mostrando o progresso conjunto dos requerimentos técnicos e de segurança.

Quadro 2-12: Segurança no SDLC

	Inicio	Adquirir/ Desenvolver	Implementar	Operar/ Manter	Descarte
SDLC	• Definição de necessidades • Percepção da necessidade • Vinculo da necessidade com a missão e os objetivos de desempenho • Avaliação das alternativas para inversão de recursos financeiros • Preparação para a revisão dos investimentos e orçamento	• Declaração funcional das necessidades • Pesquisa de mercado • Estudo de viabilidade • Análise de requerimentos • Análise das alternativas • Análise do Custo-Benefício • Estudo sobre a conversão e software • Análise de custo • Plano de gerenciamento de risco	• Instalação • Inspeção • Teste de aceite • Treinamento dos usuários • Documentação	• Medição da desempenho • Modificação de contratos • Operação • Manutenção	• Definição do descarte • Troca ou venda • Projeção da organização interna • Transferência e doações • Contrato para a liquidação
Considerações de segurança	• Categorização da segurança • Avaliação preliminar dos riscos	• Avaliação dos riscos • Análise dos requerimentos funcionais de segurança • Análise dos requerimentos que asseguram a segurança • Consideração e reporte dos custos • Planejamento da segurança • Desenvolvimentos dos controles de segurança • Desenvolvimento dos testes de segurança e sua avaliação • Planejamento dos componentes	• Inspeção e aceite • Sistema de integração • Certificação em segurança • Reconhecer a segurança	• Gerenciamento de configuração e controle • Monitoramento contínuo	• Preservação da informação • Higienização da mídia • Descarte de hardware e software

Fonte: NIST (2004 a)

Esta estrutura de trabalho descreve os principais parâmetros para o planejamento e tece considerações sobre as especificações necessárias para aquisição dos sistemas de informação, envolvendo os procedimentos iniciais, desenvolvimento ou aquisição, implementação e descarte.

A documentação e análise de vulnerabilidades incluem a avaliação rotineira e prévia dos documentos sobre os riscos gerais de TI e os relatórios emitidos pelos sistemas de segurança, tais como: auditoria, anomalias, revisão de segurança, testes e avaliações. Neste contexto, também devem ser consideradas as vulnerabilidades associadas aos sistemas de TI, tais como erros nos sistemas, pacotes adquiridos ou processos.

Os sistemas de maior criticidade podem submeter-se a testes preventivos (ferramentas automáticas, testes e avaliações de segurança etc.).

Outra abordagem do Risco Técnico refere-se ao tratamento de problemas técnicos associados com a nova ou emergente tecnologia. O risco técnico em sistemas físicos pode ser sintetizado pela elevação dos problemas advindos da aplicação de novos processos, materiais, ou subsistemas antes de compreender os parâmetros de controle de desempenho, custo, operação com segurança ou falhas não previstas. Pode ocorrer se as previsões comerciais de tecnologia se estenderem fora dos domínios conhecidos ou pré-estabelecidos ou, provenientes de interações inesperadas e crescentes de novas combinações de subsistemas ou componentes computacionais.

Contudo, os elementos de risco técnico não são facilmente caracterizados, pois envolve a previsão de como a ciência se comportará diante da condução dos experimentos, interpretação dos resultados e sua aplicação em situações reais. Os elementos dos riscos técnicos são caóticos, uma vez que dependem de pessoas e do ambiente, tal qual as leis da ciência, os elementos de risco técnico são interdependentes. O conhecimento e a mitigação dos riscos tecnológicos estão relacionados às leis da ciência, aos padrões dos processos racionais e a personalidade das pessoas (NIST, 2000).

O Risco Técnico pode se manifestar em três fases no processo de desenvolvimento do produto, basicamente são: Invenção ou conceito, Atendimento das necessidades do mercado, e Comercialização. A invenção ou conceito descreve o tipo de pesquisa realizada em Corporações ou Universidades, que dentre outros aspectos de exposição ao risco também tratam do gerenciamento e transferência da propriedade intelectual ou do conhecimento consagrado na pesquisa.

Os processos de desenvolvimento de tecnologia requerem revisões de prováveis problemas tecnológicos, ou mesmo daqueles conhecidos, para que cada um seja medido por um método uniforme. Esta informação é destinada a criar uma descrição dos riscos para nova tecnologia.

A transferência do objeto da pesquisa até seu acabamento na forma de um produto e torná-lo disponível ao público, passa pela seleção da tecnologia e pela concepção do produto, com isso cria novos conceitos, inova

processos e gera novos riscos, dentre os conflitos do desenvolvimento de novas tecnologias e o sucesso do seu produto existe a necessidade de especificar procedimentos de mitigação de risco, dentre os quais o NIST (2000) destaca:

- Requerimentos de disponibilidade de competências e tecnologia complementar: O desenvolvimento de novas tecnologias requer novas competências técnicas, novo perfil técnico, ferramentas e processos. É importante assegurar a integração da nova tecnologia com aquela existente e seus respectivos sistemas;
- Especificação das metas: A nova tecnologia move-se em torno do produto, o desempenho deve ser caracterizado e quantificado em termos dos objetivos da especificação do produto. Portanto, o risco é afeto ao desempenho insuficiente, relacionados aos parâmetros de qualidade, velocidade, realização e custo;
- Disponibilidade da cadeia de elementos: O sucesso de um novo produto requer o envolvimento de outras atividades relevantes, além de tecnologia;
- Diferenciação de Produto: Um novo produto é sustentado e oferece uma combinação de funções, características, recurso, economias etc., que o diferenciam daqueles existentes. O risco está associado a falhas de especificação e planejamento do produto, que pode comprometer a eficácia da tecnologia empregada, o que implica na evolução de diversos riscos;
- Aceitação de Mercado: Equívocos no desenvolvimento de nova tecnologia motivados pelo desconhecimento dos clientes, competição e dinamismo do mercado podem ser mensurados.

Embora os riscos técnicos sejam considerados como mais controláveis, sua análise está associada a outras fontes, uma vez que lançamentos tecnológicos são inseridos na incerteza do mercado, cujos riscos atendem a outros fatores. A exemplo da Figura 2-3.

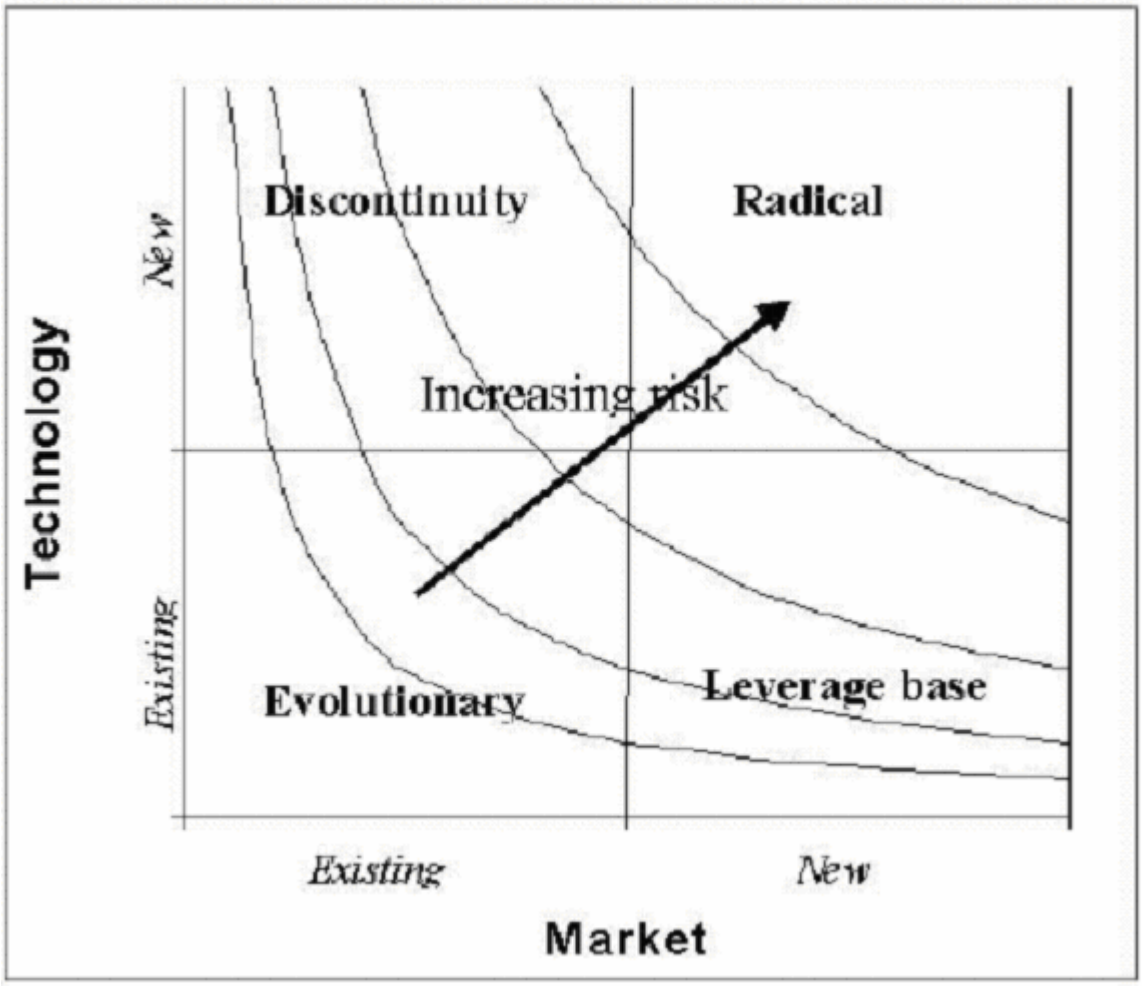

Figura 2-3: Quadrante do Risco
Fonte: NIST (2000)

Embora o gerenciamento de risco proporcione maior conforto, admite-se a existência de dificuldades na identificação, análise e mensuração dos riscos. O estudo do NIST sugere o balanceamento entre a abordagem analítica e a abordagem intuitiva. Endossa também a preservação de acordos explícitos sobre a valoração dos riscos associados entre tecnologia e mercado.

2.4.5 Riscos no Âmbito das Universidades

Desde o início da utilização de computadores nas atividades desenvolvidas pelas universidades, há registro de ameaças que utilizaram vulnerabilidades para a realização de ataques direcionados aos computadores. Kuong (1974), menciona em sua obra *Computer Security, Auditing and Control* perdas materiais diretas, decorrente da destruição dos computadores em quatro universidades, ocorridas no período entre 1969 e 1971. Em outros ataques o prejuízo financeiro direto alcançou o valor de US$ 3,5 milhões. Adicionalmente

menciona que em apenas uma universidade o material produzido de pesquisa científica fora totalmente destruído, ao custo de 1,3 milhão horas/homem pesquisador. Observe-se que danos desta natureza não podem ser mensurados em valores financeiros.

As circunstâncias da época demonstram que os ataques sofridos pelas universidades foram exclusivamente de ordem física às instalações onde se localizavam os Centros de Processamentos de Dados, denominação utilizada à época para as edificações que centralizavam as atividades e rotinas destinadas ao tratamento de informações. Atualmente, os riscos de ordem física permanecem e continuam a exigir proteção e controle para manter as instalações apropriadamente confiáveis, porém o desenvolvimento das comunicações e a disseminação da Internet distribuíram o trânsito e o armazenamento das informações em diversos canais de comunicação e ambientes de tratamento. Como reflexo dessa nova estrutura que envolve os sistemas de informação, há necessidade de apropriar os mecanismos de segurança e controle na proporção adequada de cada elemento de informação, com o objetivo de evitar fatos recentes que repetiram a perda de produção cientifica acumulada por 20 anos sobre cruzamentos genéticos e seleção de espécies, na invasão e destruição dos laboratórios da empresa Aracruz Celulose, nas proximidades de da cidade de Porto Alegre/RS. (Folha de São Paulo, 9.3.2006).

Também deve ser abordado, no aspecto da segurança das informações, o sistema que visa assegurar a confiabilidade dos resultados alcançados em pesquisas, com objetivo de evitar fraudes científicas, como aquela verificada nos trabalhos do pesquisador sul-coreano Woo Suk Hwang, no campo da clonagem humana, que envolveram falsificações (Folha de São Paulo, 28.12.2005).

A Revista Veja (2007), destaca as novas descobertas da engenharia genética, que passaram a produzir em laboratório DNA sintético, tornando possível à criação de vírus, bactérias ou qualquer outro tipo de organismos que até então não existiam na natureza. Muitas pesquisas

começaram a usar o DNA sintético com objetivos nobres e direcionados ao bem estar da população, conforme apresentado no Quadro 2-13.

Quadro 2-13: Projetos de DNA Sintético

Objetivo da Pesquisa	Projeto
• Detectar e tratar doenças, retardar o envelhecimento e produzir combustíveis alternativos	Biobricks – Instituto de Tecnologia de Massachusetts
• Modificar o processo de produção de remédio da malária, que é complexo e caro	Artemisinina – Universidade da Califórnia – Berkeley
• Descobrir a quantidade mínima de genes, necessários para um organismo vivo, com isso seria criado um microorganismo artificial programável	Genoma Mínimo – Instituto Craig Venter
• Identificar tumores, matar as células cancerosas e prevenir que o tumor reapareça no mesmo local	Custom-built – Universidade da Califórnia – São Francisco
• Tratar doenças, reparar tecidos, produzir energia e eliminar gases tóxicos do efeito estufa	Los Alamos Bug – Laboratório Nacional de Los Alamos

Fonte: Revista Veja (2007)

Segundo a revista, a Internet dispõe de informação sobre instruções para isolar uma célula ou como fazer uma bactéria brilhar sob luz ultravioleta. Contudo, alerta sobre os riscos decorrentes do acesso irrestrito ao resultado destas pesquisas, vez que seu uso por entidades criminosas poderá criar transtornos jamais observados, com conseqüências incalculáveis.

A importância dos sistemas de informação e da infra-estrutura das universidades pode ser observada pela capacidade computacional crescente e representativa. A organização TOP500 (2006) tem a finalidade de criar estatísticas sobre o alto desempenho de computadores instalados em entidades de variados segmentos. A posição gerada em junho de 2006 mostrou que entre as 500 entidades que dispunham dos computadores com a maior capacidade de processamento, 16,6% eram universidades e 21,8% eram organizações de pesquisa. Essa posição também demonstrou que os 20 computadores de maior capacidade pertenciam às organizações de pesquisa (16) e universidades (4).

O cenário de incerteza, foi agravado após os ataques terroristas de 11 de setembro de 2001, nos Estados Unidos da América do Norte, em razão de acentuar a preocupação mundial sob a perspectiva de novas incursões. Dentre estas, há possibilidade de utilização de material advindo de pesquisas em novas

fontes energéticas, em descobertas no campo da química e da biologia, dentre outros. Consideram-se também os riscos associados às atividades de ensino, quanto aos dados de avaliação, cadastro, registros de diplomas, atestados etc.; que podem estar sujeitos as adulterações do seu conteúdo original, falsificações ou simplesmente mau uso.

O processo de inovação tecnológica, amplamente desenvolvido pelas pesquisas conduzidas nas universidades estão associadas a integração dos riscos de negócio, da infra-estrutura computacional e dos sistemas de informação, apresentados pelo NIST sob o tema de Risco Técnico.

CAPÍTULO 3 – TECNOLOGIAS DE SEGURANÇA E CLASSIFICAÇÃO DAS INFORMAÇÕES

Ao longo da história observa-se a predominância de utilização de técnicas destinadas a preservar o sigilo da estratégia militar e das ações diplomáticas que conduzem ao crescimento dos governos, povos etc. Em contrapartida, aqueles que demonstraram pouca habilidade no uso desses recursos amargaram perdas substanciais que chegaram à aniquilação de suas culturas, decorrente da submissão aos vencedores das guerras.

Contudo, a transformação da sociedade, impulsionada pela marcante, veloz e barateada evolução tecnológica, inseriu elementos de tecnologia nos processos e produtos corporativos, bem como nos hábitos cotidianos da população. A importância da participação dos recursos técnicos denota excessiva dependência e requer o aprimoramento e atualização dos controles e das condições de segurança, uma vez que os dispositivos técnicos e os processos são efêmeros.

Uma das principais implicações das recentes descobertas nas redes de comunicação e dos dispositivos computacionais é a dissociação de tempo, quanto à delimitação dos horários de atendimento das corporações, uma vez que a integral disponibilidade é requisito indispensável para a maioria dos produtos ou serviços. Outra conseqüência é a alteração dos processos de negócio, pois estão desvinculados da localização física das corporações. A essas implicações denominou-se mobilidade. Adicionalmente, a cobrança por resultados de qualidade comprovada, custo e prazos diminutos, levou a aproximação das atividades operacionais aos mecanismos de segurança, sob risco de comprometer o sucesso e a continuidade das empresas.

Também houve mudança substancial das características técnicas, que passaram a tratar as informações em tempo real e descentralizou o processamento, ao custo de ampla utilização de redes de comunicação rápidas e eficientes.

Este capítulo pretende apresentar procedimentos significativos para assegurar que os dados se mantenham íntegros, confiáveis, disponíveis e confidenciais. Assim como, demonstrar algumas iniciativas com objetivo de proteger as informações.

3.1 Criptologia

Criptologia é a ciência composta pelos estudos da criptografia e da criptoanálise. De acordo com Ungaretti (2002), a criptografia visa à comunicação secreta, por meio de técnicas para cifrar ou codificar informações consideradas importantes pelos seus proprietários, portanto se apresenta legível somente ao emissor e ao destinatário. Enquanto que a criptoanálise é voltada à obtenção da informação no seu formato original a partir de um código cifrado, ou seja, destina-se à quebra dos algoritmos criptográficos.

Para preservar o conteúdo das mensagens ininteligíveis, a criptografia clássica possui uma seqüência de bits aleatória e secreta, denominada chave. Este elemento, embora não contenha informações, representa a peça fundamental do mecanismo de segurança aplicado às informações que devem ser resguardadas, o que requer cuidado e atenção para manter o seu sigilo na geração, no tratamento e na distribuição das chaves (Fernandes 2001).

As principais bases de criptografia são apoiadas em modelos matemáticos que exploram a limitação computacional na realização dos cálculos. Segundo Fernandes (2001), há estudos que indicam que esta limitação poderá ser solucionada na medida que a computação quântica possa ser implementada, cujo conceito está baseado nas leis da física e na incerteza natural da mecânica quântica. Esta nova visão computacional obrigatoriamente nos remeteria à revisão dos modelos criptográficos existentes, eventualmente nos induzirá a optar por mecanismos que utilizem a plataforma computacional quântica e, novos procedimentos de criptografia.

O uso de criptografia quântica tornaria possível a identificação de tentativas de monitoramento, pelo fato do menor movimento de leitura provocar uma inconsistência na comunicação. Os padrões criptográficos atuais não

possuem dispositivos que apresentem tal nível de sensibilidade ao monitoramento passivo, pois o simples acesso de leitura aos dados não provoca nenhuma modificação no seu conteúdo.

Fernandes (2001) relata que os experimentos recentes indicam que sua aplicação é restrita apenas para a transmissão de informações, uma vez que no armazenamento, devido à ausência de movimento, não existem fótons. Em experimentos foram implementadas conexões entre a Casa Branca, Pentágono e outros links com bases militares, a uma distância máxima de 60 km que utilizam cabos de fibra óptica de alta pureza. Distâncias superiores apresentaram taxas de erros de bit causado pelo princípio de incerteza de Heisemberg, que trata da impossibilidade de medir simultaneamente a posição e a velocidade do elétron, quando são usados conceitos clássicos, aplicáveis em partículas ou ondas, para explicar o comportamento dos elétrons.

3.1.1 Histórico da Criptologia

Posto que a criptografia visa garantir o sigilo das informações, nos primórdios da civilização restringiu-se aos ambientes militar e diplomático, assim, era tratada como destacada arma de guerra, pois protegia o bem de maior valor para um governante: as informações sigilosas, que poderiam conduzi-lo a tomar as decisões acertadas em situações de acentuada crise.

O artigo de Ungaretti (2002) descreve que remonta ao século XVIII, na Europa, o surgimento das Câmaras Negras, para onde eram desviadas as correspondências de interesse dos governos para serem copiadas antes de seguir seus destinos. Nessas câmaras, grupos de matemáticos e lingüistas tratavam de desvendar as mensagens capturadas na forma cifrada. Naquela época, os governos ocupavam-se em construir sistemas criptográficos seguros, simultaneamente se capacitavam na arte de quebrar os códigos de seus adversários.

A Primeira Guerra Mundial foi palco da influência da criptologia nos destinos dos povos. Naquela época, o serviço de inteligência inglês interceptou um telegrama enviado pelo Ministro do Exterior Alemão, Arthur Zimmermann, endereçado para o Presidente do México, onde o governo alemão

propunha uma aliança contra os Estados Unidos. Com este argumento em mãos, os ingleses convenceram o governo americano a participar diretamente na guerra (Ungaretti, 2002).

Durante a Segunda Guerra Mundial os americanos foram surpreendidos pelo ataque a Pearl Harbor, pois não foram capazes de prever a operação conduzida pelos japoneses, apesar de terem interceptado e decifrado mensagens diplomáticas daquele governo onde havia indicações de um possível ataque. Contudo, a situação foi revertida pelos americanos ao longo do conflito por meio da quebra das cifras japonesas "*Red*" e "*Purple*", além de preservar sua principal cifra, a "*Sigaba*".

O avanço das telecomunicações, da informática e das redes de computadores abriu novos horizontes para o desenvolvimento de novas aplicações. Como conseqüência outros segmentos, além dos militares e diplomatas, passaram a demandar soluções que atendessem às necessidades de segurança da informação para uma gama das tecnologias emergentes. Com isso, a criptografia saiu do domínio governamental tornando-se pública, tanto para pesquisas nos centros universitários, quanto para uso em atividades privadas.

Seu desenvolvimento foi incrementado no ambiente acadêmico, o que levou ao surgimento de inovações, dentre as quais se destacou a invenção de uma criptografia de chave pública, que iniciaria a fase dos códigos “inquebráveis”. Nos anos 90, Phil Zimmermann criou e disseminou pela Internet o algoritmo de nome *Pretty Good Privacy* (PGP), programa que popularizou a criptografia de chave pública no ambiente de Internet.

Constata-se que qualquer sistema de informação, em especial aqueles voltados à segurança, deve ser submetido a testes regulares a fim de comprovar a efetividade proposta e proceder às alterações necessárias.

3.1.2 Encriptação

A criptografia ou encriptação consiste na função de transformação de um texto simples ou natural em texto cifrado, parametrizada por uma chave.

A utilização desta função destina-se a restringir o acesso ao texto simples somente às entidades detentoras da chave usada na função. A complexidade das funções de criptografia evoluiu com o desenvolvimento computacional e com a criação de modelos matemáticos.

Segundo Tanenbaum (2003) criptoanalista possui conhecimento dos métodos genéricos usados para a encriptação dos textos simples, fato que lhe facilita a descobrir o conteúdo dos textos criptografados. Entretanto o Principio de Kerckhoff define que os algoritmos devem ser públicos e, apenas as chaves utilizadas na encriptação devem ser secretas.

Um exemplo dos primeiros métodos de criptografia é citado por Buchmann (2001) é a cifração de Caesar com a chave cinco para a palavra CRYPTOGRAPHY, onde obteríamos HWDUYTLWFUMD, de acordo com o Quadro 3-1.

Quadro 3-1: Cifração de Caesar

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

Fonte: Buchmann (2001)

A cifração de Caesar poderá ser facilmente modificada de maneira que o texto original e o texto cifrado, podem ser reajustados em todas as seqüências. Novamente a chave de espaço é Z26.

A cifração de Caesar utiliza 26 chaves, por essa razão é fácil determinar o texto original obtido pela cifração por intermédio de tentativas sobre todas as possíveis chaves e verificando se o texto original é razoável, dessa forma nos permite obter a chave de texto usada.

3.1.3 Criptoanálise

A criptoanálise trata do estudo destinado a solucionar as mensagens cifradas, os quais serão objetos de classificação, a título de melhor compreensão.

Para dificultar os ataques aos sistemas criptográficos é necessário preservar o segredo de todos os componentes deste sistema. Contudo, não é claro o nível de segurança obtido, vez que os ataques são realizados de formas variadas. As observações referem-se a interceptações de textos cifrados que estão em uso. Também abordam tentativas de obtenção de informações provenientes de pessoas que conhecem a estrutura atual de sistemas criptográficos em uso.

A criptoanálise moderna assume que os responsáveis pelos ataques conhecem os sistemas criptográficos em uso. Apenas as chaves secretas e os textos originais são dados como secretos. Os agressores tentam recuperá-los por meio dos textos cifrados ou também descobrir o valor das chaves em utilização. De acordo com Buchmann (2001), existem algumas formas mais conhecidas de ataques, são elas:

- Ataque ao texto cifrado: o invasor conhece o texto cifrado e tenta recuperar o texto original ou a chave de criptografia;
- Ataque decorrente do conhecimento do texto original: o invasor conhece o texto original e o correspondente texto cifrado, ou mesmo parte de ambos, visa recuperar a chave criptográfica ou decriptar outros textos cifrados;
- *Chosen-plaintext*: o invasor é conhecedor de técnicas de encriptação, mas desconhece a chave criptográfica. Ele tenta obter a chave a partir de um texto original conhecido;
- *Chosen-plaintext adaptive*: o invasor é hábil em técnicas criptográficas e também para selecionar um novo texto original e a respectiva função criptográfica, por isso é denominada adaptativa. É utilizado para obter a chave criptográfica;
- *Chosen-ciphertext*: O invasor pode decriptar o texto cifrado, mas desconhece a chave. A partir da escolha de um texto cifrado visa o conhecimento da chave.

3.1.4 Algoritmos Criptográficos

Buchmann (2001) menciona duas classes de algoritmos criptográficos: simétricos (ou de chave secreta) e assimétricos (ou de chave pública). Os algoritmos simétricos utilizam uma mesma chave tanto para cifrar como para decifrar. Nos algoritmos assimétricos há duas chaves distintas, uma para cifrar e outra para decifrar (a chave de decifração não pode ser obtida a partir da chave de cifração), por isso os algoritmos assimétricos geram as chaves aos pares (uma para cifrar e outra para decifrar).

Os algoritmos simétricos exigem que a chave seja secreta, de conhecimento exclusivo do emissor e do receptor. Portanto, é requerido um canal seguro para a transmissão da chave ao interlocutor. A Figura 3-1 ilustra a operação de um algoritmo criptográfico simétrico.

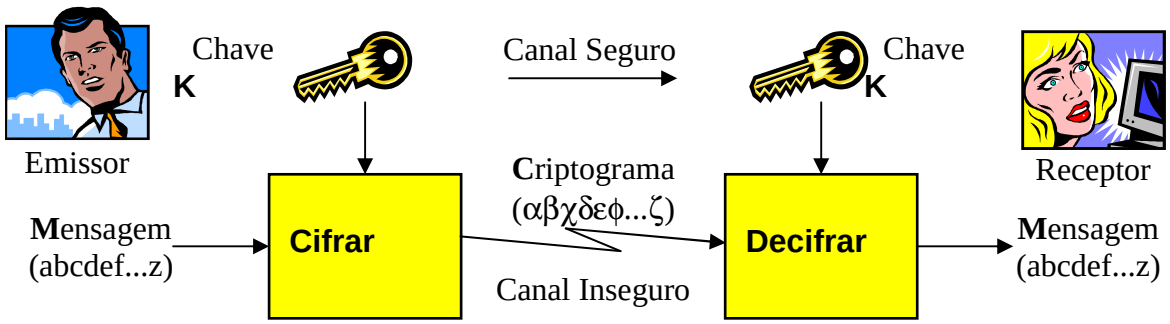

Figura 3-1: Uso de Algoritmo Criptográfico Simétrico (chave secreta)
Fonte: http://www.sbis.org.br

Por outro lado, os algoritmos assimétricos permitem que a chave de cifração seja de conhecimento público, por isso denominada chave pública, o que torna desnecessários os cuidados na transmissão da chave. Com isso, qualquer entidade ou pessoa pode cifrar mensagens com uma chave pública, contudo somente o destinatário, detentor da correspondente chave de decifração (denominada chave privada, ou secreta), poderá decifrá-la, pois esta é do conhecimento restrito do responsável pela geração do seu par de chaves. Na Figura 3-2, há uma ilustração da operação de um algoritmo assimétrico.

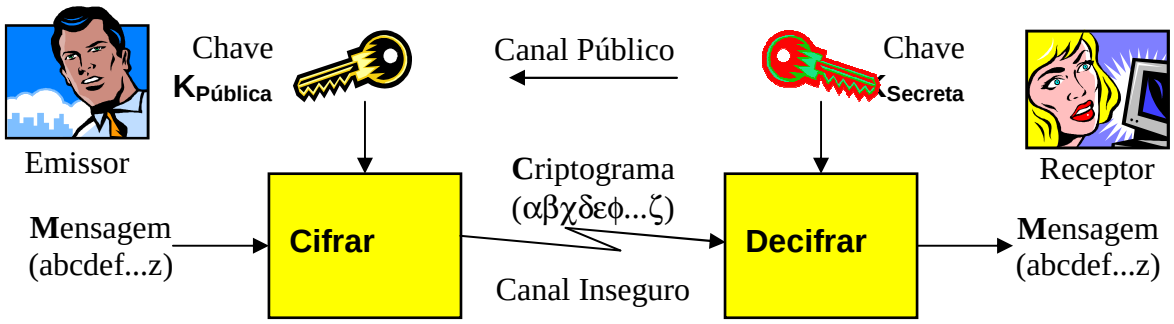

Figura 3-2: Uso de Algoritmo Criptográfico Assimétrico (chave pública)
Fonte: http://www.sbis.org.br

Computacionalmente, os algoritmos simétricos demonstram maior eficiência, o que permite altas taxas de cifração, por essa razão é aceitável o uso simultâneo de ambos tipos de algoritmo.

3.1.4.1 Algoritmo RSA

Buchmann (2001) descreve a idéia que deu origem à criação do algoritmo RSA, surgiu após um dia de discussões sobre criptografia baseada nas teorias de Whitfield Diffie e Martin Hellman publicadas na obra *New Direction in Crytography*, que introduziu o conceito de criptografia com chaves públicas. A discussão envolvia os pesquisadores do *Massachusetts Institute Technology* (MIT) Ronald L. Rivest, Adi Shamir and Leonard M. Adleman. Em setembro de 1977, o conceito do algoritmo criado pelos pesquisadores do MIT, foi publicado pela revista *The Scientific American*, fato este que tornou o RSA mundialmente conhecido e levou os três pesquisadores a fundarem a empresa RSA Data Security, Inc., que leva as iniciais dos seus nomes.

O algoritmo RSA está fundamentado em Teorias Clássicas dos Números, pois baseia-se na dificuldade computacional de fatorar o produto de dois números primos grandes. A complexidade é acentuada na medida que a quantidade de bits utilizada para descrever os números envolvidos é aumentada. Por exemplo, um número de 100 dígitos utiliza cerca de 350 bits. As implementações atuais chegam a usar 1024 bits.

Neste algoritmo é aplicado o conceito de chave pública, portanto são gerados dois pares de chaves, observando que o segundo número não

pode ser derivado do primeiro, de maneira que uma mensagem encriptada com o primeiro par possa ser apenas decriptada com o segundo par.

Esta propriedade assegura que o primeiro número possa ser divulgado a alguém que pretenda enviar uma mensagem encriptada ao detentor do segundo número, já que apenas essa pessoa pode decriptar a mensagem. O primeiro par é designado como chave pública, e o segundo como chave secreta.

3.2 Assinaturas Digitais

A assinatura digital é o criptograma resultante da cifração de um determinado documento, por meio da chave secreta de quem assina o algoritmo assimétrico. A verificação da assinatura é feita pela decifração deste criptograma (assinatura) com a chave pública correspondente. A leitura de uma mensagem somente é factível por intermédio da perfeita correspondência entre a chave pública, usada pelo receptor, e sua respectiva chave privada, em poder do emissor da mensagem. Este fato assegura a identidade do emissor, vez que somente este detém o conhecimento da chave privada.

A integridade também é garantida pela geração da assinatura digital, pois a criação do criptograma, além da chave privada, tem como base o conteúdo da mensagem, que é submetida à função de *Hashing*. Esta função criptográfica usa um método de autenticação sobre um resumo extraído do conteúdo original; gera como produto uma mensagem de saída denominada de *Hash* da mensagem, de tamanho fixo (geralmente 128 a 256 bits) independentemente do tamanho do conteúdo original (entrada) (Cormen 2002).

É importante destacar que em face da recuperação da mensagem, por meio de chave pública, o sigilo do documento assinado digitalmente não é preservado. Caso se trate de um documento confidencial, será necessária a implementação de processo adicional de criptografia.

3.3 Certificados Digitais e Autoridades Certificadoras

A redução do custo das comunicações e do processamento de transações em tempo real, direcionou a utilização da nova plataforma computacional baseada na Internet para realizar suas operações.

Após a ocorrência de incidentes de segurança que subtraíram valores consideráveis, monetários ou intangíveis, mas igualmente importantes, os Certificados Digitais se apresentam como a solução para autenticar usuários.

Certificado Digital é um documento (eletrônico) que contém a chave pública de um usuário (ou processo) e os seus dados de identificação. Este documento deve ser assinado por uma Autoridade Certificadora, que atesta sua integridade e origem.

O padrão mais utilizado para certificados digitais é o denominado X-509, o qual prevê, dentre outras informações possíveis, os dados da chave pública do usuário; nome do usuário proprietário da chave; nome da organização associada; data de emissão do certificado e; período de validade da chave (Custódio, 2003).

3.4 Infra-estrutura de Chaves Públicas (ICP)

O desenvolvimento da internet gera uma demanda por segurança jurídica para todo tipo de negócio impulsionado pela facilidade de comunicação moderna, adicionado a todos os demais requisitos destinados à preservação da fidedignidade das informações.

No âmbito governamental, essa revolução foi observada nas atividades de arrecadação dos impostos e taxas que impõe a necessidade de processar e armazenar as respectivas informações de maneira segura e inviolável. Para alcançar este objetivo, o governo federal optou pela implementação de Certificação Digital, com a intenção de, posteriormente, estender ao público de forma geral, (Rezende 2001).

Em face da característica de insegurança da Internet foi atribuído a ICP-Brasil o papel de neutralidade necessária para autenticar a identidade dos usuários de forma a certificar a autenticidade do conteúdo da transmissão das informações. É condição *sine qua non* a preservação dessa neutralidade e da independência para assegurar a inexistência de qualquer ingerência sobre os registros dos certificados, dos signatários e do conteúdo das mensagens certificadas pela ICP-Brasil.

A ICP–Brasil foi instituída para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, daqueles que utilizem certificados digitais. É um conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de estabelecer os fundamentos técnicos e metodológicos de um sistema de certificação digital baseado em chave pública (Rezende 2001).

3.5 Controle de Acesso

Nos conceitos atuais de TI as funcionalidades da autorização e autenticação são adequadamente implementadas por um eficiente sistema de controle de acesso que determinará aos usuários seus respectivos direitos nos sistemas computacionais.

Por isso, o controle de acesso às informações tornou-se uma questão fundamental, principalmente nos sistemas virtuais onde impõe a utilização de poderosa arquitetura e desafios administrativos em todos os níveis dos projetos computacionais. Sob a perspectiva de negócios, o controle de acesso possui potencialidade para promover uma condição ótima de compartilhamento e permuta de recursos, contudo, provoca a potencialidade de elevação dos custos, exposição desautorizada ou corrupção do valor da informação.

Em razão da categorização dos aspectos de segurança das informações, o controle de acesso é crítico para preservar a confidencialidade e integridade, por intermédio de concessões de acesso exclusivo aos usuários autorizados. Os modelos, sistemas e terminologia de controle de acesso foram desenvolvidos ao longo das últimas décadas, cuja importância dos seus principais elementos e seus relacionamentos, segundo Ferraiolo *et al.* (2003), destacamos a seguir.

Usuário, refere-se ao termo utilizado para as pessoas que utilizam os sistemas computacionais. Em muitos sistemas o usuário individual pode ter múltiplos logins, que podem ser ativados simultaneamente. O instante que o usuário dialoga com o sistema de informação é denominado Seção.

O processo computacional ativo, por demanda do usuário, é denominado Tópico. Todas as ações do usuário no sistema computacional requerem que diversos programas estejam ativos, o que significa que múltiplos Tópicos estão em operação.

Os Objetos se referem a qualquer recurso acessível pelo sistema computacional entre os quais se incluem periféricos, impressoras, base de dados etc. Embora os modelos de controle de acesso permitam tratar estes elementos como Objetos, tradicionalmente são considerados como entidades passivas, que apenas contém ou recebem informações.

Operações são os processos invocados pelos Tópicos. Os modelos de controle de acesso baseados em regras requerem distinção clara entre Operação e Tópico. Exemplo, um usuário de um terminal ATM (*Automatic Teller Machine*), introduz seu cartão e digita corretamente sua senha de acesso, o programa de controle em operação denomina-se Tópico. Porém, este ativa mais de uma Operação, tal como depósitos, saques, extratos etc.

3.6 Privilégio Mínimo

Permissões ou privilégios são autorizações para efetuar uma ação do sistema. O privilégio mínimo é uma prática seletiva para atribuir permissões aos usuários, de forma que não sejam concedidas permissões além daquelas necessárias para realizar suas funções. Este princípio evita problemas decorrentes de poderes individuais para efetuar ações desnecessárias e potenciais prejuízos. A questão decorre dos mecanismos para definir um sistema de permissões para agregar funções ou deveres correspondentes às regras do Usuário ou do Tópico ativo que atenda ao usuário.

Nesse contexto, o Privilégio Mínimo provê de maneira racional a definição e separação de fronteiras que irão direcionar os mecanismos de controle de acesso. Manter a aderência ao princípio do privilégio mínimo é um desafio administrativo significativo e requer a identificação das funções e especificações das permissões requeridas por cada função e as restrições do usuário para o domínio com seus privilégios mínimos e nada mais.

A estrita aderência ao privilégio mínimo requer diferentes níveis individuais de permissão para diferentes tempos, dependendo da tarefa ou funções de acordo com o ambiente onde as permissões serão concedidas.

A RAND Corporation reporta que desde 1970 implementou uma análise de segurança para o *Department of Defense – USA* (DoD) *Computer System*. Inclui a definição de um método de implementação multi-nível (documentos classificados por nível de segurança: Confidencial, Secreto ou Ultra-secreto) (Cassiolato; Lastres 2000).

Bell e LaPadula (DoJ, 1995) formalizaram regras de controle de acesso militar em um modelo matemático apropriado para definir e avaliar a segurança dos sistemas computacionais. Dentre outros aspectos, destaca-se a regra que determina que os usuários somente possuem permissão para acessar informações que estejam classificadas no seu nível de autorização. Conceitualmente é uma política simples, conhecida e seguida, cuja implementação, em um sistema computacional, pode levar a equívocos motivados por inesperadas interações entre diferentes componentes e também pode fragilizar os sistemas. O modelo de Bell-LaPadula é importante porque provê um modelo formal (i.e., matemática) de uma política de segurança multi-nível, fazendo o possível para analisar as propriedades do modelo em detalhes.

Duas regras básicas são requeridas no modelo formal: a primeira regra resume-se em "*no read up*" e "*no write down*", ou seja, para o usuário com o nível de autorização especial não é permitido a leitura das informações abaixo daquele nível. Exemplo, o usuário com autorização *Secret* não possui permissão de ler informações *Top secret*.

O usuário com nível de autorização especial, pode gravar informações somente no mesmo nível ou nos níveis acima. Exemplo, caso o usuário se encontre no nível de permissão denominado *Secret*, os programas e os processos operados por este usuário não permitem que sejam gravadas informações no nível *Confidential* (abaixo), apesar disso poderá gravá-las em uma condição superior, ou seja no nível *Top Secret*. Nota-se que esta regra é aplicável e recomendável aos processos em operação pelo computador.

O modelo da Bell LaPadulla (DoJ,1995) incluiu a noção de categorias, que encaminha para uma interrupção vertical de comportamentos de segurança através dos níveis. Para ter próprios níveis de autorização, solicita-se ao usuário autorizações adicionais para todas as categorias relacionadas ao documento classificado. Por exemplo, o documento pode ser classificado como *Secret*, nuclear, NATO. Para acessar o documento o usuário necessitará autorização de *Secret* ou acima e, também deve ser autorizado em duas categorias – nuclear e NATO. Essa política assegura que a classificação da informação não será rebaixada seja por ação acidental ou dolosa.

3.7 Classificação das Informações

O modelo de classificação de informações apresentado a seguir foi baseado na “Ordem Executiva” No. 12.958 – Classificação das Informações de Segurança Nacional, do Departamento de Defesa dos Estados Unidos da América do Norte, cuja emissão foi de responsabilidade do presidente Clinton em abril de 1995. Esta ordem descreveu um sistema uniforme para classificar, proteger e re-classificar informações de segurança nacional, proteger os cidadãos, as instituições democráticas e a participação na comunidade das nações (*Department of Justice USA;* 2005).

3.7.1 Classificação Original

Os padrões de classificação devem atender a requisitos de importância de cada informação e as possíveis conseqüências ou risco na condição de ocorrer o acesso por indivíduos ou grupos que não sejam autorizados. Para selecionar as informações que apresentem necessidade de preservar as condições de segurança, foram definidos os seguintes critérios:

- Deve existir uma autoridade formal para acompanhar e validar o resultado obtido na classificação da informação;
- É condição obrigatória que a informação pertença à organização, ou tenha sido produzida sob sua responsabilidade ou, seja destinada para sua utilização;

- A informação pode fazer parte de uma ou mais Categorias de Risco, descritas em tópico especifico; e
- A autoridade original por validar a classificação deve assegurar que a divulgação desautorizada da informação pode resultar em danos, assim esta autoridade deve identificá-las, descrevê-las e encaminhá-las para classificação.

A condição de ausência de classificação ou desclassificação implica que a informação não apresenta necessidade de preservar seu sigilo, o que representa sua condição Pública.

A informação classificada em qualquer um dos níveis não será re-classificada automaticamente em conseqüência de divulgação desautorizada da informação.

3.7.2 Níveis da classificação

A informação pode ser classificada nos seguintes níveis:

- "*Top Secret*" será aplicado à informação, cuja divulgação desautorizada pode causar danos excepcionalmente graves à segurança;
- "*Secret*" será aplicado à informação, cuja divulgação desautorizada pode causar danos sérios à segurança;
- "*Confidential*" será aplicado à informação, cuja divulgação desautorizada pode causar danos à segurança.

3.7.3 Categorias da Classificação

As Categorias de Classificação descrevem as categorias de informação de maior interesse. Por se tratar de uma organização governamental o DoJ destacou os grupos de informação

- Planos Militares, Sistema de Armamentos, ou operações;
- Informações sobre governos estrangeiros;

- Atividades de Inteligência, inclusive aquelas especiais, recursos de inteligência ou métodos ou criptografia;
- Atividades do governo americano em território estrangeiro;
- Assuntos relacionados a segurança nacional tal como tecnologia ciências ou problemas econômicos; ou
- Programa do governo americano para salvaguardar recursos e materiais nucleares.

3.7.4 Duração da Classificação

O dinamismo de mudanças observado no fluxo dos sistemas de informação é refletido na necessidade de ajustar as necessidades quanto à preservação do sigilo. A seguir, encontram-se as circunstâncias que podem justificar as possíveis alterações sobre a classificação original da informação.

a) A autoridade responsável poderá estabelecer uma data ou um evento específico que promova nova classificação ou até mesmo a desclassificação. A data ou o evento não deverá exceder o horizonte de tempo definido no parágrafo (b);

b) Se a autoridade original da classificação não puder determinar uma data ou um evento específico para a revisão da classificação, a informação estará marcada para que a alteração possa ocorrer em dez anos a partir da data referente à classificação original, exceto nas circunstâncias descritas no parágrafo (d);

c) A autoridade original pode estender o prazo de validade sucessivamente, porém não é permitido que cada solicitação exceda o período de dez anos. Este parágrafo não se aplica a aquelas informações classificadas com prazo de retenção permanente;

d) Quando da classificação original, a autoridade responsável poderá isentar a re-classificação no prazo de dez anos, o que significa a classificação permanente.

3.7.5 Identificação e *Markings*

A documentação apropriada de todo o processo de classificação das informações em face da sua importância, é essencial para manutenção e aderência aos seus objetivos, permitir o entendimento das equipes e pessoas envolvidas e dar andamento a futuras reavaliações da classificação original.

Além de classificar as informações de maior importância é necessário documentar apropriadamente todos os dados relativos à classificação, seja na face de cada informação ou grupo de informações, a fim de evitar eventuais falhas de identificação e marcas. A determinação do governo americano sugere mencionar o histórico dos níveis de classificação; a identidade dos envolvidos na validação; instruções de re-classificação e justificativa.

Cada informação ou grupo de informações originais classificadas deve, por meio de marcação, indicar as parcelas classificadas, com os níveis aplicáveis da classificação, as parcelas isentas da re-classificação e relacionar as parcelas que não são classificáveis (públicas).

3.7.6 Classificação Derivativa

A derivação dos atributos da informação a titulo de preservação do sigilo, trata sobre o repasse da sensibilidade de uma informação para outra, originado por relacionamentos que provocam a alteração da classificação das informações.

Para a informação classificada como derivativa, baseada em fontes múltiplas, carregará a frente à data ou o evento para a re-classificação que corresponde ao período mais longo da classificação entre as fontes.

3.8 Redes Neurais Artificiais

As primeiras informações sobre neuro-computação tiveram origem na década de 40 (Russell; Norvig, 2004), por intermédio dos artigos publicados pelo neurofisiologista McCulloch e do matemático Walter Pitts. Estes sugerem a construção de um dispositivo baseado no cérebro humano. Rosenblatt (1958), descreveu um modelo computacional probabilístico para mostrar a organização

e o estoque de informação no cérebro humano. Este modelo representava uma rede neural artificial e foi batizado de *Perceptron*.

As redes neurais foram inspiradas na estrutura e na função de neurônios biológicos, por isso aprendem com a interação de padrões que servem de exemplo, sem requererem um conhecimento das relações entre as variáveis sob investigação. O neurônio recebe uma ou mais entradas e transforma a soma daquelas entradas em um valor de saída, o qual é transferido para outro neurônio. A comunicação entre os neurônios é feita por estímulos transmitidos entre os elementos da rede. No caso do sistema nervoso central a comunicação ocorre através de diferentes concentrações de Na+ (Sódio) e K+ (Potássio). O resultado desta comunicação se estende a todo corpo humano, onde está distribuído um sistema altamente complexo de neurônios. A comunicação entre os neurônios celulares ocorre por impulsos elétricos temporais (Cardoso *et al.*, 1999).

A rede neural artificial é um conjunto de unidades processadoras (ou módulos) que simulam neurônios biológicos e são interconectados por um conjunto de pesos (análogos às conexões sinápticas no sistema nervoso), o qual permite tanto processamento serial quanto paralelo das informações tratadas pela rede (Astion; Wilding, 1992; Roush *et al*., 1996; Xin, 1999). Os “neurônios” da rede podem receber entradas excitatórias ou inibitórias de outros neurônios (Forsström; Dalton, 1995) e produzem uma saída, que geralmente é uma função não linear da entrada da rede (Astion; Wilding, 1992). Em contraste com muitos sistemas especialistas, as redes neurais artificiais não dependem de algoritmos pré-definidos (Lee *et al*., 1999).

Fenômenos complexos são aqueles que envolvem variáveis conhecidas como causalmente dependentes, porém a dependência está além de uma relação linear ou não linear do tipo polinomial de primeira ordem. Os fenômenos complexos têm sido área fértil para o desenvolvimento de modelos com redes neurais. Redes neurais, mesmo que implementadas com sucesso, permitem apenas simular ou emular o fenômeno modelado, não oferecendo por si só a possibilidade de se simplificar, generalizar ou reduzir a teoria por trás do

fenômeno complexo. Neste sentido, podem ser consideradas como uma panacéia pragmática que funciona, mas não se sabe porquê (Kovács, 1996).

Forsström e Dalton (1995) acrescentam a essa visão de Kovács, o entendimento que à medida que o aprendizado ocorre, o erro entre a saída da rede e a saída desejada diminui. Portanto, o conhecimento adquirido pela rede, está codificado nos pesos das conexões entre os neurônios. Devido a este fato, é praticamente impossível interpretar o conhecimento aprendido por qualquer rede de retropropagação. Esta é a razão que justifica a denominação de “caixa preta” atribuída às redes neurais.

Elas aprendem a calcular uma saída corretamente a partir de um padrão de entrada, mas elas raramente revelam, sob qualquer forma inteligível, o conhecimento que está por trás dos seus julgamentos.

Vantagens das redes neurais artificiais:

- Os cálculos são feitos em neurônios individuais;
- Permitem executar tarefas complexas para realizar o aprendizado por meio dos exemplos dados, ao invés das técnicas de estatística convencional;
- Aplicação de informações qualitativas e quantitativas nos mesmos modelos;
- Considerando que o produto obtido pela rede não está atrelado diretamente às suposições de distribuição de dados, não se exige homocedasticidade, tal qual nas demais funções estatísticas;
- Ajuste à análise de dados não lineares e multivariados, vez que os fenômenos tratados apresentam comportamento não é linear.

Desvantagens das redes neurais artificiais:

- O conhecimento aprendido não pode ser expresso em regras, ou seja, não existe uma equação inteligível que possa ser mostrada;
- A validação da rede é mais difícil diante da estatística convencional;
- As redes neurais precisam de elevado volume de dados para as etapas de treinamento, aprendizado e validação.

Tratando-se de arquiteturas computacionais, redes neurais artificiais são sistemas baseados numa aproximação à computação pautada em nós interligados em uma rede, apresentando uma modelagem inspirada nesse funcionamento do cérebro humano (Fausett, 1994). A Figura 3-3 exibe um modelo simplificado de uma rede neural.

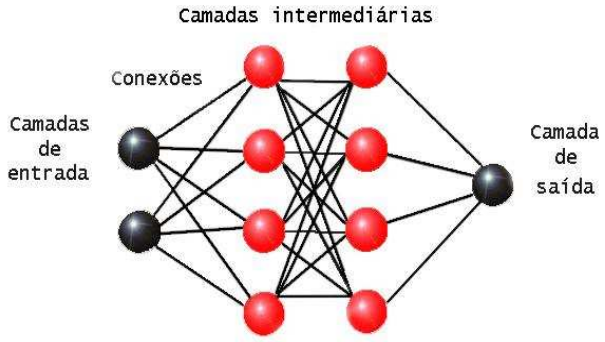

Figura 3-3: Rede Neural

Redes neurais artificiais são compostas de nós simples (ou neurônios), cujo estado pode ser representado por valores numéricos de ativação. Dessa forma, cada nó gera uma saída baseada em sua ativação. Os nós conectam-se pelas arestas rotuladas com pesos, e o valor da saída de um nó é transmitido a todos os nós conectados a este. Através destas ligações, a saída de um nó pode influenciar as ativações de outros nós. Cada nó calcula sua ativação através da soma ponderada de suas entradas, e determina a saída pela função de valoração. Portanto, o aprendizado das redes ocorre pelas alterações dos pesos nas conexões.

As vantagens que podem ser consideradas na aplicação das redes neurais artificiais são em geral relacionadas a sua praticidade no aprendizado de aproximação de funções a partir de exemplos (Neto; Nicoletti, 2005). A saída da rede são funções que de alguma maneira convergem para determinado ponto.

Numa maneira mais genérica de se explicar, as operações de neurônio podem ser estabelecidos da seguinte maneira (Russell; Norvig, 2004):

- Sinais são apresentados à entrada;
- Cada sinal se multiplica por um peso que indica sua influência na saída;

- Uma soma ponderada dos sinais que produzem um nível de atividade é calculada;
- Se este nível excede um limite (*threshold*), a unidade produz uma saída.

Ainda segundo Russel (2004), uma rede neural artificial é definida por:

- Existência de um padrão de processamento e conexão entre os neurônios;
- Processamento que ocorre através dos processadores básicos (neurônios);
- Uma função de ativação que representa o estado do neurônio;
- Uso de um algoritmo de treinamento (também chamado algoritmo de aprendizagem).

A responsável em estabelecer o estado do neurônio (chamado de ativação) é a função de ativação. O valor dessa função depende do estimulo recebido (externo ou interno, proveniente de outros neurônios). Por sua vez, a saída dos neurônios depende do valor de ativação. Essas saídas interagem com o restante da rede através das conexões sinápticas de cada neurônio. Portanto, na fase de treinamento, neurônios enviam sua saída aos outros elementos da rede a qual estão conectados. A função de ativação provoca mudança de estado do neurônio, embora existam outros tipos de funções, inclusive para calcular o nível de ativação dos neurônios.

Segundo Haykin (1999), uma rede neural artificial consiste em unidades de processamento simples que armazenam conhecimento experimental e o tornam disponível para o uso. Ele também sugere que é possível compará-la ao cérebro humano em dois aspectos. Primeiramente é necessário um processo de aprendizagem para que a rede adquira conhecimento a partir do ambiente em que se encontra. O segundo aspecto refere-se ao armazenamento do conhecimento adquirido que ocorre nas conexões entre os neurônios (pesos sinápticos).

Basicamente, há três funções principais na montagem de uma rede (Neto; Nicoletti, 2005). Cada uma possui uma propriedade específica.

A primeira função denomina-se soma, pois combina as entradas do neurônio num valor. Cada entrada depende dos valores transmitidos e dos pesos sinápticos das conexões, pelas quais ocorre à transmissão. A função soma mais usada é o produto interno definido pela Equação 1.

$$dj = \sum_{i=0}^{n} W_{ij} X_i \qquad (1)$$

Após executar a função soma, a função de ativação calcula o nível de atividade ou estado de um neurônio. Ao término, associa-se a ativação do neurônio a um valor de saída, por intermédio da função de saída.

O processo cognitivo de uma rede neural artificial (ou algoritmo de aprendizado) ocorre pelo ajuste dos pesos das conexões. Para tanto, há um conjunto de regras, baseadas em exemplos históricos, que determinam os ajustes nos pesos das conexões.

3.8.1 Utilização de Redes Neurais Artificiais em outras áreas

As redes neurais são usadas com o objetivo de classificar e reconhecer padrões: reconhecer e gerar fala; predizer índices financeiros, tais como taxas de câmbio de moedas; localizar a origem de pontos no radar, otimizar processos químicos; reconhecer alvos e detectar minas bélicas; identificar células cancerosas; reconhecer anormalidade cromossômica; detectar fibrilação ventricular; predizer trajetórias de reentrada de naves espaciais; reconhecer automaticamente caracteres escritos à mão; sexar rostos, entre outros (Cheng; Titterington, 1994).

Em sua origem as redes neurais serviram a indústria militar, porém, atualmente têm seu uso crescente em bancos, em aplicações de cartões de crédito e comércio eletrônico, como método para evitar fraudes eletrônicas nestas operações (O'Sullivan, 1999; Estock, 1999). As redes neurais reconhecem padrões específicos de comportamento de gastos do proprietário do cartão de crédito, aprendem a partir de suas experiências passadas, e podem ser re-treinadas, adaptando-se a uma situação especificas.

Bruno (1999), divulgou um produto que utilizou redes neurais artificiais para interagir com os clientes de bancos em processos de solicitação de financiamentos e demais serviços realizados em tempo real.

Uysal e El Roubi (1999) compararam o uso de redes neurais artificiais e a regressão múltipla para análise de demanda em turismo. O estudo revelou que as redes neurais artificiais têm melhores resultados em termos de predição e acurácia. Goodman (1999) comparou as redes neurais artificiais e métodos estatísticos. Concluiu que sobre o destaque das redes neurais artificiais no reconhecimento de padrões no desenvolvimento de modelos biologicamente reais que possuem as vantagens das atuais RNAs.

Cross *et al.* (1995) afirmaram que o emprego de redes neurais artificiais na medicina humana se verifica no desenvolvimento de ferramentas decisórias, destinadas a auxiliar os médicos menos experientes, fornecendo-lhes conhecimento alicerçado em um grande número de casos. Também foi utilizada na tomada de decisão em suportes diagnósticos, seja na forma de sistema estatístico ou baseado em regras.

Outros autores exploram o assunto, sugerindo que redes neurais terão um papel importante no suporte decisório em um futuro próximo. Forsström e Dalton (1995) abordam o uso de redes neurais artificiais como ferramentas em medicina clínica, como método de análise por imagens, processamento de sinais e medicina laboratorial.

3.8.2 Tipos de aprendizado

No processo de aprendizado, de acordo com Neto e Nicoletti (2005), os algoritmos podem pertencer a grupos distintos: supervisionados, não-supervisionados e construtivos.

No aprendizado, por meio de algoritmos supervisionados, para cada vetor ou padrão de treinamento, são associadas classes (ou vetores de saída). Segundo os autores (Neto; Nicoletti, 2005), durante a fase de treinamento, o algoritmo tenta ajustar os pesos das conexões de maneira que a

saída da rede coincida com a classe (ou vetor de saída) associada ao exemplo, para cada exemplo do conjunto de treinamento.

O aprendizado não-supervisionado (uso de algoritmo não supervisionado) é mais usado em sistemas de classificação. Neste tipo de algoritmo, não existe uma saída desejada para cada entrada. A rede é treinada por excitações ou padrões de entrada e, de forma arbitrária, organiza a saída em padrões e categorias. Para cada entrada é fornecida uma resposta que indique a classe a qual determinada entrada pertence. Se o padrão de entrada não corresponde às classes que já existem, uma nova classe é gerada. O aprendizado não supervisionado trabalha com modificações dos pesos de conexões. Dessa forma os padrões de entrada são agrupados. Uma rede que utiliza o algoritmo não supervisionado é a *Self Organization Map* (*SOM*) de Kohonen ou Konets.

Na utilização dos algoritmos neurais construtivos, o aprendizado não demanda uma arquitetura de rede fixa, antes do início do treinamento. Segundo Chen *et al*. (2006), algoritmos de aprendizagem construtivos ajudam na construção de redes neurais artificiais mínimas para a classificação de padrões. Para Neto e Nicoletti (2005), a principal característica deste modelo de aprendizado é a construção dinâmica das camadas intermediárias da rede, à medida que vão sendo necessárias para o treinamento. Essa característica determina que a definição da arquitetura da rede seja interligada ao próprio processo de aprendizado. Neste caso, ambos os processos, o de treinamento e o de construção de rede, acontecem simultaneamente e são independentes.

O aprendizado construtivo é iniciado por uma rede sem nenhum neurônio intermediário. Os neurônios são adicionados à rede à medida que o treinamento progride. Os processos de adição de neurônios e de treinamento da rede terminam quando se atinge um desempenho satisfatório, diante de critérios previamente definidos.

3.8.3 Estruturas de Rede

Segundo Russell e Norvig (2004), há duas categorias principais na estrutura de fluxo de uma rede neural artificial. As redes acíclicas ou redes de

alimentação direta e redes cíclicas ou redes recorrentes. Por definição a rede de alimentação direta é representada pela sua função de entrada. Desse modo, não possui camadas intermediárias de neurônios internos para processamento. A rede recorrente efetiva a alimentação das entradas, utilizando a própria saída. Fausett (1994), diz que nesse tipo de rede os níveis de ativação dos neurônios podem chegar num estado estável ou caótico e ainda exibir oscilações durante o processo de treinamento. A rede responde a determinadas entradas de acordo com seu estado inicial, que por sua vez depende das entradas anteriores. Conclui-se, que redes recorrentes (divergente das redes de alimentação direta) podem possuir memória de curto prazo, tornando-as de semelhante ao funcionamento do cérebro humano.

3.8.3.1 Redes neurais de uma única camada (*Perceptrons*)

Para Fausett (1994) redes neurais de uma única camada ou redes de *perceptron* são aquelas onde todas as entradas são conectadas diretamente às saídas, levando em consideração que cada unidade de saída é independente das unidades de entrada. Pode-se observar um exemplo de rede de *perceptron* na Figura 3-4 a seguir:

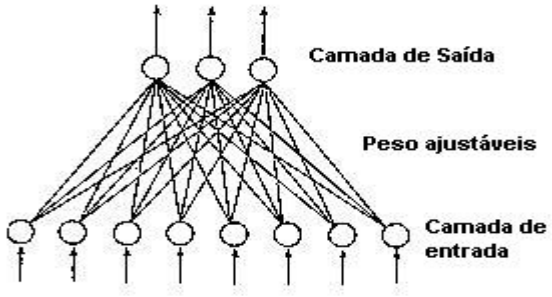

Figura 3-4: Rede de *Perceptron*

Segundo Haykin (1999), a rede de *perceptron* aprende conceitos. Pode aprender a responder com verdadeiro (1) ou falso (0) de acordo com as entradas apresentadas e pelo estudo repetido dos exemplos reportados. De forma geral, os pesos dos vínculos de entrada da rede não tem efeito sobre as outras unidades de saída.

Para Russell e Norvig (2004), ao usar a função de ativação de limiar é possível visualizar o *perceptron* como a representação de uma função booleana. Como resultado, além das funções booleanas elementares (E, OU e

NÃO), funções booleanas de ordem complexa podem ser representadas de maneira compacta. Como exemplo, pode-se citar a função maioria, que tem como saída 1 somente se mais da metade dos valores de suas entradas forem iguais a 1. A representação dessa função por um *perceptron* pode ser dada com cada W_j=1 e limiar W_0=*n* / 2. A quantidade de interações de uma árvore de decisão nesse processo seria maior, pois necessitaria de $O(2^n)$ nós para representar essa função.

O processo de treinamento de *perceptron*s é feito através de um algoritmo simples de aprendizagem, chamado regra-delta (Fausett, 1994). Neste algoritmo há um cálculo de erros entre a saída de dados calculada e a saída desejada. Através desse processo o algoritmo ajusta os pesos sinápticos, que convergem às entradas para uma resposta da rede.

Conforme a Figura 3-5 e a Figura 3-6 a seguir, os *perceptron*s de uma camada são capazes de aprender sobre problemas linearmente separáveis (podem ser separados por uma reta no hiperplano). A limitação desta rede neural se encontra, então na reduzida gama de problemas que consegue tratar. Para problemas que envolvem classificação de variados perfis, este tipo de modelagem de rede não é o mais indicado.

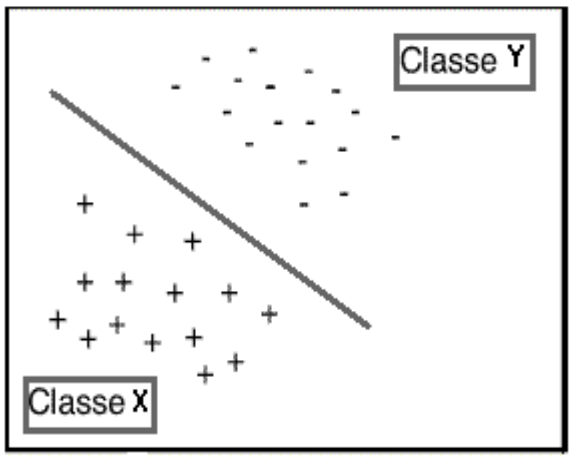

Figura 3-5: Classes Linearmente Separáveis

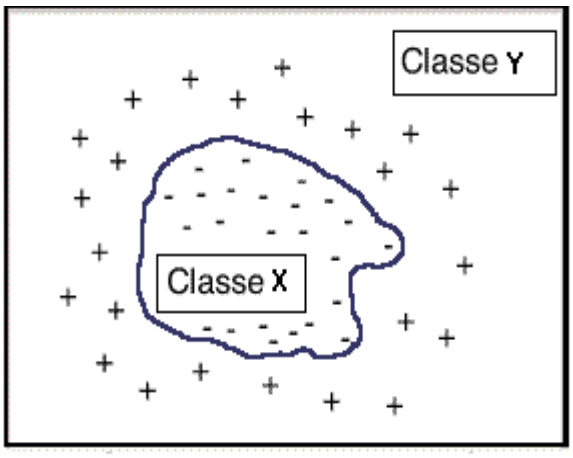

Figura 3-6: Classes Não Linearmente Separáveis

3.8.3.2 *Perceptrons* de várias camadas

As redes (ou *perceptron*s) de várias camadas podem ser consideradas como redes com unidades ocultas (Russel, 2004). Também denominadas como rede de três camadas ou rede de duas camadas.

Ainda segundo Russell e Norvig (2004), “a vantagem de adicionar camadas ocultas é que ela aumenta o espaço de hipóteses que a rede pode representar”. Por isso, compreende-se que a rede *perceptrons* de várias camadas apresenta um processamento mais dinâmico.

Quanto aos algoritmos de aprendizagem para esta rede, Russel define que são semelhantes aos algoritmos de *perceptrons* de uma camada, diferenciando-se na condição que podem apresentar várias saídas. Para isso, usa um vetor de saída (intermediário) ao invés de um único valor, assim, cada exemplo tem um vetor de saída. Outra diferença entre uma rede de camada única e uma rede de várias camadas é a clareza do erro na camada de saída, enquanto que nas camadas ocultas há maior dificuldade de compreensão, pois juntamente com os dados de treinamento não se tem a informação do valor que os nós ocultos realmente possuem.

3.8.3.3 Redes de Kohonen

Uma especialização das redes neurais são as redes de Kohonen (2001) ou *Konets*. Foi desenvolvida por Teuvo Kohonen no início da década de 80. (Kohonen, 2001; Suuronen, 2001). De acordo com Wangenheim (2006), Kohonen desenvolveu pesquisas em modelos de inter-relacionamentos intrínsecos em distribuições de padrões, e partir de 1980 voltou-se à descoberta de um modelo de auto-organização de informações e um processo de aprendizado indutivo, capaz de ser usado como modelo de aprendizado e organização de informações no neocórtex cerebral de um animal superior.

Segundo Francisco (2004), o estudo de Kohonen foi motivado pela característica do cérebro humano de organizar informações em muitas regiões, de forma que entradas sensoriais distintas são representadas por mapas computacionais topologicamente ordenados.

As *Konets* são redes competitivas, de aprendizado não-supervisionado, não busca a solução ótima, apenas uma solução viável, com bom resultado.

Esta rede é composta por um conjunto de unidades de saída e um vetor com n unidades de entrada. A Figura 3-7, baseada em Damelincourt (2006), detalha a fase de treinamento de uma rede neural de Kohonen: cada saída corresponde a um nó em um *grid* bidimensional, que por sua vez está conectado a um nó de entrada. A fase de treinamento (automática, sem intervenção do usuário) consiste em apresentar as entradas repetidas vezes à rede, de maneira que a distribuição dos nós de saída corresponda à distribuição dos nós de entrada, de acordo com os pesos existentes na rede.

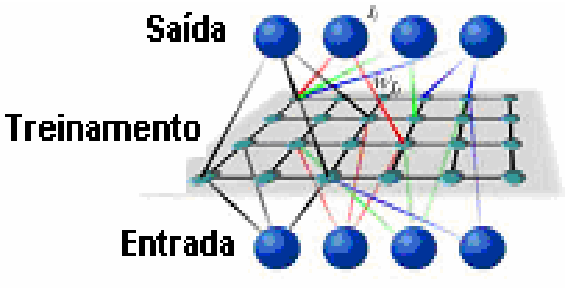

Figura 3-7: Treinamento da Rede de Kohonen

Conforme se vê na Figura 3-7, cada unidade de entrada é avaliada e agrupada dentro da possibilidade de treinamento da rede. Quanto maior a quantidade de entradas e de repetições para treinamento da rede, maior a quantidade de grupos criados.

Nessa rede, a grade da camada intermediária de treinamento é usualmente bi-dimensional. Mapas auto-organizáveis básicos, de forma ilustrativa, podem ser comparados com uma rede feita por linhas de tecido. Cada neurônio (após o processo de treinamento) fica nas intersecções da rede.

A meta principal de um mapa auto-organizável é transformar uma entrada (de um padrão qualquer) num mapa de saída com uma ou duas dimensões. De maneira análoga podemos enxergar as *Konets* também como se fossem redes de pesca recém tiradas do mar. Imagina-se, então que em cada nó dessa rede se encontre um peixe de determinada espécie. Randomicamente,

escolhe-se um peixe de determinado nó como *pivot*, e para esse peixe verifica-se qual é o peixe, de outro nó, que mais se assemelha ao primeiro. Quando o peixe mais parecido é encontrado, é aproximado ao *pivot*, de acordo com seu grau de similaridade dos seus atributos. O mesmo procedimento é aplicado aos peixes dos nós adjacentes que mais se assemelhava ao *pivot*. Após repetir este procedimento por mais de 3000 vezes nota-se que os peixes formaram regiões de agrupamentos claras nessa rede, onde os peixes de tamanho, cores e características semelhantes se aproximam.

3.8.3.3.1 Treinamento da rede

Na superfície de entrada da rede, para cada parâmetro de saída representado, é atribuído um peso. Cada neurônio armazena um vetor de pesos, cada vetor de pesos correspondente a uma das entradas de um vetor de entradas. Quando surge uma nova entrada, cada neurônio da rede calcula seu nível de ativação através da definição 2:

$$\sqrt{\sum_{i=0}^{n}(weight_i - input_i)^2} \qquad (2)$$

Onde $weight_i$ é o *i*-ésimo elemento do vetor de pesos e, $input_i$ é a *i*-ésima entrada. O neurônio com o menor nível de ativação (mais próximo ao vetor de entrada, no espaço euclidiano) pode ajustar seus pesos de maneira a aproximar-se do vetor de entrada, tal qual outros se aproximam de seus vizinhos.

Segundo Francisco (2004) e Haykin (2001), são três os processos envolvidos na formação dos mapas:

- Competição: para cada padrão de entrada apresentado à rede somente uma unidade do *grid* será ativada. Esta unidade é denominada neurônio vencedor, pois é ativada pela função discriminante (que provê a base para a competição dos neurônios).
- Cooperação: o neurônio vencedor determina o centro de uma vizinhança topológica de neurônios excitados lateralmente, provendo as bases para a cooperação entre tais neurônios vizinhos.

- Adaptação Sináptica: nesta fase, os pesos sinápticos são ajustados para o vetor de pesos vencedor, assim os neurônios excitados aumentam os valores individuais da função discriminante em relação ao padrão de entrada, por meio de ajustes aplicados aos pesos sinápticos correspondentes. Caso um padrão semelhante seja apresentado novamente à entrada, a resposta do neurônio vencedor será gradativamente aumentada nesse processo.

Considere-se que o treinamento de uma rede de Kohonen é feito de modo competitivo e não supervisionado. O algoritmo atende as seguintes etapas (Kohonen, 2001; Roussinov, 2001):

- Inicializar nós de entrada, saída e pesos: A primeira etapa consiste em criar um *grid* bidimensional de *m* possíveis nós de saída. Organiza-se o *grid* como um grafo bipartido, inicializando os pesos $weight_{ij}$ das conexões entre cada um dos *i*-ésimos nós de entrada e cada j-ésimo nó do *grid* com valores aleatórios. Cada um dos j-ésimos nós de saída está associado a um vetor de pesos $weight_{ij}$.
- Fornecer dados de entrada: A medida em que são fornecidos os dados de entrada e têm início a interação com o sistema, as informações sobre as preferências e aspectos importantes são gradativamente apresentadas à rede. Cada *i*-ésima entrada do usuário em um dado tempo *t* é representada por um vetor $v_i(t)$.
- Calcular distância no espaço euclidiano: A terceira etapa consiste em computar a distância euclidiana *dj* entre cada um dos vetores de entrada $v_i(t)$ e o vetor de pesos $weight_{ij}$:

$$d_j = \sum_{i=0}^{n-1} (v_i(t) - weight_{ij}(t))^2 \qquad (3)$$

- Selecionar o nó vencedor *j** e atualizar os pesos de *j** e de seus vizinhos: Nesta etapa é selecionado o nó vencedor *j** , que produz a menor distância *dj*. Também ocorre a atualização dos pesos que visa diminuir a distância de *j** e de seus vizinhos em relação a *vi(t)*:

$$weight_{ij}(t+1) = weight_{ij}(t) + n(t)v_i(t) - weight_{ij}(t) \qquad (4)$$

onde η é um coeficiente de ajuste de erro entre 0 e 1 que diminui ao longo do tempo. Após essas atualizações, os nós na vizinhança de *j** estarão mais similares ao vetor de entradas $v_i(t)$.

- Rotular regiões no mapa: Após a etapa de treinamento, a cada saída atribui-se o maior peso como um termo de valoração, conhecido como “termo de vitória” (*winning term*). Todos os nós da vizinhança com o mesmo termo são agrupados em clusters, representando regiões conceitualmente próximas.

De acordo com Kohonen (2001), a estrutura básica da rede consiste em duas camadas de neurônios conectados pelos pesos. A camada de entrada é conectada a um vetor de entrada do conjunto de dados e a camada de saída forma um mapa que consiste de uma grade retangular onde são dispostos vários neurônios.

Pode-se dizer também (Suuronen, 2001) que os mapas auto-organizáveis são baseados em aprendizagem competitiva, ou seja, os neurônios de saída da rede competem entre si para serem ativados, sendo que somente um neurônio de saída ou um neurônio por grupo fica ativado em cada momento.

Destaca-se que numa *Konet* a aprendizagem não é supervisionada, o que implica na não obrigatoriedade de obter uma saída correta (ou o nó mapeado) para uma entrada. No processo de treinamento, o algoritmo não decide qual é a melhor opção que se aproxima de determinada entrada, pois simplesmente a encontra e ajusta os pesos, portanto, o resultado representa uma ordenação por quesitos de similaridade, onde o algoritmo, ao final do processo, não identifica um valor especifico, apenas apresenta uma lista ordenada.

Ao final do treinamento verifica-se que a localização dos neurônios vencedores está ordenada de tal forma, que um sistema de coordenadas é criado na grade, para diferentes características de entrada. A característica principal da rede é a formação de um mapa topográfico dos padrões de entrada, no qual as localizações espaciais (ou coordenadas) dos neurônios na grade são diretamente relacionadas aos padrões de entrada. A resposta a esse processo

competitivo de treinamento, ao final de uma iteração, é a localização do neurônio de entrada no mapa.

Num treinamento baseado em cerca de 2000 apresentações, cada área determinada do mapa torna-se responsável por uma das combinações de atributos de ocorrência e para um dos elementos de entrada. Se uma entrada cujo tipo já foi anteriormente mapeado for apresentada novamente à rede, no mapa de saída ela será posicionada na mesma região das anteriores. (Kohonen, 2001).

3.8.3.3.2 Aplicações

Vasconcelos (2001), mostra que a forma básica do modelo de Kohonen foi proposta em 1982. Versão atual foi exposta em 1997, onde se mantém o núcleo básico apenas acrescido de ampliações e variações.

Ainda segundo Vasconcelos (2000), Kohonen enfatiza a importância dos modelos de redes neurais, a disposição física dos neurônios e as relações entre vizinhanças dos neurônios no processamento da informação.

Com base na última versão, as redes *Self Organization Maps – SOM* são amplamente usadas como recurso estatístico para análise multivariada (Suuronen, 2001), pois convertem grandes e variados volumes de dados em proporções menores. Para tanto, esse tipo de rede é caracterizada pela facilidade em agrupar elementos. Por esse método, os dados similares são mapeados por neurônios próximos (Kohonen, 2001).

As redes, com esses atributos, podem ser aplicadas à mineração de dados, como meio para visualizar um rol de dados complexo. (Suuronen, 2001). Também é possível empregar em atividades de processamento digital de imagem, reconhecimento de voz, processamento de linguagem natural, controles de processos, análise de índices econômicos em bolsa de valores, diagnósticos gerais na área industrial, diagnósticos da área médica, assim como análises biomédicas em geral, as quais incluem reconhecimento de padrões de choro de bebês, reconhecimento de padrões de ondas cerebrais em pessoas com epilepsia, reconhecimento de padrões cerebrais em pesquisas relacionadas

a fases do sono. Neste tipo de aplicação, as linhas de gráfico de pulsos elétricos cerebrais mapeadas através de um eletro-encefalograma são digitalizadas e seus padrões são agrupados por semelhança para reconhecimento de estudos de padrões cerebrais em estado de vigília, assim como nos demais estágios do sono.

3.9 Análise de Clusters

Análise de Clusters é uma função útil na mineração de dados para descobrir grupos e identificar distribuições e padrões de dados. Pode ser entendido como um determinado conjunto de dados em grupos (Cluster), de tal forma que os elementos contidos em um cluster são mais semelhantes entre si, do que outros elementos de clusters diferentes (Guha *et al.*, 1998).

Para Hair et al (1998) é nome que se dá para ao grupo de técnicas que propõe o agrupamento de objetos baseados em características próprias. Portanto classifica objetos, onde cada objeto é similar aos demais existentes naquele cluster, respeitando critérios previamente definidos para a seleção. Então, temos que a situação interna do cluster é homogênea e a situação externa ao cluster é heterogênea.

Assim, a principal preocupação no processo de formação de clusters é revelar a organização de padrões em grupos "sensatos", que nos permitem descobrir semelhanças e diferenças, bem como obter conclusões úteis acerca dos clusters formados. Sua aplicação se expande por diversos domínios, tais como nas ciências biológicas, ciências da saúde e engenharia. Análise de cluster pode ser encontrada sob diferentes nomes e diferentes contextos, como a aprendizagem não supervisionada (padrão de reconhecimento), taxonomia numérica (biologia e ecologia), tipologia (ciências sociais) e a partição (gráfico em teoria) (Theodoridis e Koutroubas, 1999).

No processo de agrupamento, não existem classes predefinidas e tampouco exemplos que possam mostrar quais tipos de relações seriam válidas entre os dados, o que é compreendido como um processo não supervisionado (Berry e Linoff, 1996). Por outro lado, a classificação é um processo de atribuição de um item de dados a um conjunto de categorias predefinidas

(Fayyad *et al*., 1996). Portanto, a análise de clusters produz categorias iniciais e a classificação dos dados ocorre durante o processamento.

O processo de agrupamento pode resultar em diferentes partições de um conjunto de dados, que atendem ao critério previamente especificado. Desta forma, há necessidade de um pré-processamento antes da geração dos clusters. As principais etapas, para o desenvolvimento de clusters, encontram-se representadas na Figura 3-8 (Fayyad *et al*., 1996):

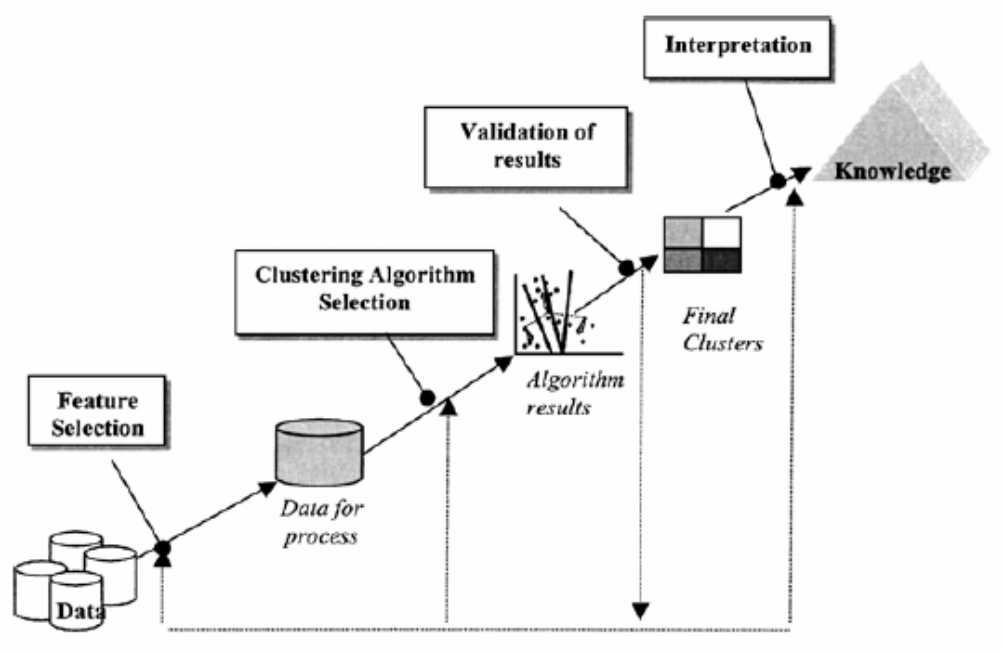

Figura 3-8: Etapas no Desenvolvimento de Clusters
Fonte: Fayyad et al. (1996)

O detalhamento dessas etapas encontra-se a seguir.

- Característica da seleção: o objetivo é selecionar adequadamente os recursos sobre os quais a agregação será realizada de modo a codificar o máximo de informações possíveis, relativa à missão de nosso interesse;
- Algoritmo do Clustering: esta etapa se refere à escolha de um algoritmo que resulte na definição de um esquema de agrupamento de dados, que apresente Medidas Aproximadas e Critérios de Agrupamento, que compreende:

    i) Medidas Aproximadas: quantifica a semelhança entre dois dados. Na maioria dos casos, temos que garantir que todos os recursos

selecionados contribuem igualmente para o cálculo da medida de proximidade;

ii) Critério de agrupamento: pode ser expresso através de uma função de custo ou algum outro tipo de regra. Deve-se levar em conta o tipo de agrupamento que se espera para definir um critério de agrupamento.

Hair *et al*. (1998) sugere adicionalmente que o algoritmo compare simultaneamente as duas variáveis ou grupos, através da correlação entre os objetos ou pela medida de aproximação do espaço bidimensional para cada distância entre as indicações de similaridade.

- A validação dos resultados: a precisão do resultado do algoritmo de agrupamento é verificada por critérios e técnicas adequadas. Algoritmos de agrupamento definem os clusters que a priori não são conhecidos, independentemente dos métodos de agrupamento, a partição final dos dados requer algum tipo de avaliação na maioria das aplicações (Rezaee *et al*., 1998);
- Interpretação dos resultados: Em muitos casos, os especialistas na área devem integrar os resultados do agrupamento com outras evidências experimentais e análise, a fim de obter uma conclusão mais apurada.

Análise de cluster ou Clustering é um importante instrumento em uma série de aplicações em diversas áreas de negócios e ciência. A seguir, encontra-se um resumo das orientações básicas, onde a análise de cluster é aplicada (Theodoridis e Koutroubas, 1999):

- Compressão de dados: em vários casos, a quantidade de dados disponíveis é muito grande e há elevada demanda de processamento. Clustering pode ser utilizado para particionar um conjunto de dados em uma quantidade interessante de clusters. Uma vez que o processamento de dados foi definido como uma entidade, foram adotadas as definições de clusters representativas nesses processos;
- Hipótese geração: é utilizada, a fim de inferir algumas hipóteses relativas aos dados. Por exemplo, podemos encontrar uma variedade de dados com dois

significativos grupos de clientes com base em sua idade e no tempo gasto em compras. Com isso, é possível inferir algumas hipóteses para os dados, tais como "os jovens compram a noite", "velhos compram de manhã";

- Hipótese de testes: é utilizado para a verificação da validade de uma hipótese. Por exemplo, considerando a hipótese: "Os jovens vão comprar à noite". A verificação de sua autenticidade pode ser efetuada pela análise de cluster de um conjunto de lojas, onde cada loja é representada pelos detalhes do cliente (idade, emprego etc) e os prazos das operações. Pela análise de cluster, teria-se a formação de um cluster "jovens que compram durante a noite". Dessa forma, a hipótese é apoiada através da análise de cluster;
- Previsão: é aplicada ao conjunto de dados e aos agrupamentos que são caracterizados pelos tipos de padrões que pertencem a estes grupos.

Padrões desconhecidos podem ser classificados em clusters específicos com base na similaridade de suas características, com isso obtém-se o conhecimento relacionado aos dados extraídos. Por exemplo, a análise de cluster é aplicada a um conjunto de dados de doentes infectados pela mesma doença. O resultado é uma série de grupos de pacientes, de acordo com a reação às drogas específicas. Um novo paciente classificado em um determinado cluster terá automaticamente definida a sua medicação.

Ao formar os grupos homogêneos, a pesquisa no campo acadêmico poderá alcançar três objetivos (Hair et al., 1998):

- Descrição da taxonomia: a mais tradicional utilização de análise de clusters tem sido a proposta de exploração e formação de taxonomia (base empírica para a classificação de objetos). Pode também gerar hipóteses relacionadas às estruturas dos objetos. Em face de sua visão técnica-exploratória, pode ser usada para confirmar as propostas. Se a estrutura proposta pode ser definida para os objetos, a análise de cluster pode ser aplicada a uma tipologia (Classificação baseada em teoria);
- Simplificação de dados: derivada da taxonomia simplifica a perspectiva das observações. Com a definição da estrutura, as observações podem ser

agrupadas o que favorece a análise dos dados. Considerando as “dimensões” ou estrutura das variáveis, a análise de clusters pode realizar a mesma tarefa. Ao invés de uma visão geral, obtém-se uma única visão, permitindo ver todos os elementos de cada cluster e relacionar suas características gerais;

- Identificação dos relacionamentos: definidos os clusters e as respectivas estruturas de dados, é possível revelar o relacionamento entre as observações. A simplificação da estrutura por meio de análise de clusters pode retratar relacionamentos ou similaridades e diferenças não reveladas previamente.

De forma abrangente, algumas aplicações típicas do agrupamento estão nos seguintes campos:

- Negócios: o agrupamento pode ajudar aos profissionais de marketing a descobrir grupos significativos nas suas bases de clientes, caracterizados pelo padrão de compras;
- Biologia: ela pode ser usada para categorizar genes com semelhante funcionalidade e obter conhecimentos em estruturas inerentes às populações;
- Análise de Dados Espaciais: devido à grande quantidade de dados espaciais que podem ser obtidos a partir de imagens por satélite, equipamentos médicos, Sistemas de Informação Geográfica (GIS) etc, é caro e difícil para os usuários examinar os dados espaciais em detalhe. A análise de clusters ajuda a automatizar o processo de análise e compreensão dos dados espaciais. Ele é usado para identificar e extrair características interessantes e padrões que podem existir em grandes bases espaciais;
- Mineração da Web: é usada para descobrir grupos significativos de documentos na Web para auxiliar a descoberta de informações.

Em termos gerais, o agrupamento pode servir como um pré-requisito para o processamento de outros algoritmos, tais como a classificação, que posteriormente podem identificar novos clusters.

Há uma variedade de métodos de clustering propostos, os quais podem ser classificados em: Tipo de dados utilizados como entrada do algoritmo; Critério de similaridade entre dois pontos definidos para o clustering e; Teoria e conceito fundamental para o embasamento da análise de cluster.

CAPÍTULO 4 - PROPOSTA DE UM MÉTODO PARA CLASSIFICAR AS INFORMAÇÕES

Em que pese os ativos se concentrarem no conhecimento e nas informações, num cenário em que as corporações se encontram em ascendente dependência da infra-estrutura computacional e dos sistemas de informação, os investimentos em controle e segurança ainda são imprecisos e criam situações que expõem estes ativos às ameaças crescentes e evolutivas, motivadas por agentes cada vez mais preparados e focados. Por esse motivo, este estudo visa à assertiva proteção dos ativos através da diferenciação daqueles de maior relevância, especificamente representados por dados e informações.

O ponto de partida das metodologias, estruturas de trabalho ou padrões internacionais voltados à segurança das informações destacam a importância da classificação, de maneira que sejam revestidas de maior controle e proteção aquelas informações relevantes aos interesses da organização proprietária dos dados. Conseqüentemente a proteção será decrescente até alcançar as informações de menor importância.

Os levantamentos realizados em artigos acadêmicos e algumas organizações brasileiras, não identificaram dispositivos destinados a classificar as informações com base em rotinas automáticas, uniformes e evolutivas. Atualmente, os procedimentos aplicados à classificação das informações são subjetivos e manuais, e não asseguram sua uniformidade e eficácia. Esta imprecisão encarece os custos de segurança e, expõem os ativos a ameaças diversas.

4.1 Escolha do Objetivo de Segurança e Macro Visão do Método

Em face deste panorama, este trabalho se propõe a desenvolver um método destinado a classificação das informações, que pode ser norteado pelos três objetivos de segurança citados anteriormente (integridade, confidencialidade e disponibilidade).

Entretanto, apenas um objetivo de segurança será utilizado neste estudo, cuja seleção buscou atender aquele que requer uma clara definição de similaridade entre os elementos de um mesmo grupo e, acentuadas diferenças entre os diversos grupos.

Com isso, temos que a Integridade é requisito fundamental para todos, ou pelo menos a maioria dos dados e informações processados, armazenados e transmitidos num ambiente computacional, portanto as diferenças entre os possíveis grupos a serem criados, quanto a integridade, são sutis e reduzidas. Embora em menor proporção, as diferenças entre os possíveis grupos a serem criados quanto ao requerimento de Disponibilidade, ainda não seriam tão relevantes, assim, este objetivo de segurança também não será tratado neste estudo.

O objetivo de segurança de maior variação entre os possíveis grupos a serem tratados é o da Confidencialidade, pois entre a informação que apresenta o maior nível de sigilo e aquela que possui a obrigatoriedade legal de ser pública, podem ser criados diversos grupos com atributos de acentuadas diferenças. Portanto, o método para classificar as informações será desenvolvido para tratar a Confidencialidade.

A visão panorâmica da metodologia proposta está apresentada na Figura 4-1 (próprio autor). O detalhamento das etapas será descrito ao longo deste capítulo.

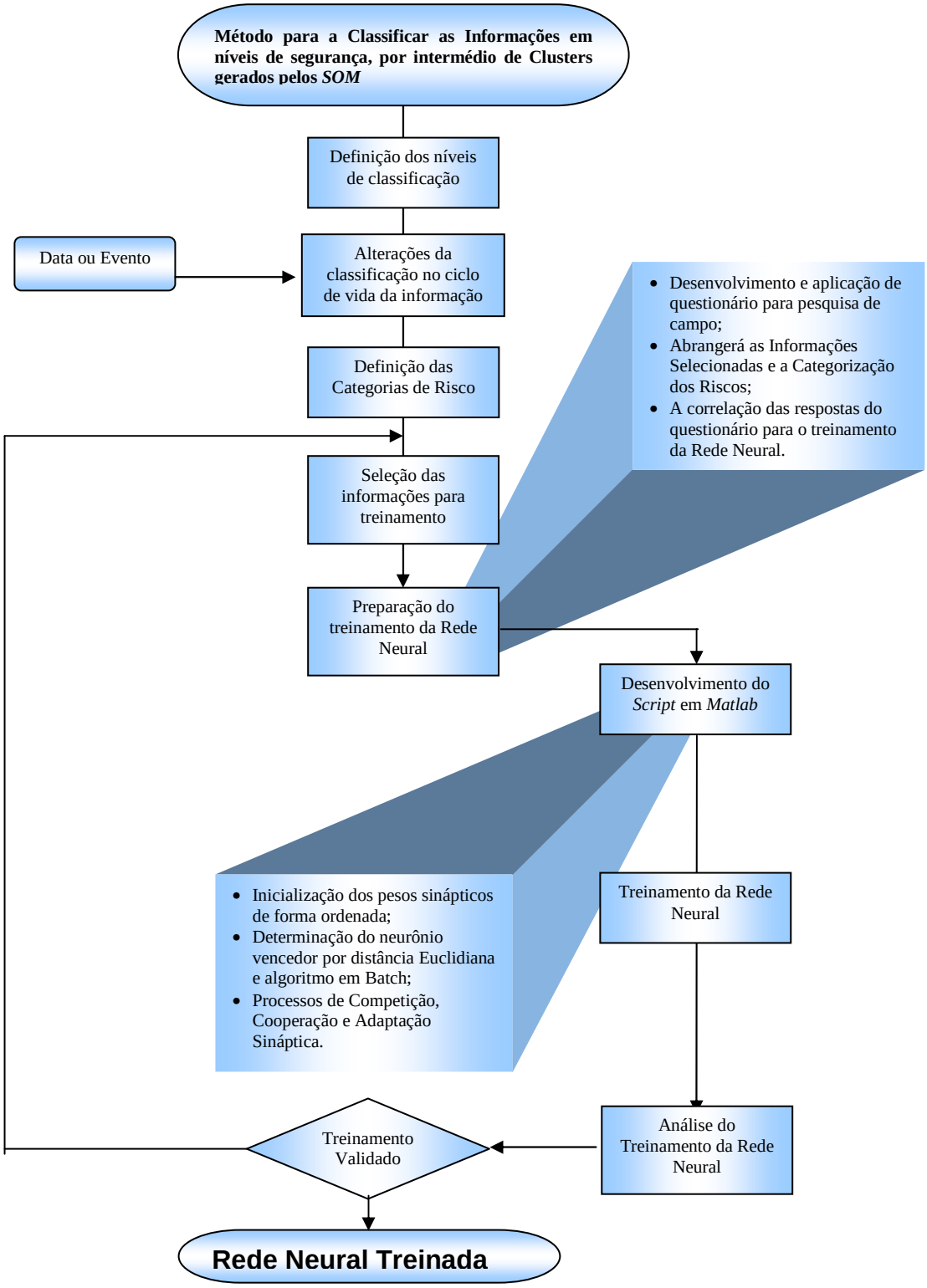

Figura 4-1: Etapas do Método de Classificação de Informações

4.2 Conceito, Regras e Critérios para Classificar as Informações

A classificação das informações visa atender a maioria dos requisitos descritos nas estruturas de trabalho e padrões internacionais citados neste estudo. Os principais processos foram baseados na “Ordem Executiva” No. 12.958 – Classificação das Informações de Segurança Nacional, do Departamento de Defesa dos Estados Unidos da América, cuja emissão foi de responsabilidade do presidente Clinton em abril de 1995 (*Department of Justice USA;* 2005). Esta ordem descreveu um sistema uniforme para classificar e proteger informações relativas à segurança do país, proteger os cidadãos, as instituições democráticas e a participação na comunidade das nações.

Os critérios identificados consideraram a abordagem do *National Institute of Standards and Techonology* (2000 e 2002) e também observando os padrões recomendados pela norma ISO/IEC NBR 17799, que trata especificamente aspectos de segurança da informação.

4.2.1 Requisitos da Informação para a Classificação

Os padrões de classificação devem atender a requisitos da importância de cada informação norteado pelas possíveis conseqüências ou risco associado na hipótese de ocorrer o acesso por indivíduo ou grupos de pessoas não autorizados. Por conseguinte, as informações a serem classificadas devem atender aos seguintes requisitos:

- A informação deve pertencer à própria entidade ou tenha sido produzida sob sua responsabilidade ou, seja destinada para sua utilização;
- A informação pode fazer parte ou apresentar relevância equivalente a uma ou mais Categorias de Risco, descritas em tópico especifico.

4.2.2 Níveis da Classificação

A classificação da informação deverá atender ao nível de confidencialidade requerido por suas características e do contexto ao qual está inserida. Este método fundamentou-se nas possíveis conseqüências da

exposição de cada informação a ameaças internas ou externas. Dessa maneira foram criados três níveis de confidencialidade, conforme descritos a seguir:

- “Altamente Secreta” será aplicado à informação, cuja divulgação desautorizada pode causar danos excepcionalmente graves à segurança;
- “Secreta” será aplicado à informação, cuja divulgação desautorizada pode causar danos à segurança;
- “Interna” será aplicado à informação, cuja divulgação desautorizada pode causar danos administráveis pelo gerenciamento de risco.

4.2.3 Duração da Classificação

O dinamismo de mudanças observado no fluxo dos sistemas de informação é refletido na necessidade de ajustar à preservação do sigilo. Há circunstâncias que justificam alterações sobre a classificação original da informação ou sua atribuição dos níveis de confidencialidade.

Poderá existir uma data ou um evento específico que determine a re-classificação da informação. Exemplo, a publicação das Demonstrações Financeiras de uma empresa de capital aberto, cujo nível de confidencialidade é o mais alto até à véspera de sua publicação, entretanto a partir dessa data torna-se uma informação pública.

Embora a informação possa ser re-classificada quanto à demanda por confidencialidade no seu ciclo de vida, as alterações ou re-classificações não serão contempladas diretamente neste método.

Contudo, a perspectiva de uma re-classificação, quanto a Confidencialidade da informação, será indispensável para a atribuição dos pesos destinados ao treinamento da rede neural, pois contemplar esta perspectiva deverá elevar o valor do referido peso, devido à necessidade de optar pelo maior nível de impacto decorrente da exposição indevida daquela informação. Esta orientação será repassada aos profissionais que imputarão os pesos iniciais.

4.3 Categorias de Risco

As Categorias de Risco representam as circunstâncias em que dados ou informações estão sujeitos às ameaças e denota uma perspectiva de risco, o que compreende a possibilidade de materialização e os impactos motivados pela divulgação não autorizada das informações. Abrange os impactos legais, operacionais, financeiros ou de propriedade intelectual.

As Categorias de Risco foram baseadas na Classificação dos Riscos Operacionais sugeridos pelo *Bank International of Settlements*, que auxiliou a elaboração dos riscos decorrentes de falhas de controle no ambiente computacional, que causam impacto nas atividades de negócio. Esta mesma abordagem relativa à importância das atividades primárias (de negócio) é apresentada pelo *National Institute Standards and Technology* na descrição do Risco Técnico, onde destaca a necessidade da integração do risco técnico (infra-estrutura de TI) e do risco de negócio.

As etapas destinadas à categorização dos riscos, quanto a Confidencialidade das informações, foram subsidiados pelo modelo desenvolvido pelo *US Department of Justice*, cujo principal objetivo é prover a proteção das informações do governo federal e, por conseguinte, proteger o cidadão americano. Também foram aplicadas, no desenvolvimento do modelo proposto, as diretrizes do *National Institute Standards and Technology* e do *International Organization for Standardization* e *International Electrotechnical Commission*.

As definições das Categorias de Risco, que direcionam a formulação deste método, estão vinculadas aos estudos do gerenciamento de riscos, dos impactos, ameaças e vulnerabilidades. Assim, a formulação de um quadro destinado a auxiliar na definição das Categorias de Risco, foi originada pela integração dos seguintes quadros: Quadro 2-6, Fatores de Risco e Eventos de Perda (Adaptado pelo autor *BIS*, 2001); Quadro 2-7: Descrição dos Tipos de Eventos de Risco Operacional (Adaptado pelo autor *BIS*, 2001); Quadro 2-10: Ameaças Humanas: Origem, Motivação e Ações (Adaptado do *NIST*, 2002) e

Quadro 2-11: Vulnerabilidades e Ameaças (Adaptado do *NIST*, 2002). Esta consolidação originou o Quadro 4-1.

Quadro 4-1: Definição das Categorias de Risco

Objetivo da Ameaça	Motivação	Fatores de Vulnerabilidade	Ações	Categoria de evento	Definição da Categoria
Hacker e Cracker	Desafio Ego Rebelião	• Pessoas	Hacking Engenharia social Quebra dos sistemas de proteção de Intrusões Acesso desautorizado aos sistemas	• Fraudes internas (vide Quadro 2-11 Vulnerabilidades e Ameaças)	• Perdas devidas a atos com intenção de defraudar a instituição, violar regulamentos, a lei ou política interna (exclui discriminação), que envolvam ao menos uma parte interna.
Crime computacional	Destruição da informação Divulgação ilegal da informação Ganho financeiro Alteração ilegal de dados		Crime computacional Ato fraudulento Suborno Trapaça Sistema de intrusão	• Fraude externa	• Perdas devidas a atos com a intenção de defraudar a instituição, violar regulamentos, lei ou política interna (exclui discriminação), que sejam cometidos por uma terceira parte.
Terrorismo	Blackmail Destruição Explosão Vingança	• Sistemas	Bombas terroristas Informações de guerra Ataque aos sistemas de informação Sistemas de falsificação	• Práticas empregatícias e segurança no ambiente de trabalho	• Perdas devidas a atos inconsistentes com as condições empregatícias. Violações de acordos sanitários ou de segurança trabalhista ou perdas com danos de acidentes de trabalho ou de ações de discriminação de qualquer tipo (inclui assédio sexual).
Espionagem industrial (empresas, governos etc.)	Vantagem competitiva Espionagem econômica	• Processos	Exploração econômica Roubo de informação Intrusão à privacidade pessoal Engenharia social Penetração nos sistemas Acesso não autorizado aos sistemas	• Clientes, produtos e práticas de negócio	• Perdas oriundas de falhas em cumprir obrigações com clientes ou perdas por causa de desenhos/estruturas de produtos.
Ações internas (treinamento insuficiente, descontentamento, maldade, negligência, desonestidade ou funcionários demissionários)	Curiosidade Ego Inteligência Ganho monetário Vingança Eros não intencionais e omissões (erros de sistemas e falhas de infra-estrutura)	• Eventos Externos	Assalto ou ataque por funcionários *Blackmail* Pesquisa sobre a propriedade das informações *Abuse computer* Fraude e roubo Suborno Input de informações falsas ou corrompidas Interceptação Códigos maliciosos Venda de informações pessoais Erros de sistemas Intrusão nos sistemas Sabotagem nos sistemas Acesso não autorizado aos sistemas	• Danos a ativos físicos • Interrupção de negócios e falhas nos sistemas • Execução, entrega e gestão de processos	• Perdas oriundas de danos a ativos físicos. • Perdas devidas a qualquer interrupção do negócio ou falhas em sistemas • Perdas oriundas de falha no processamento de transações, ou gestão de processos, de relações com parceiros comerciais e vendors.

Fonte: Adaptado do BIS - sombreado (2001) e NIST (2002)

A composição dos sistemas de informação e dos fluxos dos processos que interagem com as entidades, representa com relativa clareza os eventos de maior importância, as possíveis vulnerabilidades e ameaças mencionadas no Quadro 2-11 ou destas derivadas. Este panorama permite observar os riscos associados à atividade objeto de análise, o que direciona a produção das Categorias de Risco.

4.4 Escolha da Técnica Adaptativa e o Treinamento da Rede Neural

Após o entendimento do problema e sua contextualização, iniciou-se o estudo de alternativas de Redes Neurais de Inteligência Artificial com foco no desenvolvimento do modelo destinado à formação de clusters, que representam os três níveis relativos ao objetivo de segurança Confidencialidade (Altamente Secreta, Secreta e Interna), definidos pela similaridade de suas características.

A escolha da técnica adaptativa de rede neural destinada à implementação do modelo envolveu o estudo das Redes Bayesianas, Sistemas Especialistas e os Mapas Auto-Organizáveis de Kohonen (*SOM*).

O *SOM* de Kohonen foi à técnica selecionada em razão de não demandar conhecimento prévio para sua execução e tampouco requerer a intervenção ou acompanhamento de profissionais, uma vez que se trata de aprendizado não supervisionado. Porém, o principal motivo de sua escolha recaiu pela sua especialidade na formação de clusters, ou agrupamento, principal objetivo deste estudo.

O próximo passo é a seleção de um grupo de informações para proceder ao treinamento da rede neural. Este grupo deve ser representativo, de maneira que alcance o maior número de produtos, processos, atividades e entidades envolvidas.

Por isso a composição dessas informações necessita identificar as rotinas e atividades de maior importância, o que pode ser produzido com base nos fluxos operacionais e das informações. Complementarmente, as entidades que são representativas na geração, no tratamento ou na utilização das informações (funcionários, clientes, acionistas, governo etc.), são inseridas

na análise que definirá a composição das informações destinadas ao treinamento da rede neural.

Uma vez que as Categorias de Risco e as Informações para o treinamento da rede neural foram estabelecidas, a compreensão e absorção do conhecimento e da experiência dos profissionais que desempenham atividades de controle, segurança, qualidade ou afins, se dará por intermédio da correlação entre as Categorias de Risco e as Informações.

A correlação será obtida através do preenchimento de uma tabela, onde as Informações se encontram nas linhas e as Categorias de Risco nas colunas.

- Cada informação será associada a todas as Categorias de Riscos, subtendendo-se que, hipoteticamente, tenha ocorrido à divulgação indevida da informação. As categorias de riscos representam as respectivas conseqüências ou impactos;
- Existe a possibilidade que algumas informações apresentem mais de um tipo de requerimento de segurança, dependendo do estágio que a informação esteja situada no respectivo ciclo de vida. A alteração do requerimento de segurança é conduzida por um evento ou prazo pré-estabelecido. Neste caso, será considerada a perspectiva que apresentar maior exposição ao risco e, portanto as conseqüências de maior severidade. Exemplos, as informações sobre as demonstrações financeiras de uma empresa de capital aberto, antes da publicação obrigatória do balanço demandam sigilo, pois o impacto de um acesso indevido seria alto, entretanto, após sua publicação tornam-se acessíveis por todos. Assim, a correlação deverá considerar o mais alto nível de impacto requerido para as demonstrações financeiras, portanto, anterior à sua divulgação;
- A representação do nível de impacto, a ser preenchido na planilha de correlação, será dada pela atribuição de valores inteiros, entre zero e dez, onde os maiores valores representam o maior impacto e decresce até o menor impacto reproduzido pelo valor zero;
- Sugere-se que o preenchimento seja realizado de maneira que cada Informação seja correlacionada com todas as Categorias de Risco;

- Uma vez que a planilha foi preenchida por diversos profissionais, os dados serão consolidados em uma única versão através da média aritmética simples. Este resultado representará os dados de entrada para o treinamento da rede neural.

Em face de a solução optar pelo desenvolvimento de uma Rede Neural não supervisionada, especificamente a Rede de Kohonen – *SOM*, para a classificação das informações, levou a considerar a recomendação do próprio autor (Kohonen, 2001), que indica o uso de softwares para Mapas Auto-Organizáveis que tenham sido submetidos à ampla quantidade de testes com a finalidade de obter maior segurança dos resultados, por considerar que a Rede Neural *SOM* não produz um resultado único, a exemplo dos algoritmos matemáticos determinísticos. Por esses motivos, o software escolhido para o treinamento da Rede Neural foi o *Matlab* versão 6.5 e como recurso auxiliar para o processamento de algumas funções e para a visualização dos resultados empregou-se *SOM Toolbox for Matlab 6.5*.

O software *Matlab* foi desenvolvido pela MathWorks Inc., constitui um ambiente de programação destinado à computação técnica e possui versões para diferentes sistemas operacionais, inclusive MS Windows que foi usada para efeito deste experimento. As principais características deste recurso são a linguagem de alto nível e um ambiente interativo para o desenvolvimento de algoritmos, visualização e análise de dados, voltados para a computação numérica. Tais características se destinam a uma diversidade de aplicações, dentre as quais se destacam o processamento de sinais e imagem, comunicação, controles, testes e medidas, modelo financeiro e biologia computacional.

As funcionalidades do *Matlab* 6.5 são ampliadas pelos recursos do *SOM Toolbox*. Dentre outros, possibilita resolver classes de problemas particulares em diversas áreas. Para os Mapas Auto-Organizáveis, o *SOM Toolbox* auxilia o pré-processamento das informações de entrada, na geração inicial dos dados, no treinamento da rede (utilizando diversas topologias), na visualização e na análise das propriedades e das informações dos Mapas Auto-Organizáveis (Vesanto *et al*., 2000). Estes dispositivos encontram-se disponíveis na Internet pelo *Department of Computer Science and* Engineering

da *Helsinki University of Technology* através da licença GNU (*General Public License*).

Na visão estrutural, a utilização foi separada em quatro etapas (Vesanto *et al*., 2000):

- Leitura dos dados de entrada: a formatação das informações a serem tratadas pela Rede Neural é concentrada em uma tabela, composta pela amostra das Informações (linha) relacionadas com as Categorias de Risco estabelecidas (coluna). Este conjunto de informações é carregado para o *Matlab* através de comandos do *SOM Toolbox*;
- Pré-processamento dos dados: significa a preparação das informações para o processamento, onde são normalizadas. O algoritmo para Mapas Auto-Organizáveis utiliza a métrica Euclidiana Quadrática para medir a distância entre vetores, o que necessário para utilizar o software *Matlab*, uma vez que o espaço entre as variáveis deve atender a uma mesma base de referência, assim prevalece a equidade de unidade entre as variáveis;
- Inicialização e Treinamento: São utilizados dois algoritmos para inicializar os dados (randômica e linear) e dois de treinamento (seqüencial e lote) utilizados pelo *Matlab*. Assim, o treinamento é feito em duas etapas. Na primeira é realizada com um raio de vizinhança e taxa de aprendizagem relativamente maiores do que os valores utilizados na segunda fase;
- Visualização e Análise: existem várias funções para visualização do Mapa Auto-Organizável. Estas estão divididas em:
    - Visualização de células ou hexágonos: que demonstra o estado de saída do reticulado;
    - Visualização de gráficos: que demonstra um reticulado com gráficos simples em cada unidade do mapa.

Na fase do treinamento, a avaliação dos resultados alcançados auxilia a estabelecer a quantidade de épocas, ou quantidade de treinamentos da rede neural, necessários para atingir um patamar confiável da classificação das informações obtida. Observa-se que a quantidade de épocas para o

treinamento está adequado à medida que a variação dos resultados torna-se imperceptível ao aumento da quantidade de épocas.

A primeira etapa refere-se à leitura dos dados de entrada contidos em uma tabela. Para tanto, esta tabela de entrada foi constituída da seguinte forma:

- Parâmetros de contextualização: serão relacionadas às informações selecionadas para o experimento que compõe o domínio de algumas atividades;
- Parâmetros de avaliação: enumeração das Categorias de Risco relacionadas às características das atividades que compõe o contexto das Informações que serão submetidas ao treinamento da rede.

O produto alcançado pelo processamento obtido do *Matlab SOM Toolbox*, permitirá visualizar os agrupamentos das informações em clusters.

A primeira análise dos resultados é visual e permite identificar os clusters gerados no processo de treinamento da rede neural. A título ilustrativo, as Figuras 4-2 e 4-3 apresentam um resultado hipotético de um treinamento.

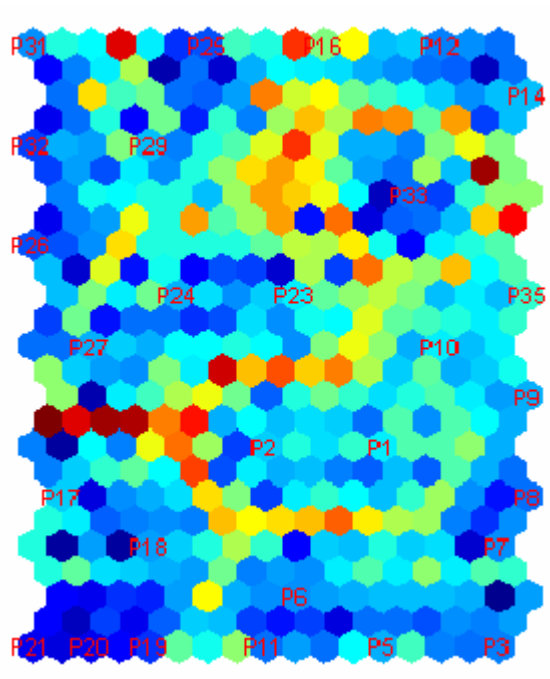

Figura 4-2: Produto Inicial

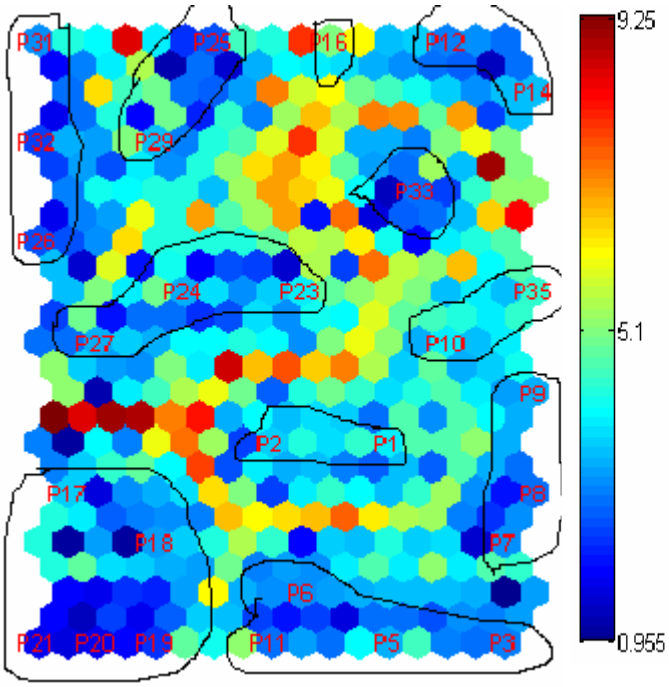

Figura 4-3: Produto Agrupado e Escala

Na Figura 4-2 está representado o produto bruto do treinamento obtido pelo processamento do software *Matlab*, com a utilização do recurso *SOM Toolbox* denominado U-Matriz que auxilia a apresentação visual dos resultados, bem como sua compreensão através da geração dos *Labels*.

Nesta figura observa-se a formação dos clusters por agrupamento físico, ou proximidade, dos elementos de informação representados pela letra "P" adicionada ao número de sua posição na tabela. Contudo, a distância euclidiana está configurada pelas cores de cada hexágono, cuja ordem de grandeza está representada na escala da Figura 4-3.

Portanto, as células ou hexágonos de coloração de maior proximidade ao vermelho, significam as maiores distâncias Euclidianas. Neste caso, torna-se significativo o agrupamento por proximidade e também identifica as grandes lacunas diferenciadas pelas cores próximas ao vermelho. No exemplo, foram delimitados onze grupos, conforme apresentados na Figura 4-3.

Neste exemplo, ainda há informações que não se encontram relacionadas nas Figuras 4-2 e 4-3. Deve-se ao agrupamento de algumas informações na mesma célula ou hexágono, o que inviabilizaria sua apresentação gráfica. Para tanto, o Quadro 4-2 mostra as informações que se encontram desta condição.

Quadro 4-2: Informações Agrupadas

Número do Hexágono	Informação Apresentada	Informação Agrupada
5	P26	P28
13	P21	P22
40	P25	P30
82	P33	P34
92	P12	P13
106	P14	P15
117	P3	P4

Fonte: O próprio autor

Após a identificação dos clusters gerados por similaridade dos elementos que compõem as Categorias de Risco, inicia-se a análise quantitativa, com o objetivo de proceder à distribuição dos clusters de informações gerados em três novos grupos, que representarão os três níveis do objetivo de segurança de Confidencialidade dessas informações, ou seja, Altamente Secreta, Secreta e Interna.

O objetivo do treinamento por intermédio de redes neurais de inteligência artificial é agrupar as informações de maior similaridade quanto à potencialidade de impacto ou risco. A próxima etapa tem por finalidade detalhar a análise numérica dos pesos fornecidos pelos profissionais de maior conhecimento dos aspectos de segurança, de forma que permita delimitar os clusters criados nos três níveis de Confidencialidade.

A análise numérica considerará, para cada cluster gerado, a média dos pesos atribuídos aos seus componentes (informações). Após o cálculo das médias, os clusters serão relacionados em ordem decrescente. As maiores médias representam o grupo de informações que demandam maior proteção quanto ao sigilo.

Contudo a atribuição do nível “Altamente Secreta” requer ao menos a pontuação média equivalente a cinco. Embora o valor cinco tenha considerado a média do intervalo de pesos que foram atribuídos, não apresenta fundamentação técnica, portanto, está sujeito a alterações evolutivas à medida que o método seja utilizado.

CAPÍTULO 5 - ESTUDO DE CASO PARA INFORMAÇÕES ACADÊMICAS

Neste Capítulo, o Estudo de Caso visa representar a aplicação do método descrito no Capítulo 4 em um segmento de atividade que contemple características diversificadas em seus processos e atividades e, preferencialmente, não apresente estruturas pré-estabelecidas de segurança, como seriam as empresas que atuam em segmentos de reconhecida exposição ao risco de ameaças perenes, tais como a indústria financeira.

As universidades contemplam todas as atribuições de cunho administrativo, corriqueiras em todo tipo de corporação, e também as atividades pedagógicas e de pesquisa. Em razão dessas particularidades e do perfil de seu público, as características de risco e dos impactos são diferenciados. Além disso, as universidades atendem a legislações específicas emanadas do Ministério da Educação e outras regulamentações voltadas à pesquisa cientifica. Esta diversidade de situações consolidou a escolha das informações do ambiente acadêmico para a implementação do método de classificação das informações, quanto à preservação da confidencialidade nos sistemas de informação e no ambiente computacional das universidades.

A condução e o exercício da pesquisa cientifica representa uma responsabilidade significativa no papel das universidades, pois demanda a compreensão dos novos e representativos elementos de risco, para alcançar a eficácia do gerenciamento de risco tecnológico, mencionado no Capítulo 2, deve considerar a elevada capacidade computacional existente nos centros de pesquisa.

Adicionalmente, o vínculo cooperativo entre os centros universitários, as corporações e a sociedade de forma geral, que caracterizou e incrementou o processo evolutivo vivido nas últimas décadas, poderia associar-se às ações ilícitas, servindo ao intento terrorista ou à expansão do crime organizado, através da disponibilidade, involuntária, de sua infra-estrutura computacional ou de suas informações.

Uma vez escolhido o ambiente universitário, inicia-se o levantamento das principais rotinas, fluxos da informação e atuação dos principais agentes (funcionários, clientes, acionistas, governo etc.) para identificar as Categorias de Risco e o grupo de Informações destinadas ao treinamento da rede neural. Essas informações devem ser representativas, de maneira que alcance o maior número de produtos, processos, atividades e agentes envolvidos.

Desde o início da década de 60, se observam registros de incidentes de segurança nas instalações dos centros de processamento de dados das universidades, que configuraram expressivos prejuízos de ordem material e financeira.

Porém, o novo cenário tecnológico também passou a demonstrar perdas relacionadas com as informações e o conhecimento, por meio de ocorrências que envolveram trabalhos de pesquisa cientifica e o fluxo de informações próprias das universidades.

5.1 Categorização dos Riscos das Universidades

As Categorias de Risco representam as circunstâncias em que dados ou informações estão sujeitos à ameaça, eventualmente materializada, de sua divulgação não autorizada. Para efeito deste Estudo de Caso, o impacto apresentado está relacionado ao objetivo de segurança da Confidencialidade e abrange os impactos legais, operacionais, financeiros ou de propriedade intelectual.

As principais referências para a definição das Categorias de Risco deste Estudo de Caso foram a Classificação dos Riscos Operacionais sugeridos pelo *Bank International of Settlements*, que auxiliou na elaboração dos riscos, decorrentes de falhas de controle no ambiente computacional, que causam impacto nas atividades de negócio. Abordagem complementar foi extraída dos estudos realizados pelo *National Institute Standards and Technology* na descrição do Risco Técnico, onde destaca a necessidade de integrar o risco essencialmente técnico (infra-estrutura de TI) e o risco de negócio. A consolidação dessas visões de risco encontra-se no Quadro 4-1 e

serviu para nortear a composição das Categorias de Risco relativas às informações das universidades.

As particularidades dos processos inerentes às funções pedagógicas e de pesquisa foram obtidas através da análise sobre a documentação que registra os procedimentos das universidades requeridos pelo padrão ISO 9000, disponibilizados pela entidade de ensino Instituto Paulista de Ensino e Pesquisa. A este trabalho, foi acrescida a indagação realizada junto a alguns professores e coordenadores de curso.

Considerando os principais agentes participantes que podem expor-se aos riscos característicos do ambiente acadêmico, foram criadas 28 Categorias de Risco, apresentadas no Quadro 5-1.

Quadro 5-1: Categorias de Risco

	Categorias de Risco (Coluna)
1	Causaria impacto à segurança ou controle da Universidade
2	Causaria impacto na especificação de dispositivos de segurança
3	Causaria impacto à propriedade intelectual
4	Serve para transgressão legal
5	Serve para transgressão da ordem social
6	Serve para transgressão da integridade de pessoas
7	Serve para transgressão normativa
8	Serve para lesar a instituição ou o acionista
9	Serve para lesar o aluno
10	Serve para lesar os fornecedores
11	Serve para lesar Órgão regulador/fiscalizador
12	Causaria impacto operacional ao aluno
13	Causaria impacto operacional ao professor
14	Causaria impacto operacional ao funcionário
15	Causaria impacto operacional à universidade
16	Causaria impacto financeiro para o aluno
17	Causaria impacto financeiro para o professor
18	Causaria impacto financeiro para o funcionário
19	Causaria impacto financeiro para a universidade
20	Causaria impacto legal para o aluno
21	Causaria impacto legal para o professor
22	Causaria impacto legal para o funcionário
23	Causaria impacto legal para a administração da universidade
24	Causaria impacto na infra-estrutura de TI da universidade
25	Causaria impacto no plano estratégico da universidade
26	Causaria impacto no plano acadêmico de pesquisa
27	Causaria impacto no plano pedagógico
28	Causaria impacto à imagem institucional da universidade

Fonte: O próprio autor

Estas Categorias de Risco são associadas a cada informação escolhida para o treinamento da rede neural. Esta associação visa atender a uma pergunta implícita sobre o impacto da divulgação não autorizada, daquela informação, frente à determinada Categoria de Risco.

A categorização dos riscos abrangeu os principais agentes, os riscos operacionais ocasionados por falhas dos sistemas de informação, da infra-estrutura ou procedimentos operacionais. Os riscos legais atendem à pluralidade de Órgãos do Ministério da Justiça, do Ministério da Educação e Cultura etc.

As questões de cunho estratégico, tais como plano estratégico, a imagem institucional e infra-estrutura de TI também compuseram a categorização utilizada, assim como as eventuais ameaças que possam afetar a sociedade.

5.2 Seleção das Informações destinadas a Aplicação do Estudo de Caso

Inicialmente determinaram-se os principais agentes que interagem no âmbito da segurança das informações, são os professores, alunos, administradores, fornecedores, comunidade local e o acionista.

De forma semelhante à composição da Categorização dos Riscos, a Seleção das Informações para o treinamento da rede neural, necessitou vislumbrar o entendimento das atividades cotidianas de uma universidade, dividi-las em grupos de afinidade e, em cada grupo, relacionar aquelas que sejam mais representativas, de maneira que alcancem o maior número de produtos, processos, atividades e agentes envolvidos.

Para tanto, também se buscou o entendimento de alguns fluxos operacionais por onde transitam e são armazenadas as informações de maior importância e são objetos de proteção por diversos recursos de segurança.

O conhecimento necessário foi obtido por meio da análise da documentação que registra os principais processos no padrão ISO 9000 da entidade de ensino Instituto de Paulista de Ensino e Pesquisa. Outros dados acadêmicos foram extraídos da Plataforma Lattes (Plataforma Lattes, 2007), apresentada, de forma ampla, no Quadro 5-2.

Quadro 5-2: Grupos de Atividades e Informações

	Grupo de Atividade e Informação	Informação
Informações Operacionais	Requisitos de ingresso à Instituição de Ensino	• Requisitos de titulação, técnicos e habilidade para os professores, • Requisitos de titulação, técnicos e habilidade para os funcionários • Requisitos de titulação, técnicos e habilidade para os alunos
	Dados cadastrais	• Histórico e currículo dos professores • Histórico e currículo dos funcionários • Histórico e currículo dos alunos
	Informações sobre a evolução do aluno	• Registro do perfil do ingresso (aluno) • Registro do perfil do egresso (aluno)
	Necessidades técnicas	• Infra-estrutura demandada por curso e disciplina (recursos técnicos, locais adequados, orçamento etc.)
	Avaliações	• Registro e histórico das avaliações de discentes; • Registro e histórico das avaliações do Corpo Docente • Registro e histórico das avaliações do Curso • Registro e histórico das avaliações da Disciplina • Registro e histórico das avaliações da infra-estrutura do curso • Registro e histórico das avaliações dos Órgãos fiscalizadores (MEC, Receita Federal etc.), auditorias etc. • Registro e histórico das avaliações das atividades pedagógicas, cognitivas e sócio-culturais
	Registro dos eventos em sala de aula (diário de classe)	• Localização da sala de aula • Série e turma • Curso • Período letivo • Disciplina • Professor • Carga horária estabelecida • Dia da semana e horário das aulas • Registro de presença dos alunos • Registro de falta dos alunos (total) • Quantidade de aulas realizadas • Registro de data e conteúdo aplicado em sala • Observações diversas • Registro sintetizado das ausências e das notas dos alunos
	Plano de ensino por disciplina	• Unidade de Ensino • Curso • Disciplina • Carga horária • Docente • Objetivos Gerais • Objetivos Cognitivos • Atitudes • Ementa do curso • Quadro de Competências • Quadro de habilidades • Quadro de bases tecnológicas • Quadro de pré-requisitos • Quadro de recursos institucionais • Bibliografia geral • Bibliografia complementar • Metodologia de ensino • Critérios de avaliação • Pesquisa • Atividades extraclasse • Recursos institucionais • Atividades interdisciplinares • Cronograma – conteúdo a ser desenvolvido

Quadro 5-2: Grupos de Atividades e Informações (Continuação)

Exemplos de Informações Administrativas	Marketing	• Campanhas publicitárias • Verba orçada para publicidade • Normas e procedimentos
	Contabilidade	• Publicação das demonstrações contábeis e financeiras • Detalhamento dos lançamentos contábeis • Fluxo contábil
	Finanças	• Planejamento orçamentário consolidado • Disponibilidade e movimentação de recursos financeiros • Lançamentos financeiros
	Fiscal/Legal	• Plano estratégico tributário • Declarações e informações aos Órgãos reguladores • Recolhimentos efetuados, notas fiscais
	Recursos humanos	• Salário do corpo diretivo • Folha de pagamento • Avaliação de desempenho profissional, informações cadastrais etc.
	Sistema de informação	• Parâmetros criptográficos • Topologia da rede local e estrutura • Plano de contingência
Corporativas		• Missão • Regimento • Plano de Desenvolvimento Institucional • Estrutura das Divisões e Departamentos • Organograma • Políticas para Gestão de Pessoas • Política contra invasão • Política de segurança • Plano de desenvolvimento de normas e procedimentos • Projeto Pedagógico (Diretrizes curriculares do MEC, Regimento interno, Novos aportes da comunidade cientifica e Diretrizes do Plano Pedagógico Institucional) • Plano Acadêmico • Plano de ensino • Plano de disciplinas (definições cognitivas e inter-relacionamento) • Análise de viabilidade do curso • Controle sobre o desenvolvimento dos cursos • Registro de Atas sobre reuniões deliberativas
Pesquisa Científica (Plataforma Lattes)	Pessoais do pesquisador	• Endereço • Formação • Titulação • Atuação profissional • Idiomas • Prêmios e títulos
	Produções técnicas	• Softwares • Produtos • Processos • Trabalhos técnicos • Outras produções técnicas
	Produções biográficas	• Artigos publicados • Livros e capítulos • Trabalhos em eventos • Texto em jornal ou revista • Outras produções bibliográficas
	Demais produções e trabalhos	• Produção artística ou cultural • Orientações concluídas • Orientações em andamento • Demais trabalhos

Fonte: O próprio autor

As informações relativas à produção científica devem ser protegidas para garantir os três objetivos de segurança, à época do seu desenvolvimento (após a conclusão é pública), em consonância com as suas características de risco, conforme análise de cada objetivo a seguir:

- Confidencialidade – preservar o acesso às pesquisas por pessoas e recursos autorizados, tempestivamente considerar seu estágio de maturidade tecnológica ou eventual cenário político instável. Em especial se o tema possa causar transgressões legais (internas ou a tratados internacionais), político-sociais, ambientais, física aos cidadãos. Também visa à proteção de direitos legais.
- Integridade – está relacionada com a defesa da propriedade de direito autoral e da manipulação indevida dos dados de entrada ou produzidos no curso da pesquisa
- Disponibilidade – abrange a correta e tempestiva acessibilidade da produção cientifica ao longo do seu ciclo de vida, visa atender à regulamentação que a rege e também a sua preservação.

O resultado deste levantamento deu origem às informações destinadas ao treinamento da Rede Neural. Foram selecionadas 35 informações, distribuídas em: base cadastral dos agentes envolvidos (sombreadas de 1 a 11), pesquisa cientifica, atividades pedagógicas (sombreadas 17 a 22), informações administrativas e informações sobre a infra-estrutura de TI (sombreadas 33 a 35). Estas informações encontram-se no Quadro 5-3.

Quadro 5-3: Informações Selecionadas

	Informações Selecionadas (Linha - P)
1	Histórico e currículo professores
2	Histórico e currículo funcionários
3	Histórico e currículo alunos
4	Perfil ingresso aluno
5	Perfil egresso aluno
6	Histórico de avaliações Discentes
7	Histórico de avaliações Docente
8	Histórico de avaliações Curso e disciplinas
9	Histórico de avaliações Infra-estrutura
10	Histórico de avaliações Órgãos Fiscalizadores
11	Histórico de avaliações atividades diversas
12	Pesquisa de softwares de segurança
13	Pesquisa de recursos de criptografia
14	Pesquisa de produção de energia
15	Pesquisa de desenvolvimento de armas
16	Pesquisa que tabula informações de empresas
17	Objetivos Cognitivos da Universidade
18	Objetivos do curso
19	Ementa dos cursos
20	Quadro de competências
21	Quadro de bases tecnológicas
22	Quadro de pré-requisitos
23	Marketing – Campanhas publicitárias
24	Marketing – Verba orçamentária de publicidade
25	Cont – Demonstrações contábeis Financeiras
26	Cont – Fluxo contábil
27	Fin – Disponibilidade e movimentação recurso
28	Fin – Lançamentos financeiros
29	Fiscal – Plano estratégico tributário
30	Fiscal – Informações para Órgãos Reguladores
31	RH – Proventos do corpo diretivo
32	RH – Dados sobre a folha de pagamento
33	Sist. Inf. – Parâmetros criptográficos
34	Sist. Inf. – Topologia da rede local
35	Sist. Inf. – Plano de contingência

Fonte: O próprio autor

O critério de seleção também buscou identificar conjunto de informações que apresentassem alteração na sua condição de confidencialidade, uma vez que um evento ou uma data específica provoque a alteração do nível de sigilo. Por exemplo, durante o desenvolvimento o conteúdo da pesquisa é restrito aos pesquisadores envolvidos, após sua conclusão torna-se público.

A escolha dessas informações também relevou grupos com características peculiares quanto a confidencialidade, que não estendem necessariamente suas propriedades às outras informações similares. Por exemplo, o *curriculum vitae* do professor é obrigatoriamente público, contudo suas informações cadastrais não se sujeitam a mesma exigência.

As considerações sobre determinadas particularidades são necessárias para a formulação da correlação entre as Informações e as Categorias de Risco. Por conseguinte, para efeito de atribuição dos pesos para o treinamento da rede neural, prevalecerá à requisição de maior proteção.

O exemplo das informações sobre a pesquisa cientifica, receberia a pontuação mais alta, pois a demanda por maior sigilo ocorreria na fase de desenvolvimento da pesquisa (informações de acesso limitado). Neste caso, ao longo do ciclo de vida da informação caberia a definição de procedimentos para a atualização do nível do objetivo de segurança quando ocorre a conclusão da pesquisa, tornando-a pública.

O segundo exemplo, destaca o zelo exigido ao atribuir os pesos com precisão, sem expandir indevidamente algumas propriedades a outras informações similares quanto ao seu conteúdo (dados sobre os professores), porém diferentes quanto à demanda por proteção.

5.3 Correlação entre as Categorias de Risco e as Informações para o Treinamento da Rede Neural

Os pesos para o treinamento da Rede Neural visam obter o conhecimento de profissionais envolvidos nas atividades concernentes à segurança ou afins no ambiente acadêmico. Para alcançar esse objetivo foram acionados quatro representantes de setores de controle, segurança, qualidade e coordenação de universidades diferentes.

Aos representantes foram encaminhadas orientações e recomendações sobre o preenchimento de uma planilha definida para esta finalidade, onde as informações estão situadas nas linhas e as categorias de risco nas colunas. Estas orientações atendem às especificações descritas no Capítulo 4 – Proposta de um Método de Informações.

A planilha apresenta a conjugação dos quadros Quadro 5-1 (Categorias de Risco – colunas), relacionadas no Quadro 5-3 (Informações Acadêmicas – linhas). Onde cada informação foi relacionada às Categorias de Risco com valores entre 0 e 10. A pontuação é crescente de acordo com a estimativa de aumento do impacto e severidade causados pela divulgação indevida da informação.

Todas as correlações colhidas junto aos profissionais pesquisados, foram consolidadas pela média aritmética simples, sem arredondamento dos valores após o cálculo. O resultado alcançado está apresentado no Quadro 5-4.

Quadro 5-4: Correlação das Categorias de Risco e as Informações

Correlação para Treinamento da Rede

L\C	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
1	5,5	3,5	2	3	2	5	3,5	3	1,5	1,5	1,5	3,5	5,5	1,5	4,5	1	4,5	1	4,5	1	4,5	1,5	4,5	2,5	5	6	5	4,5
2	3,5	1,5	1,5	5	3	3	3,5	3	1,5	2	3,5	4	2,5	4	5	1,5	3	5,5	4,5	1,5	2,5	5	4,5	1,5	4	1,5	1,5	2,5
3	5	2	4	3	2	3	3,5	3	5,5	3,5	5,5	6	1,5	1,5	4	4,5	3,5	3	6	6	3,5	1,5	7	4	6,5	5,5	6	7,5
4	3,5	3,5	5	4	1	2,5	3,5	3	7,5	1,5	1,5	3,5	5	1,5	5	2	1,5	1,5	1,5	3,5	2	1,5	3	2	3,5	5	5	8
5	4	2	4	4,5	1	3,5	3,5	3	5,5	2	2	6	4	2	4,5	2,5	1,5	1,5	5,5	5	1,5	4	5	1,5	4	4	5	9
6	3,5	1,5	5,5	7,5	2	2,5	5	5,5	6,5	1,5	2	7	6,5	2	6,5	4,5	5	1,5	6,5	5	4,5	1	7,5	1,5	5	5,5	5	7,5
7	3,5	2	5,5	7,5	2	2,5	5	4,5	3,5	2	3	5,5	7	1,5	8,5	3,5	8	1,5	6,5	3,5	7	1,5	5	1,5	7,5	7,5	7	5
8	5	5,5	5	9	4	2,5	5	5,5	5,5	2	3,5	6,5	6	1	9	3	3	3	4,5	5	1,5	1,5	9	3,5	6,5	7	7,5	9
9	4	7	4	4	4	6	6,5	6,5	4,5	4,5	4,5	6	4,5	4,5	5,5	3,5	3,5	4	4,5	4	3,5	3,5	4,5	7	4,5	3,5	4	6,5
10	5	4	3,5	4	4,5	4	6,5	6	3,5	3,5	5	6	4	3,5	5	4	4	4	5	3,5	3,5	3,5	4,5	4	6	5	5	6,5
11	1,5	2	1,5	1,5	2	1,5	4,5	2,5	1,5	1,5	1,5	2	2,5	2	2	1	2	1,5	2,5	1	1,5	1,5	2,5	1	2,5	1,5	2,5	4
12	5	4,5	3	3,5	3	3	3,5	5	2,5	3	1	1,5	1,5	1,5	2	1,5	1,5	1,5	3	2	2	1	3,5	5	2,5	2,5	1,5	3,5
13	4,5	5	3	2	2	2,5	4	4,5	2	1	1	1,5	1,5	1,5	2	1,5	1,5	1,5	2,5	1,5	2	1	2,5	4	2	2,5	1,5	2,5
14	4,5	4,5	3	5	5	5,5	5	4,5	2,5	1,5	1	2,5	1,5	1,5	2	1,5	1,5	1,5	2,5	2	2	1	3,5	4	3	2,5	1,5	3
15	5,5	4,5	3	5,5	5,5	5,5	4,5	4,5	2,5	1	1	5	5	5	5,5	1,5	1,5	1,5	5,5	5	3	1	5,5	4	4	2,5	1,5	5,5
16	5	4,5	3	5,5	4	3,5	5,5	5,5	2,5	2	1	2	2,5	2,5	3	1,5	1,5	1,5	4,5	5	3,5	1	5,5	4	2,5	2,5	1,5	5,5
17	3	1,5	3,5	1,5	1,5	1,5	4	4,5	4	2	1,5	4,5	4	2	5	2	1,5	1,5	3	1	1,5	1	2,5	2	5	5	8,5	8
18	3	3,5	5	1,5	1,5	1,5	6	3	3	1	1	4,5	4,5	1	4,5	3	3	1	4,5	3	3	1	1	1	5	5	8,5	8
19	4,5	5	5	1,5	1,5	1,5	4	1,5	3	1	1	5	5,5	3	5	4,5	3,5	1	3,5	3	3	1	3	3	5	5	8,5	8
20	3	3,5	3,5	3,5	1,5	1,5	4	1,5	3	1	1	4,5	5	1	3,5	3	5	1	5	1	3	1	3	1	5	5	8,5	8
21	4,5	5,5	5	2	1,5	1,5	3,5	2,5	1,5	1,5	1	5	5,5	5	5,5	3,5	1,5	1	5,5	1	1,5	1,5	2	5,5	5	5	8,5	8
22	1	1	3,5	1,5	1	1,5	3,5	1,5	1	1	1	7	4	4	4	1,5	1,5	1	1,5	1	1	1	1,5	1,5	4	3,5	7	6,5
23	7	7	5,5	6	4,5	1,5	3	4	5,5	2,5	2	4,5	4	5,5	4,5	2	1,5	1,5	7,5	3,5	1,5	1,5	6,5	4	9	3,5	3,5	4,5
24	3,5	4,5	3	2,5	2,5	2	4,5	7	2	2	3	1,5	2	3,5	6	2	2	2	7	1	1	1	2,5	3,5	8	4	3,5	4,5
25	6,5	7	1,5	9	2	2	7	8	1,5	4	5	1	1	1	5,5	1,5	1,5	1,5	6,5	1	1	1	9	2	6	4	4	6
26	5,5	6	1	6	1,5	1,5	6,5	7,5	1,5	3,5	5	1,5	1,5	1,5	5,5	1,5	1,5	1,5	6	1	1	1	6	1,5	6	3,5	3,5	6
27	5,5	6	1	6	2,5	3	6	8,5	2	3,5	5	2	2,5	2	6	1,5	1,5	1,5	7	1	1	1	6,5	1,5	5,5	4	3,5	6
28	5,5	6	1	8,5	2,5	3	6	8,5	1,5	5	5	2	2	2	6	1,5	1,5	1,5	5	1	1	1	8,5	1,5	5,5	4	3,5	6
29	5	6	1	7,5	1,5	2	6	8	1,5	4,5	5	1,5	1,5	1,5	6	1,5	1,5	1,5	6,5	1,5	1,5	1	8,5	1,5	8	4	3,5	6
30	5	6	1,5	8	2	2	7,5	8,5	4	5	7	2,5	2,5	2,5	7	2,5	2,5	2,5	8	2,5	2,5	2,5	9	1,5	6,5	4,5	4	6
31	9	6	1	9	5	5,5	7,5	9	1	3	4,5	1	1	1	6	1,5	1,5	1,5	6,5	1	1	1	9	1,5	5	3,5	3,5	6
32	8,5	6	1	9	5	5	7,5	8	2	4	4,5	1,5	2	2	5,5	1	2	2	6	1	2,5	2,5	9	1,5	5	3,5	3,5	6
33	8	6	6,5	5,5	3,5	2	5	5	3,5	3,5	1,5	4,5	4,5	5	7,5	4,5	2	2	7,5	2,5	2,5	2,5	5	8	7,5	3,5	3	7,5
34	8	9,5	7	3,5	3	3	4,5	3	3,5	3,5	2	4,5	6,5	6,5	7	4,5	2,5	2,5	7,5	2,5	2,5	2,5	5	8	6,5	3,5	3	7,5
35	8	9,5	5,5	2,5	2	2	3,5	4,5	3,5	4	3	7	7	7	5,5	5	2,5	2,5	8,5	2	2	2	4,5	9	6,5	4	6	7

Fonte: O próprio autor

5.4 Desenvolvimento do *Script* em *Matlab* e Treinamento da Rede Neural

Com base no resultado obtido na pesquisa, a planilha de correlação representa os dados de entrada para o programa de treinamento da Rede Neural. Este programa executa o treinamento da Rede Neural, para atender a esta finalidade foi desenvolvido o *script,* em *MatLab* 6.5, auxiliado por funções fornecidas pelo recurso *SOM Toolbox*.

O *script* implementado obedece a três etapas, constituídas por: Construção do Conjunto de dados; Treinamento do Mapa e Visualização.

Na etapa preliminar ao processamento, a normalização dos dados seria necessária para equalizar os valores que retratam os espaços das variáveis, com a finalidade de evitar distorções no computo da distância Euclidiana. Contudo, em face ao preenchimento da tabela de correlação apresentar uniformidade na formatação dos dados, pois todos os dados de entrada são inteiros e limitados ao intervalo de zero a dez, não foi necessário submetê-los à função de normalização do *SOM Toolbox*, portanto, os dados da forma que se encontram na tabela de correlação, estão preparados para o início do treinamento da Rede Neural.

O primeiro passo do treinamento da rede é a determinação do neurônio vencedor, pelo processo competitivo. O mapa de entrada utilizou a distância Euclidiana Quadrática e o algoritmo em *Batch* para o cálculo da menor distância que indicará o neurônio vencedor.

No processo de aprendizado cooperativo os neurônios de saída estão topologicamente próximos, ativam-se reciprocamente para aprender com as informações de entrada (Kohonen, 2001). O neurônio vencedor no processo competitivo determina o centro desta vizinhança topológica de neurônios cooperativos (Haykin, 2001).

O algoritmo para a criação do *SOM* inicia os pesos sinápticos da Rede Neural de duas formas. A primeira, utiliza valores aleatórios ao que se denomina inicialização randômica. A outra forma, inicia os pesos sinápticos de forma ordenada (Kohonen, 2001; Haykin, 2001), o que permite convergir mais rapidamente. Este processo é chamado “inicialização linear” e envolve ainda a definição de um modelo de entrelaçamento do vetor que pode ser: retangular, hexagonal, ou de alguma forma irregular. Para este estudo de caso os pesos sinápticos foram inicializados de forma linear, com os valores apresentados no Quadro 5-4.

Após a inicialização linear, os dados de entrada são submetidos aos processos de Competição, Cooperação e Adaptação Sináptica, para a formação do *SOM* (Haykin, 2001).

CAPÍTULO 6 – RESULTADOS E CONCLUSÕES

6.1 Visualização dos Resultados

O entrelaçamento hexagonal tem um melhor resultado visual (Kohonen, 2001), pois todos os seis vizinhos do neurônio têm a mesma distância. Enquanto que os 8 vizinhos do entrelaçamento retangular não tem distâncias iguais. Por isso, escolheu-se o entrelaçamento hexagonal. Os resultados serão apresentados com o recurso do *SOM Toolbox* denominado U-Matriz que auxilia a apresentação visual e a compreensão através da geração dos *Labels*.

O resultado obtido da exploração dos dados está apresentado graficamente. A Figura 6-1 mostra as matrizes de intensidades de cores, onde os hexágonos com a menor distância Euclidiana estão representados pela cor azul. Enquanto que os hexágonos de coloração vermelha mostram as maiores distâncias entre os demais hexágonos em sua volta. A proporção das Distâncias Euclidianas pode ser analisada pela cores da barra de escala vertical apresentada na Figura 6-2.

Na própria Figura 6-2 os clusters, que agruparam as informações com as características de risco de maior semelhança, identificados pelos grupos de hexágonos da cor azul, que foram delimitados e constituíram seis grupos distintos. Esta delimitação é dada por análise visual dos clusters gerados.

A Figura 6-1 também mostra a representação Hexagonal (*Labels*) onde estão destacadas, em letras vermelhas, as Informações Selecionadas identificadas pelos respectivos números mencionados no Quadro 5-3 – Informações Selecionadas para o Estudo de Caso, acrescido da letra *P*. Estas se destacaram devido a sua maior influência para a formação dos clusters, obtidas por intermédio do processamento do *Best Matching Unit* (BMU), pois criaram o ponto de atração dos neurônios vencedores, que norteou o cálculo da distância Euclidiana.

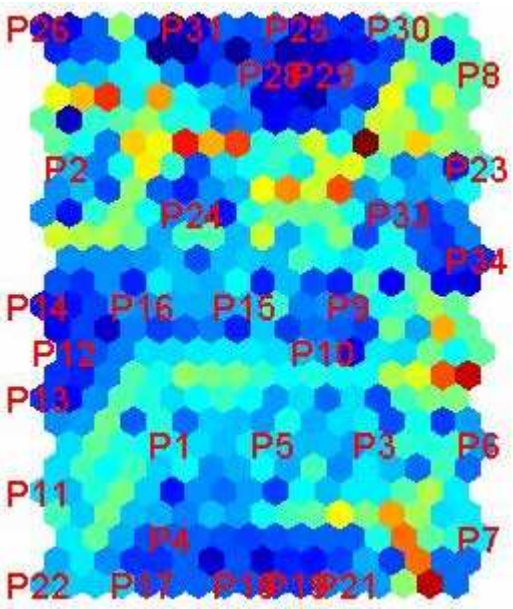

Figura 6-1: Produto Inicial do Treinamento

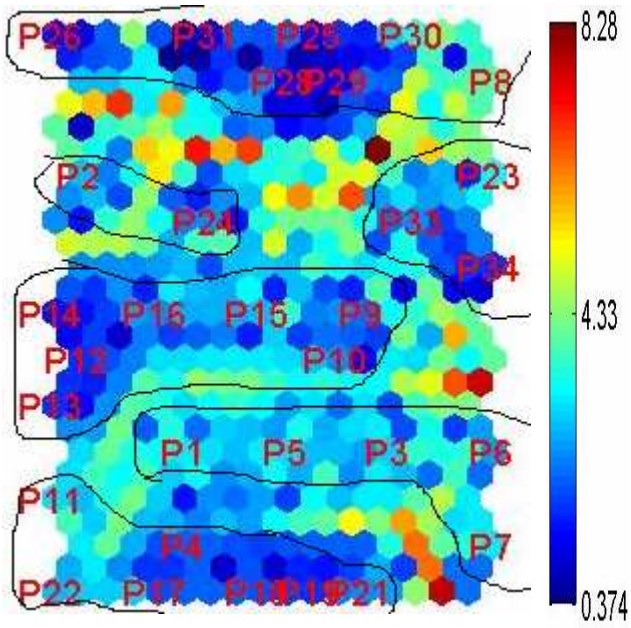

Figura 6-2: Produto Agrupado do Treinamento e Escala

Note-se que algumas informações não foram retratadas nas Figuras 6-1 e 6-2 devido ao fato de ocuparem o mesmo hexágono de algumas informações apresentadas. O Quadro 6-1 mostra as faltantes, a informação compartilhada e o hexágono correspondente.

Quadro 6-1: Informações Agrupadas no Treinamento

Número do Hexágono	Informação Apresentada	Informação Agrupada
1	P26	P27
7	P12	P14
27	P31	P32
52	P18	P20
53	P25	P28
78	P19	P21
110	P34	P35

Fonte: O próprio autor

A primeira coluna do Quadro 6-1, “Número do Hexágono”, mostra a posição do hexágono no plano reticulado e destina-se a visualização da distância física entre as informações. A coluna “Informação Apresentada” relaciona aquelas mencionadas nas Figuras 6-1, 6-2 e 6-3 e, a última coluna mostra as informações que não foram apresentadas anteriormente, por ocuparem o mesmo hexágono das informações da segunda coluna.

Complementarmente a Figura 6-3 apresenta os *Labels*, sem as tonalidades de cores que representam as distâncias Euclidianas, bem como as sobreposições determinadas pela quantidade de informações nos Hexágonos,

entre os parênteses. A Figura 6-4 expõe todas as posições do plano reticulado de maneira a facilitar a visualização e o posicionamento dos hexágonos.

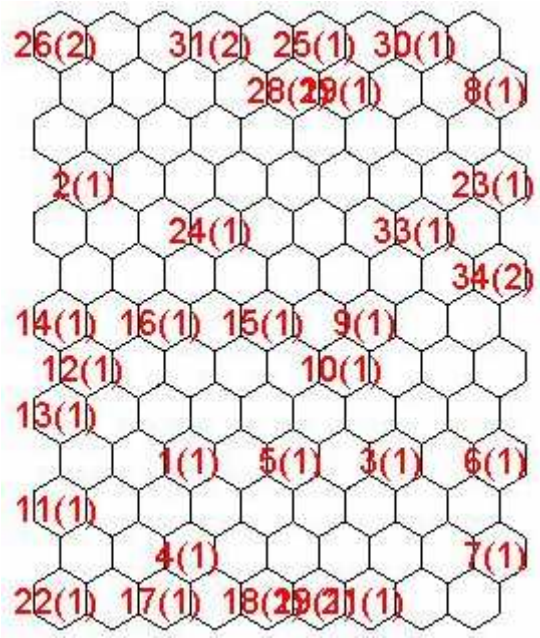

Figura 6-3: *Labels* e Sobreposição

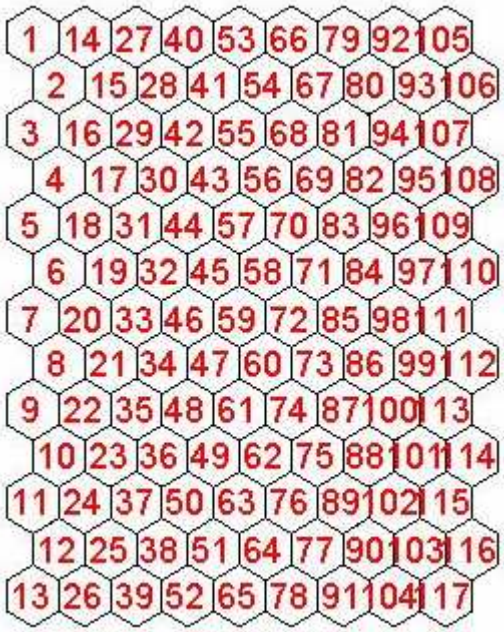

Figura 6-4: Ocupação do Plano Reticulado

Os hexágonos que apresentam mais de uma informação são mostrados por meio de uma tabela gerada pelo *SOM Toolbox* (Quadro 6-1), que além da sobreposição também mostra a posição ocupada dentro do plano reticulado (Figura 6-4), para facilitar a compreensão das informações que compõe os clusters.

Estes recursos permitiram criar os agrupamentos em razão da similaridade entre as informações, dando origem aos clusters denominados por letras, conforme o Quadro 6-2.

Quadro 6-2: Formação dos Clusters

Clusters	Ref.	Informação
A	1	Histórico e currículo professores
A	3	Histórico e currículo alunos
A	5	Perfil egresso aluno
A	6	Histórico de avaliações Discentes
A	7	Histórico de avaliações Docente
B	2	Histórico e currículo funcionários
B	24	Marketing – Verba orçamentária de publicidade
C	4	Perfil ingresso aluno
C	11	Histórico de avaliações atividades diversas
C	17	Objetivos Cognitivos da Universidade
C	18	Objetivos do curso
C	19	Ementa dos cursos
C	20	Quadro de competências
C	21	Quadro de bases tecnológicas
C	22	Quadro de pré-requisitos
D	8	Histórico de avaliações Curso e disciplinas
D	25	Cont – Demonstrações contábeis Financeiras
D	26	Cont – Fluxo contábil
D	27	Fin – Disponibilidade e movimentação recurso
D	28	Fin – Lançamentos financeiros
D	29	Fiscal – Plano estratégico tributário
D	30	Fiscal – Informações para Órgãos Reguladores
D	31	RH – Proventos do corpo diretivo
D	32	RH – Dados sobre a folha de pagamento
E	9	Histórico de avaliações Infra-estrutura
E	10	Histórico de avaliações Órgãos Fiscalizadores
E	12	Pesquisa de softwares de segurança
E	13	Pesquisa de recursos de criptografia
E	14	Pesquisa de produção de energia
E	15	Pesquisa de desenvolvimento de armas
E	16	Pesquisa que tabula informações de empresas
F	23	Marketing – Campanhas publicitárias
F	33	Sist. Inf. – Parâmetros criptográficos
F	34	Sist. Inf. – Topologia da rede local
F	35	Sist. Inf. – Plano de contingência

Fonte: O próprio autor

Uma vez que os grupos foram formados, teve início o processo de apuração da relevância de cluster de informações entre os seis grupos gerados.

Esta fase consiste no cálculo das médias aritméticas simples de cada cluster. O cálculo atenta a todos os valores atribuídos às informações que constituem o cluster. Estes valores são aqueles conferidos pelos profissionais especialistas em controle, qualidade, segurança e demais atividades afins.

O resultado deste cálculo indica a pontuação relativa aos impactos decorrentes da possível efetivação de ameaças. Os clusters foram ordenados decrescentemente, enunciando aqueles de maior exposição ao risco concernente ao objetivo de segurança da Confidencialidade.

A comparação entre as médias obtidas por cada cluster levou a considerar o nível de Confidencialidade requerido por cada cluster, apresentado no Quadro 6-3.

Quadro 6-3: Níveis de Confidencialidade

Clusters	Informação	Média	Confidenc.
F	Marketing – Campanhas publicitárias		
F	Sist. Inf. – Parâmetros criptográficos	5,72	Altamente Secreta
F	Sist. Inf. – Plano de contingência		
F	Sist. Inf. – Topologia da rede local		
D	Cont – Demonstrações contábeis Financeiras		
D	Cont – Fluxo contábil		
D	Fin – Disponibilidade e movimentação recurso		
D	Fin – Lançamentos financeiros		
D	Fiscal – Informações para Órgãos Reguladores	4,94	Altamente Secreta
D	Fiscal – Plano estratégico tributário		
D	Histórico de avaliações Curso e disciplinas		
D	RH – Dados sobre a folha de pagamento		
D	RH – Proventos do corpo diretivo		
A	Histórico de avaliações Discentes		
A	Histórico de avaliações Docente		
A	Histórico e currículo alunos	4,19	Secreta
A	Histórico e currículo professores		
A	Perfil egresso aluno		
E	Histórico de avaliações Infra-estrutura		
E	Histórico de avaliações Órgãos Fiscalizadores		
E	Pesquisa de desenvolvimento de armas		
E	Pesquisa de produção de energia	3,90	Secreta
E	Pesquisa de recursos de criptografia		
E	Pesquisa de softwares de segurança		
E	Pesquisa que tabula informações de empresas		
C	Ementa dos cursos		
C	Histórico de avaliações atividades diversas		
C	Objetivos Cognitivos da Universidade		
C	Objetivos do curso		
C	Perfil ingresso aluno	3,65	Interna
C	Quadro de bases tecnológicas		
C	Quadro de competências		
C	Quadro de pré-requisitos		
B	Histórico e currículo funcionários	3,63	Interna
B	Marketing – Verba orçamentária de publicidade		

Fonte: O próprio autor

Resumidamente, este resultado retrata o produto obtido pelo processamento da Rede Neural *SOM* de Kohonen, adicionado aos cálculos da média apresentados no método proposto neste estudo. A definição pelos níveis de “Altamente Secreta” para os clusters F e D se deve à condição de ambos apresentarem pontuação próxima ao valor cinco, conforme proposto no Capítulo 4.

6.2 Conclusão sobre os Resultados alcançados no Estudo de Caso

O propósito deste trabalho foi descobrir os grupos que mantenham similaridade dos seus elementos por intermédio de um padrão voltado às suas características de risco. O processamento da Rede Neural de Inteligência Artificial realizou a tarefa de identificar os grupos que possuem a mesma natureza. Esta similaridade foi norteada pelas Categorias de Risco aplicadas para as informações tratadas no âmbito das universidades. Logo, esta meta inicial foi cumprida.

Contudo, a análise do desenvolvimento, da implementação e dos resultados obtidos no Estudo de Caso nos permite a formulação de algumas considerações que visam à evolução deste método.

As informações destinadas ao treinamento da Rede Neural, quando formuladas estavam distribuídas inicialmente em: base cadastral, pesquisa cientifica, atividades pedagógicas, administrativas e de infra-estrutura de TI. Esta distribuição envolveu naturalmente um nível de similaridade entre os elementos, uma vez que há poucos hexágonos de coloração vermelha escura, que expõem as maiores distâncias Euclidianas. A seguir, estão apresentadas as similaridades observadas em cada grupo gerado após o treinamento da rede:

- A: composto somente por informações da base cadastral;
- B: duas informações e grupos diferentes;
- C: maioria dos elementos faz parte das atividades pedagógicas;
- D: maior parte das informações pertence às funções administrativas;
- E: maioria dos dados está relacionada à pesquisa cientifica; e
- F: predominância das informações é de infra-estrutura de TI.

Os grupos formados ratificam a pré-existente similaridade parcial entre os seus elementos, embora esta não tenha sido prevista na seleção das informações para o treinamento da rede. Embora se apresente em menor escala, se observa a mescla de informações originadas em atividades diferentes, nos novos grupos formados.

O resultado também abrangeu os riscos decorrentes de todas as atividades desempenhadas pelas universidades, o que envolve a administração, pedagogia e pesquisa cientifica. Estes riscos compreendem as propriedades, características e requerimentos legais inerentes aos processos das universidades, as quais devem ser refletidas na correlação entre as Informações e as Categorias de Risco. O produto dessa correlação é preponderante para formação dos grupos ou clusters, e também para a determinação dos níveis de Confidencialidade.

Por essa razão, a formulação da correlação necessita de amplo conhecimento, pelos responsáveis de sua confecção, das diretrizes estratégicas, processos e atividades de uma universidade, acrescidos de vivência e percepção das ameaças existentes e aquelas que possam se materializar e, principalmente dos possíveis impactos às entidades que se relacionam com o ambiente acadêmico. Embora os impactos possam originar-se na infra-estrutura computacional ou nos sistemas de informação, serão contabilizados ou sensibilizarão as atividades operacionais, financeiras, administrativas etc.

No desenvolvimento do Estudo de Caso, se verificou a necessidade de ampliar as explicações e as discussões junto às pessoas entrevistadas, de forma a auxiliar a visão de risco e impacto a cada correlação realizada. Portanto, o sucesso da aplicação do método descrito neste trabalho mantém dependência direta da capacitação e conhecimento dos profissionais que constroem a correlação.

Outro fator relevante na formulação dos pesos na correlação é a possibilidade de alterar a condição de sigilo em face da ocorrência de um determinado evento ou datas pré-estabelecidas. Esta circunstância foi sugerida aos profissionais pesquisados, pois prevaleceu, quando identificada, a demanda de sigilo de maior nível.

O Estudo de Caso demonstrou que a aplicação do método apresentado é factível através dos Mapas Auto-Organizáveis de Kohonen, com a adequada e assertiva categorização dos riscos. Os resultados alcançados

pelo treinamento da Rede Neural se mostraram compatíveis nos grupos que foram gerados.

O produto da classificação das informações concernentes ao nível de Confidencialidade observados neste caso prático, leva a conclusão que sua aplicação pode estender-se a outros segmentos, na indústria de base, no segmento financeiro, no comércio, organizações não governamentais, governos etc. Dessa maneira atingindo aos objetivos de apresentar um método para classificação das informações que seja baseado no conhecimento e experiência acumulada de profissionais, seja uniforme, sistemático e assertivo.

O emprego deste método traz como benefício a condição de aprimoramento do dimensionamento dos investimentos em segurança e, principalmente, prover os mecanismos de proteção que sejam mais apropriados às características de cada informação, obtendo maior efetividade na mitigação dos riscos dos sistemas de informação e da infra-estrutura computacional.

6.3 Trabalhos Futuros

No cenário em que os processos de negócio não conseguem acompanhar a velocidade de inovação tecnológica, quanto a sua aplicabilidade, a própria tecnologia propicia condições que além dos benefícios esperados, também serve de insumo para ameaças e ataques inusitados.

As organizações se preparam com investimentos maciços e crescentes para prover maior proteção para seus ativos, por intermédio de recursos técnicos e metodológicos de segurança, contudo, de eficácia e eficiência questionáveis em razão de não haver instrumentos para medição.

O método de classificação implementado pelos *SOM* de Kohonen atende a primeira etapa de um processo de segurança porque separa as informações relevantes, que requerem maior proteção, daquelas que possuem características que não demandam a preservação de sigilo. Portanto, doravante surge a perspectiva de explorar as novas etapas de implementação de segurança, o que representa um conjunto de trabalhos que abrangem:

- Desenvolver um método, derivado deste apresentado, que trate simultaneamente todos os objetivos de segurança (confidencialidade, disponibilidade e integridade) de aplicação integrada e maior alcance na mitigação dos riscos;
- Em complemento a implementação deste modelo, sugere-se desenvolver e implantar novos modelos que possam ser Integrados a este primeiro destinados a direcionar os equipamentos e recursos de segurança à medida do nível de classificação das informações. De forma que as informações definidas como “Altamente Secreta” recebam indicações de uma gama de dispositivos de segurança mais adequados à sua condição, assim como nos outros dois níveis de confidencialidade;
- Em face da importância da fase de categorização dos riscos, seria necessário e útil o desenvolvimento de método ou mecanismos que auxiliem identificação e quantificação na composição dos riscos.

REFERÊNCIAS BIBLIOGRÁFICAS

ASTION; Michael L.;WILDING, Peter. *The application of back propagation neural networks to problems in pathology and laboratory medicine*, Arch Pathol Lab Med, 1992.

BACEN. Banco Central do Brasil. Os Princípios Essenciais da Basiléia. Tradução e editoração eletrônica: Jorge R. Carvalheiro. Tradução em dez. 1997 e revista em fev. 2000. Disponível em:<http://www.bcb.gov.br> Acesso em: 16 out.2007.

BERNSTEIN, P. L. *Against the Gods: the remarkable story of Risk*. John Wiley &Sons, Inc. New York, 1997.

BERRY, M.J.A. and LINOFF, G. *Data Mining Techniques For Marketing, Sales and Customer Support*. John Wiley & Sons, Inc., USA, 1996.

BIS-*Bank for International Settlements*. (1997) *Core Principles for Effective Banking Supervision*. *Basel Committee on Banking Supervision*. Disponível em: <http://www.bis.org>. Acesso em: 4 set. 2007.

BIS-*Bank for International Settlements* (2001). *Overview of The New Basel Capital Accor*". *Technical report, Bank for International Settlements*, Disponível em: http://www.bis.org, Acesso em: 18 abril 2007.

BIS-*Bank for International Settlement* (2003), "*Basel Committee on Banking Supervision – Risk Management Principles for Electronic Banking*", Disponível em: <http://www.bis.org >, Acesso em: 17 março 2007.

BIS-*Bank for International Settlements*. (2004) *The joint Forum Credit Risk Transfer*. *Basel Committee on Banking Supervision*. Disponível em: <http://www.bis.org>. Acesso em: 04 jun. 2007.

BLAKLEY B., MCDERMOTT E., GEER D. *Information Security is Information Risk Management*. Communications of the ACM, 2002.

BRUNO, Maria. *Targeting banking customers at the right point*, Bank Technology News, 1999.

BUCHMANN, J. A.; *Introduction to Cryptography*; Springer, 2001.

BUNGE, M., Teoria e Realidade. São Paulo: Editora Perspectiva, 1974.

CALLAN, Daniel E.; Lasky, Robert E.; Fowler, Cynthia G. *Neural networks applied to retro cochlear diagnosis*, 1999.

CAQUETTE, J. B.; Altman, E. I.; Narayanan, P. Gestão do Risco de Crédito – O próximo Grande Desafio. Rio de Janeiro:Qualitymark Editora Ltda., 1999.

CARDOSO, Silvia Helena; Sabbatini, Renato M. E. (1999), Como Funcionam as Células Nervosas. São Paulo: Universidade Estadual de Campinas, Disponível em: <http://www.cerebromente.org.br/n09/fundamentos> Acesso em: 20 fev. 2007;

CASSEN, Revista Caros Amigos, Ed. Casa Amarela São Paulo, set.1999

CASSIOLATO, J. E., Lastres H. M. M. (2000) .Sistemas de Inovação: Políticas e Perspectivas.Revista Parecerias Estratégicas. Disponível em <http:www.cgee.org.br/parcerias>, Acesso em: 28 dez. 2007.

C-H CHEN; R. G. PAREKH; J. YANG; K. Balakrishnan; V. Honavar, *Analysis of Decision Boundaries Generated by Constructive Neural Network Learning Algorithm*. EUA: Iowa State University. Disponível em: <http://archives.cs.iastate.edu>.Acesso em: 5 out.2007.

CHENG, B.; Titterington, D. M. *Neural Networks: a review from a statistical perspective*, *Statistical Science*, Vol. 9, No. 1, pp. 2-30, 1994.

CORMEN, Thomas H.; Leiserson;Charles E.; Rivest, Ronald L.;Stein Clifford; Algoritmos Teoria e Prática; Editora Elsevier; 2002

CROSS, Simon S.; Harrison, Robert F.; Kennedy, R. Lee. "*Introduction to neural networks*", Lancet,. 1995.

CROUHY, M; GALAI, D; MARK, R. *Risk Management*, New York, McGraw Hill, 2001.

CRUZ, M. "Modelagem Quantitativa de Risco Operacional". In: Duarte Jr., A.M., Varga, G. (org.) Gestão de Riscos no Brasil. Rio de Janeiro, Financial Consultoria, 2003.

CUSTÓDIO, R. F.; Graaf, J.; Dahab, R.; "GT Infra-estrutura de chaves públicas para o âmbito acadêmico (ICP-EDU)", 2003, Disponível em: <http://www.rnp.br/pd/gts2004-2005/chaves_publicas.html>. Acesso em: 02 out.2007

DAMELINCOURT, Jérome, "*Modèle de Kohonen*", VieArtificielle.com, Disponível em: <http://www.vieartificielle.com/article/?id=62>. França. Acesso em: 20 out. 2007.

DANTAS, Marcos. A Lógica do Capital-Informação: a fragmentação dos monopólios e a monopolização dos fragmentos num mundo comunicações globais.2 ed. Rio de Janeiro:Contraponto, 1996.

Departament of Justice USA (1995), Executive, "*Order 12,958 - Classified National Security Information*", Disponível em:<http:www.usdoj.gov> , Acesso em: 22 dez. 2007.

DUARTE Jr., A. M.Risco: definições, tipos, medição e recomendações para seu gerenciamento. Resenha BM&F, n. 114, dez. 1996. Disponível em:<http://www2.bmf.com.br/cimConteudo/W_ArtigosPeriodicos/00752004.pdf >. Acesso em : 20 out. 2007.

DYBOWSKI, Richard; Gant, Vanya. *Artificial neural networks in pathology ans medical laboratories*, 1995.

ESTOCK, K. "*Nifty neural networks*", Independent Banker, 1999.

Exame Vip, "Seu dinheiro vai acabar", edição 264, publicação em abril/2007.

FARAHMAND F., S. B. Navathe, G. P. Sharp, and P. H. Enslow. Managing "*Vulnerabilities of Information Systems to Security Incidents*". Communications of the ACM, 2003.

FAUSETT, L. V, "*Fundamentals of Neural Networks*", New Jersey: Prentice-Hall PTR,. Cérebro humano, 1994

FAYYAD, M.U., Piatesky-Shapiro, G., Smuth P., Uthurusamy, R. (1996). Advances in Knowledge Discovery and Data Mining. AAAI Press.

FERNANDES, D. M., Criptografia Quântica, Artigo, 2001. Disponível em: <http://www.gta.ufrj.br/grad/01_2/cripto/>. Acesso em 2 ago. 2007

FERRAIOLO D. F., Kuhn D. R., Chandramouli R., *Computer Security Series Role-Based Access Control,* Artech House Inc, 2003;

FORSSTRÖM, Jari J.; Dalton, Kevin J. "*Artificial neural networks for decision support in clinical medicine*", Annals of Medicine; 1995.

FRANCISCO, Claudia Aparecida Cavalheiro, Rede de Kohonen: Uma ferramenta no estudo das relações tróficas entre as espécies de peixes. Curitiba: Universidade Federal do Paraná, 2004;

GARFINKEL, S.; Spafford, G.; *Practical Unix and Internet Security*, O'Reilley & Associates, 1996;

GEER D. Jr, Hoo K. S., and Jaquith A. *Information Security: Why the Future Belongs to The Quants*,IEEE Security & Privacy, Vol. 1, No. 4, pp. 24-32, 2003.

GITMAN, Lawrence J. Princípios de administração financeira. São Paulo: Harbra, 1997.

GOLLMANN D. "*Computer Security*". John Wiley & Sons. Inc., 605 Third Avenue, New York, NY 10158-0012, 1999.

GUHA, S., Rastogi, R., and Shim K. (1998). CURE: An Efficient Clustering Algorithm for Large Databases. In Proceedings of the ACM SIGMOD Conference.

HAIR J.F.; Anderson R. E., Tatham R. L.; Black W.C.; *Multivariate Data Analisys*. EdHaykin, S. Neural Networks: "*Comprehensive Foundation*", New Jersey: Prentice-Hall, 1999.

HAYKIN, S., "Redes Neurais: Princípios e prática", Ed. Bookman, 2001;

IOSCO. *International Organization of Securities Comissions*. *Risk Management and Control Guidance for Securities Firms and Their Supervisors*. Disponível em: <http://www.iosco.org>. Acesso em 13 out. 2007.

ISO-International Organization for Standardization; 2005, Disponível em: <http://www.iso.org>. Acesso em: 22 jul. 2007.

ITGI-IT Governance Institute, *Framework Control Objectives. Management Guidelines Maturity Models* (2007), Disponível em: <http://www.itgi.org>, Acesso em: 17 ago. 2007.

JORION, P. *Value at Risk: The New Benchmark for Controlling Market Risk.* New York: Mc Graw Hill, 1997.

KIRBY, Yvonne Kochera; Mcnew, Ronald W.; Kirby, John D.; Wideman Jr., Robert F. "*Evaluation of logistic versus linear regression models for prediting pulmonary hypertension syndrome (Ascites) using cold exposure or pulmonary artery clamp models in broilers*", Poultry Science, 1999.

KOHONEN, T., *Self-Organizing Maps*, Berlin: Springer-Verlag, 2001.

KOVÁCS, Zsolt lászló. "Redes Neurais Artificiais: fundamentos e Aplicações: um texto básico", 1996.

KUONG J. F., *Computer Security, Auditing and Controls*.Management Advisory Publications Series on, 1974;

KURTZMAN, J. A Morte do Dinheiro (Como a economia eletrônica desestabilizou os mercados mundiais e criou o caos financeiro). São Paulo: Atlas, 1995.

LAKATOS, E. M. & MARCONI, M. A., *Metodologia científica*. 2 a. ed., São Paulo, 1995.

LEE, A.; Ulbricht, C.; Dorffner, G. "*Application of artificial neural networks for detection of abnormal fetal heart rate pattern: a comparasion with conventional algorithms*", 1999.

LÉVY, P. "O Que é Virtual". São Paulo: Ed. 34, 1997.

MARSHALL, C. "Medindo e Gerenciando o Risco Operacional em Instituições Financeiras", Qualitymark, 2002.

NEGROPONTE, Nicholas "Civilização Digital".Coletânea HSM Management e-business e tecnologia – Atores e Conceitos Imprescindíveis, 2001.

NETO, Luis Garcia Palma; Nicoletti, Maria do Carmo,. Introdução às Redes Neurais Construtivas. São Carlos: Edufscar, 2005;

NIST- *National Institute of Standards and Technology* (2000), "*Managing Technical Risk:Understanding Private Sector Decision Making on Early Stage, Technology-based Projects*", Disponível em: <http://www.nist.gov>, Acesso em 3 nov. 2007

NIST- *National Institute of Standards and Technology* (2002), *Risk Management Guide for Information Technology System*, Disponível em: <http://www.nist.gov>, Acesso em:20 out. 2007

NIST- *National Institute of Standards and Technology* (2004 a), "*Security Consideration in the Information System Development Life Cycle*", Disponível em: <http://www.nist.gov>, Acesso em 20 out. 2007

NIST- *National Institute of Standards and Technology* (2004 b), "*Standards for Security Categorization of Federal Information and Information System*", Disponível em: <http://www.nist.gov>, Acesso em 24 out. 2007

O'SULLIVAN, O. "*Who's that knocking on my portal?*", US Banker, 1999.

PEREIRA, L. de C. "O Risco Operacional em Instituições Financeiras e a Influência de Fatores do Ambiente Externo", Dissertação de Mestrado Apresentada ao Programa de Pós-Graduação em Economia, da Universidade Federal de Santa Catarina. Florianópolis, junho de 2004a.

PLATAFORMA LATTES (2007); Disponível em: <http://lattes.cnpq.br>; Acesso em 3 fev. 2007.

REZAEE, R., Lelieveldt, B.P.F., and Reiber, J.H.C. (1998). A New Cluster Validity Index for the Fuzzy c-Mean.Pattern Recognition Letters.

REZENDE, Pedro Antonio Dourado de; "Sobre a criação da ICP-Brasil"; Depto. Da Ciência da Computação – Universidade Federal de Brasília, Artigo, 2001. Disponível em <http://www.cic.unb.br/docentes/pedro/trabs/ICP.htm#2.> Acesso em 9 out. 2007.

ROSENBLATT, Frank "*The perceptron: a probabilistic model for information storage and organization in the brain*". Psychological Review, 1958

ROUSH, W. B.; Kirby, Y. Kochera; Cravener, T. L.; Wideman Jr., R.F. "*Artificial neural network prediction of ascites in broilers*", Poultry Science, 1996.

ROUSSINOV, D. G., Chen, H., "*Information navigation on the web by clustering and summarizing query results*", Information Processing and Management, 37(6):pp.789-816, 2001.

RUSSELL, S. J. and Norvig, P., Inteligência Artificial, 2. ed., Campus, 2004.

SALMON, P., História e Critica, Coimbra, Editora Almedina, 1979

SCHNEIER, B., Segurança.com: Segredos e Mentiras sobre a Proteção Digital; Rio de Janeiro; Campus, 2001

STALLINGS, W., *Redes e Sistemas de Comunicação de Dados*, 5ª.edição, São Paulo, Elsevier Editora, 2005

SUURONEN, Tomi. *Java2 Implementation of Self-Organizing Maps based on Neural Networks utilizing XML based Application Languages for Information Exchange and Visualization*. Espoo: Vantaa Institute of Technology Departament, 2001.

TANENBAUM, Andrew S.; "Redes de Computadores"; 2003

THEODORIDIS, S. and Koutroubas, K. (1999). Pattern Recognition. Academic Press.

THE ECONOMIST, "*Digital money – The end of the cash era*", publicada em 15/2/2007; Disponível em: <hppt://www.economist.com/opinion/displaystory.cfm?story_id=8702890>, acesso em: 13 jun. 2007.

THOLUDUR, Arun; Ramirez, W. Fred, "*Neural-network modeling and optimization of induced foreign protein production*", AIChE Journal, 1999.

TOP500 ORGANIZATION, 2006, Disponível na Internet http:www.top500.org. Acesso em 30 mar. 2007;

TORANZOS, Fausto I. Estatística. São Paulo: Mestre Jou, 1969.

UNGARETTI, Ricardo; Revista Com Ciência; "O uso de software livre em criptografia: razões históricas"; Artigo publicado em, 2002

UYSAL, M.; El ROUBI, M. S. '*Artificial neural networks versus multiple regresión in tourim demand analisys*", Journal of travel research, 1999.

VASCONCELOS, Nivaldo Antônio Portela de. Mapas Auto-Organizativos e suas Aplicações. Rio de Janeiro, Universidade Federal do Rio de Janeiro, 2000.

VEJA REVISTA, edição 2012 "Biologia – Em busca da Vida Artificial", 13/06/2007

VESANTO, J.; Himberg, J.; Alhoniemi, E.; Parhankangas. J. *SOM Toolbox for Matlab 5*, Espoo, Helsinki University of Technology, 2000

WANGENHEIM, Aldo Von. Reconhecimento de Padrões. Florianópolis: Universidade Federal de Santa Catarina. Disponível na Internet em: http://www.inf.ufsc.br/~awangenh/RP/subsimbolicas1.pdf. Acesso em: 23 nov. 2007

XIN, H. "*Assessing swine thermal confort by image analysis of postural behaviors*", 1999.

BIBLIOGRAFIA COMPLEMENTAR

AIDAR, Carlos Miguel e Costa, Marcos; Jornal Folha de São Paulo; "Velha burocracia e novos arapongas virtuais"; publicada em 17.7.2001

ANNONYMOUS MAXIMUM SECURITY. Sams Publishing, 201 West 103rd St., Indiana, 46290 USA, 2003.

ASSESSORIA DE COMUNICAÇÃO DO CONSELHO DA JUSTIÇA FEDERAL, "Momento histórico marca união dos tribunais em prol da modernização", 03.10.2005. Disponível em: <http://www.iti.br/twiki/bin/view/Main/PressRelease2005Oct03A>. Acesso em 12 out. 2007

ATHENIENSE, Alexandre R.. A Privacidade na ICP-Brasil, 2002, Disponível em: <http://www.revistajuridicaunicoc.com.br/midia/arquivos/ArquivoID_24.pdf>. Acesso em: 21 out. 2006.

ATHENIENSE, Alexandre, Artigo “ICP-Brasil ABDI irá discutir projeto de lei em Belo Horizonte”, Revista Consultor Jurídico, 6 de junho de 2002. Disponível em: <http://conjur.estadao.com.br/static/text/12498,1>. Acesso em 16 nov. 2007.

BORGES, J. P. V; Padilha, T. P. P. Modelagem do Processo de Aprendizado Colaborativo Através de Redes Bayesianas. In: VII Encontro de Estudantes de Informática do Estado de Tocantins, 2005, Palmas. Palmas, 2005.

BURGOS, Frederico; Guimarães L. Germano e, Carvalho, Paulo Roberto A., Grupo de Trabalho de Segurança do Sistema de Pagamentos Brasileiro, “Manual de Segurança de Mensagens do SPB” versão 2.3, dezembro.2005. Disponível em: <http://www.bcb.gov.br/?SPBSEGUR>, Acesso em: 8 nov.2007

CARVALHO, S. D. de, Martins, W. (2005) “Mapas auto-organizáveis Aplicados a sistemas tutores inteligentes”, Revista da Escola de Engenharia Elétrica e de Computação, Universidade Federal de Goiás, Disponível em: <http://www.alfa.br/revista/pdf/1.pdf> Acesso em: 5 dez.2007.

CHANDLER, Jr. A. D. .*Strategy and Structure: chapters in the history of the industrial enterprise*, 19th ed. MIT Press, Cambridge, Massachusetts, 1995.

CONSULTOR JURÍDICO, revista; “Mais agilidade STJ passar a integrar comitê gestor de ICP Brasil”; 23 de março de 2005. Disponível em: <http://conjur.estadao.com.br/static/text/33716,1>. Acesso em: 7 set. 2006

CONSULTOR JURÍDICO; ”STJ passa a integrar comitê gestor de ICP Brasil” (2005). Disponível em: <http://conjur.estadao.com.br/static/text/33716>, Acesso em: 15 dez.2007.

CUSTÓDIO, Ricardo F., “GT ICP EDU II”, 2005, Disponível em: <http://www.rnp.br/pd/gts2004-2005/chaves_publicas.html>. Acesso em: 12 agosto 2007.

DEBAN (Departamento de Operações Bancárias e de sistemas de Pagamentos) do Banco Central do Brasil, “Sistema de Pagamentos Brasileiro”, dezembro.2004, Disponível em <http://www.bcb.gov.br/htms/novaPaginaSPB/spb-textocompleto-pdf.pdf>. Acesso em: 28 dez. 2007.

EGAN, M. David; Mather, Tim, “*The executive Guide to Information Security: Threats, Challenges and Solutions*”, 2005;

ELETRÔNICO, Governo, “Código aberto Netscape também terá o certificado digital brasileiro”, Revista Consultor Jurídico, 31.03.2003. Disponível em: < http://conjur.estadao.com.br/static/text/6387,1>. Acesso em 10 out. 2007.

FLORENZANO, M. B. Borba; “Moeda e Concepção de Valor na Polis Grega”, Boletim do CPA, Campinas, nº 4, jul./dez. 1997, Disponível: <http://venus.ifch.unicamp.br/cpa/boletim/boletim04/16florenzano.pdf>, Acesso em: 13 jun.2007.

GALBRAITH, J. K. “Uma Breve História da Euforia Financeira”. São Paulo: Pioneira, 1992.

GERCHMANN, L**. .**Mulheres depredam Fábrica de Celulose no Rio Grande do sul. Jornal Folha de São Paulo, 9 março 2006.

GIARRATANO, Joseph; Riley, Gary. “*Experts Systems – Principles and Programming*”. EUA: PWS Publishing Company, 1998.

GOODMAN, P.H.; Harrel Jr, F.E. *Neural networks: advantages and limitations for bioestatistical modeling*”, 1999. Disponível em: <www.scs.unr.edu/nevprop>.Acesso em: 25 nov.2007.

GRAAF, Jeroen van de, Laboratório de Computação Científica (LCC/UFMG), “GT ICP3-EDU - Smart card virtual e autoridade certificadora distribuída”, 2006. Disponível em: < http://www.rnp.br/pd/gts2005-2006/icp-edu.html>. Acesso em: 12 dez. 2007.

HERTZ, J., Krogh, A., Palmer, R. G. “*Introduction to the theory of neural computation*”, Boston Addison-Wesley Longman Publishing Co, 1991.

HONKELA, T., “*Self-Organizing Maps in Natural Language Processing*” Tese de Doutorado. Universidade de Tecnologia de Helsinki, Finlândia., 1997.

HOWGEGO, C. “*Ancient History from Coins*”, Routledge, 1995.

INSTITUTE OF DIRECTORS. “*The King Report on Corporate Governance for South Africa*”, Institute of Directors, South Africa, 2002.

INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO, Cartilha “Certificação Digital entenda e utilize”, julho.2005. Disponível em: <http://www.iti.br/twiki/pub/Main/Cartilhas/brochura01.pdf>. Acesso em: 8 dez. 2007.

JACKSON, Peter. “*Introduction to Expert Systems*”. EUA: Addison Wesley, 1990.

KELLER, Robert. Tecnologia de Sistemas Especialista – Desenvolvimento e Aplicação. São Paulo: Makron Books, 1991.

KRITZINGER-von Solms E. and L. A. M. Strous. “*Information Security: a Corporate Governance Issue*”. Integrity and Internal Control in Information Systems V, 2003.

LACROIX, L. Monnaie et Colonisation dans l’Occident Grec. Bruxelas, 1966.

LÉVY, P., As Tecnologias da Inteligência: O Futuro do Pensamento na era da Informática, Editora 34, 1993.

LISKA A. *The Practice of Network Security*. Prentice Hall, Upper Saddle River, New Jersey 07458, 2003.

MADUEÑO, Denise. Jornal Folha de São Paulo; São Paulo 5. jul.2001

MARCHIORI, P. Z., (2002).Gestão da Informação Compatibilidade Profissional. Disponível em: <http:www.scielo.Br>.Acesso em: 11 out. 2007.

MARKOWITZ, H. M., Portfolio Selection. Journal of Finance, 1952.

MARQUES, R. L.; Dutra, Inês. Redes Bayesianas: o que são, para que servem, algoritmos e exemplos de aplicações. Rio de Janeiro:Universidade Federal do Rio de Janeiro, , Disponível em: <http://www.cos.ufrj.br/~ines/courses/cos740/leila/cos740/Bayesianas.pdf> Acesso em: 27 dez. 2007.

MARTIN,T. “Why did the Greek polis originally need coins?” Historia, 1996.

MEDIDA PROVISÓRIA No. 2200-2 de 24 de agosto de 2001 Institui a Infra-estrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituo Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

MICROSOFT CORPORATION. Deloitte & Touche *Employees Use Digital Dashboard to Drive Success and Work/Life Balance*. Technical report, Disponível em: <http://www.microsoft.com/resources/casestudies/CaseStudy.asp?casestudyid =11627>, Acesso em: 20 abril 2004.

NGUYEN, Hung T. Walker, Elbert A. *A first course in Fuzzy Logic*. EUA: Chapman & Hall/CRC, 2000.

OLIVEIRA, Evandro. ICP-Brasil Evolução com equilíbrio e correção, 2002.Disponível em: <http://www.prodemge.mg.gov.br/revistafonte/arquivos_pdf/icp-brasil.pdf>. Acesso em: 02 agosto 2006.

OSBORNE,R.; *Greece in the making*; B.C. Routledge,1996.

PEARL, Judea; Russel, Stuart. *Bayesian Networks*. Los Angeles:University of California, UCLA Cognitive Systems Laboratory - Technical Report , 2000.

PEROTTO, Filipo Studzinski, Modelagem do Conhecimento, Sistemas Especialistas e o Projeto SEAMED. Porto Alegre:Universidade Federal do Rio Grande do Sul, 2001. Disponível em: <http://www.sbc.org.br/reic/edicoes/2001e1/cientificos/Modelagem_do_Conhecimento_Sistemas_Especialistas_e_o_Projeto_SEAMED.pdf>.Acesso em: 18 dez. 2006

REDE NACIONAL DE PESQUISA - RNP, *Growing interaction between security groups of the Brazilian and Spanish academic networks - CAIS’s analyst was a juror in Rediris’s challenge*, abril 2004. Disponível em: <http://www.rnp.br/en/news/2004/not-040412.html >. Acesso em: 2 jun. 2006

REZENDE, Pedro Antonio Dourado de, Privacidade e Riscos num Mundo de Chaves Públicas, out. 2003. Disponível em: <http://www.cic.unb.br/docentes/pedro/sd.htm >. Acesso em: 2 dez. 2006.

STONEBURNER G., A. Goguen, and A. Feringa. *Risk Management Guide for Information Technology Systems*. Technical report, National Institute of

STANDARDS AND TECHNOLOGY, Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>, Acesso em: 17 abril 2004.

TANSCHEIT, Ricardo. Sistemas Fuzzy. Rio de Janeiro: Pontifícia Universidade Católica, 2007. Disponível na Internet em: < http://www.ica.ele.puc-rio.br/cursos/download/ICA-Sistemas%20Fuzzy.pdf> Acesso em: 10 jan. 2007

Information Security Risk Assessment Practices of Leading Organizations. Technical report, United States General Accounting. Disponível em:<http://www.gao.gov/special.pubs/ai00033.pdf>, Acesso em: 17 abril 2007.

Bancos tentam descobrir o novo papel das agências. Valor Econômico,São Paulo, 21 junho.2007. Seção de Finanças.

ZADEH, Lotfi A.; Kacprzyk, Janusz. "*Computing with words in Information Intelligent System I – Foundation*", EUA: Physica-Verlag, 1999.