“Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE”

Viviane Luciana de Oliveira

Trabalho Final de Mestrado Profissional em Computação

Instituto de Computação

Universidade Estadual de Campinas

Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE

Viviane Luciana de Oliveira

Campinas, 23 de fevereiro de 2006

Banca Examinadora:

- **Prof. Dr. Antonio Montes**
  CenPRA - Centro de Pesquisas Renato Archer
- **Prof. Dr. Célio Cardoso Guimarães (Suplente)**
  Instituto de Computação – IC / UNICAMP
- **Prof. Dr. Julio César López Hernández**
  Instituto de Computação – IC / UNICAMP
- **Prof. Dr. Marco Aurélio do Amaral Henriques (Suplente)**
  Depto. de Computação e Automação Industrial - Fac. de Eng. Elétrica e de Computação - UNICAMP
- **Prof. Dr. Ricardo Dahab (Orientador)**
  Instituto de Computação – IC / UNICAMP

FICHA CATALOGRÁFICA ELABORADA PELA
BIBLIOTECA DO IMECC DA UNICAMP

Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Oliveira, Viviane Luciana de

OL4u Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE / Viviane Luciana de Oliveira -- Campinas, [S.P. :s.n.], 2006.

Orientador : Ricardo Dahab

Trabalho final (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Computação.

1. Publicação especial NIST. Segurança da informação. 2. Octave. 3. Gerenciamento de risco. I. Dahab, Ricardo. II. Universidade Estadual de Campinas. Instituto de Computação. III. Título.

Título em inglês: A comparative study of risk management methodologies FIRM, NIST SP 800-30 and OCTAVE

Palavras-chave em inglês (Keywords):1. NIST special publication. Information security. 2. Octave. 3. Risk management.

Área de concentração: Metodologia e Técnicas de Computação

Titulação: Mestre em Computação

Banca examinadora: Prof. Dr. Ricardo Dahab (IC-UNICAMP)
Prof. Dr. Antonio Montes (CenPRA)
Prof. Dr. Julio César López Hernández (IC-UNICAMP)

Data da defesa: 23/02/2006

“Uma análise comparativa das metodologias de gerenciamento de risco FIRM, NIST SP 800-30 e OCTAVE”

Este exemplar corresponde à redação final do Trabalho Final devidamente corrigido e defendido por Viviane Luciana de Oliveira e aprovado pela Banca Examinadora.

Campinas, 23 de fevereiro de 2006.

Orientador: Prof. Dr. Ricardo Dahab

Trabalho Final apresentado ao Instituto de Computação, UNICAMP, como requisito parcial para obtenção do título de Mestre em Computação na área de Engenharia de Computação.

À DEUS por me dar tantas oportunidades e permitir que eu tenha pessoas tão boas perto de mim...

Aos MEUS PAIS: Neide e Olimpio por tudo que fizeram e fazem por mim, pela força nas horas difíceis, pela dedicação incondicional....

Ao MEU AVÔ: Francisco que sempre torceu por mim e estará para sempre em minha memória e em meu coração...

Aos MEUS IRMÃOS: Marco e Cássio por sempre me incentivarem e me auxiliarem em tudo que estava ao alcance deles...

Agradecimentos

Ao meu orientador Prof. Dr. Ricardo Dahab agradeço pelo apoio e orientação durante o desenvolvimento deste trabalho, e pelo empenho em torná-lo um material que agregasse valor ao leitor.

À PricewaterhouseCoopers, em especial ao sócio Edgar D'Andrea e ao gerente Sérgio Alexandre pelo incentivo e por permitirem que eu me ausentasse algumas vezes durante o expediente para que eu pudesse comparecer à UNICAMP.

À minha amiga Betânia Ricci Bôer por ser uma grande companheira durante o curso, e por sempre me dar dicas quanto a elaboração dessa dissertação.

Ao Walter Yajima pelo carinho, companheirismo, e pelas críticas construtivas que contribuíram para o aprimoramento deste trabalho.

Resumo

O Gerenciamento de Risco de TI têm se tornado uma preocupação constante das organizações, em função da importância que o ambiente tecnológico passou a representar para o negócio das empresas ao longo das últimas décadas. Concomitantemente, cada vez mais as empresas têm de estar aderentes às regulamentações externas que afetam o nicho de mercado em que estão inseridas. O Gerenciamento do Risco, em particular, é um requerimento sujeito a essas regras. Entender e tratar adequadamente tais riscos, visando minimizar impactos negativos nas operações das organizações é o principal objetivo do processo de Gerenciamento de Risco de TI. A escolha de uma boa metodologia de Gerenciamento de Risco de TI, adaptada às necessidades da organização, é um dos requisitos chaves para o sucesso deste processo. Nessa dissertação discutiremos todo o conceito relacionado ao tema Gerenciamento de Risco de TI, e compararemos três metodologias de Gerenciamento de Risco de TI amplamente utilizadas.

Abstract

Information Technology (IT) Risk Management has become a continuous concern for organizations due to the increasing importance technology has had to business over the past few decades. Simultaneously, more and more companies need to be compliant with external regulatory rules which affect the market where they act. Risk management, in particular, is a requirement subject to those rules. To understand, and properly treat, IT related risks in order to minimize negative impacts in an organization's operations is the main objective of the IT Risk Management process. Choosing a good methodology, adapted to the company's needs, is one of the key requirements for the success of this process. In this work, the conceptual background of IT Risk Management is discussed and three widely used IT Risk Management methodologies are discussed and compared.

Índice

Lista de Figuras

Lista de Tabelas

Capítulo 1 - Introdução

1.1 Motivação

O processo de Gerenciamento de Risco de Tecnologia da Informação (doravante denominado Gerenciamento de Risco de TI) visa identificar e mitigar os riscos inerentes aos ativos[1] de tecnologia que possam vir a comprometer as operações da organização, impedindo que esta possa atingir seus objetivos de negócio.

Quando a atividade principal da organização depende fortemente da tecnologia, os riscos de Tecnologia da Informação podem se transformar em riscos para o negócio, e as falhas na proteção dos ativos de TI se traduzem diretamente em perdas financeiras, comprometimento da imagem, ou redução na eficiência operacional.

As empresas precisam criar e manter um ambiente tecnológico no qual os processos de negócio possam funcionar corretamente. Esse mesmo ambiente necessita manter a confidencialidade e privacidade dos dados da organização, bem como assegurar sua integridade. O alcance de tais objetivos não depende necessariamente da implantação de hardware e software, mas muitas vezes da realização de processo de Gerenciamento de Risco de TI eficiente, no qual todos os riscos estejam mapeados e as estratégias de mitigação contempladas.

O processo de Gerenciamento de Risco é um componente necessário da estratégia de qualquer negócio, e o processo de Gerenciamento de Risco de TI está inserido no mesmo contexto. Encontrar o balanceamento adequado entre aceitar o risco, ou arcar com os custos de perda e seguro, e o custo de proteção, é uma das chaves do sucesso para o negócio.

---

[1] São considerados ativos: informações, hardware, software, documentação, dispositivos de infra-estrutura, dentre outros.

A inexistência de trabalhos nesse segmento, bem como a relevância que tem se dado ao aspecto do risco atualmente, contribuíram para a escolha do tema. Para muitas organizações, o Gerenciamento de Risco de TI, está entre os principais riscos que necessitam ser gerenciados. Esse nível de significância decorre de quatro principais tendências:

- as organizações aumentaram a dependência dos processos de negócios em seus sistemas de informação;
- a escala de investimento necessária para manter o ambiente tecnológico atualizado e protegido é alta, sendo necessário um correto balanceamento entre o investimento efetuado e o retorno obtido;
- o crescimento contínuo das vulnerabilidades nos sistemas;
- a descoberta constante de novas tecnologias e outras formas de realizar negócios; e
- requerimentos legais, por exemplo a lei Sarbanes Oxley[2].

Outros fatores que também contribuíram para a escolha do tema foram identificados a partir da minha experiência profissional na área de Gerenciamento de Risco e Segurança da Informação, os quais incluem:

- a dificuldade das empresas em estabelecer e conduzir um processo de Gerenciamento de Risco de TI eficaz;
- o baixo conhecimento das organizações quanto à existência de metodologias de Gerenciamento de Risco de TI;

[2] Sarbanes Oxley – lei de reforma corporativa, emitida pelo Congresso dos EUA que gera um conjunto de novas responsabilidades e sanções aos administradores com o objetivo de coibir práticas lesivas que possam expor as sociedades anônimas a elevados níveis de risco. No Brasil esta lei se aplica às empresas com ações negociadas no mercado de capitais dos EUA, multinacionais de capital americano, e empresas brasileiras com "American Depositary Receipts (ADRs)" nos EUA.

- a inexistência de um estudo sistemático que analise os aspectos positivos e negativos de cada metodologia, permitindo que as empresas consigam identificar qual se adapta melhor às necessidades da organização; e
- pouca literatura nacional sobre o tema.

1.2 Objetivos

Essa dissertação tem por objetivo apresentar todo o ciclo para condução do processo de Gerenciamento de Risco de TI, desde a identificação dos riscos até a escolha dos controles necessários para mitigação dos mesmos.

Adicionalmente, esse trabalho busca apresentar como diferentes metodologias de Gerenciamento de Risco de TI abordam o tema, apresentando, quando aplicável, os aspectos positivos e negativos existentes em cada uma delas.

1.3 Contribuições

As principais contribuições dessa dissertação são:

- apresentar os principais conceitos relacionados ao tema Gerenciamento de Risco de TI;

- justificar a importância da condução do processo de Gerenciamento de Risco de TI, apresentando os principais benefícios obtidos pelas empresas que o efetuam regularmente seguindo uma metodologia apropriada;

- fornecer aos Gestores de TI e profissionais que atuam nas áreas de Segurança da Informação e Gestão de Risco diretrizes de como o

processo de Gerenciamento de Risco de TI deve ser conduzido, para que a organização obtenha êxito em relação ao mesmo;

- discutir os aspectos positivos e negativos das metodologias de Gerenciamento de Risco de TI comumente empregadas, visando facilitar a análise de qual está mais aderente às necessidades da organização; e

- fornecer aos Gestores de TI um questionário contemplando os principais aspectos de TI a serem verificados durante a identificação dos riscos (Apêndice A).

1.4 Organização deste documento

Esta dissertação está estruturada em cinco capítulos, conforme segue:

- **Capítulo 1** – Introdução

- O **Capítulo 2 – O processo de Gerenciamento de Risco de TI** apresenta os principais desafios referentes à implementação de um processo de Gerenciamento de Risco de TI; a definição das principais terminologias associadas ao tema, visando facilitar o entendimento do leitor ao longo desta dissertação; e todo o ciclo de Gerenciamento de Risco de TI, o qual engloba identificação dos riscos, mitigação e monitoramento.

- O **Capítulo 3 – Análise das metodologias de Gerenciamento de Risco de TI: FIRM, NIST SP 800-30 e OCTAVE** apresenta sucintamente cada uma das metodologias, bem como a análise comparativa dos principais aspectos que compõem o processo de Gerenciamento de Risco de TI, ressaltando, sempre que aplicável, quais os aspectos positivos e negativos de cada uma delas.

- O **Capítulo 4 – Conclusão** apresenta as conclusões sobre a análise efetuada de cada uma das metodologias.

- O **Capítulo 5 – Bibliografia** relaciona toda referência bibliográfica consultada para elaboração dessa dissertação.

Capítulo 2 - O processo de Gerenciamento de Risco de TI

2.1 Introdução

Esse capítulo tem por objetivo: (1) demonstrar os principais desafios intrínsecos ao tema Gerenciamento de Risco de TI; (2) apresentar as terminologias associadas ao conceito de Gerenciamento de Risco de TI com o intuito de facilitar o entendimento ao longo dessa dissertação; e, por fim, (3) descrever o ciclo básico de Gerenciamento de Risco de TI: identificação dos riscos, mitigação e monitoramento.

Uma das finalidades desse capítulo é familiarizar o leitor com o tema, o que irá contribuir para a correta compreensão da análise comparativa apresentada no Capítulo 3, bem como para o entendimento da relevância dos aspectos escolhidos para a referida análise.

2.2 Considerações sobre o processo de Gerenciamento de Risco de TI

À medida que os recursos tecnológicos se tornaram um importante habilitador dos negócios da organização, a aplicação das noções de Gerenciamento de Risco de TI se tornou essencial. Muitas organizações acreditavam que o processo de Gerenciamento de Risco de TI estava atrelado somente à adoção de soluções tecnológicas eficazes, sejam estas hardware ou software. Durante muito tempo esta visão deturpada contribuiu para justificar o não estabelecimento de um processo de Gerenciamento de Risco de TI, visto que a cada ano os recursos financeiros destinados à área de Tecnologia se tornaram cada vez mais escassos.

A responsabilidade pelo processo de Gerenciamento de Risco de TI recai, na grande maioria das vezes, nos gestores de tecnologia. Entretanto, não existe um consenso sobre qual a melhor maneira de conduzir esse processo. Em geral, os gestores buscam balancear os riscos aos quais as organizações estão suscetíveis e suas respectivas conseqüências, com os custos envolvidos na

minimização dos riscos; entretanto, o ponto de equilíbrio varia largamente. Alguns gestores são altamente avessos ao risco, outros são 'tomadores' do risco. O único ponto que há em comum entre essas duas categorias é que, ambos reconhecem a importância de se ter um adequado conhecimento e compreensão de todos os riscos de TI, bem como dos componentes de negócio impactados pelos mesmos.

As empresas devem ser cautelosas no entendimento da verdadeira natureza dos riscos. Se os gestores forem extremamente rígidos na contenção dos riscos, os gastos com a minimização dos mesmos serão elevados, podendo causar implicações financeiras significativas, que venham a reduzir a vantagem competitiva da organização perante o mercado no qual atua. Concomitantemente, caso os riscos sejam tratados com descrédito, incidentes inesperados podem ocorrer, com os mais variados impactos, podendo inclusive tirar a organização do mercado. Cabe destacar que nem sempre os riscos aos quais a organização está sujeita são óbvios, e até mesmo a existência de um programa de Gerenciamento de Risco de TI bem estruturado pode não conseguir identificá-los.

De modo algum estamos contradizendo a eficácia do programa de Gerenciamento de Risco de TI; ressaltamos apenas que a instauração desse deve ser feita de modo abrangente e estruturado. O objetivo do Gerenciamento de Risco de TI não é eliminar todos os riscos em sua plenitude, mas sim reduzí-los a um nível aceitável, onde as falhas estão previstas e consideradas dentro deste limite. Em geral, as empresas podem se posicionar de quatro formas distintas perante o risco: aceitar, reduzir / controlar, transferir (adoção de seguros) ou evitar.

Conforme COHEN (2003; p. 9), há diferentes abordagens para implementação de um programa de Gerenciamento de Risco de TI. Assim, para a adoção do modelo que melhor se adapte às necessidades da organização, alguns fatores devem ser considerados, dentre eles a quantidade de esforço necessário para condução do processo, os riscos envolvidos na situação (tecnológicos ou procedurais) e a quantidade de informações disponíveis para determinação dos riscos.

2.2.1 Principais desafios do processo de Gerenciamento de Risco de TI

A identificação dos riscos relacionados à tecnologia da informação é o processo mais difícil de ser conduzido, quando comparado aos demais tipos de riscos. Isso decorre principalmente da dificuldade de mensuração da probabilidade de incidência das ameaças e respectivos custos associados com os impactos causados, conforme mencionado abaixo:

- alguns custos, tais como a perda de confidencialidade, integridade ou disponibilidade são difíceis de se quantificar;

- embora o custo de hardware e software seja possível de se estimar, muitas vezes não é possível precisar os custos indiretos envolvidos, tais como possíveis perdas de produtividade que podem ocorrer quando novos controles são implementados, ou quando os controles existentes estão comprometidos; e

- falhas na obtenção de informações atualizadas e precisas podem dificultar o processo de determinação de quais riscos tecnológicos são mais significativos para o negócio da organização, bem como quais controles são mais efetivos, quando avaliados sob a ótica do custo x benefício.

Outro ponto a ser destacado é que muitas organizações fazem algumas suposições e cometem ações errôneas no processo de Gerenciamento de Risco de TI, dentre elas:

- a confiança nos sistemas existentes e controles adotados tende a crescer com o passar do tempo; assim, o mapeamento dos possíveis riscos não se faz necessário, exceto no caso em que exista algum motivo para contradizer essa premissa;

- as gerências de nível médio e a alta administração negligenciam a adoção de controles preventivos;

- as gerências de nível médio possuem um entendimento incorreto ou descaracterizado das ameaças;

- as gerências ignoram o efeito do tempo, ou seja, não reconhecem a necessidade da análise de risco ser realizada periodicamente;

- as organizações adotam uma abordagem reativa e resistente quanto ao Gerenciamento de Risco de TI, visto que não há um retorno financeiro imediato sobre essa atividade;

- as gerências ignoram as interdependências entre os recursos tecnológicos e perdas indiretas ocorridas;

- as organizações subestimam as implicações das mudanças incrementais, ou seja, sempre que mudanças são feitas na organização, outras vulnerabilidades podem ser introduzidas;

- o processo de Gerenciamento de Risco de TI é conduzido por profissionais sem o adequado preparo, impedindo a identificação dos riscos; e

- as vulnerabilidades são agrupadas inadequadamente, fazendo com que algumas fragilidades não fiquem em evidência.

Nas seções “2.3 Conceitos preliminares” e “2.4 O processo de Gerenciamento de Risco de TI: identificação; mitigação e monitoramento” apresentaremos os principais conceitos referentes ao tema e o ciclo básico de Gerenciamento de Risco de TI.

2.3 Conceitos preliminares

2.3.1 Risco

O risco pode ser classificado e tratado como uma oportunidade, uma incerteza ou uma ameaça.

De acordo com D'ANDREA (2001; p. 51) "o risco como oportunidade está centrado no investimento e tem base em iniciativas estratégicas. Quanto maior for o risco, maior o potencial de retorno, e, paralelamente, maior pode ser o potencial de perda". Nesta visão, onde o risco é compreendido como uma oportunidade, ações pró-ativas e ofensivas (não defensivas) são adotadas pelos gestores, com o propósito de que sejam obtidos resultados positivos.

O risco como incerteza está relacionado à eficiência operacional; neste caso, o gerenciamento do risco consiste em adotar técnicas que equilibrem a variação entre o resultado projetado e o real obtido. Neste cenário, em geral, é difícil de se estimar o risco existente; na realidade, os gestores trabalham com intervalos de valores, dentro dos quais são feitas as previsões.

O risco como ameaça, escopo deste trabalho, refere-se à abordagem mais tradicional, na qual a preocupação está atrelada à ocorrência de efeitos negativos como por exemplo perda financeira, fraude, roubo, comprometimento da imagem e reputação, infração legal, falhas tecnológicas, dentre outros. Nas situações em que o risco é visualizado como uma ameaça, os gestores atuam fortemente de maneira preventiva, a fim de minimizar o impacto causado para a organização caso o risco se materialize.

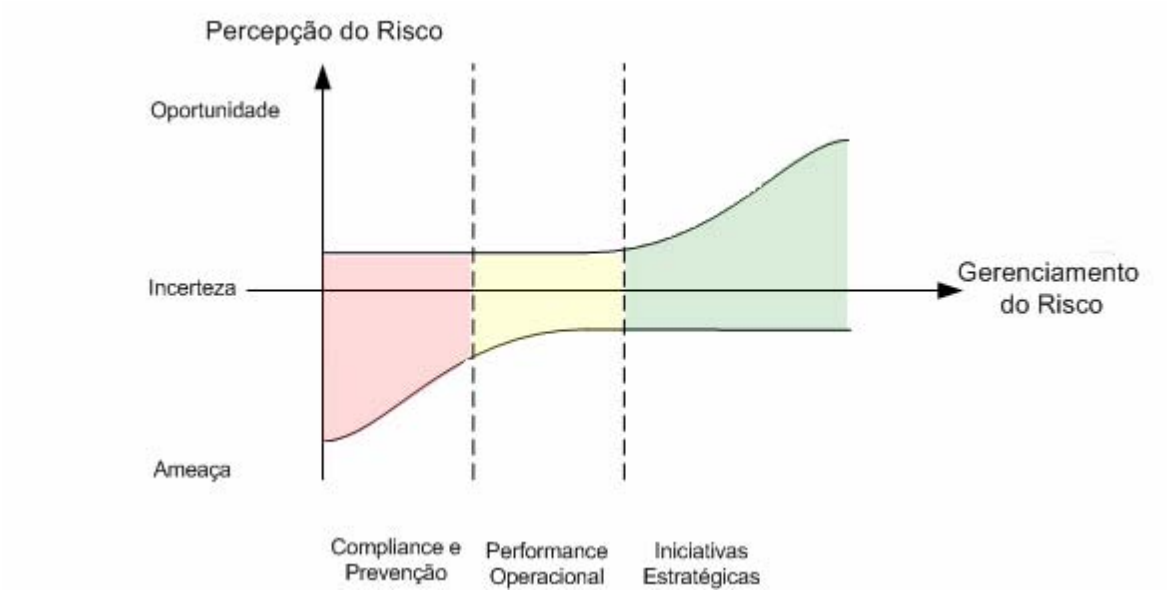

Figura 1: Percepção do risco

Numa abordagem conceitual, o risco pode ser definido como a probabilidade de uma ameaça específica explorar uma vulnerabilidade existente.

$$\text{RISCO} = \text{AMEAÇA} + \text{VULNERABILIDADE} \qquad (1)$$

Riscos são eventos futuros incertos que podem influenciar a organização no alcance dos seus objetivos, sejam estes estratégicos, financeiros ou operacionais. De modo mais amplo, o risco é um conceito fundamental que tange todos os processos da organização, nos mais diversificados setores da indústria.

Como pode ser observado pela equação (1), o risco é diretamente proporcional ao volume de ameaças e vulnerabilidades aos quais o ativo está suscetível. Assim, para que o risco seja reduzido, as ameaças e / ou as vulnerabilidades devem ser minimizadas.

2.3.2 Ameaça

O conceito de ameaça pode ser definido como uma atividade deliberada, ou não intencional, com o potencial de causar danos aos ativos.

As ameaças podem ser classificadas em três grandes grupos: (1) ameaças humanas, (2) ameaças não humanas (ou ambientais) e (3) desastres naturais. As ameaças humanas podem sofrer um segundo nível de segregação, intencional ou não intencional, e estão diretamente relacionadas às ações realizadas pelos indivíduos. Na categoria de ameaça humana intencional enquadram-se os "hackers", "crackers" e funcionários descontentes. Em contrapartida os funcionários com poucos conhecimentos sobre aspectos tecnológicos podem ser classificados como ameaça humana não intencional.

As ameaças não humanas (ou ambientais) compreendem hardware, software, dispositivos tecnológicos, "bugs", falhas elétricas, dentre outros.

Os desastres naturais como terremoto, incêndio, enchentes, etc. constituem a terceira categoria de ameaças.

Conforme o INFORMATION SECURITY FORUM (2001; p. 06), são consideradas ameaças "os meios pelos quais a confidencialidade, integridade e disponibilidade da informação podem ser comprometidas." Nesta mesma abordagem, são consideradas categorias de ameaça: (1) mau funcionamento de hardware e software; (2) perda de serviço, equipamento ou recursos; (3) conseqüências não previstas durante um processo de gerenciamento de mudanças; (4) erro humano e violação no acesso.

A quantificação real dos impactos causados por uma ameaça está diretamente relacionada à probabilidade de materialização da mesma, ou seja, a probabilidade da ameaça tornar-se um incidente de segurança.

2.3.3 Vulnerabilidade

As vulnerabilidades são definidas como circunstâncias que aumentam a probabilidade de materialização de uma ameaça, contribuindo para que ela ocorra com maior freqüência, maior impacto, ou ambos concomitantemente. As vulnerabilidades podem ser decorrentes de fraquezas existentes nos controles de segurança (sejam estes procedimentos, controles tecnológicos ou físicos), ou originadas por situações especiais. Muitas vezes o conceito de vulnerabilidade é interpretado como ausência de segurança.

As vulnerabilidades contribuem para o risco do ambiente, pois colaboram para que a ameaça se concretize. Podemos observar pela seqüência abaixo que as vulnerabilidades levam à ameaça, e conseqüentemente a ameaça nos leva ao risco.

VULNERABILIDADE ➔AMEAÇA➔ RISCO

É importante salientar que a existência de uma ameaça por si só não representa um risco para a organização. Ela passará a se tornar um risco caso ela faça uso, ou a grosso modo, “se aproveite”, da existência de vulnerabilidades nos dispositivos de segurança e / ou controles. As vulnerabilidades precisam ser reduzidas ou eliminadas para que os ativos estejam protegidos.

2.3.4 Impacto

O impacto refere-se ao dano causado no ambiente tecnológico ou ao negócio devido à exploração de uma vulnerabilidade por uma ameaça. Esse impacto deve ser analisado considerando o quanto as propriedades da informação (confidencialidade, integridade e disponibilidade, tais propriedades serão explicadas no item “2.3.6 Propriedades da Informação” desta dissertação) foram afetadas. Durante uma análise de risco, outros tipos de impacto também são considerados, dentre eles o financeiro e de imagem da organização.

O impacto causado pela exploração de uma vulnerabilidade deve ser analisado quantitativamente e qualitativamente. Podemos utilizar uma analogia simples para exemplificar essa afirmação. Suponha que ocorra um assalto em uma luxuosa casa em um dos bairros mais refinados da cidade, em que foram roubados quatro televisores. Ao mesmo tempo, ocorria um assalto na periferia, onde fora roubado apenas uma única televisão. Se considerarmos apenas a análise quantitativa, concluímos que o impacto causado no primeiro assalto é maior do que no segundo, visto que neste último apenas houve um único televisor roubado. Entretanto, ao efetuarmos uma análise qualitativa, concluímos que o impacto causado no segundo assalto é muito superior ao primeiro, visto que para uma família de baixa renda, a reposição do televisor terá um grande impacto no orçamento familiar e poderá levar um longo período de tempo para ser reposto, enquanto no primeiro caso, esse processo será muito mais rápido. Como podemos observar, a análise do impacto deve levar em consideração todo o contexto em que o evento está inserido.

2.3.5 Ativos

Muitas metodologias de análise de risco iniciam o processo pela identificação e classificação dos ativos. O termo ativo possui um significado bastante amplo, e pode englobar recursos tangíveis e intangíveis. Dentre os recursos tangíveis encontramos hardware, documentos impressos, mídias magnéticas, etc. Em relação aos recursos intangíveis os principais são os dados e informações, embora o aspecto software e a imagem / reputação da organização também sejam considerados como ativos. Cabe destacar que alguns autores também classificam as pessoas como ativos.

Os ativos são os principais afetados por uma ameaça. Em função disso, os ativos críticos da organização precisam ser corretamente identificados, e as respectivas vulnerabilidades mapeadas, permitindo assim que contramedidas sejam adotadas evitando que as vulnerabilidades conhecidas sejam exploradas pelas ameaças.

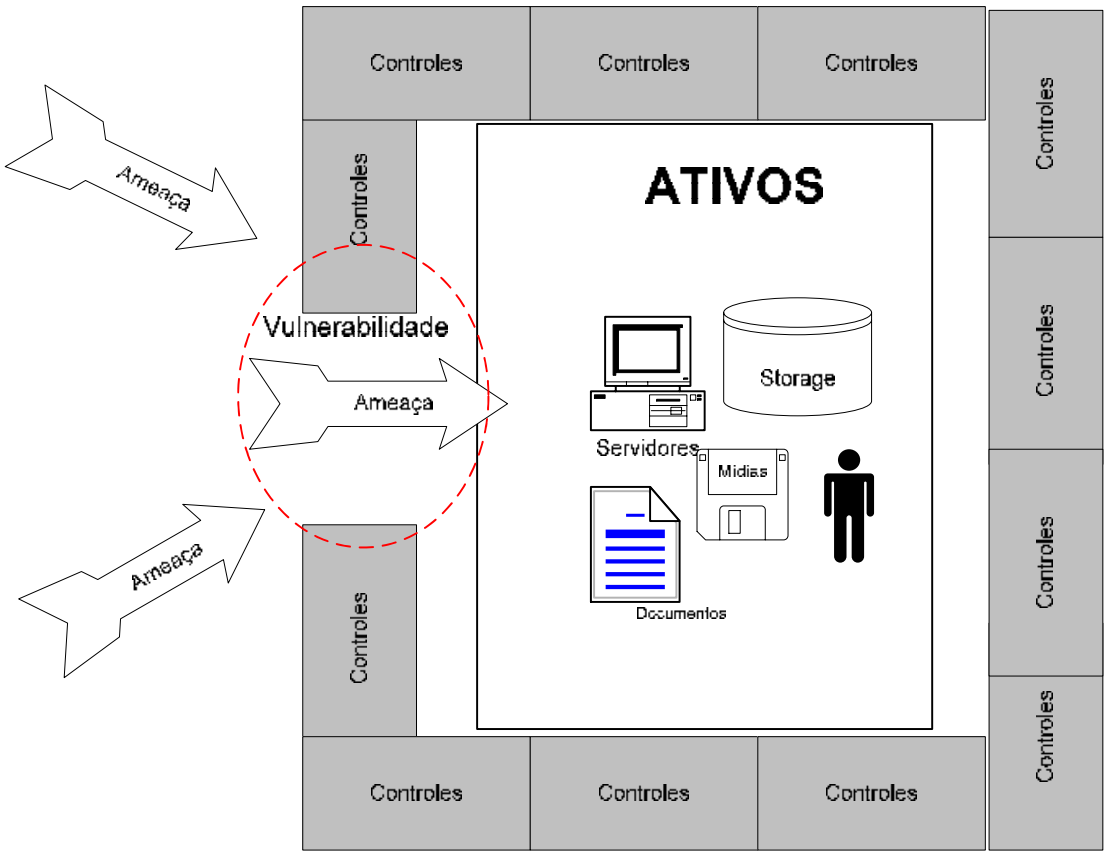

Figura 2: Inter-relacionamento entre Ameaça x Vulnerabilidade x Ativo

2.3.6 Propriedades da Informação

Em geral, sempre que ocorre a exploração de uma determinada vulnerabilidade por uma ameaça, uma ou mais propriedades da informação são comprometidas. São consideradas propriedades da informação: confidencialidade, integridade e a disponibilidade. As respectivas definições são apresentadas abaixo:

- **Integridade**: assegura que a acuracidade da informação, ou seja, sua exatidão esteja preservada. A integridade da informação é perdida sempre que alterações não autorizadas nas informações são feitas de modo intencional ou acidental. O uso contínuo de informações cuja integridade tenha sido comprometida pode acarretar em decisões incorretas, fraudes, ou outros danos à organização.

- **Confidencialidade:** assegura que a informação é acessível somente para àquelas pessoas que estão autorizadas a acessá-las. A perda da confidencialidade pode causar diversos danos à organização, dentre elas a perda de credibilidade perante o mercado, ações legais, dentre outros.

- **Disponibilidade:** refere-se à condição na qual a informação está disponível, no formato necessário, sempre que solicitada. Perda de funcionalidades do sistema e efetividade operacional, por exemplo, podem resultar na indisponibilidade de informações.

2.3.7 Controle

Controles são consideradas práticas, procedimentos ou mecanismos que podem proteger um ativo contra uma ameaça, reduzir a vulnerabilidade, limitar o impacto de evento indesejável, detectar incidentes de segurança e facilitar o processo de recuperação do ambiente. A proteção dos ativos requer que sejam feitas diferentes combinações de controles para implementar as camadas de segurança necessárias.

De acordo com ISO IEC TR 13335-1(1996; p. 09), os controles são empregados com uma das seguintes finalidades: detecção, proteção, prevenção, limitação, correção, recuperação, monitoramento e conscientização. A seleção adequada dos controles é essencial para assegurar que os ativos estejam adequadamente protegidos. Dentre os diversos tipos de controles existentes, podemos mencionar:

- firewalls de rede;
- criptografia;
- software antivírus;
- backups;
- mecanismos de controle de acesso;
- geradores de energia;
- assinatura digital; e
- procedimentos operacionais, etc.

2.4 O processo de Gerenciamento de Risco de TI: Identificação; Mitigação e Monitoramento

Um dos propósitos dessa dissertação, além de apresentar uma análise comparativa de três metodologias de Gerenciamento de Risco de TI comumente empregadas, é apresentar uma visão geral de quais etapas compõem o processo de Gerenciamento de Risco de TI, independente da metodologia.

Existem diferentes modelos e métodos para condução do processo de Gerenciamento de Risco de TI, e a extensão da análise e os recursos empregados podem variar dependendo do escopo do levantamento e da disponibilidade de dados e informações confiáveis. Adicionalmente, a disponibilidade de dados pode afetar a forma como o risco é mensurado, ou seja, a adoção de uma abordagem quantitativa ou qualitativa. Uma abordagem quantitativa geralmente estima o

custo monetário do risco e das técnicas de minimização do mesmo baseado (a) na probabilidade que um evento prejudicial ocorra, (b) no custo de potenciais perdas, (c) no custo das ações de mitigação que podem ser adotadas. Quando dados confiáveis referentes à probabilidade de materialização da ameaça e custos não estão disponíveis, somente a abordagem qualitativa poderá ser adotada, e neste caso, os riscos são definidos de modo mais subjetivo, em geral utilizando escalas como alto, médio e baixo. Assim, o processo de avaliação de riscos dependerá fortemente da experiência prévia do profissional que está conduzindo o processo de análise de riscos.

O processo de Gerenciamento de Risco de TI é estruturado em três grandes etapas conforme apresentado pela Figura 3:

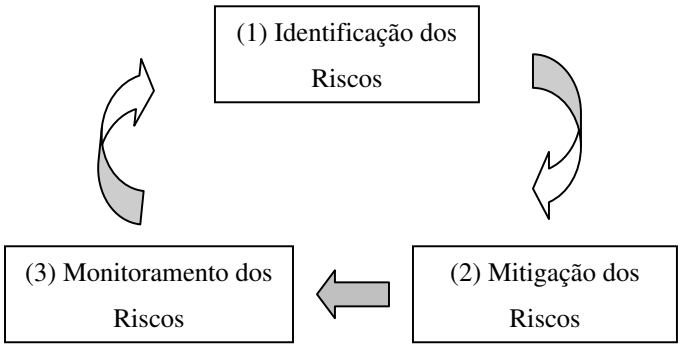

Figura 3: Ciclo de Gerenciamento de Risco de TI

(1) Identificação dos riscos: a identificação ou avaliação de riscos é a primeira etapa do processo de Gerenciamento de Risco de TI. Essa etapa visa mapear todas as potenciais ameaças aos quais os ativos estão suscetíveis, bem como as vulnerabilidades que estes possuem. As atividades como (a) avaliação da probabilidade de materialização das ameaças e (b) estimativa dos impactos causados também são contempladas nessa etapa do processo.

Embora todas etapas do ciclo de Gerenciamento de Risco de TI sejam importantes, a etapa de Identificação dos Riscos é essencial, visto que ela fornece subsídios para as fases subseqüentes. Uma vez que os riscos e ameaças mudam com o passar do tempo, é importante para a organização efetuar periodicamente a reavaliação dos riscos e reconsiderar a eficiência das estratégias adotadas para a mitigação dos mesmos.

(2) Mitigação dos riscos: a etapa de mitigação consiste na seleção de estratégias a serem adotadas para eliminação ou minimização dos riscos. Durante a etapa de mitigação aspectos financeiros são considerados, visto que os recursos empregados na mitigação dos riscos não podem ser superiores à possível perda financeira que o risco acarretaria, caso a ameaça se materializasse.

(3) Monitoramento dos riscos: os riscos devem ser continuamente monitorados visto que as ameaças, vulnerabilidades e os próprios ativos alteram-se com o passar do tempo. Assim, novos riscos virão à tona e outros já mitigados podem se tornar uma preocupação. Dessa forma, o processo de Gerenciamento de Risco de TI é algo contínuo e evolutivo. A Figura 3 apresentada acima demonstra a continuidade desse ciclo.

2.4.1 Identificação dos riscos

Num processo de Gerenciamento de Risco de TI, a etapa de identificação dos riscos é considerada como essencial, visto que ela é o alicerce de todas as demais etapas. É a partir das informações levantadas nesta etapa que os gestores terão informações suficientes para a tomada de decisões.

A etapa de identificação do risco normalmente é composta por três atividades básicas: (1) determinar o escopo de avaliação e a metodologia; (2) coletar e analisar a informação e (3) interpretar os resultados da avaliação de risco, a fim de definir qual a melhor estratégia para eliminação ou mitigação dos riscos na etapa seguinte.

Existem diferentes componentes envolvidos no processo de identificação e determinação dos riscos, dentre os quais destacamos: ameaças, vulnerabilidades, impacto, probabilidade e controles. Para que possamos definir adequadamente os riscos, é necessário avaliar cada um dos componentes mencionados e mapear corretamente os ativos escopo da análise.

2.4.1.1 Definição do escopo

A definição do escopo de análise deve ser o primeiro passo a ser realizado durante a etapa de identificação de riscos. A avaliação deve estar focada nas áreas (entende-se como áreas processos e / ou ativos) onde o grau de risco é desconhecido, ou conhecido e classificado como alto.

Os diferentes processos e ativos podem ser analisados em maior ou menor profundidade, e não precisam necessariamente seguir a mesma metodologia de análise. A definição de um escopo bem delimitado contribui para que a análise seja feita de forma mais efetiva.

A execução de um inventário prévio dos ativos é uma atividade que auxilia na definição de um escopo adequado. O inventário de ativos consiste em identificar todos os recursos considerados críticos para a organização, quais processos de negócio estes suportam, e o grau de relevância dos mesmos para o negócio. Quando possível, a representatividade do ativo deve ser expressa também em termos financeiros. Baseado nessa análise a organização tem subsídios para definir o nível de proteção condizente com o ativo, e especificamente para o processo de Gerenciamento de Risco de TI, para quais ativos o processo de identificação de ameaças e vulnerabilidades deverá ser conduzido com maior refinamento.

De acordo com WHITMAN (2003; p.127), existem alguns questionamentos a serem feitos durante a etapa da identificação da relevância de um determinado ativo:

- Qual ativo é mais crítico para o sucesso da organização? Quais ativos são essenciais para seus objetivos estratégicos, e quais são meramente acessórios?

- Quais ativos de informação geram as maiores receitas? Ou seja, a criticidade de um determinado ativo pode ser avaliada pela participação do mesmo na geração de receitas. Organizações sem fins lucrativos avaliam esse aspecto considerando a importância do ativo para a capacidade produtiva da organização.

- Quais ativos de informação geram os maiores lucros? Deve ser avaliado como a lucratividade de uma determinada empresa / negócio depende de um ativo em particular.

- Quais ativos de informação são mais dispendiosos ao serem substituídos? Conseqüentemente, se o custo de substituição de um determinado recurso for elevado, os controles a serem aplicados para proteção dos mesmos deverão ser aprimorados.

- Quais ativos de informação impactam negativamente a imagem da organização caso sejam danificados?

Todos os questionamentos mencionados devem ser considerados e ponderados no momento da avaliação da importância de um determinado ativo para a organização. Cabe à organização determinar pesos específicos para cada um dos aspectos mencionados acima.

Alguns aspectos devem ser considerados durante a definição do escopo, dentre eles:

- relevância do processo / ativo para o negócio: quanto mais relevante for o recurso, mais detalhada deve ser a análise, conforme já mencionado anteriormente;

- magnitude das mudanças ocorridas no ambiente tecnológico, desde a última análise;

- interações com entidades externas; e

- necessidade de atendimento às legislações específicas, aplicáveis ao nicho de mercado no qual a organização está inserida.

Não existe uma regra única em relação à análise de risco; em geral as organizações adotam um modelo híbrido para efetuar esta análise. A abordagem metodológica adotada, bem como o

escopo de trabalho definido, influenciam diretamente na (1) quantidade de esforço necessário para realização da análise e (2) na qualidade dos resultados obtidos após o término do processo.

2.4.1.2 Coleta de informações

Identificação de ameaças

O conceito de ameaça já foi apresentado detalhadamente no item 2.3 – Conceitos Preliminares. De maneira sucinta, podemos definir ameaça como sendo todo evento que possa causar impactos indesejáveis aos ativos. As ameaças podem ser de natureza humana, não humana ou um desastre natural.

O propósito do processo de identificação de ameaças é mapear todas as fontes de potenciais ameaças que são inerentes aos recursos de tecnologia da informação, e que possam impactá-los negativamente. Uma grande variedade de ameaças circunda os ativos de informação, e cada ameaça possui um potencial diferente para atacar cada um dos ativos. As conseqüências das ameaças podem variar consideravelmente: algumas afetam a confidencialidade ou integridade dos ativos, outros afetam a disponibilidade dos mesmos. Se considerarmos que toda potencial ameaça pode e irá atacar os ativos da organização, o escopo de atuação num processo de Gerenciamento de Risco de TI se expandirá consideravelmente. Assim caberá ao responsável pela condução do processo o uso do bom senso na identificação das ameaças.

As ameaças possuem características próprias que fornecem importantes informações sobre as mesmas, por exemplo:

- fonte (interna ou externa);
- motivação (ex.: ganho financeiro, vantagem competitiva);
- freqüência de ocorrência; e
- severidade da ameaça.

São considerados exemplos de ameaças comumente encontradas:

- Ex-funcionários e funcionários descontentes: essa ameaça está classificada na categoria humana, intencional. Diversas pesquisas demonstram que grande parte dos incidentes de segurança ocorridos são realizados por ex-funcionários e / ou funcionários descontentes. Isso ocorre em função de tais usuários possuírem um conhecimento profundo dos processos de negócio e respectivos sistemas tecnológicos que os suportam. A motivação para esse tipo de ação em geral é a vingança.

- Erros e omissões: essa ameaça pode ser classificada na categoria de humana, intencional ou não. Ela é uma importante ameaça para a integridade dos dados e sistemas, visto que muitas vezes os controles de validação sistêmicos não conseguem identificar todas as ocorrências de erros. Cabe destacar que esse tipo de ameaça não é proveniente somente daqueles usuários que efetuam a digitação de um grande volume de informações, mas também de qualquer usuário que faça a edição de dados no sistema. Em algumas situações, o erro é visualizado não somente como uma ameaça, mas também como uma vulnerabilidade do sistema, visto que o sistema permitiu que o erro ocorresse.

- Comprometimento da infra-estrutura: essa ameaça é classificada como uma ameaça não humana. A perda da infra-estrutura de suporte, como energia elétrica, falha na rede de comunicação, interrupção no fornecimento de água, falhas nos serviços de transporte, problemas na rede de esgoto, dentre outros, podem comprometer (ou até mesmo interromper) a operação do ambiente de tecnologia.

- “Hackers” ou “crackers”: ambos são considerados como uma ameaça humana intencional. De acordo com GEUS (2003; p. 51), “... hackers, por sua definição original, são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas, mas sim como um desafio às suas habilidades... Os crackers são elementos que invadem sistemas para roubar informações e causar

danos às vítimas". De maneira geral, os "hackers" e "crackers" são considerados como uma ameaça constante, visto que é impossível prever sua forma de atuação, e conseqüentemente, torna-se inviável assegurar que a organização esteja totalmente protegida contra qualquer tipo de ação nesse sentido. Essa característica é acentuada pelo fato de que diariamente surgem novas tecnologias cujas vulnerabilidades nem sempre são conhecidas pelos gestores das áreas de tecnologia. Outro ponto a ser destacado é que, muitas vezes, a perda financeira resultante da ação de um "hackers" e / ou "cracker" é de difícil mensuração, se considerarmos que o principal fator afetado é a imagem da organização.

De acordo com WHITMAN (2003; p. 134), existem 9 categorias de ameaças, as quais estão relacionadas na tabela abaixo:

Ameaça	**Exemplo**
Erro humano ou falha	Acidentes, erros cometidos por funcionários
Comprometimento de propriedade intelectual	Pirataria, violação de "copyright"
Atos deliberados de espionagem	Acesso não autorizado a dados
Atos deliberados de sabotagem ou vandalismo	Destruição dos sistemas ou informação
Atos deliberados de roubo	Confisco ilegal de equipamentos ou informações
Ataques deliberados de software	Vírus, "worms", macros, negação de serviço
Falhas técnicas ou erros de hardware	Falha de equipamento
Falhas técnicas ou erros de software	"Bugs", problemas de codificação
Obsolescência tecnológica	Tecnologia antiquada ou em desuso

Tabela 1: Exemplos de Ameaças

Em geral, as ameaças humanas sempre são materializadas a partir de uma motivação. A tabela abaixo do STONEBURNER (2002; p. 13), exemplifica este conceito:

Fonte de ameaça	**Motivação**	**Ações da ameaça**
"Hacker", "cracker"	Desafio Ego Rebeldia	Engenharia social Intrusão nos sistemas e interrupções Acesso não autorizado ao sistema
Terrorismo	Destruição Vingança	Penetração no sistema Negação de serviço
Espionagem industrial	Obtenção de vantagem competitiva Espionagem econômica	Roubo de informação Engenharia social

Tabela 2: Motivação das ameaças

Cada organização deve mapear a lista de potenciais ameaças às quais os recursos tecnológicos estão sujeitos, visto que estas mudam de organização para organização. Por exemplo, se considerarmos uma empresa situada no 19º andar de um prédio, dificilmente ela terá problemas de enchentes, ao contrário de uma galeria localizada no subsolo.

Anualmente o CSI/FBI realiza uma pesquisa intitulada "Computer Crime/Security Survey" cujo objetivo é identificar as grandes tendências referentes à segurança da informação. Esta pesquisa é conduzida pelo Computer Security Institute em conjunto com o Federal Bureau of Investigations e no ano de 2004 foi respondida por 481 empresas de diferentes segmentos. Como resultado da pesquisa, as principais ameaças identificadas, bem como a curva de crescimento das mesmas durante os últimos cinco anos são ilustradas na figura a seguir (GORDON; 2004; p. 9):

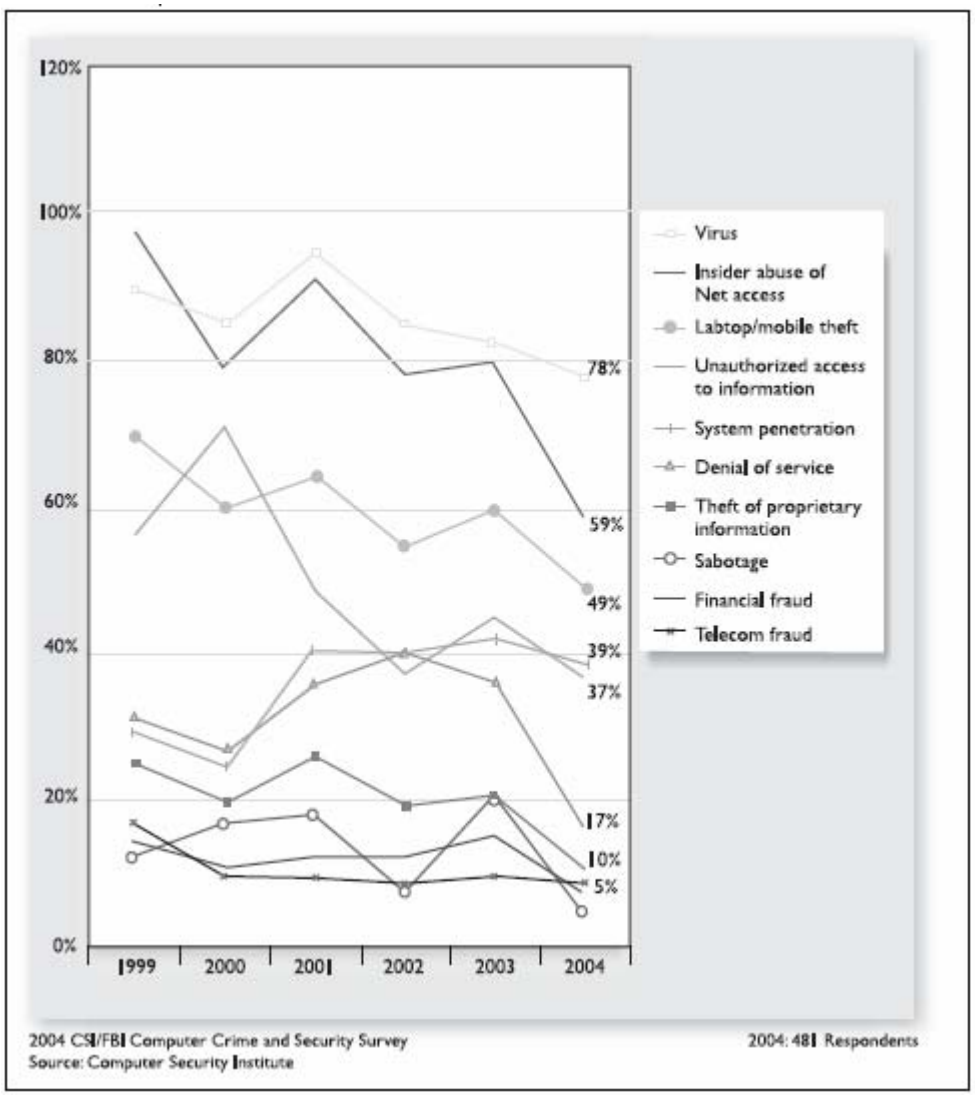

Figura 4 : Tipos de ameaça e mau uso dos ativos de informação

Algumas ameaças podem afetar mais do que um único ativo; em tais situações o impacto poderá variar dependendo do ativo afetado. Por exemplo, a existência de um vírus em uma estação de trabalho pode ter um impacto limitado e localizado, enquanto que a existência do mesmo vírus em um servidor da rede pode causar um impacto mais abrangente.

Em virtude das contínuas mudanças que ocorrem no ambiente tecnológico, as ameaças e vulnerabilidades se alteram com o passar do tempo. Isso significa que a identificação de ameaças e vulnerabilidades deve ser constantemente reavaliada. De acordo com COHEN (2003; p.10) a

avaliação as ameaças deverá ocorrer conforme a periodicidade apresentada na Tabela 3. Nesta tabela também são apresentados quais níveis hierárquicos dentro da organização deverão ser notificados quando da identificação de novas ameaças, e com qual periodicidade.

	Impacto		
Ameaça	**Baixo**	**Médio**	**Alto**
Baixa probabilidade	Anualmente. Gerência de nível médio.	Ciclo de revisão 6 meses. Alta administração atualizada anualmente.	Altas conseqüências em geral são originadas por altas ameaças. De qualquer modo a análise deve ser contínua. Alta administração atualizada mensalmente.
Média probabilidade	9 – 12 meses. Gerência de nível médio.	Ciclo de revisão 3-9 meses. Alta administração atualizada trimestralmente.	Contínuo. Alta administração atualizada mensalmente.
Alta probabilidade	6 meses. Gerência de nível médio.	Ciclo de revisão 3-6 meses. Alta administração Atualizada trimestralmente.	Contínuo. Alta administração atualizada mensalmente.

Tabela 3: Periodicidade para reavaliação dos riscos

No processo de tratamento das ameaças, quando as conseqüências são baixas e as ameaças altas, as organizações, em geral, evitam o risco, pois a complexidade de lidar com altas ameaças versus

baixas conseqüências não compensa o esforço empregado. Quando as conseqüências são altas, raramente as ameaças são baixas. Neste caso as reavaliações devem ser constantemente efetuadas.

As definições referentes aos conceitos de probabilidade e impacto serão apresentadas a seguir nos itens “2.4.2.2 Definição de probabilidade” e “2.4.2.3 Definição de impacto”, dessa dissertação.
A Figura 5 apresentada abaixo demonstra como deve ser feito o tratamento do risco, considerando o nível de ameaça e impacto ao qual a empresa está sujeita.

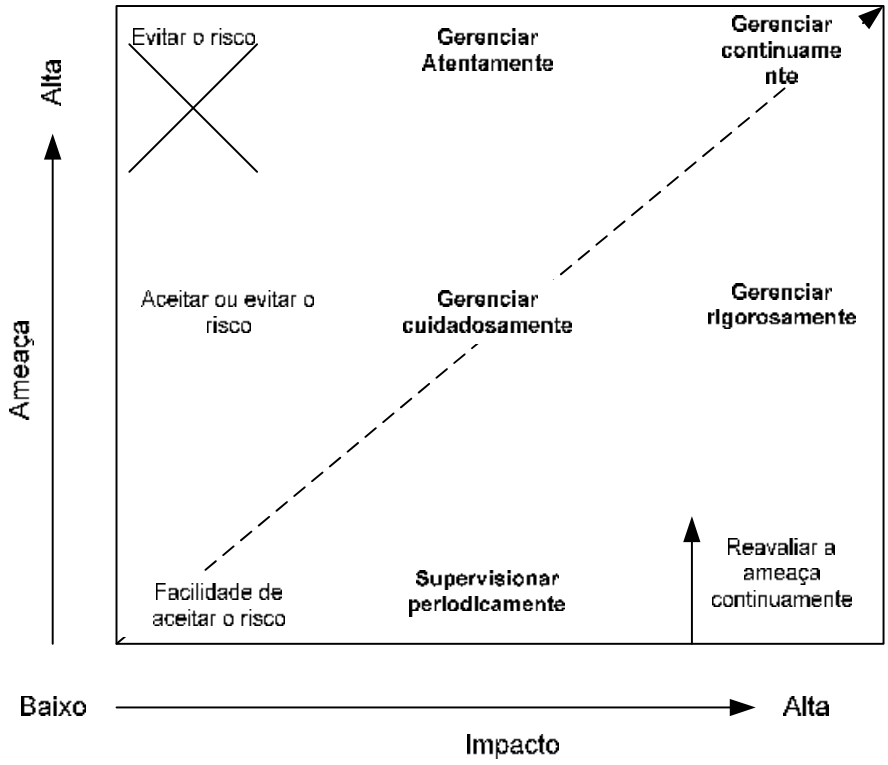

Figura 5: Mapa de Ameaça x Impacto

Identificação das vulnerabilidades

Todos os recursos tecnológicos estão sujeitos a algum grau de vulnerabilidade. A identificação das vulnerabilidades consiste em mapear as “fragilidades” existentes nos recursos e processos de Tecnologia da Informação, as quais poderiam ser exploradas por potenciais fontes de ameaças.

A presença de uma ameaça não significa que ela irá necessariamente causar prejuízos, danos ou perdas de qualquer natureza. Para se tornar um risco, a ameaça precisa explorar vulnerabilidades existentes nos ativos, nos sistemas de segurança ou nos controles internos empregados pela organização.

Concomitantemente, ambientes nos quais existam fraquezas nos controles empregados são muitas vezes mais propensos à ocorrência de incidentes. As circunstâncias relacionadas abaixo também representam vulnerabilidades-chaves que intensificam a probabilidade da ocorrência de incidentes:

- alto grau de mudança no ambiente;
- ambientes informatizados em larga escala;
- tecnologia de rede complexa;
- maturidade das tecnologias empregadas; e
- volume de acesso por terceiros.

Existem diferentes tipos de vulnerabilidades, e as metodologias necessárias para determinar a existência das mesmas irá variar dependendo da natureza do ativo envolvido. As vulnerabilidades relacionadas ao ambiente de tecnologia dividem-se, em geral, em vulnerabilidades técnicas e não técnicas.

As vulnerabilidades técnicas e não técnicas, associadas ao ambiente de tecnologia da informação, podem ser identificadas por meio de alguns métodos de levantamento de informações. Esses métodos dividem-se em:

- **Entrevistas**: nesta abordagem são realizadas entrevistas com os interlocutores responsáveis pelos processos e recursos tecnológicos, cujo objetivo é identificar a forma como os recursos e processos são operados e gerenciados. Visitas “on-site” também são necessárias para obter informações sobre aspectos físicos da

localidade onde os recursos tecnológicos são hospedados e identificar possíveis vulnerabilidades relacionadas às instalações físicas.

- **Revisão de documentação**: a revisão de documentação existente, como por exemplo, relatórios prévios de auditoria, relatórios de avaliação de risco, resultados de testes do sistema, relatórios de teste de ferramentas de diagnóstico do ambiente, políticas de segurança, podem fornecer informações significativas sobre os controles de segurança utilizados e planejados para o ambiente de Tecnologia da Informação.

- **Utilização de ferramentas automatizadas de varredura**: técnicas automatizadas podem ser utilizadas para coletar informações eficazes sobre os sistemas. Por exemplo, uma ferramenta de mapeamento de rede pode identificar os serviços que são executados em um amplo grupo de "hosts" e fornecer de modo rápido um diagnóstico dos principais sistemas. Entretanto, deve-se observar que algumas ferramentas automatizadas de identificação de vulnerabilidades podem gerar alguns alertas denominados "falsos positivos". Isso decorre do fato de tais ferramentas não avaliarem o contexto no qual a vulnerabilidade foi identificada, mas somente a vulnerabilidade.

- **Questionário**: distribuição de questionários que abordem questões pertinentes aos controles de segurança utilizados. Estes questionários devem ser encaminhados aos gestores responsáveis pelos processos e recursos tecnológicos. Em função do uso de questionário ser um processo impessoal, ele deverá ser utilizado preferencialmente nas situações em que o acesso ao gestor for dificultado.

No Apêndice A foram apresentados alguns questionários que podem ser utilizados para direcionar a identificação dos controles implementados e possíveis vulnerabilidades no ambiente de tecnologia. Tal questionário foi elaborado a partir da minha experiência prévia em trabalhos de análise de risco e poderá contribuir significativamente para as organizações que não possuam um direcionamento para essa atividade, pois muitas vezes os gestores não sabem quais são os aspectos essenciais a serem mapeados, e a forma de abordá-los.

A obtenção de informações sobre vulnerabilidades também pode ser feita por intermédio dos relatórios publicados pelos fornecedores de hardware e software. Em geral, quando são publicadas as vulnerabilidades dos produtos, os fornecedores também disponibilizam “hot fixes”, “service packs”, “patches” com o propósito de eliminar ou mitigar os riscos.

É importante ressaltar que muitos fornecedores se referem a seus produtos como ferramenta de Gerenciamento de Risco de TI, quando na realidade são apenas ferramentas de gerenciamento de vulnerabilidades e tem como finalidade principal identificar falhas no ambiente que permitiriam uma ação indevida. Conforme apresentado ao longo do Capítulo 2, o processo de Gerenciamento de Risco de TI é um processo muito mais abrangente e complexo.

Em virtude da relevância dos aspectos “identificação dos ativos críticos”, “identificação de ameaças” e “identificação de vulnerabilidades”, todos foram considerados requisitos essenciais na comparação das metodologias de Gerenciamento de Risco de TI apresentadas no Capítulo 03.

2.4.2 Avaliação do risco

A avaliação do risco consiste em atribuir uma pontuação específica referente ao risco ao qual o ativo de informação está suscetível. Quando essa pontuação não significa nada em termos absolutos, ela pode ser útil no julgamento do risco relativo introduzido por cada ativo de informação.

De acordo com WHITMAN (2003; p. 154), “risco é a probabilidade de ocorrência de uma vulnerabilidade, multiplicado pelo valor do ativo de informação, menos a porcentagem de risco mitigado pelos controles atuais, mais a incerteza do atual conhecimento da vulnerabilidade”.

Dois aspectos extremamente relevantes para o correto entendimento do risco, são apresentados a seguir: probabilidade e impacto.

2.4.2.1 Relacionamento dos principais elementos que compõem o processo de Gerenciamento de Risco de TI

A Figura 6 abaixo demonstra como os principais elementos da análise de risco estão inter-relacionados. Como pode ser observado, para que a determinação do risco ao qual os ativos estão suscetíveis seja precisa, é necessário que cada um dos elementos (ameaças, vulnerabilidades, controles e ativos) sejam conhecidos.

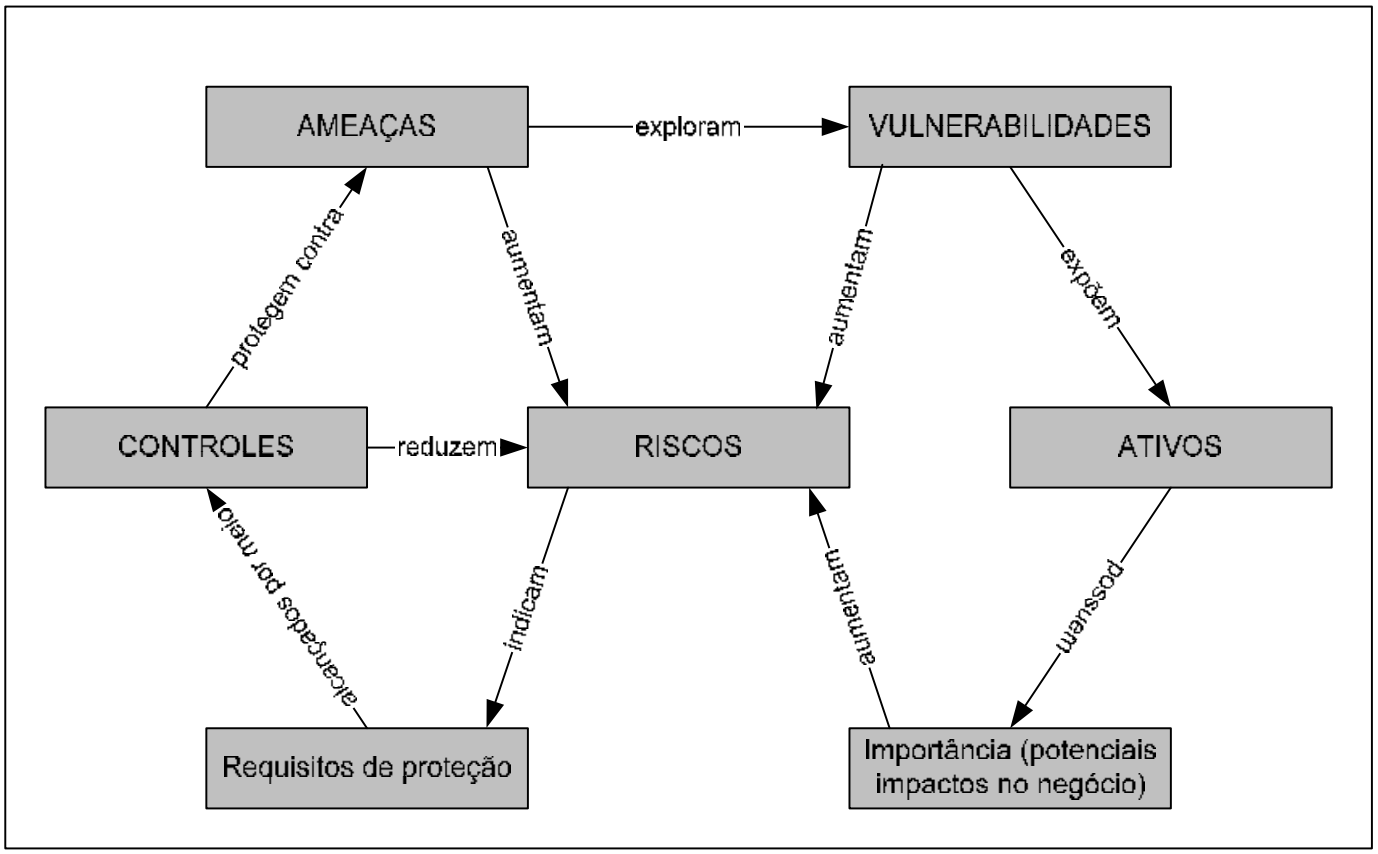

Figura 6: Relacionamentos no processo de Gerenciamento de Risco de TI

2.4.2.2 Determinação da probabilidade

A probabilidade é o fator de incerteza envolvido no risco. É o índice que indica as chances de uma vulnerabilidade ser explorada, com sucesso, por uma ameaça.

De acordo com STONEBURNER (2002;p.21), para derivar um índice que represente a probabilidade que uma potencial vulnerabilidade seja explorada por uma ameaça, os seguintes fatores devem ser considerados:

- origem e motivação da ameaça;
- natureza da vulnerabilidade; e
- existência e efetividade dos controles empregados.

A probabilidade de que uma potencial vulnerabilidade possa ser explorada por uma dada ameaça pode ser classificada em alto, médio ou baixo. A Tabela 4 descreve cada um dos critérios:

Nível de probabilidade	**Descrição**
Alta	A origem da ameaça é altamente motivada e suficientemente capaz de ser exercida, e os controles empregados para evitar que a vulnerabilidade seja explorada são ineficientes. O evento é esperado e quase certo de que aconteça.
Médio	A origem da ameaça é motivada e capaz, mas os controles adotados podem impedir que a vulnerabilidade seja explorada. O evento poderá ocorrer alguma vez.
Baixo	A origem da ameaça é falha ou incapaz, ou os controles adotados para prevenir ou impedir sua ocorrência são eficazes. O evento poderá ocorrer em circunstâncias excepcionais.

Tabela 4: Classificação de níveis de probabilidade de concretização de ameaças

A publicação especial do STONEBURNER (2002; p. 30) sugere que sejam atribuídos os seguintes valores para a probabilidade: 1.0 para Alto, 0.5 para Médio e 0.1 para Baixo.

Exemplificando, a probabilidade do recebimento de um e-mail contendo vírus deveria ser classificada com 1.0; enquanto que a probabilidade de um meteoro cair no CPD, tende a 0.1. Nessa classificação não existe a possibilidade de adotar o valor 0, visto que uma vulnerabilidade com probabilidade zero de ocorrência não deve ser considerada durante o processo de análise de risco. Os pesos atribuídos às probabilidades são utilizados posteriormente no cálculo do nível de risco.

Embora sejam sugeridos os valores acima, cabe ao responsável pela análise de risco definir os valores que reflitam o contexto de segurança da organização.

2.4.2.3 Determinação do impacto

Impacto é a conseqüência de um incidente indesejado, causado deliberadamente ou acidentalmente e que afeta os ativos da organização.

A determinação do impacto consiste em mensurar o impacto adverso causado no ambiente, resultante da exploração de uma vulnerabilidade por uma ameaça.

O impacto causado no ambiente estará diretamente relacionado à importância do ativo para a organização; neste contexto, a realização do inventário prévio dos ativos contribui consideravelmente para a determinação correta do impacto, conforme já abordado anteriormente.

Para definição do impacto é necessário que o proprietário do ativo participe dessa atividade, visto que este profissional conhece profundamente todas as interdependências em relação a esse ativo e o valor que o mesmo possui para a empresa.

A identificação do valor de um determinado ativo é uma atividade extremamente complicada, visto que um mesmo ativo pode possuir valores diferentes de organização para organização, dependendo da forma como o mesmo é percebido pela empresa, e das características individuais do ativo. Para alguns ativos é fácil determinar seu valor, por exemplo, os custos de substituição de um determinado equipamento. Em contrapartida, para outros ativos, a mensuração do valor é difícil ou quase impossível. Por exemplo, se considerarmos o valor da informação referente ao lançamento de um determinado produto, é algo difícil de ser mensurado, e que poderá causar

grandes impactos para a organização, se for revelada em um momento inapropriado. Adicionalmente, alguns ativos têm seu valor modificado ao longo do tempo, decorrente das modificações sofridas pelo ativo, ou do trabalho empenhado sobre o mesmo. Abaixo estão relacionados alguns aspectos a serem considerados na definição do valor do ativo:

- custo de substituição;

- custo de fornecimento do ativo aos usuários;

- custo de proteção do ativo (de acordo com WHITMAN (2003; p. 168) "esta é uma questão cíclica, ou seja, o custo de proteção depende do valor do ativo, e o valor do ativo depende do custo de proteção");

- representatividade do ativo para o proprietário;

- custo de propriedade intelectual;

- valor para a concorrência;

- perda do lucro decorrente da indisponibilidade do ativo; e

- perda da produtividade enquanto o ativo estiver indisponível.

O impacto na segurança pode ser expresso em termos de perda ou degradação nos serviços e recursos, ou por meio da combinação dos seguintes fatores: integridade, disponibilidade e confidencialidade.

A adequada mensuração do impacto permite que seja feita uma análise apropriada entre os resultados de um incidente, e o custo das medidas de segurança necessárias para proteção contra tal incidente, permitindo assim um balanceamento correto. A freqüência de ocorrência de um incidente indesejado deve ser levada em consideração. Esse aspecto é particularmente importante quando os danos causados por cada ocorrência são baixos, mas o efeito cumulativo de diversos incidentes sucessivos é alto.

Embora a maioria, se não todos, os incidentes tenham algum tipo de impacto financeiro, mensurá-lo representa uma séria dificuldade ao processo de Gerenciamento de Risco de TI. Por exemplo, o impacto financeiro de um incidente pode ser:

- indireto, conseqüentemente difícil para avaliar (ex.: o comprometimento da imagem da organização pode ou não levar à perda de vendas ao longo do tempo, bem como a queda na prospecção de novos negócios);

- distribuído através das diferentes áreas do negócio, tornando difícil conseguir visualizar o impacto como um todo (ex.: degradação da performance do negócio decorrente de um intermitente mau funcionamento do sistema de e-mail); e

- muito pequeno para ser mensurado individualmente embora o impacto cumulativo de muitos incidentes possa ser substancial (ex.: interrupção de uma aplicação que é executada isoladamente em um "desktop" da rede).

Os impactos tangíveis podem ser medidos quantitativamente em relação à perda do lucro, no custo de reparar o sistema, ou no nível de esforço necessário para corrigir o problema causado pela ação bem sucedida de uma ameaça. Outros impactos, como comprometimento da imagem, perda de credibilidade, danos aos interesses da organização, não podem ser mensurados em unidades específicas, mas podem ser qualificados ou descritos em termos de alto, médio e baixo impacto.

Abordagem qualitativa x abordagem quantitativa

Conforme já mencionado anteriormente, há dois métodos fundamentalmente diferentes aplicados à mensuração do impacto: a análise qualitativa e a análise quantitativa.

- **Abordagem qualitativa**

Na análise qualitativa todas as métricas aplicadas são subjetivas por natureza, assim essa abordagem não provê unidades de medida que permitam quantificar a magnitude dos impactos, e conseqüentemente a análise de custo-benefício de qualquer controle é dificultada.

Nesta abordagem, a análise final do risco é classificada em categorias definidas pelo responsável pela análise, as quais podem variar entre alto, médio e baixo.

Magnitude do impacto	**Definição**
Alto	A exploração da vulnerabilidade pode resultar na (a) perda dos principais ativos / recursos da organização; (b) pode violar significativamente a reputação da organização, ou impedir que ela alcance seus objetivos; (c) acarretar em perdas humanas (morte) ou sérias lesões; (d) comprometer as operações de negócio com significantes conseqüências negativas aos clientes, processos ou sistemas.
Médio	A exploração da vulnerabilidade pode resultar em (a) perda de ativos ou recursos sofisticados; (b) prejudicar a reputação / interesses da organização, ou impedir que ela cumpra sua missão. É esperado que o evento acarrete em uma perda financeira intermediária, ou resulte em interrupções no negócio com conseqüências negativas.
Baixo	A exploração da vulnerabilidade pode resultar na (a) perda de ativos tangíveis ou pode (b) afetar visivelmente a missão, reputação ou interesse da organização. Não é esperado que o evento resulte em perdas financeiras significativas ou outros impactos duradouros ao negócio. Quaisquer problemas ocorridos serão facilmente contidos.

Tabela 5: Magnitude de impacto

Obviamente, a tabela acima apenas sugere uma determinada categorização para a magnitude do impacto, a qual poderá ser modificada adaptando-se às necessidades da empresa.

- **Abordagem quantitativa**

A maior vantagem da análise quantitativa do impacto é que ela provê a medida da magnitude do impacto, a qual pode ser utilizada nas análises de custo benefício dos controles. Uma desvantagem é que, dependendo da unidade de medida adotada para expressar essa análise, ela pode não ser tão clara, necessitando que o resultado seja interpretado de maneira qualitativa.

Alguns indicadores utilizados para mensurar o impacto quantitativamente incluem:

- freqüência de exploração da vulnerabilidade por uma determinada ameaça, em um determinado período de tempo;
- custo decorrente da exploração da vulnerabilidade pela ameaça; e
- valor do ativo;

ALE – "Annual Loss Expenctancy"

Uma técnica popular de análise quantitativa é o ALE – "Annual Loss Expectancy" (Expectativa Anual de Perda). Neste método são consideradas as seguintes variáveis: o impacto financeiro estimado resultante de um evento desfavorável, a freqüência de ocorrência por ano, o valor do ativo e o fator de exposição:

$$ALE = SLEF(\$) * ARO$$

Onde: SLEF= "*Single Loss Exposure Value"* (Valor Unitário de Exposição à Perda)
ARO = "*Annual Rate of Occurence"* (Taxa Anual de Ocorrência)

O SLEF é obtido a partir da seguinte fórmula:

$$SLEF(\$) = AV \times EF$$

Onde: AV = "*Asset Value"* (Valor do Ativo)

EF = "*Exposure Factor"* (Fator de Exposição). Representa em valores percentuais a perda sofrida pelo ativo em decorrência do risco identificado.

Exemplo: Se considerarmos o Valor do Ativo (AV) $ 1 milhão, o Fator de Exposição (EF) 50%, e a Taxa Anual de Ocorrência (ARO) de 10% (1/10 , ou seja, 1 vez em dez anos), a Expectativa Anual de Perda (ALE) seria:

$$SLEF(\$) = AV \times EF = \$\ 1\ 000\ 000 * 50\% = 500\ 000$$
$$ALE = SLEF(\$) * ARO = 500\ 000 * 1/10 = 50\ 000$$

O valor estimado de $ 50 000 significa que a organização pode investir em controles de segurança até a ordem de $ 50 000 por ano para evitar a ocorrência ou reduzir o impacto da ameaça em questão.

De acordo com CCCURE (1999;p.12), algumas ressalvas devem ser feitas em relação às fórmulas para cálculo da ALE:

- aspectos como efetividade das contramedidas implementadas e o grau de incerteza não são contemplados pelo algoritmo ALE; e

- o cálculo não distingue efetivamente entre ameaças de baixa freqüência / alto impacto e alta freqüência / baixo impacto.

Aspectos como o valor do ativo e a freqüência de ocorrência de um determinado evento negativo são difíceis de serem definidos e podem dificultar a aplicação das fórmulas apresentadas acima.

Conforme WHITMAN (2003; p. 171), algumas empresas utilizam uma outra fórmula, a CBA ("Cost Benefit Analysis"), para avaliar se a implementação de um determinado controle acarretará em benefícios para a organização. A CBA pode ser calculada após a implementação do novo controle, ou apenas ser calculada como uma estimativa:

CBA = ALE (antes da implementação do controle) – ALE (depois da implementação do controle) – AC

onde:

ALE = "Annual Loss Expenctancy" (Expectativa Anual de Perda),
AC = "Annual Cost" (custo anual) do controle.

Em virtude da relevância do aspecto "determinação do impacto", ele foi considerando um requisito essencial na comparação das metodologias de Gerenciamento de Risco de TI apresentadas no Capítulo 03.

2.4.2.4 Determinação do risco

Nesta seção do documento buscamos apresentar os conceitos básicos referentes à determinação do risco, a qual está baseada na metodologia NIST SP 800-30. Existem outras abordagens para determinação do risco, apresentadas no Capítulo 3.

A determinação do risco somente é possível após o conhecimento (1) da probabilidade de acontecimento da ameaça; (2) da magnitude do impacto causado caso uma determinada vulnerabilidade seja explorada; e (3) da eficiência dos controles empregados para minimização dos riscos.

Uma abordagem comumente adotada para representação dos riscos é a utilização da Análise Qualitativa, na qual é elaborada uma matriz quadrada tendo no eixo das ordenadas a probabilidade de ocorrência da ameaça, e no eixo das abscissas o impacto causado pela ameaça.

O tamanho da matriz dependerá da granularidade com a qual pretende-se conduzir o processo de avaliação de risco. Em geral, utiliza-se uma matriz 3x3 sendo que, tanto a probabilidade quanto o impacto, são classificados em três categorias: alto, médio e baixo, já definidas anteriormente nas Tabelas 4 e 5, respectivamente.

Cada uma das categorias recebe um peso específico, definido pelo responsável pela análise de risco. Conforme STONEBURNER (2002; p.: 24), a Figura 7 demonstra o conceito apresentado anteriormente:

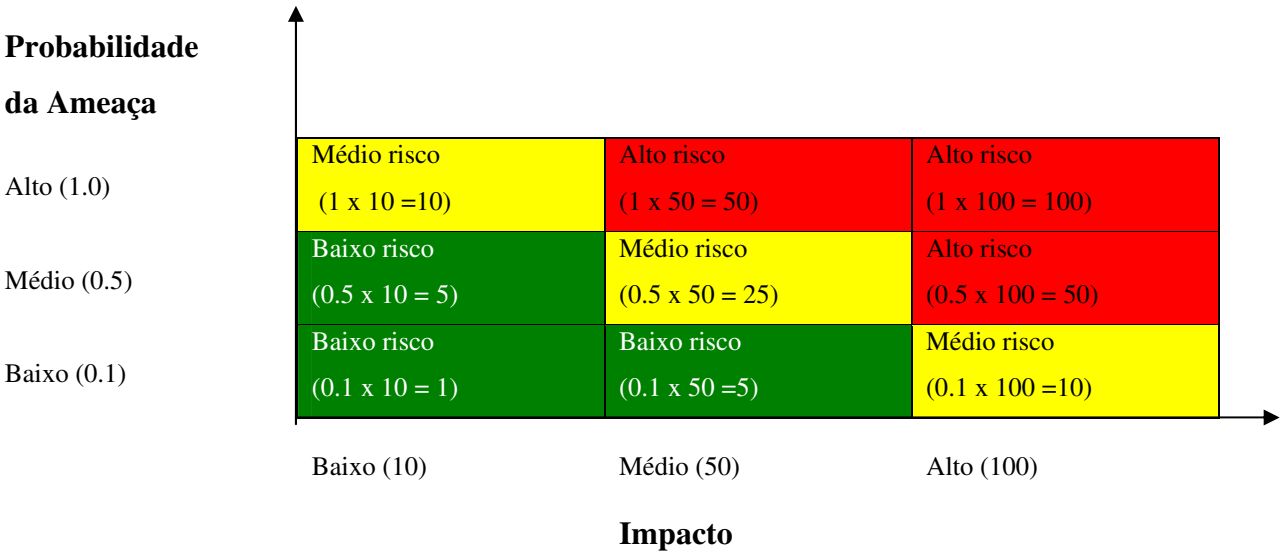

Figura 7: Matriz de nível de Risco

Na Figura 7 cada uma das escalas representa o risco ao qual o ativo está exposto, considerando a probabilidade de ocorrência de uma determinada ameaça, versus o impacto causado pela mesma ameaça.

Devemos considerar a seguinte interpretação para cada um dos níveis propostos:

- **Alto risco:** Há uma forte necessidade de que sejam aplicadas medidas corretivas imediatas, visto que há uma média->alta probabilidade da ameaça se materializar e causar danos às operações da organização.

- **Médio risco:** Medidas corretivas deverão ser tomadas em um curto período de tempo, visto que o provável impacto pode ser alto.

- **Baixo risco:** Neste caso deverá ser avaliado se a organização deseja tomar ações corretivas para minimizar o risco, diminuindo as perdas, ou decidirá apenas aceitá-lo.

Outras metodologias apresentam outras formas de determinação do risco, porém os fatores considerados, na grande maioria das vezes, são: (1) probabilidade de materialização da ameaça; (2) magnitude do impacto causado, caso uma determinada vulnerabilidade seja explorada; e (3) eficiência dos controles empregados para minimização dos riscos.

Em virtude da relevância do aspecto "determinação do risco", ele foi considerando um requisito essencial na comparação das metodologias de Gerenciamento de Risco de TI apresentadas no Capítulo 03.

2.4.3 Mitigação dos riscos

Uma vez identificados os riscos aos quais os ativos estão suscetíveis, inicia-se a etapa de mitigação dos riscos. A mitigação dos riscos consiste na seleção, priorização, avaliação e implementação de controles de segurança cuja finalidade é reduzir os riscos a um nível aceitável.

A eliminação completa dos riscos geralmente é inviável, devido ao alto custo envolvido nesse processo. Assim, cabe à alta administração e gerências de nível médio decidir sobre quais

controles serão implementados, ou seja, quais riscos serão minimizados e quais riscos serão assumidos pela organização.

Em geral as organizações adotam a abordagem do menor custo durante a seleção dos controles, porém esta pode ser uma estratégia arriscada caso os controles não sejam adequadamente avaliados. Adicionalmente, a necessidade de atendimento a determinadas legislações, ou seja, a necessidade de adoção dos controles mandatórios, pode impedir que abordagem mencionada acima seja empregada.

2.4.3.1 Opções para mitigação dos riscos

De fato, há somente três abordagens possíveis para mitigação dos riscos: (a) evitar o risco, (b) controlar / reduzir o risco ou (c) transferir o risco. Embora algumas bibliografias mencionem, a (d) aceitação do risco como estratégia de mitigação, esta não é efetivamente uma estratégia com tal finalidade, visto que ele consiste apenas no reconhecimento do risco, e não no tratamento do mesmo. Abaixo segue o detalhamento de cada uma das abordagens:

- **Evitar o risco**: Evitar o risco consiste em impedir a exploração de uma determinada vulnerabilidade. Em geral essa é uma das abordagens preferidas, visto que é mais fácil evitar o risco do que lidar com ele depois de materializado. A ação de evitar o risco é obtida através da contenção das ameaças, da remoção das vulnerabilidades nos ativos, e por meio da aplicação dos controles necessários, o que inclui implementação ou modificação de procedimentos ou tecnologia.

- **Controlar (ou reduzir) o impacto do risco**: O controle do impacto do risco é uma das abordagens mais comuns no tratamento dos riscos. Neste caso ocorre o reconhecimento do risco e a adoção de mecanismos para monitorá-lo e gerenciá-lo. Nesse contexto de redução do impacto causado pelo risco estão inseridos os Planos de Continuidade de Negócios, o Plano de Recuperação de

Desastres, e o Plano de Resposta a Incidentes. A adoção de cada uma dessas estratégias depende da habilidade da organização de detectar e responder ao ataque o mais rápido possível.

De acordo com WHITMAN (2003; p. 161) podemos definir, de modo sucinto:

- Plano de Resposta a Incidentes: ações que as organizações adotam durante os ataques. São aplicados no momento do incidente.

- Plano de Recuperação de Desastres: estratégias para limitar as perdas antes e durante os desastres, instruções passo a passo para retomar a normalidade. São medidas adotadas a curto prazo.

- Plano de Continuidade de Negócios: estratégia adotada para assegurar a continuidade dos negócios da organização, quando o desastre ocorrido tomou grandes proporções. Em geral requer re-alocação das operações.

- **Transferir o risco:** A transferência do risco é uma das opções adotadas pelas empresas quando a adoção de controles para minimizar o risco não é possível. Neste caso, a opção comumente adotada pelas empresas é a aquisição de seguros. Assim, caso o risco se materialize, as perdas ocorridas são recompensadas por um terceiro. A transferência ocorre principalmente quando as perdas são muito grandes, estando além das possibilidades da organização. Cabe destacar que, quando a transferência do risco é a estratégia adotada, é importante que seja verificada a solvência da organização para qual está se fazendo a transferência do risco, a fim de assegurar que, caso ocorra um incidente a saúde financeira da seguradora permitirá o ressarcimento dos prejuízos.

O estabelecimento de contratos formais entre as duas entidades que se relacionam, no qual estão compartilhadas responsabilidades, também é considerada uma forma de transferência de risco entre as partes.

De acordo com WHITMAN (2003; p. 158), algumas vezes a transferência do risco é feita não somente com a contratação de seguros, mas também por meio da contratação de empresas especializadas para o desempenho de determinadas atividades. Neste caso o risco envolvido nessas atividades é gerenciado pela empresa terceira. Desse modo, observamos que também ocorre a transferência dos riscos, ainda que indiretamente.

- **Aceitar o risco:** A aceitação do risco consiste no reconhecimento da existência do risco e na decisão de aceitar as possíveis conseqüências caso o risco se materialize. A ação de aceitação do risco pode ser uma decisão de negócio consciente ou inconsciente. Existem situações nas quais devido aos altos custos envolvidos no processo de mitigação do risco, a única estratégia possível é a aceitação. Em geral, quando as empresas não adotam nenhuma ação para contenção do risco, automaticamente os riscos são aceitos. É prudente que a organização tenha claramente mapeados quais riscos estão sendo aceitos e quais serão tratados.

  De acordo com WHITMAN (2003; p. 161), a estratégia de aceitação do risco é considerada como consciente, e válida, quando a organização efetua algumas ações, dentre elas:

  - determina o nível de risco;
  - avalia a probabilidade de um ataque;
  - estima a perda potencial que os ataques podem causar;
  - efetua uma análise de custo benefício; e
  - avalia a aplicabilidade de cada tipo de controle.

A partir das ações acima, a organização tem condições de decidir conscientemente pela aceitação do risco, visto que tais levantamentos permitirão à organização visualizar adequadamente que o custo de proteger um determinado ativo não justifica o investimento a ser feito em segurança. Muitas vezes conclui-se que o custo de substituição do ativo é menor que o custo de proteção do mesmo.

A seleção da abordagem mais aderente às necessidades da organização dependerá do volume de investimentos disponíveis a serem aplicados no gerenciamento dos risco, do ramo de atuação da empresa, bem como do direcionamento estratégico da mesma. Algumas empresas simplesmente assumem adotar como estratégia única a transferência do risco, porém esta estratégia nem sempre é válida para qualquer negócio, visto que alguns aspectos não poderão ser restabelecidos. Por exemplo, em uma instituição financeira que não possua nenhum controle preventivo contra desastres em seu CPD, caso ocorra algum incidente grave que indisponibilize suas operações, milhares de correntistas (pessoa física e / ou jurídica) estarão impossibilitados de efetuarem suas transações (pagamentos, recebimentos, transferências, etc). Assim, ainda que o banco re-estabeleça suas operações e indenize seus correntistas, muitos deixarão de operar nesta instituição e os prejuízos da organização serão muito maiores do que os valores assegurados, podendo até mesmo acarretar na extinção da organização.

A tabela abaixo pode ser utilizada como suporte na decisão de qual estratégia adotar referente a estratégia de mitigação dos riscos:

Aceitável	**Transferível**	**Reduzível**	**Ação**
Não	Não	Não	Evitar o risco
Não	Não	Sim	Reduzir e reavaliar
Não	Sim	Não	Adotar seguros (transferência) ou evitar o risco
Não	Sim	Sim	Balancear a adoção de seguro (transferência) ou reduzir o risco
Sim	Não	Não	Aceitar ou evitar o risco

Sim	Não	Sim	Balancear a redução com o custo de aceitação
Sim	Sim	Não	Aceitar ou adotar seguros (transferência)
Sim	Sim	Sim	Balancear todas as opções e adotar a mais viável

Tabela 6: Opções para mitigação do risco

Conforme mencionado anteriormente, nem todos os riscos podem ser totalmente mitigados; dessa forma, sempre haverá um risco residual que a organização terá que aceitar. O risco residual pode ser definido como todo risco potencial remanescente após os controles de segurança terem sido aplicados. Há um risco residual associado com cada ameaça / vulnerabilidade. Isto decorre do fato de que eliminar todas as potenciais ameaças (e vulnerabilidades) pode ser financeiramente inviável para a empresa.

Riscos Residuais = Total de Riscos – Riscos Mitigados

As organizações podem analisar a redução do risco (em função do aprimoramento dos controles existentes ou da implementação de novos) por meio da mensuração da redução da probabilidade de ocorrência da ameaça ou da vulnerabilidade, os dois parâmetros que definem o nível de mitigação do risco.

A interpretação do risco residual, bem como a forma como tratá-lo, varia de organização para organização. Cabe destacar que o objetivo da área de Segurança da Informação/ Riscos não é eliminar o risco residual, mas apenas controlá-lo de modo que esteja na zona de conforto para a organização. A alta administração da empresa deve ser informada sobre quais riscos residuais ela está sujeita.

Uma vez identificados todos os riscos e desde que a organização não tenha adotado como estratégia a aceitação dos mesmos, a próxima etapa é a análise e definição dos controles a serem implementados para mitigação dos riscos. A implementação de defesas deve ser feita por camadas, controle sobre controle.

Em geral, a alta administração estará mais propensa a minimizar aqueles riscos que apresentam maior possibilidade de perdas financeiras, bem como aqueles que estão sujeitos a regulamentação específica do ramo de atuação no qual atua e / ou aplicação de multas contratuais.

A análise de controles é uma atividade extremamente cautelosa, na qual o analista que a estiver executando deverá:

- identificar o controle mais adequado para cada vulnerabilidade;
- efetuar a associação de controle versus vulnerabilidade para todas as ameaças relacionadas;
- identificar para cada ameaça qual a redução do risco obtida com a implementação do controle, ou seja, para cada ameaça determinar se o controle irá reduzir a freqüência da ameaça, reduzir o fator de exposição, ou ambos e com que grau.

Em virtude da complexidade intrínseca à atividade de seleção de controles, é necessário que ela seja apoiada em ferramentas automatizadas que consigam manipular todas as variáveis mencionadas e gerar resultados precisos. Algumas das ferramentas disponíveis no mercado são:

- Risk Watch, Inc. - Risk Watch For Information Systems & 17799, Version 9.2.1
- Omini Software - Pense Tecnologia De Informação, Version 1.0
- Citicus Limited - Citicus One Release 1.31
- Infosecure - Israc (Infosecure Risk Assessment And Compliance) Tool, Version 4.2.10

É importante destacar que os controles empregados, por si próprios, podem conter vulnerabilidades, o que resultará em novos riscos para a organização. Assim, muita cautela deverá ser adotada na seleção dos controles visando não apenas reduzir os riscos existentes, mas também não introduzir novos riscos no ambiente.

As etapas comumente adotadas referentes à mitigação dos riscos incluem: (1) priorização das ações; (2) avaliação dos controles disponíveis; (3) análise de custo x benefício e (4) seleção do controle.

Em virtude da relevância do aspecto “mitigação do risco” e “risco residual”, ambos foram considerados requisitos essenciais na comparação das metodologias de Gerenciamento de Risco de TI apresentadas no Capítulo 03.

2.4.3.1.1 Tipos de controles

Os controles podem ser classificados de diferentes formas. Uma delas é classificá-los de acordo com sua natureza, por exemplo, controles gerenciais, operacionais e técnicos. Outro método é efetuar a categorização por área funcional: sistemas aplicativos, telecomunicações, redes, desenvolvimento de sistemas, operações, etc. Uma terceira abordagem é classificá-los de acordo com o objetivo ou propósito a que se destinam; neste caso a divisão seria: preventivos, detectivos ou corretivos. Nesta última abordagem, alguns autores ainda incluem os controles diretivos e os de recuperação, porém essa divisão não é comumente aceita, visto que os controles diretivos podem ser inseridos nas três categorias, e os controles de recuperação podem ser classificados como controles corretivos.

Independente da nomenclatura utilizada, o objetivo do controle é contribuir no alcance dos objetivos da organização. A natureza do controle e a quantidade a ser implementada estão diretamente relacionados aos riscos aos quais a organização está exposta. Cabe destacar que, controles que estão disponíveis nos recursos tecnológicos mas não estão adequadamente implementados fornecem nenhuma proteção.

Ainda em relação ao uso de controles, existem três aspectos a serem abordados: controles complementares, controles compensatórios e controles contraditórios. Controles complementares são aqueles que, quando combinados, se tornam mais eficazes no aprimoramento da segurança do ambiente do que se utilizados isoladamente. Controles compensatórios são aqueles que

compensam a fraqueza existente pela não implementação (ou implementação inadequada) de outros controles. E os controles contraditórios são aqueles que, quando implementados, anulam a existência de outros. Esses três aspectos devem ser considerados quando da implementação de novos controles, visando mitigar o risco existente.

2.4.3.1.2 Categorias de controles por objetivo

Abaixo, detalhamos as categorias de controles existentes, de acordo com o objetivo a que se propõem:

- **controles preventivos**: compreendem todas as metodologias, práticas, ferramentas, tecnologias, para aprimorar a confiabilidade dos recursos. Tem por função impedir ou minimizar que eventos indesejáveis ocorram, evitando a incidência de erros, omissões ou ações maliciosas, e principalmente impedindo que os riscos se materializem. Em geral, a adoção de controles preventivos é melhor quando comparados aos detectivos ou corretivos. Cabe destacar que nem sempre é possível a implementação de controles preventivos; além disso, muitas vezes eles não são economicamente viáveis.

  São exemplos de controles preventivos: segregação de funções, mecanismos de controle de acesso físico / lógico, software antivírus, conscientização, classificação das informações, firewall; dentre outros.

- **controles corretivos**: compreendem informações, procedimentos e instruções que tem por funções (1) minimizar o impacto causado pela ameaça; (2) corrigir problemas identificados pelos controles detectivos; (3) identificar a causa dos problemas; (4) corrigir erros; e modificar procedimentos para evitar a ocorrência de problemas futuros.

São exemplos de controles corretivos: plano de contingência, extintores, dentre outros.

- **controles detectivos**: controles que detectam que um erro, omissão ou ação maliciosa ocorreu. Os controles detectivos dão um "feedback" sobre a segurança do ambiente e se os controles preventivos atingiram seus objetivos. Controles detectivos incluem técnicas manuais e automatizadas e metodologias para medição da efetividade dos controles preventivos.

  São exemplos de controles detectivos: trilhas de auditoria, alarmes, IDS – "Intrusion Detection Systems", e câmeras de monitoramento, dentre outros.

2.4.3.1.3 Categorias de controle por natureza

Abaixo, detalhamos as categorias de controles existentes, de acordo com a natureza dos mesmos:

- **controles gerenciais**: os controles gerenciais focam no gerenciamento da segurança de TI e dos riscos relacionados ao ambiente. Exemplos de controles gerenciais incluem: gerenciamento de risco, conscientização, política de segurança da informação, plano diretor de TI/Segurança, definição de papéis e responsabilidades, treinamento, dentre outros.

- **controles operacionais**: estes estão relacionados principalmente à operacionalização dos procedimentos de segurança estabelecidos. Esses controles muitas vezes requerem conhecimentos específicos (treinamento) e devem ser suportados por documentações detalhadas de todas as atividades a serem desempenhadas pelos colaboradores.

- **controles técnicos**: os controles técnicos podem variar desde medidas simples até medidas complexas e em geral envolvem a arquitetura dos sistemas, pacotes de segurança e um mix de hardware e software. Todos esses componentes trabalham juntos à proteção dos dados e informações sensíveis.

2.4.3.2 Abordagem para implementação dos controles

a. Priorização das ações

A estratégia de mitigação dos riscos deve ser elaborada a partir da classificação atribuída a eles. Preferencialmente, as ações a serem implementadas necessitam ser priorizadas de acordo com a classificação que os riscos receberam. Todos os riscos classificados como "altos" e "médios" devem receber um tratamento especial.

b. Avaliação dos controles disponíveis

Para cada um dos riscos identificados é necessário avaliar os controles para mitigação dos mesmos. Durante esta etapa, a viabilidade deve ser avaliada (exemplo.: compatibilidade, aceitação pelo usuário, etc) e a efetividade (exemplo: grau de proteção e nível de mitigação do risco) do controle devem ser avaliadas. O objetivo é selecionar a opção de controle mais apropriada para minimizar o risco.

c. Análise de custo x benefício

A análise de custo x benefício tem por objetivo demonstrar que os custos de implementação dos controles podem ser justificados pela redução no nível de risco. A análise de custo x benefício pode ser quantitativa ou qualitativa.

Durante a análise de custo x benefício alguns aspectos devem ser avaliados:

- determinação do impacto causado pela implementação do novo controle;
- determinação do impacto da não implementação do novo controle;
- estimativa dos custos de implementação, que compreendem:
  - custos com hardware / software;
  - custos de treinamento dos colaboradores afetados pelo novo controle;
  - custos de contratação de mão de obra;
  - custos de manutenção;
- criticidade do recurso cujo controle estará protegendo, possibilitando analisar a importância ou não da implementação do controle.

A alta administração deve estabelecer qual o nível de risco aceitável pela organização. O impacto do controle pode ser avaliado, e o controle incluído ou excluído, após a organização determinar o nível aceitável de risco ao qual aceita estar suscetível. Esse nível varia de organização para organização; entretanto alguns critérios devem ser adotados durante a seleção de controles:

- se o controle reduz o risco mais do que necessário, provavelmente haverá uma alternativa menos dispendiosa;
- se o controle for mais dispendioso do que a redução de risco oferecida, outro controle deverá ser selecionado;
- se o controle não reduz o risco suficientemente, outra alternativa deverá ser avaliada; e
- se o controle fornece redução suficiente do risco e apresenta um bom custo x benefício, então ele provavelmente será a alternativa mais apropriada.

Um único controle pode solucionar uma ou mais vulnerabilidades para uma ou mais ameaças; dessa forma essa característica deverá ser considerada durante o processo de análise de custo x benefício de um determinado controle.

d. Seleção do controle

Com base na avaliação feita dos controles disponíveis, bem como no resultado da análise de custo x benefício realizada para cada um dos controles, é possível efetuar a seleção do controle a ser implementado.

Em virtude dos controles não serem independentes e freqüentemente atuarem em conjunto, o processo de seleção deve considerar essas possíveis interdependências. Durante o processo de seleção de um controle deve-se atentar para que falhas não sejam deixadas, propiciando que os controles implementados sejam desprezados, permitindo possíveis danos ao ambiente.

No caso da implementação de novos sistemas ou mudanças significativas nos existentes, a seleção do controle deverá contemplar uma revisão na arquitetura de segurança. A arquitetura de segurança da aplicação tem como propósito descrever quais requisitos de segurança deverão ser atendidos, podendo contemplar controles técnicos ou procedurais.

2.5 Monitoramento

O ambiente de tecnologia está em constante mudança; atualizações, expansões e substituições de componentes são continuamente realizadas. Adicionalmente, os procedimentos operacionais estabelecidos se alteram com o passar do tempo, muitas vezes decorrentes da rotatividade de pessoal em determinadas funções. Todas essas mudanças significam que novos riscos estão sendo "inseridos" no ambiente, e que outros previamente mitigados podem voltar a se tornar uma preocupação. Conseqüentemente, o processo de Gerenciamento de Risco de TI deve ser algo contínuo e abrangente.

Preferencialmente deve ser estabelecida uma periodicidade para realização da análise de risco. Entretanto, a organização deve ser flexível também para realizá-la sempre que sentir necessidade, ou sempre que novos elementos forem inseridos no ambiente.

O uso dos controles deve ser monitorado para assegurar que eles estejam funcionando corretamente, e que as mudanhças no ambiente não prejudicarão a efetividade dos controles. Basicamente deve ser verificado se o controle está funcionando, e se a eficácia do controle está dentro dos padrões previstos e estabelecidos como aceitáveis. Revisões automatizadas da segurança do ambiente, bem como o uso de recursos de auditoria, como "logs" e trilhas de auditoria são recursos que dão suporte a esse processo. Essas ferramentas também podem ser utilizadas para detectar eventos indesejáveis ocorridos no ambiente.

Em virtude da relevância do aspecto "continuidade do processo de gerenciamento de risco", ele foi considerando um requisito essencial na comparação das metodologias de Gerenciamento de Risco de TI apresentadas no Capítulo 03.

No próximo capítulo apresentaremos três metodologias de Gerenciamento de Risco de TI comumente empregadas e uma análise comparativa de como essas metodologias abordam os principais elementos do Gerenciamento de Risco de TI, apresentados ao longo do Capítulo 2.

Capítulo 3 - Análise das metodologias de Gerenciamento de Risco de TI: FIRM, NIST SP 800-30 e OCTAVE

3.1 Principais aspectos das metodologias FIRM, NIST SP 800-30 e OCTAVE

OCTAVE

A metodologia Operationally Critical Threat, Asset and Vulnerability Evaluation Methodology (OCTAVE) versão 2.0, datada de 2001, foi desenvolvida pelo Software Engineering Institute como uma metodologia de análise de risco adaptável para o uso em organizações públicas ou privadas, que possuam mais de duzentos empregados. OCTAVE fornece um meio pelo qual uma organização consegue entender e endereçar todos os riscos técnicos e organizacionais referentes à segurança da informação.

A OCTAVE é uma metodologia qualitativa de análise de risco desenvolvida para identificar:

- ativos críticos de informação;
- ameaças que afetam os ativos críticos;
- vulnerabilidades associadas com tais ativos; e
- níveis atuais de risco referentes aos ativos críticos.

Esta metodologia auxilia a organização a entender melhor os resultados de suas avaliações de risco, de modo que possa desenvolver, ou refinar adequadamente, as estratégias de segurança para proteção dos ativos, e os planos de mitigação desenvolvidos conforme os requerimentos de segurança de cada ativo.

A OCTAVE apresenta algumas atividades preliminares que necessitam ser conduzidas antes do início da avaliação e oito principais processos relacionados diretamente com a análise de risco, os quais foram divididos em três fases:

- Na fase de inicialização, a equipe destinada à condução do processo executa as atividades preliminares, as quais incluem: (1) obter o comprometimento da alta administração, os quais devem atuar como "responsáveis" durante a aplicação da OCTAVE; (2) selecionar os profissionais das áreas de negócio e TI que possuam conhecimentos adequados para atuarem na equipe de análise (grupo principal responsável por liderar e executar as atividades propostas pela OCTAVE); e (3) fornecer os treinamentos necessários para a equipe de análise e demais participantes do processo.

- Na Fase 1, a equipe de análise conduz um workshop com a alta administração para identificar os ativos críticos de informação e documentar as ameaças às quais os ativos estão sujeitos, os requerimentos de segurança, as práticas atuais adotadas como estratégias de proteção, e as vulnerabilidades encontradas na organização relacionadas ao ativo crítico. Adicionalmente, esta equipe de análise atua juntamente com a alta administração para definir quais áreas operacionais farão parte do escopo de avaliação de risco, onde será aplicada a metodologia OCTAVE.

  Ainda na Fase 1, a equipe de análise conduz um workshop com os gerentes das áreas operacionais, o qual é muito parecido com o workshop conduzido com a alta administração, para obter as expectativas referentes aos mesmos aspectos. Esse mesmo workshop também é conduzido com o staff das áreas de negócio e TI, visando obter um detalhamento técnico mais apurado.

- Na Fase 2, a equipe de análise trabalha muito próxima ao "staff" de TI (ou consultorias externas, se necessário) para identificar os denominados "sistemas de interesse" (aqueles sistemas que estão fortemente relacionados a pelo menos um dos ativos classificados como crítico). Em geral são empregadas ferramentas automatizadas (software) para efetuar o diagnóstico das vulnerabilidades existentes em cada componente essencial de infra-estrutura que suporta os ativos críticos.

- Na Fase 3, a equipe de análise completa o processo de análise de risco por meio da consolidação das informações obtidas nas Fases 1 e 2. Ainda nesta fase é concluída a definição de um critério de avaliação de risco para determinar o que será considerado um alto, médio ou baixo impacto para a organização. A equipe então atualiza o perfil de ameaça / risco de cada ativo com a descrição do impacto e aplica o critério de avaliação de risco definido previamente para documentar se cada risco teria um alto, médio ou baixo impacto para a organização.

Utilizando as informações criadas na Fase 1 quando a alta administração / gerência operacional / staff compararam as práticas de segurança da organização com o Catálogo de Práticas (documento contendo as boas práticas de segurança que integra a metodologia OCTAVE), e combinado com o resultado da análise de risco, a equipe de análise elabora um "draft" da estratégia de proteção, a qual irá preservar as boas práticas existentes na organização e também contemplará as contramedidas necessárias para as vulnerabilidades organizacionais identificadas durante a execução da OCTAVE. É então desenvolvido um plano de mitigação de risco para os ativos críticos, e são listadas as ações de curto prazo a serem executadas, identificadas como necessárias durante o desenvolvimento das estratégias de longo prazo. Esta fase final é concluída com a equipe de análise revisando junto à alta administração os principais riscos mapeados durante a fase de levantamento, e ajustando as Estratégias de Proteção da Organização / Plano de Mitigação de Riscos e Lista de Ações. Esta atividade tem por objetivo assegurar a obtenção do comprometimento da alta administração com os resultados da OCTAVE, garantindo que a percepção da alta administração tenha sido refletida e que os resultados estejam em conformidade com a missão e objetivos da organização.

NIST SP 800-30

O National Institute of Standards and Technology Special Publication 800-30 é um conjunto de diretrizes para o gerenciamento dos riscos de segurança da informação publicada pelo NIST em julho de 2002 para uso por organizações públicas ou privadas. Estas diretrizes foram elaboradas

para proverem os fundamentos para o desenvolvimento de um programa efetivo de Gerenciamento de Risco de TI, o qual está baseado na proteção dos ativos de informação.

Esta metodologia fornece elementos cruciais relacionadas ao tema Gerenciamento de Risco de TI, permitindo que os usuários possam conduzir o ciclo completo deste processo, o qual abrange a identificação do risco, mitigação do risco e avaliação contínua. O NIST fornece uma visão geral em relação aos seguintes elementos de Gerenciamento de Risco de TI:

- **Gerenciamento de risco e o inter-relacionamento no ciclo de desenvolvimento de sistemas ("systems development life cycle" – SDLC):** esta metodologia especifica quando e como o gerenciamento de risco deve ser incluído no SDLC, ou seja, apresenta as cinco fases do SDLC e direciona qual atividade de gerenciamento de risco é apropriada para cada uma das fases.

- **O processo de Gerenciamento de Risco de TI:** a metodologia apresentada pelo NIST tem por finalidade fornecer uma abordagem sistemática para gerenciamento dos riscos, conduzindo o usuário da metodologia por etapas, sendo que para cada uma delas são apresentadas as entradas e saídas esperadas, e o encadeamento da fase atual com a próxima. As nove etapas abrangidas pelo NIST SP 800-30 são:

  - Etapa 1 - Caracterização do Sistema: nesta etapa a função, criticidade e sensibilidade dos ativos (definidos no escopo da avaliação) são mapeados por meio de diversas técnicas de obtenção de informações.

  - Etapa 2 - Identificação das Ameaças: nesta etapa as ameaças são identificadas e agrupadas de acordo com a motivação de cada uma e suas respectivas ações.

  - Etapa 3 - Identificação das Vulnerabilidades: nesta etapa é elaborada uma lista de vulnerabilidades técnicas e não técnicas associadas com os sistemas de TI, que podem ser exploradas por fontes potenciais de ameaça.

- Etapa 4 - Análise dos Controles: esta etapa visa avaliar a efetividade dos controles empregados atualmente, ou que se planeja empregar, para minimizar ou eliminar a probabilidade de uma ameaça explorar uma vulnerabilidade.

- Etapa 5 - Determinação da Probabilidade: define a probabilidade de uma fonte de ameaça explorar uma vulnerabilidade específica de um determinado ativo.

- Etapa 6 - Análise de Impacto: esta etapa consiste em mensurar o impacto adverso causado pela exploração de uma vulnerabilidade por uma ameaça.

- Etapa 7 - Determinação do Risco: esta etapa define os prováveis níveis de risco para os ativos de informação que estejam sob análise.

- Etapa 8 - Recomendações de Controle: define quais controles devem ser empregados para mitigar ou eliminar os riscos identificados nas etapas anteriores.

- Etapa 9 - Documentação dos Resultados: menciona que todos os resultados das etapas anteriores do processo de Gerenciamento de Risco de TI devem estar documentados.

- **Processo de mitigação do risco:** O NIST SP 800-30 fornece algumas diretrizes e informações para priorizar, avaliar, e implementar controles para redução dos riscos mapeados.

A publicação NIST SP 800-30 também contempla alguns apêndices elaborados para suportar as etapas apresentadas anteriormente. Dentre eles temos:

- ferramentas e fórmulas para determinar os níveis de risco para os ativos de informações;
- as vantagens e desvantagens de utilizar técnicas quantitativas versus qualitativas durante as avaliações de risco;
- uma lista de questões para mapeamento de informações, a ser empregada nas entrevistas de levantamento; e
- um exemplo de relatório de consolidação de resultados da análise de risco efetuada.

FIRM

A FIRM é uma abordagem prática para condução do processo de Gerenciamento de Risco de TI, a qual foi elaborada pelos membros que participam do Information Security Fórum[3] os quais, em sua maioria são profissionais que ainda atuam em áreas relacionadas ao tema, o que contribuiu para que o conteúdo da metodologia abordasse aspectos e dificuldades comumente encontradas pelas empresas, permitindo uma maior proximidade da realidade nas colocações e recomendações. A versão atual da metodologia foi publicada em março de 2000.

Esta metodologia é composta por dois documentos, sendo que um deles contém somente conceitos fundamentais para compreensão do tema e algumas informações complementares referentes ao processo de Gerenciamento de Risco de TI, o qual foi denominado "Fundamental Information Risk Management – Supporting Material".

Os principais objetivos dessa metodologia são:

- destacar os requisitos fundamentais do processo de Gerenciamento de Risco de TI;

[3] Information Security Fórum é uma associação independente, sem fins lucrativos, composta por profissionais que se reúnem para resolver questões relacionadas a segurança da informação. Os membros do ISF são profissionais renomados com profundo conhecimento e experiência sobre o tema.

- fornecer ferramentas práticas, elaboradas para o alcance dos requisitos fundamentais de Gerenciamento de Risco de TI;
- explicar como adaptar as ferramentas às necessidades individuais de cada organização; e
- explicar como aplicar a abordagem de Gerenciamento de Risco de TI nas operações do dia-a-dia.

A metodologia FIRM está estruturada em nove capítulos (ou partes, conforme nomenclatura adotada pela mesma), as quais são denominadas:

1. Introdução: Este capítulo do documento apresenta como a metodologia está estruturada, quais os objetivos do documento, os símbolos utilizados para compreensão da mesma; e onde poderão ser obtidas informações adicionais sobre as terminologias empregadas.

2. Definindo o contexto: este capítulo define o escopo de atuação da metodologia, e quais aspectos estão ou não cobertos pela metodologia.

3. Desenvolvendo uma abordagem prática: este capítulo visa demonstrar o que as empresas têm feito para o monitoramento dos aspectos de segurança e quais as principais dificuldades comumente encontradas pelas organizações na implementação de um processo de "monitoramento de segurança da informação", e algumas formas de superá-las.

4. Definindo o propósito e escopo: conforme a própria denominação deste capítulo, aqui os autores abordam como principais tópicos o (1) objetivo do Gerenciamento de Risco de TI e (2) qual a abrangência de execução do mesmo.

5. Mapeando as estratégias de comunicação e funções envolvidas: nesse capítulo é enfatizada a importância de se possuir uma estratégia de comunicação durante a condução de um processo de Gerenciamento de Risco de TI, sendo que nesse capítulo são

apresentadas quais entidades devem ser envolvidas, qual o papel a ser desempenhado por cada uma delas e como deve ser a estratégia de comunicação para alcance de todos.

6. Identificando métodos de obtenção de informação: Neste capítulo os autores reforçam que a obtenção de informações precisas é um aspecto essencial para a correta tomada de decisões, e apresenta algumas "ferramentas" para o levantamento das informações essenciais. Todo o mapeamento de informações necessárias para mensuração do risco, como por exemplo a criticidade dos ativos, ameaças, vulnerabilidades, dentre outros, são obtidas a partir de um formulário denominado "Information Risk Scorecard" apresentado nessa seção.

7. Definindo um processo construtivo de monitoramento: Neste capítulo o autor reforça a necessidade de que seja criado um processo construtivo para monitoramento da segurança das informações. Este processo deve encorajar os colaboradores a contribuírem com as informações necessárias para determinação e identificação dos riscos. Deve-se atentar para que não seja visto como um processo que visa identificar falhas e culpados, pois nesse caso dificilmente terá resultados positivos.

   Basicamente o processo construtivo de monitoramento está dividido em duas fases: Fase I: Encorajamento e Fase II: Comunicação. Essas duas fases são divididas em dez etapas, as quais estão relacionadas abaixo:

   Etapa 1: Identificar os "proprietários" dos recursos a serem monitorados.
   Etapa 2: Encaminhar o "Information Risk Scorecard" aos proprietários dos recursos de informação.
   Etapa 3: Identificar coordenadores locais para complementar as informações do "Information Risk Scorecard".
   Etapa 4: Informar os proprietários das informações sobre os resultados obtidos a partir do "Information Risk Scorecard".
   Etapa 5: Identificar as prioridades para ação.

Etapa 6: Auxiliar os "proprietários" a reduzir os altos riscos referentes aos recursos de informação.

Etapa 7: Re-encaminhar o "Information Risk Scorecard" aos proprietários dos recursos de informação.

Etapa 8: Analisar os resultados obtidos a partir do "Information Risk Scorecard" e compará-lo com os da Etapa 4.

Etapa 9: Avaliar o status de segurança da empresa, principais ações de sucesso e necessidade para ações adicionais.

Etapa 10: Apresentar o relatório para a alta administração e acordar prioridades para ação e novos objetivos.

8. Comunicação concisa dos resultados: esse capítulo visa orientar quais informações deverão ser contempladas nos relatórios de consolidação dos resultados do processo de Gerenciamento de Risco de TI, visto que o processo de monitoramento de segurança da informação somente será efetivo quando conseguir capturar a atenção dos tomadores de decisão, ou seja, a alta administração, as pessoas chaves das áreas de negócio, e os "proprietários" responsáveis pelos recursos de informação.

9. "Guidelines" de implementação: Neste último capítulo o autor apresenta a abordagem prática para a implementação da FIRM. A implementação da abordagem prática está dividida em seis grandes etapas e para cada uma delas os autores fazem uma proposição do tempo a ser despendido. O esforço envolvido em cada etapa está diretamente associado ao tamanho e estrutura organizacional da empresa.

Dentre os nove capítulos mencionados, somente os capítulos de 4 a 8 focam a abordagem estruturada de Gerenciamento de Risco de TI dessa metodologia.

3.2 Análise comparativa dos aspectos relevantes de cada metodologia

A seguir comparamos as as três metodologias de Gerenciamento de Risco de TI, FIRM, OCTAVE e NIST SP 800-30, utilizando como base os elementos essenciais de Gerenciamento de Risco de TI, apresentados no capítulo "2. O processo de Gerenciamento de Risco de TI".

Considerando que as três metodologias abordam o mesmo assunto, ou seja, identificar os riscos relacionados aos ativos de informação, elas são muito similares nas fases que compõem a estrutura básica delineada no Capítulo 2: identificação dos riscos, mitigação e monitoramento. As diferenças existentes entre as metodologias estão baseadas em atividades e /ou produtos específicos gerados dentro dessas fases. Em todas as metodologias, as fases obedecem à mesma ordem cronológica.

A fim de possibilitar a comparação entre os documentos, identificamos alguns aspectos os quais julgamos mais relevantes, e que nortearão nossa comparação. São eles:

- Estrutura dos documentos
- Escopo da metodologia
- Pré-requisito do processo de Gerenciamento de Risco de TI
- Envolvimento da alta administração
- Identificação dos ativos críticos
- Mapeamento de vulnerabilidades
- Identificação de ameaças
- Análise dos controles atualmente empregados
- Análise do impacto no ambiente
- Determinação do risco
- Controles para mitigação dos riscos
- Continuidade do processo de Gerenciamento de Risco de TI
- Tratamento do risco residual

- Nível de utilização internacional da metodologia
- Nível de aderência a requisitos legais

Detalharemos a seguir cada um desses aspectos. Para cada um dos requisitos foram inseridos comentários subjetivos os quais estão destacados em itálico. Essa notação foi adotada somente no item em 3.2 desta dissertação, visando facilitar a identificação de tais comentários.

3.2.1 Estrutura dos documentos

Esse aspecto visa avaliar como as metodologias estão estruturadas em termos de facilidade de compreensão, clareza na exposição do tema e diferenciais da metodologia.

FIRM

A metodologia FIRM é composta por dois volumes: o primeiro, denominado "Fundamental Information Risk Management", compreende toda a metodologia para condução do processo de análise de risco; o segundo, denominado "Fundamental Information Risk Management - Supporting Material", é complementar ao primeiro, e contém todos conceitos necessários para entendimento do tema, os formulários utilizados pela metodologia, e todos os apêndices que complementam o primeiro volume.

Em termos de conteúdo a metodologia é bem detalhada e busca em vários momentos apresentar dados que sejam obtidos a partir de "cases" de sucesso, ou pesquisas efetuadas pelo órgão responsável pela elaboração da metodologia, o "Information Security Fórum", a fim de embasar as colocações efetuadas.

Durante a leitura do material observamos que é utilizada uma grande quantidade de símbolos para enfatizar determinados conceitos ou referências, porém devido à diversidade de símbolos e significados, em alguns momentos tal recurso não surte o efeito desejado, tornando o texto extremamente poluído.

Outro aspecto negativo identificado é a quantidade de referências feitas a documentos externos, publicados pelo próprio ISF, não disponíveis ao leitor, o que faz com que em determinados momentos informações complementares não possam ser facilmente obtidas.

Em relação ao conteúdo, observamos alguns diferenciais em relação às demais metodologias, os quais relacionamos abaixo:

- a metodologia apresenta as principais dificuldades encontradas pelas empresas para implementação do processo de Gerenciamento de Risco de TI;

- define detalhadamente as funções das principais entidades envolvidas no processo de Gerenciamento de Risco de TI: alta administração, comitê executivo, auditoria, área de segurança, coordenadores locais de segurança, proprietário da informação, usuário final;

- reforça a importância de se adotar uma estratégia de comunicação que envolva todas as entidades relacionadas ao processo, o que irá contribuir para o sucesso do processo;

- possui um formulário bem estruturado para mapeamento dos riscos, denominado "Information Risk Scorecard", e exemplifica como deve ser o preenchimento do mesmo, e a compilação dos resultados;

- descreve as diretrizes a serem seguidas para condução do processo de Gerenciamento de Risco de TI e fornece "checklists" que auxiliam na verificação de conclusão de todas as etapas e uma estimativa de tempo para cada uma delas; e

- recomenda detalhadamente como devem ser elaborados os relatórios para apresentação dos resultados à alta administração.

NIST SP 800-30

A metodologia apresentada pelo NIST é bem mais sucinta quando comparada às demais utilizadas nessa análise.

A linguagem utilizada em todo o documento é bastante clara e de fácil entendimento, embora o documento focalize a apresentação de muitos conceitos e definições. Todas as referências externas mencionadas no documento são publicações do próprio NIST, as quais também se encontram disponíveis para consulta, o que conforta o leitor e permite a busca por maiores detalhamentos.

Para cada etapa do processo de Gerenciamento de Risco de TI, a metodologia estabelece claramente as entradas esperadas, e as saídas a serem geradas; isso garante a consistência do documento, e o encadeamento das atividades. Em alguns momentos a metodologia é falha por não apresentar muitos detalhes práticos quanto à implementação, bem como por não exemplificar efetivamente os produtos a serem gerados. Os questionários apresentados como sugestão de programa de trabalho e o exemplo de relatório a ser emitido é bastante simplificado, necessitando que o responsável pela implementação da metodologia complemente o material, o que irá requerer um esforço adicional. Outro ponto a ser ressaltado é que em nenhum momento é feita referência aos "cases" de sucesso onde houve a implementação da metodologia.

Quanto ao conteúdo, esta metodologia também apresenta alguns diferenciais, os quais relacionamos abaixo:

- inter-relaciona o processo de Gerenciamento de Risco de TI com o ciclo de desenvolvimento de sistemas;

- apresenta sucintamente as funções dos participantes do processo de Gerenciamento de Risco de TI;

- relaciona algumas técnicas para o levantamento das informações;

- foca detalhadamente a questão da análise dos controles já empregados no ambiente;

- sugere como deve ser elaborada a estratégia de mitigação dos riscos; e

- aborda a questão do custo x beneficio durante a seleção dos controles a serem implementados para mitigação dos riscos.

OCTAVE

A metodologia OCTAVE, se comparada com as demais apresentadas anteriormente, é uma das mais extensas em termos de volume. Ela está estruturada em dezoito volumes, sendo que cada volume corresponde ao que ela denomina de "processo". Os volumes apresentam um breve sumário sobre o respectivo conteúdo e uma visão geral dos demais volumes para que o usuário tenha uma visão completa dos processos.

Todas as atividades de cada um dos volumes são extremamente detalhadas. Visando facilitar o entendimento do leitor para cada um dos processos são demonstradas quais são as entradas esperadas, as saídas geradas, e as planilhas de apoio a serem preenchidas durante a execução do processo. Adicionalmente, são apresentados diversos exemplos práticos dos resultados a serem alcançados, o conteúdo dos slides para as apresentações a serem conduzidas, e até mesmo o roteiro a ser seguido em cada um dos "workshops", o que inclui perfil dos participantes, duração, temas a serem abordados, atividades a serem conduzidas em conjunto, dentre outras.

O grande diferencial apresentado pela metodologia OCTAVE é que ela envolve todos os níveis hierárquicos para levantamento das informações pertinentes ao processo de Gerenciamento de Risco de TI.

Em relação ao seu conteúdo, o grande aspecto positivo é o nível de detalhe fornecido, o que permite que qualquer pessoa possa conduzir o processo, sem necessariamente ter um profundo conhecimento prévio sobre o tema.

3.2.2 Escopo das metodologias

Esse aspecto tem por objetivo avaliar em que profundidade é abordado o tema Gerenciamento de Risco de TI, ou seja, se abrange o ciclo todo apresentado no Capítulo 2: identificação dos riscos, mitigação e monitoramento.

FIRM

A FIRM é uma metodologia que apresenta um enfoque muito prático, e isso decorre principalmente por ter sido elaborada por profissionais atuantes no mercado. Em relação ao seu escopo, ela está focada especificamente na identificação dos riscos, e construção de um processo cíclico para condução do mesmo. Estratégias de mitigação não são contempladas pela metodologia sendo apenas referenciada a necessidade das mesmas. Um aspecto extremamente positivo encontrado nessa metodologia, é que ela apresenta qual deve ser o papel de cada uma das entidades envolvidas nesse processo (alta administração, auditoria, proprietário da informação, área de segurança, etc) e qual deve ser a estratégia de comunicação para envolvimento de cada um deles. Outro ponto que difere em seu escopo, é que a metodologia também demonstra qual a melhor forma para que os resultados sejam reportados a alta administração.

NIST SP 800-30

A NIST SP 800-30 fornece um guia pertinente ao tema Gerenciamento de Risco de TI de forma mais ampla, fazendo referência inclusive ao ciclo de desenvolvimento de sistemas, o que é um diferencial em relação às outras metodologias.

Pode-se dizer que a NIST SP 800-30 abrange todo o ciclo de Gerenciamento de Risco de TI, porém com diferentes níveis de profundidade em cada uma das fases. O Capítulo 5, em particular, que aborda aspectos pertinentes à estratégia de mitigação, é extremamente detalhado, contemplando desde a definição dos tipos de controles existentes até um roteiro para avaliação do uso de controles e análise de custo / benefício.

OCTAVE

A metodologia OCTAVE foca detalhadamente todas as atividades relacionadas à execução do processo de Gerenciamento de Risco de TI . Essa metodologia prevê uma análise profunda para identificação dos riscos, superior à da NIST 800-30 e equivalente à da FIRM. A OCTAVE explica detalhadamente os métodos a serem aplicados para identificar e analisar os ativos de informação, as ameaças, os riscos e formular planos e estratégias para mitigar, transferir ou gerenciar o risco.

Na OCTAVE todo o processo de levantamento de informações é baseado em "workshops" que devem ser conduzidos com os profissionais da organização, abrangendo desde a alta administração até o corpo técnico. Nessa metodologia são apresentados os roteiros detalhados para condução dos "workshops", incluindo os materiais necessários para execução do "workshop" até mesmo os questionamentos a serem feitos ao público, conceitos a serem explicados e exemplos de resultados a serem esperados para cada atividade.

Comentário geral:

Em termos de escopo, com exceção da metodologia FIRM, que não aborda o aspecto referente a elaboração de estratégia de mitigação dos riscos, todas as demais atendem ao ciclo completo de Gerenciamento de Risco de TI apresentado no Capítulo 2.

3.2.3 Pré-requisitos do processo Gerenciamento de Risco de TI.

Esse item tem por objetivo analisar quais são as atividades preliminares a serem executadas antes do início da condução do processo de Gerenciamento de Risco de TI.

FIRM

A metodologia FIRM não define quais são os pré-requisitos para condução do processo de Gerenciamento de Risco de TI. No Capítulo 9 da metodologia, denominado "Implementation Guidelines" são apresentados alguns "checklists" com todas as atividades a serem desempenhadas e uma estimativa de carga de trabalho. Dentre essas atividades é mencionada a necesidade de identificar quais os recursos necessários para condução do processo, porém não é feita nenhuma proposição de quais seriam esses requisitos mínimos.

NIST SP 800-30

A NIST SP 800-30 não faz qualquer menção aos requisitos necessários para iniciar e conduzir o processo de Gerenciamento de Risco de TI.

OCTAVE

A metodologia OCTAVE é a única que aborda esse aspecto em maior profundidade. Ela possui um volume inteiro dedicado às atividades preliminares a serem conduzidas antes do ínicio do processo de identificação de risco de TI.

De acordo com esta metodologia, as atividades preliminares listadas são apenas um dos cenários possíveis para iniciar a condução do processo, outras formas poderão ser escolhidas dependendo da experiência das pessoas envolvidas. Entretanto, existe uma atividade preliminar que, independente da forma como será realizado o processo, a OCTAVE considera imprescindível,

que é a obtenção do apoio da alta administração. Para a OCTAVE nenhuma outra ação deverá ser feita antes que se tenha obtido esse comprometimento.

As atividades preliminares listadas pela OCTAVE são:

- obtenção do patrocínio da alta administração;

- seleção dos membros que farão parte da equipe de análise;

- definição dos aspectos logísticos (reserva de sala de reunião, projetores, agendamento de horário das reuniões, etc);

- coleta de documentação existente referente ao escopo da análise (inventário de hardware e software, diagrama da rede, políticas e procedimentos de segurança existentes, relatórios de auditoria, dentre outros);

- treinamento da equipe de análise, para que estes possam desempenhar corretamente suas atividades;

- seleção dos participantes das áreas de negócio e TI, os quais contribuirão durante os levantamentos do processo de identificação de ativos, vulnerabilidades e ameaças; e

- preparação dos produtos esperados como resultado de cada atividade.

Comentário geral:

O direcionamento de quais são os requisitos mínimos necessários, a serem verificados antes do início do processo de Gerenciamento de Risco de TI é muito importante. Muitas organizações iniciam o processo sem ter um visão clara de quais são os requisitos mínimos necessários e isso

pode levar a um insucesso. Em geral, os grandes fatores de fracasso de um processo de Gerenciamento de Risco de TI, relacionados a essa etapa preliminar são:

- *falta de comprometimento da alta administração;*

- *falta de preparo da equipe que o está executando, pois poucos profissionais possuem um entendimento claro do significado do risco;*

- *falta de planejamento adequado do escopo de atuação, pois as organizações querem, em geral, abranger o maior número de ativos possíveis, sem se preocupar com a relevância para o negócio;*

Outros aspectos que acarretam o fracasso de um processo de Gerenciamento de Risco de TI estão relacionados no Capítulo 2 - 2.2 Considerações sobre o processo de Gerenciamento de Risco de TI.

Dessa forma, conforme mencionado anteriormente, as metodologias FIRM e NIST SP 800-30 possuem uma grave deficiência nesse aspecto de definição de requisitos preliminares, o que pode fazer com que o usuário da metodologia inicie o processo tendo uma visão deturpada do esforço requerido para execução do mesmo.

3.2.4 Envolvimento da alta administração

Esse aspecto tem como propósito avaliar como a alta administração é envolvida no processo de Gerenciamento de Risco de TI.

FIRM

A metodologia FIRM ressalta a importância do envolvimento da alta administração em diversos momentos. No Capítulo 5, denominado "Mapeando as estratégias de reporte e funções envolvidas", a metodologia é enfática dizendo "estudos de caso indicam que o comprometimento da alta administração é crucial. Sem ele o processo de Gerenciamento de Risco de TI se transforma em algo altamente fragmentado ou nada". A metodologia também reforça que em função da baixa consciência que a alta administração possui em relação aos processos de análise de risco, cabe ao responsável pela análise de risco envolvê-los direcionando suas atuações.

Esta metodologia também propõe qual estratégia de comunicação deverá ser adotada para obtenção do envolvimento de todas as entidades que, de alguma forma, estão relacionadas ao processo. Nesse contexto a alta administração também aparece, como aprovadora para algumas atividades, dentre as quais as mais importantes são: aprovação da execução do processo de análise de risco, revisão dos resultados, e definição / aprovação das medidas para mitigação dos riscos mapeados.

Outra grande preocupação da metodologia é a forma como os resultados obtidos durante a análise de risco serão relatados para a alta administração. Assim, ela destina um capítulo da metodologia exclusivamente para sugerir a forma como os dados obtidos deverão ser apresentados, garantindo um correto entendimento da gravidade dos mesmos, visando assegurar que a alta administração estará comprometida com as ações de mitigação para correção dos mesmos.

Embora a atuação da alta administração não seja constante durante todas as atividades propostas por essa metodologia, é nítido que há o envolvimento da alta administração e que embora a atuação seja pontual, possíveis distorções nos resultados dificilmente ocorrerão.

NIST SP 800-30

A NIST SP 800-30 não enfatiza a questão de obtenção do envolvimento da alta administração durante a condução do processo. Somente no Capítulo 2 desta metodologia, denominado "Risk Management Overview" é feita uma breve apresentação das funções essenciais relacionadas ao processo de Gerenciamento de Risco de TI e nesse momento é mencionado qual seria o "papel" da alta administração nesse contexto. De acordo com esta metodologia, temos que "a alta administração é em última instância responsável por assegurar que a missão da organização seja cumprida. Dessa forma, ela deve garantir que os recursos necessários para que missão seja cumprida estejam disponíveis. Devem também avaliar e incorporar o resultado da análise de risco no processo de tomada de decisão."

É possível notar pela definição acima que, na visão da NIST SP 800-30, a alta administração assume um papel passivo, ou seja, ela deve fornecer os subsídios necessários para condução do processo e absorver os resultados, porém não atua ativamente nas atividades conduzidas para identificação dos riscos, nem ao menos tem suas percepções e expectativas refletidas nos resultados gerados. Essa forma de atuação pode ser perigosa para a organização, por dois motivos: (1) o foco de atuação durante a condução da análise de risco pode não vir de encontro ao que a alta administração esperava, e o que ela julgava crítico; (2) existem informações relativas à estratégia da organização a médio e longo prazo que somente a alta administração detém. Assim, tais aspectos podem não terem sido considerados na determinação do impacto / risco; (3) o envolvimento dos demais níveis poderá não ocorrer, ou gerar resistências, visto que não há o apoio explícito da alta administração.

OCTAVE

A metodologia OCTAVE considera que o envolvimento da alta administração é a primeira ação a ser feita ao se decidir efetuar um processo de Gerenciamento de Risco de TI. Para ela é essencial que a alta administração tenha consciência de como ocorre o processo de avaliação, quais resultados serão obtidos e qual o valor agregado para o negócio, qual a demanda de tempo que

essa atividade irá requerer de seus profissionais e como será a continuidade do processo, uma vez que se tenha todos os riscos mapeados. Somente com o patrocínio desse nível hierárquico é que a empresa irá despender recursos financeiros e humanos e dará a devida importância para o processo de Gerenciamento de Risco de TI.

Esta metodologia considera como alta administração, a presidência e vice-presidências, diretores, comitê executivo ou qualquer outro elemento da organização que tenha autonomia para assegurar que os recursos necessários para condução do processo de Gerenciamento de Risco de TI serão empregados.

No caso específico da OCTAVE, a alta administração além de ser acionada para obtenção do patrocínio, também é envolvida nas atividades de levantamento de informações, o que contribui consideravelmente para o processo, assegurando que as percepções e preocupações desse nível hierárquico também sejam refletidas no resultado do projeto.

Comentário geral:

Como podemos observar pelas descrições acima, as metodologias FIRM e OCTAVE tratam melhor a questão referente ao envolvimento da alta administração. A metodologia NIST SP 800-30, embora faça uma breve referência a esse aspecto, é um pouco falha nesse quesito.

O envolvimento da alta administração no processo de Gerenciamento de Risco de TI é extremamente relevante, por diversos motivos. Há fatores meramente psicológicos, outros mais práticos, dentre os quais podemos citar:

- *ao verem que a alta administração está engajada no processo de Gerenciamento de Risco de TI, e que para ela são altamente importantes os resultados que serão gerados, os demais níveis hierárquicos se sentem motivados a contribuir, pois passam a enxergar essa atividade como algo positivo, e não como algo similar a uma auditoria que, em geral, visa apenas identificar falhas e culpados;*

- *a alta administração, em geral, possui uma visão abrangente do negócio da empresa, e de como cada processo de negócio está encadeado aos demais. Assim, esse nível hierárquico consegue "enxergar" de forma mais ampla qual o impacto de um determinado risco para a organização como todo. Obviamente que nesse caso não estamos fazendo referência a problemas tecnológicos, como por exemplo, falha de um roteador, de um firewall, etc;*

- *outro aspecto relevante é o fato de somente a alta administração possuir conhecimento da estratégia de negócio da empresa a curto, médio e longo prazo. Essas informações são extremamente relevantes, visto que, muitas vezes um risco que hoje parece ter um baixo impacto para a organização, amanhã, devido a uma mudança de estratégia (ex.: lançamento de um produto, entrada em novos mercados, etc) pode ter um impacto muito maior. Como exemplo consideramos uma empresa que hoje tem um "website" institucional, no qual foram detectadas várias vulnerabilidades de segurança. Atualmente, o impacto que a empresa teria no caso de uma invasão por "hackers" seria médio para alto, visto que o principal impacto seria na imagem da organização. Agora, se considerarmos que a empresa tem como um dos objetivos estratégicos passar a comercializar via esse "website" seus produtos, a preocupação com a segurança e o impacto causado no caso de uma invasão serão muito maiores. Porém, somente a alta administração pode avaliar situações como essa, na qual é requerido o conhecimento da estratégia da organização; e*

- *ao entender e participar do mapeamento dos riscos, a alta administração irá garantir ao final do processo que as ações de mitigação definidas serão implementadas.*

3.2.5 Identificação dos ativos críticos

Esse aspecto visa avaliar quais critérios as metodologias adotam para identificação de ativos críticos, os quais serão objeto da análise.

FIRM

O processo de identificação dos ativos críticos é algo essencial durante a condução do processo de Gerenciamento de Risco de TI, visto que, é em torno desses ativos que todas as demais atividades pertinentes a esse processo serão conduzidas.

Diferentemente das demais metodologias, a FIRM utiliza o conceito de "recursos de informação" para fazer referência ao que as demais metodologias chamam de "ativos". Conforme definição da própria metodologia, "recursos de informação é uma forma abreviada de fazer referência à informação e a todos os recursos de TI a ela associados (exemplos: aplicações de negócio, instalações de computadores, redes e recursos de desenvolvimento)". Cabe ressaltar que, por essa definição, "pessoas" não são recursos que precisam ter seus riscos gerenciados, em contraposição ao que propõem as demais metodologias.

Na FIRM, a identificação da criticidade de um determinado ativo é medida por meio do formulário "Information Risk Scorecard". Esse formulário deve ser preenchido por cada um dos proprietários da informação sob análise, sendo que um dos quesitos a ser respondido é a criticidade. A criticidade é mensurada levando em consideração: (1) o impacto causado nas propriedades da informação (confidencialidade, disponibilidade e integridade) e (2) o período aceitável de indisponibilidade do ativo. De acordo com as respostas apresentadas, são aplicados pesos específicos, o que permite que se calcule um índice que determina o nível de criticidade do ativo.

Um aspecto importante a ser levantado é que a FIRM considera que " a criticidade é um dos principais determinantes do risco. Em essência, ele indica quão importante um recurso de

informação é para a empresa. Maior a criticidade, maior o risco" porém essa afirmação deve ser melhor interpretada, visto que pode gerar um entendimento conceitualmente equivocado. O fato de um recurso de informação (ou ativo) ser altamente crítico não quer dizer que ele representará um alto risco para a organização. O risco somente passará a existir se ele possuir vulnerabilidades para as quais não existam controles aplicados, e simultaneamente existam ameaças que possam explorar tais vulnerabilidades. A existência de um desses dois elementos isoladamente (vulnerabilidades / ameaças) também não representaria um risco. Tal afirmação deve ser interpretada da seguinte forma: o comprometimento de ativos críticos, devido a existência de vulnerabilidades / ameaças representa um alto risco para a continuidade dos negócios da organização.

A metodologia FIRM propõe que os recursos de informação a serem avaliados sejam definidos em conjunto com os coordenadores locais de segurança, auditoria interna, e membros da alta administração.

NIST SP 800-30

A NIST SP 800-30 utiliza o conceito de "Sistema de TI" para definir o foco de atuação da análise de risco. De acordo com a própria metodologia, "Sistema de TI refere-se a um sistema de apoio comum (exemplo: mainframe, rede local, infra-estrutura de comunicação, etc) ou uma aplicação maior que pode ser executada em um sistema de apoio para os quais o uso dos recursos de informação atendam a requisitos específicos do usuário final".

A etapa inicial da NIST SP 800-30 , denominada "Caracterização dos Sistemas" consiste exatamente em definir qual será a abrangência e profundidade em que será tratada a análise de risco. Neste caso, o NIST SP 800-30 já pressupõe que foi selecionado um sistema crítico de negócio, orientando apenas quais informações deverão ser obtidas para que seja possível delinear a amplitude do processo. Dentre as informações que o NIST SP 800-30 julga pertinente para caracterização de um sistema temos: hardware, software, interfaces dos sistemas, dados e informações processadas, pessoas que suportam ou utilizam os recursos de TI, missão do sistema,

criticidade dos sistemas (ex.: importância do sistema / informações para o negócio); sensibilidade das informações (nível de proteção requerido para que as propriedades integridade, confidencialidade e disponibilidade sejam preservadas).

De posse dessas informações, a metodologia NIST SP 800-30 reforça que o escopo de atuação deve ser coerente com as necessidades da organização e recursos disponíveis, podendo esta atuar em toda a infra-estrutura de TI, ou em recursos específicos.

OCTAVE

A metodologia OCTAVE adota o conceito de "ativo de informação", sendo que nessa definição estão abrangidos: hardware, software, dados e informações (no formato eletrônico ou impresso) e pessoas. Os três primeiros itens são agrupados dentro da categoria "Sistemas" e o item "Pessoas" permanece isolado. Essa definição difere do conceito da FIRM por considerar que as "Pessoas" devam ser tratadas como ativos, para os quais também é necessário identificar os riscos e buscar estratégias de mitigação. Nessa visão, o recurso "pessoa" é extremamente crítico para a organização e a indisponibilidade deste poderia impactar negativamente a empresa. O NIST SP 800-30 também faz referência ao item "pessoas", porém nesse caso estes aparecem somente como uma informação que auxilia na caracterização de um sistema, e não como alvo de atuação.

A OCTAVE adota um princípio um pouco diferente das anteriores. A primeira ação adotada durante a condução da OCTAVE é identificar quais ativos de informação são críticos para continuação do negócio da empresa. E essa informação é obtida após a consolidação da visão de três níveis hierárquicos dentro da organização: alta administração; gerência operacional; e staff da área de TI e negócio, conseguida por meio de workshops. A OCTAVE adota como premissa que para maximizar o retorno sobre o investimento, as atividades relacionadas ao Gerenciamento de Risco de TI deverão estar focadas nos sistemas que acarretam em um impacto significativo para o negócio da organização, ou seja, qualquer investimento efetuado em tais recursos estará de alguma forma contribuindo de forma positiva para os processos operacionais da organização.

Obviamente, a forma como a OCTAVE conduz o processo estará de alguma forma não contemplando todos os recursos críticos para organização, porém se considerarmos que esse é um processo cíclico e contínuo, outros ativos poderão ser tratados em outros momentos.

Comentário geral:

Um ponto de aprimoramento a ser colocado é que as metodologias NIST SP 800-30 e FIRM poderiam direcionar melhor a identificação / escolha de quais ativos são críticos, visto que esse ponto é crucial para continuidade e sucesso do processo.

Se observarmos isoladamente o aspecto de mapeamento dos ativos críticos, a metodologia OCTAVE apresenta a melhor forma de condução do processo. Uma das principais dificuldades durante a condução da análise de risco é a definição do que é crítico, já que diferentes níveis hierárquicos possuem diferentes percepções e necessidades em relação aos mesmos ativos. A única forma de assegurar que todas as visões estão sendo refletidas é buscar o consenso entre eles, o que propõe a metodologia OCTAVE. Muitas vezes, ao final de um processo de análise de risco, organizações detectam que investiram horas de seus profissionais e consultorias em ativos que não são essenciais para a continuidade dos negócios.

3.2.6 Mapeamento de vulnerabilidades

Esse aspecto tem por objetivo identificar como cada uma das metodologias abordam o mapeamento de vulnerabilidades.

FIRM

O mapeamento das vulnerabilidades é um componente essencial na determinação do risco. Quanto maior for a quantidade de vulnerabilidades presentes em um determinado ativo, maior a probabilidade de materialização das ameaças que exploram tais vulnerabilidades.

Na FIRM o mapeamento de vulnerabilidades também é feito por meio do "Information Risk Scorecard", na seção "Vulnerability". Entretanto, não é solicitado ao respondente informar a quais as vulnerabilidades o ativo sob análise está suscetível, e sim quais controles já foram implementados. Ou seja, o autor supõe um conjunto de vulnerabilidades padrão aos quais o ativo poderá estar suscetível, e lista um conjunto de dezessete itens de controles para os quais o proprietário da informação deverá responder o respectivo nível de maturidade. A lógica adotada é que, conhecendo a maturidade dos itens de controles listados, as vulnerabilidades que existem "por trás" de cada item de controle, ou melhor, que são minimizadas ou eliminadas pelos mesmos, também serão conhecidas.

Um aspecto negativo nessa abordagem é que as vulnerabilidades não são estáticas, muito menos comuns entre todos os recursos de informação (ativos), pois caso assim o fossem, estariam facilmente solucionadas por todas as organizações. Dessa forma, particularidades de cada recurso de informação, e de cada ambiente sob análise, não são refletidas no levantamento. A metodologia reconhece essa inflexibilidade e faz uma breve menção dizendo que eventuais customizações serão necessárias dependendo dos ativos envolvidos, devendo apenas tomar-se o cuidado de não eliminar os controles apresentados, visto que representam importantes elementos na determinação do risco.

NIST SP 800-30

A NIST SP 800-30 propõe que seja desenvolvida uma lista contendo todas as vulnerabilidades associadas ao ambiente de tecnologia, fazendo a devida relação com a fonte de ameaça que poderá explorá-la, bem como a ação que a ameaça poderá exercer no ambiente.

Por definição, a existência de ameaças ou vulnerabilidades isoladas não representam um risco para a organização; somente a combinação de ambas podem colocar em risco a continuidade dos negócios. Assim, a forma como a NIST SP 800-30 propõe esse mapeamento, facilita a visualização de onde haverá maior probabilidade de materialização das ameaças.

Essa metodologia também faz referência ao mapeamento de vulnerabilidades durante o ciclo de desenvolvimento de sistemas, tema que não é abordado pelas demais metodologias. Esse tipo de ação é de vital importância, visto que o tratamento de vulnerabilidades durante a concepção do sistema torna o ambiente muito mais seguro e é financeiramente a melhor opção, uma vez que evita re-trabalhos ou sobreposição de tecnologias.

A NIST SP 800-30 classifica as vulnerabilidades em técnicas e não técnicas. Ele propõe que, para as vulnerabilidades técnicas, sejam utilizadas algumas fontes de referência que detalham as vulnerabilidades técnicas conhecidas. Dentre as possíveis fontes são mencionados os "websites" dos próprios fornecedores, ou "sites" que costumam divulgar listas de vulnerabilidades, relatórios anteriores de análise de risco ou auditoria, dentre outros.

Para a identificação das vulnerabilidades, a NIST SP 800-30 considera a utilização de ferramentas automatizadas para diagnóstico do sistema, bem como a elaboração de roteiro de testes específicos para checagem da eficiência dos controles de segurança.

OCTAVE

A metodologia OCTAVE considera que, após o mapeamento dos ativos críticos e suas respectivas ameaças, devam ser identificados todos os “componentes de infra-estrutura” que suportam tais ativos. Deve-se compreender por “componentes de infra-estrutura” qualquer elemento que desempenha um papel importante para que o ativo crítico possa desempenhar adequadamente sua função. Durante a análise de vulnerabilidade deve-se buscar identificar quais são os “sistemas” que estão diretamente relacionados com o ativo crítico. Esses sistemas são denominados “sistemas de interesse” e compreendem um agrupamento lógico de componentes necessários para que uma determinada função seja desempenhada, ou um objetivo atingido. Em geral, os “componentes de infra-estrutura” que compõem os “sistemas de interesse” estão divididos em: servidores, componentes de rede, estações de trabalho, “laptops”, dispositivos de armazenamento, componentes “wireless”, ou qualquer outro dispositivo.

A metodologia OCTAVE propõe que a análise das vulnerabilidades tenha como foco os "componentes de infra-estrutura" dos "sistemas de interesse". Assim, ela sugere que, para se validar se realmente estamos trabalhando sobre recursos pertinentes ao "sistema de interesse", realizemos os seguintes questionamentos: (1) os componentes são utilizados quando um usuário legítimo tenta acessar o ativo crítico?; (2) um ator (responsável pela ação de uma ameaça) utiliza tais componentes para obter acesso ao ativo crítico?

Uma vez definidos os componentes chaves a serem avaliados, é necessário efetuar balanceamento do esforço necessário para avaliação do ativo versus o retorno obtido com essa atividade. Cabe ressaltar que, muitas vezes, um mesmo componente de infra-estrutura atende a diversos ativos críticos da organização. Nesse caso, uma análise aprofundada pode ser viável, dependendo da criticidade e volume de recursos que este suporte.

A OCTAVE considera que análise de vulnerabilidades poderá ser feita com o auxílio de consultores externos ou pela equipe interna; neste último caso, desde que treinados e que possuam as ferramentas automatizadas necessárias para condução do processo.

Concluída a análise das vulnerabilidades, a equipe de análise deverá atribuir uma classificação da severidade de cada vulnerabilidade. Essa classificação irá auxiliar na definição de um plano de ação para tratamento de cada um dos problemas detectados. Os critérios para definição da severidade e tempo de ação para correção poderão ser determinados pela equipe, embora a OCTAVE faça uma proposição de quais critérios poderão ser empregados.

3.2.7 Identificação de ameaças

Esse aspecto tem por objetivo identificar como é feito o mapeamento das ameaças às quais os ativos críticos estão sujeitos.

FIRM

A metodologia FIRM considera que as ameaças são quaisquer eventos que possam comprometer a confidencialidade, integridade ou disponibilidade das informações. Ela considera que não existe uma métrica específica para mensurá-las e que elas simplesmente existem. Para avaliação das ameaças às quais os ativos estão suscetíveis, foram considerados no "Information Risk Scorecard" seis categorias de ameaças:

1. mau funcionamento de hardware ou software;
2. perda de serviços, equipamento ou recursos;
3. sobrecarga;
4. erros humanos;
5. impactos não previstos decorrentes de mudanças; e
6. violação de acesso.

Para cada categoria apresentada acima é mensurada a quantidade de eventos relacionados ocorridos ao longo de um determinado período. A FIRM adota como premissa que a estimativa da probabilidade de materialização de uma determinada ameaça (nível de ameaça, conforme nomenclatura adotada pela metodologia) está diretamente relacionada ao histórico de eventos já ocorridos durante o período de análise definido. Conforme apresentado acima, pode-se notar que a FIRM não faz o tratamento das ameaças em si, e sim do nível de ameaça. Após o preenchimento do formulário é gerado um índice do nível de ameaça para o ativo em questão.

A utilização do histórico de eventos ocorridos para determinar o nível atual de ameaça é uma informação bastante significativa, porém outros fatores também devem ser levados em consideração. Dentre estes fatores, deve-se considerar principalmente os controles empregados pela organização, pois esses muitas vezes reduzem o impacto causado pela ameaça ou a probabilidade de materialização da mesma. Vamos considerar o seguinte cenário: uma empresa que nunca teve nenhum sistema antivírus instalado pode ter sido infectada dezenas de vezes pelos mais diversos vírus existentes no mercado. Num determinado momento, ela instala um

antivírus, cuja atualização é diária e automática. Se fizéssemos uma análise isolada considerando apenas o histórico de acontecimentos, deveríamos dizer que o nível de ameaça é extremamente elevado, porém, se considerarmos o controle que foi implementado (a instalação do antivírus) a probabilidade de materialização da ameaça cai consideravelmente.

NIST SP 800-30

A NIST SP 800-30 considera que deverão ser mapeadas todas as fontes de ameaças que são aplicáveis aos "sistemas de TI" objeto da avaliação de risco. De acordo com esta metodologia, as fontes de ameaça podem ser classificadas em três categorias:

- ameaças naturais: enchentes terremotos, tornados, avalanches, etc.;
- ameaças humanas: eventos ocasionados por seres humanos, os quais podem ser não intencionais ou ações deliberadas; e
- ameaças ambientais: falha elétrica por longos períodos, poluição, etc..

A NIST SP 800-30 propõe que sejam mapeadas todas as fontes de ameaça às quais os ativos estão suscetíveis, sendo que para cada um deles deverá ser elaborada uma tabela contemplando: (a) fonte de ameaça; (b) motivação e a (c) ação da ameaça.

A NIST SP 800-30 exemplifica apenas algumas fontes de ameaça, porém não propõe uma lista para ser utilizada como base, cabe ao responsável pela condução do processo mapear as ameaças pertinentes aos ativos sob análise.

OCTAVE

A metodologia OCTAVE recomenda algumas categorias para agrupamento das ameaças, de acordo com a fonte que originou as mesmas, onde temos:

- atores humanos utilizando acesso via rede;
- atores humanos utilizando acesso físico;
- problemas nos sistemas; e

- outros problemas (em geral são problemas que não podem ser gerenciados por intervenção humana, por exemplo desastres naturais).

A OCTAVE também propõe que algumas informações devem ser preenchidas para caracterização das propriedades da ameaça. Tais informações são representadas no formato de árvore, o que pode ser observado na Figura 8, sendo que para cada categoria de ameaça será elaborada tal estrutura. As informações a serem preenchidas são:

- ativo afetado: algo de valor para a organização;
- ator: quem ou "o quê" violou os requisitos de segurança (confidencialidade, integridade e disponibilidade de um ativo);
- motivação: define a intenção do ator;
- acesso: a forma pelo qual o ativo foi alcançado pelo ator; e
- resultado: o resultado imediato gerado decorrente da violação dos requisitos de segurança (revelação indevida, modificação, destruição, perda ou interrupção do funcionamento) de um ativo.

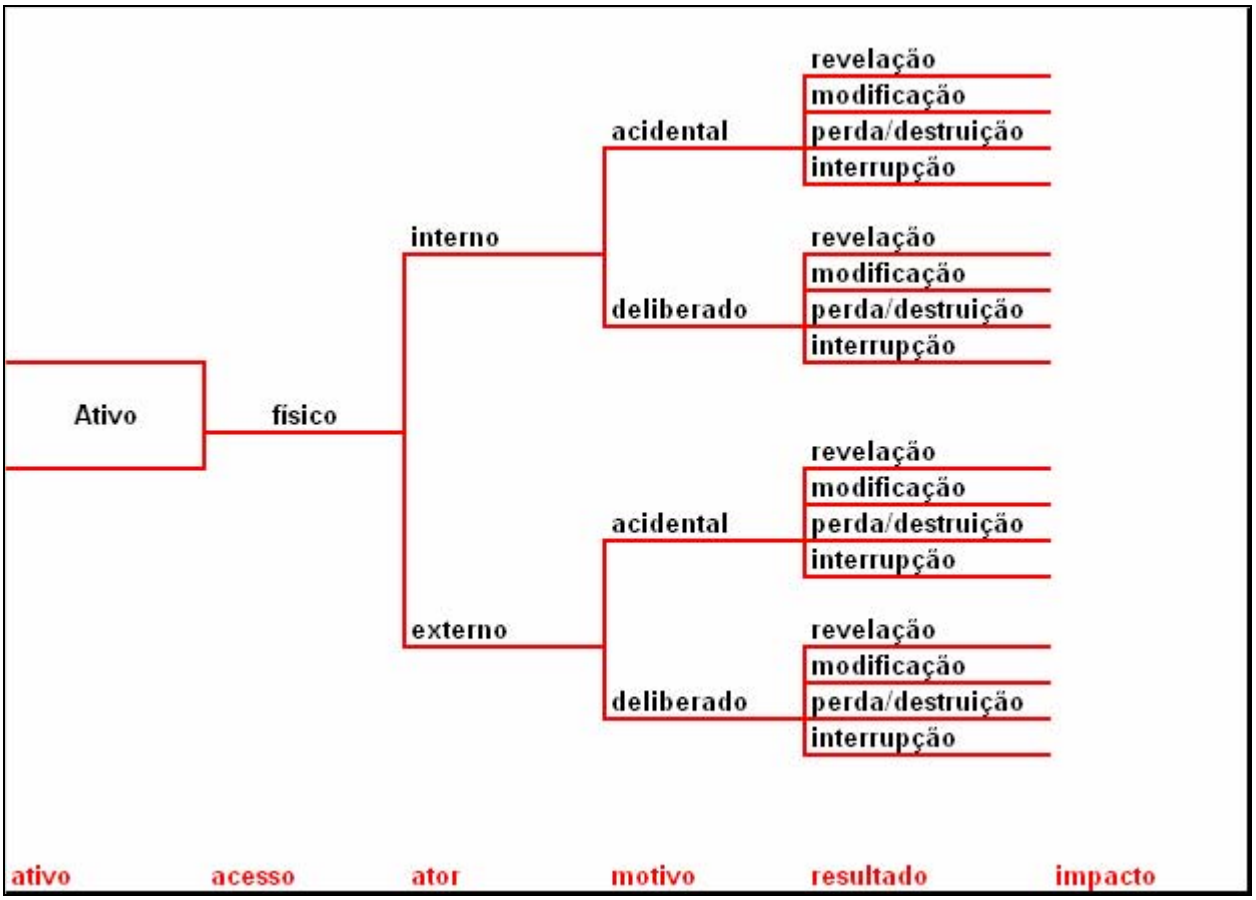

Figura 8: Caracterização em árvore das propriedades das ameaças

Tanto a metodologia NIST SP 800-30, quanto a OCTAVE são bastante similares no tratamento das ameaças. A metodologia OCTAVE apresenta como vantagem trabalhar sobre os dados que foram levantados com os diferentes níveis organizacionais envolvidos. Dessa forma, estaremos trabalhando sobre ameaças que sejam de entendimento e aceitação comum a todos que de certa forma interagem com o ativo sob análise. Outro ponto interessante abordado pela OCTAVE é que ela apresenta uma tabela relacionando os requisitos de segurança versus os resultados esperados decorrentes da ação de uma ameaça, permitindo assim que se assegure a consistência nas informações trabalhadas. Ou seja, se para um ativo foi colocado como requisito de segurança a preservação da confidencialidade do mesmo, um dos resultados esperados para as ameaças que estão relacionadas àquele ativo é a revelação indevida do ativo em questão. Caso não ocorra esse relacionamento, um dos seguintes cenários ocorreu: (1) provavelmente os resultados decorrentes das ameaças não foram mapeados adequadamente; (2) a

confidencialidade não é um requisito de segurança; (3) alguma ameaça não foi mapeada; (4) o requisito de segurança foi direcionado por uma exigência legal, e neste último caso não existe necessariamente uma ameaça que possa vir a explorá-lo.

3.2.8 Análise dos controles empregados atualmente

Aqui o objetivo é avaliar se a metodologia considera os controles já empregados antes de efetuar a determinação do risco, visto que este aspecto influi diretamente na probabilidade de materialização de uma ameaça, e conseqüentemente poderá aumentar ou reduzir o nível de risco.

FIRM

A metodologia FIRM avalia os controles empregados no ambiente durante a aplicação do formulário denominado "Information Risk Scorecard", na seção em que é feito o mapeamento das vulnerabilidades, ou seja, conforme já mencionado anteriormente, esta metodologia utiliza uma lógica inversa: a partir das deficiências nos controles são determinadas as vulnerabilidades.

Nesse item do formulário são apresentados dezessete itens de controle para os quais o responsável pelo ativo deve informar o nível de maturidade e eficácia do controle. Entretanto, a própria metodologia reconhece que o mapeamento dos controles existentes é feito de maneira superficial. Assim, ao determinar o nível de risco, o valor obtido poderá estar distorcido em relação ao cenário real da empresa.

NIST SP 800-30

A metodologia NIST SP 800-30 reconhece que a análise dos controles empregados, ou que se deseja empregar, é essencial para que se possa calcular a probabilidade de uma ameaça explorar uma determinada vulnerabilidade.

A NIST SP 800-30, nessa etapa do processo, classifica os controles basicamente em duas categorias: controles preventivos e controles detectivos, independente da finalidade (técnicos, operacionais ou gerenciais). Essa metodologia propõe que a análise dos controles existentes seja efetuada por meio de "checklists", os quais contemplem todos os requisitos de segurança que a organização deve levar em conta, e que tais "checklists" sejam periodicamente atualizados, de forma a refletir possíveis mudanças que o ambiente tecnológico tenha sofrido.

Um aspecto importante a ser ressaltado é que, embora a NIST SP 800-30 reconheça a importância da avaliação dos controles empregados para a correta determinação do risco, ele não transforma o resultado dessa análise em nenhuma métrica que influencie na quantificação do risco. Porém, de posse dessa informação, o responsável pela análise poderá avaliar melhor a magnitude do impacto e da probabilidade, fatores que influenciam na determinação do risco, conforme proposto pela NIST SP 800-30.

Assim, a NIST SP 800-30 falha ao não transformar tal informação em uma métrica a ser utilizada na determinação do risco pois, neste caso, dependendo do profissional que está conduzindo a análise, esse dado poderá ter uma interpretação favorável ou não.

OCTAVE

A metodologia OCTAVE se preocupa com a análise dos controles existentes durante a fase de elaboração da Estratégia de Segurança e do Plano de Mitigação, e não durante a etapa de determinação do risco. Nessa ocasião, para cada uma das ameaças a serem tratadas, a metodologia recomenda que seja verificado se as práticas atuais da empresa estão em conformidade com o "Volume 15: Catalog of Practices" (o qual contém recomendações de segurança em nível tático e operacional) e quais outras ações deverão ser implementadas.

Embora a OCTAVE faça a avaliação dos controles empregados, em virtude de tal análise ser conduzida somente no momento da elaboração da estratégia de segurança, e não no momento da

determinação do risco, a conclusão referente ao nível de risco poderá ser um resultado superestimado.

Comentário geral:

Podemos observar que todas as metodologias abordam a questão de avaliação dos controles existentes, porém de modos diferentes. As metodologias FIRM e NIST SP 800-30 buscam verificar os controles durante a determinação do risco, já a OCTAVE, somente irá se preocupar com tais controles durante a definição da estratégia de mitigação. Independente do momento em que ocorra a avaliação dos controles empregados e planejados essa é uma atividade que deve ser desempenhada pois permite que a organização visualize as principais fragilidades em termos de controles.

3.2.9 Análise de impacto no ambiente

Esse item tem por objetivo verificar como a metodologia trata a questão do impacto no ambiente organizacional. Avalia também se a metodologia emprega técnicas qualitativas ou quantitativas para mensuração do impacto.

FIRM

A metodologia FIRM também utiliza o "Information Risk Scorecard" para mensurar o impacto no ambiente referente aos incidentes ocorridos nos últimos doze meses. Para tal, ela adota uma escala de cinco itens, para os quais deverá ser informada a gravidade que os mesmos representam. Os itens considerados na análise são:

1. perda financeira;
2. degradação do desempenho;
3. perda de controle sobre o gerenciamento;
4. danos à reputação; e

5. crescimento prejudicado;

Como pode-se observar, a metodologia FIRM não trata o aspecto impacto causado à organização para cada ameaça / vulnerabilidade isoladamente, e sim para o conjunto de incidentes ocorridos em um determinado período de tempo.

Um aspecto negativo nessa abordagem é que, ameaças e / ou vulnerabilidades que possuam um impacto negativo significativo para o ativo crítico e / ou ambiente tecnológico, podem não ficar em evidência, podendo passar desapercebidos e até mesmo não receber a atenção devida. Ou seja, a organização pode não aplicar controles adequados para minimização de um risco que tenha grande impacto para a empresa, causando assim uma "falsa sensação de segurança".

NIST SP 800-30

A NIST SP 800-30 considera que, para se definir o impacto negativo decorrente da exploração de uma vulnerabilidade por uma ameaça, é necessário que se tenha conhecimento das seguintes informações: (1) finalidade do sistema; (2) importância do sistema para a organização e (3) sensibilidade dos dados manipulados pelo mesmo. Esta metodologia considera que tais informações podem ser facilmente obtidas a partir de análises prévias efetuadas ("Business Impact Analysis" - BIA) ou poderão ser mapeadas junto ao proprietário do sistema sob análise.

Em função da complexidade de se mensurar em termos quantitativos determinados impactos, como por exemplo, perda da confiabilidade ou perda de credibilidade, a NIST adota a análise qualitativa para tratamento do impacto. Assim, a NIST SP 800-30 classifica o impacto avaliado em alto, médio e baixo, e apresenta uma tabela contendo as definições para cada uma das magnitudes mencionadas.

Um aspecto negativo que pode ser observado é que a NIST não menciona claramente se essa análise deverá ser conduzida para todas as vulnerabilidades ou se somente para as mais críticas, ou qual o critério a ser adotado para condução dessa análise. Caso o volume de

vulnerabilidades mapeadas seja muito grande, o tempo despendido com essa atividade será extremamente elevado. Adicionalmente, os critérios utilizados para definição de alto, médio e baixo, são extremamente simplificados.

OCTAVE

A metodologia OCTAVE também adota critérios qualitativos para definição do impacto causado pela exploração de uma vulnerabilidade por uma ameaça. Os critérios adotados para classificação do impacto são similares aos do NIST SP 800-30, sendo categorizados em alto, médio e baixo, porém diferente da NIST, a metodologia OCTAVE não define de que consistem cada uma das magnitudes. A OCTAVE propõe primeiramente que o impacto seja categorizado conforme os seguintes critérios de avaliação: (1) reputação / confiança do consumidor; (2) saúde dos consumidores; (3) multas / penalidades; (4) financeiro e (5) outros (critérios que sejam específicos para uma determinada organização). De acordo com a OCTAVE, para cada uma das categorias, cada organização deverá definir o que é considerado alto, médio e baixo impacto, pois isso dependerá muito da cultura, objetivos e porte da organização. Por exemplo, uma perda financeira de $ 1.000.000 pode ser insignificante para uma grande organização, porém poderá significar a falência para outra de menor porte.

Após definição dos critérios, cada ativo crítico deverá ter o impacto da exploração de suas ameaças avaliado e classificado em alto, médio ou baixo. Quando ocorrerem situações em que, para uma única ameaça haja classificações distintas para o impacto acarretado, a classificação final deverá abranger o intervalo médio-> alto. Por exemplo, o acesso indevido por um funcionário, acarretando na **revelação** de uma determinada informação, possui um impacto **alto**, porém a **modificação** teria um impacto **médio**.

Embora a OCTAVE requeira um trabalho maior por parte da organização em definir claramente em que consistem os valores alto, médio e baixo, para cada uma das categorias de ameaças, a atividade de avaliação de cada ameaça quanto ao impacto causado estará consideravelmente simplificada e assegurará a equalização do resultado. Ou seja, o processo deixa de depender do

conhecimento prévio do profissional que o conduz, podendo ser conduzido por um número maior de profissionais, garantindo que todos adotaram o mesmo critério.

Comentário geral:

A correta determinação do impacto causado é extremamente relevante pois através dessa informação, a empresa poderá definir a priorização de seus riscos.

3.2.10 Determinação do risco

Esse aspecto avalia quais critérios (criticidade, ameaça, vulnerabilidade, impacto e probabilidade) cada uma das metodologias emprega para determinação do risco.

FIRM

A metodologia FIRM não adota uma métrica única para mensurar o risco. A determinação do risco neste caso é feita por meio da combinação de alguns fatores, sendo estes: (1) criticidade do ativo; (2) fraqueza dos controles empregados; (3) vulnerabilidades existentes; (4) circunstâncias especiais (eventos de maior gravidade ocorridos); (5) impacto no negócio e (6) nível de ameaça. A representação do risco é feita por meio de um gráfico denominado “teia de aranha” no qual é possível visualizar simultaneamente o status de cada um dos componentes. A Figura 9 exemplifica tal conceito.

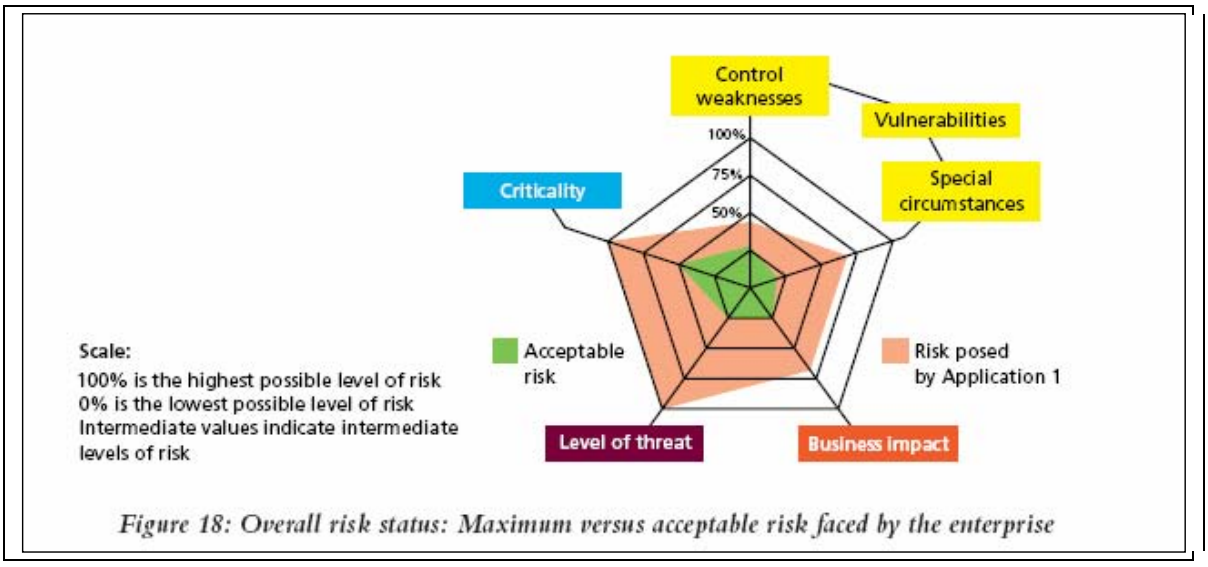

Figura 9: Representação gráfica do risco segundo a FIRM

Todos os fatores são extraídos do "Information Risk Scorecard", o qual é preenchido pelo proprietário do ativo. Com exceção dos fatores 'criticidade do ativo' e 'nível de ameaça', que possuem cálculos próprios definidos pela FIRM, todos os demais índices são obtidos com base em uma tabela, a qual define, de acordo com o preenchimento do respondente, o valor percentual correspondente de risco que representa.

A abordagem apresentada pela FIRM mostra o risco sob várias perspectivas, o que permite aos gestores entenderem claramente quais são os pontos que necessitam ser aprimorados para que o risco de um determinado ativo seja minimizado. Adicionalmente, em virtude deste gráfico representar também a criticidade do ativo, é possível enxergar claramente a representatividade (ou importância) daquele recurso para a continuidade dos negócios. De posse dessas informações torna-se mais fácil para o gestor decidir para quais recursos deverão ser direcionados os investimentos e com qual finalidade (redução das vulnerabilidades, aprimoramento dos controles existentes, etc).

NIST SP 800-30

A metodologia NIST SP 800-30 propõe que para a determinação do risco devam ser levados em consideração os seguintes fatores: (1) a probabilidade de uma fonte de ameaça explorar as vulnerabilidades existentes; (2) a magnitude do impacto causado caso a ameaça se materialize e (3) a eficácia dos controles empregados.

Basicamente, para a NIST o risco será determinado em função da (1) probabilidade de materialização e (2) impacto da ameaça. Embora seja feita referência à avaliação dos controles empregados, esse não será um aspecto mensurado diretamente. O NIST considera que ele terá um impacto indireto sobre os outros dois fatores citados acima. A não quantificação dos controles existentes é um aspecto negativo já discutido anteriormente.

Assim, o NIST propõe que seja criada uma matriz quadrada considerando o impacto e a probabilidade, sendo que para cada um dos valores atribuídos, neste caso alto, médio e baixo, sejam associados pesos específicos. A dimensão da matriz, a determinação dos pesos, bem como dos intervalos que determinam a magnitude do risco, ficará a critério de cada organização. Complementarmente, o NIST apresenta uma tabela recomendando quais ações deverão ser adotadas para cada um dos níveis de risco identificados, neste caso alto, médio e baixo.

OCTAVE

A metodologia OCTAVE adota uma abordagem diferente para determinação do risco. Ela considera que o nível do impacto causado por uma determinada ameaça irá definir o nível de risco a que a empresa está sujeita. Assim, diferente das demais metodologias de análise de risco, ela não considera a probabilidade de materialização de uma ameaça para definir o risco ao qual a empresa está sujeita. A OCTAVE defende que a probabilidade é uma métrica complexa de ser calculada e imprecisa, e mesmo quando é possível seu cálculo, ela está passível de alteração constante, devido a inúmeros fatores.

A probabilidade é o fator de incerteza envolvido no risco. É o índice que indica as chances de uma vulnerabilidade ser atacada, com sucesso, por uma ameaça. Essa incerteza reflete que eventos podem ocorrer, geralmente irão ocorrer, cedo ou tarde, mas não necessariamente dentro de um período de tempo válido. Assim, essa abordagem da OCTAVE pode conduzir a um entendimento equivocado do risco. Por exemplo, se estivermos avaliando os riscos referentes a um CPD, podemos considerar como ameaça a possibilidade de um avião cair sobre o mesmo, e neste caso, o impacto seria altíssimo, de proporções incalculáveis. Ao adotarmos o critério da OCTAVE, a conclusão seria que temos um alto risco, o qual deveria receber um tratamento imediato. Porém, se considerarmos a probabilidade de esse evento ocorrer (fator não avaliado pela OCTAVE) chegaríamos à conclusão que o risco é baixo, considerando o histórico de acidentes com aviões que temos aqui no Brasil. Dessa forma, podemos perceber que a magnitude do impacto causado por uma ameaça é uma informação importante, porém não pode ser considerada isoladamente para determinação do risco.

Comentário geral:

Pelas descrições apresentadas acima, é possível identificar que as abordagens da FIRM e da NIST SP 800-30 são as mais completas para definição do risco, sendo a da FIRM ainda mais completa. A única ressalva em relação a proposição da FIRM é que ela utiliza critérios pré-definidos para identificação das ameaças, vulnerabilidades, controles, etc., o que pode tornar o processo um pouco inflexível para o usuário da metodologia, não permitindo que a realidade do ambiente seja adequadamente refletida.

3.2.11 Controles para mitigação dos riscos

Tem por objetivo avaliar se as metodologias abordam estratégias para mitigação dos riscos.

FIRM

A metodologia FIRM não aborda o aspecto de definição de controles para mitigação do risco. Na realidade, ela apenas considera que uma vez mapeados todos os riscos, é necessário efetuar a análise de quais controles serão necessários, sendo que essa atividade deverá ser conduzida pelo proprietário da informação, com o auxílio dos coordenadores locais de segurança (quando aplicável), e a equipe que está conduzindo o processo de Gerenciamento de Risco de TI (embora nesse último caso, a contribuição esteja mais voltada a certificar que o nível de risco identificado realmente é coerente, ou seja, que ele não foi estimado maior do que realmente é).

Adicionalmente, esta metodologia faz uma breve referência às categorias de controle (preventivos, detectivos e de recuperação) no documento intitulado "Fundamental Information Risk Management – Supporting Material".

De modo geral, podemos concluir que esse aspecto é bastante falho na metodologia FIRM, visto que o mapeamento dos riscos sem a definição de uma estratégia para contenção dos mesmos possui pouco valor para a organização. Ou seja, ela identifica todos os riscos porém não possui informações suficientes para dar continuidade no tratamento dos mesmos.

NIST SP 800-30

Dentre as metodologias analisadas, a NIST SP 800-30 é uma das que aborda de forma mais detalhada a questão da mitigação do risco. Nesse documento são apresentadas as possíveis opções para mitigação do risco, dentre as quais são mencionadas:

- **Aceitar o risco**: consiste em aceitar o risco potencial e continuar operando.

- **Evitar o risco**: consiste em evitar o risco eliminando a causa do risco.

- **Limitar o risco**: implementar controles que minimizem o impacto adverso causado por uma ameaça ao explorar uma vulnerabilidade.

- **Planejar o risco**: gerenciar o risco desenvolvendo um plano de mitigação que priorize, implemente e mantenha os controles.

- **Pesquisa e reconhecimento**: minimização do risco pelo reconhecimento da vulnerabilidade e buscando controles para corrigir a vulnerabilidade.

- **Transferência do risco**: a transferência do risco ocorre utilizando outras opções para compensar a perda, tal como a contratação de seguros.

Outro aspecto importante discutido pela metodologia é a estratégia para implementação de novos controles. O autor sugere as seguintes etapas que sejam executadas:

1. Etapa 1: Priorizar as ações
2. Etapa 2: Avaliar as opções de controle recomendadas
3. Etapa 3: Efetuar uma análise de custo / benefício
4. Etapa 4: Selecionar o controle
5. Etapa 5: Atribuir responsabilidades pela implementação do controle
6. Etapa 6: Desenvolver um plano seguro de implementação
7. Etapa 7: Implementar o controle selecionado

Adicionalmente, a NIST SP 800-30 apresenta uma categorização dos controles, a qual está dividida em (1) controles técnicos; (2) controles gerenciais e (3) controles operacionais. Dentro de cada uma dessas categorias há uma segunda classificação, a qual é comum às três mencionadas anteriormente: controles preventivos, controles detectivos e de recuperação. No Capítulo 2 foi apresentada a descrição de cada uma das categorias.

É possível observar que existe uma forte preocupação por parte da NIST em orientar como deve ser a continuidade do processo, após os riscos terem sido mapeados. Apenas como ponto de atenção, cabe ressaltar que a metodologia entra em contradição em relação à categorização das ameaças. No item 3.4.2 do "Capítulo 3 – Risk Assessment", ela menciona que as categorias de controles podem ser apenas preventivos e detectivos, não menciona os de recuperação, os quais são apresentados posteriormente no capítulo 4 da metodologia. De qualquer forma, o modo como o "Capítulo 4 – Risk Mitigation" foi elaborado é de grande contribuição para o profissional que está conduzindo o processo de Gerenciamento de Risco de TI, orientando principalmente em relação ao aspecto custo benefício durante a implementação do controle e até mesmo no julgamento quanto a implementação ou não de um controle.

OCTAVE

A metodologia OCTAVE também trata a questão mitigação do risco de forma cautelosa. A OCTAVE propõe dois tipos de plano de ação a serem elaborados: a Estratégia de Proteção, o Plano de Mitigação, e a Lista de Ação. De acordo com essa metodologia não existe um relacionamento hierárquico entre todos esses documentos, eles apenas devem estar consistentes entre si.

A Estratégia de Proteção define as estratégias que uma organização utiliza para habilitar, iniciar, implementar e manter a segurança interna do ambiente. Em geral contém ações abrangentes e de longo prazo para implementação. Como exemplo, podemos citar: Plano Diretor de Segurança, Programa de Conscientização, Plano de Contingência, etc.

Os Planos de Mitigação são elaborados para reduzir os riscos para os ativos críticos. O foco de um Plano de Mitigação são os ativos, e as ações aqui relacionadas em geral são de média duração. Para cada Plano de Mitigação é necessário gerar os detalhes de implementação.

As Listas de Ações são ações de rápida implementação e que não requerem maior detalhamento sobre a forma de implementação. Por exemplo, a configuração do histórico de senha de um determinado sistema.

A metodologia OCTAVE apresenta uma abordagem bastante interessante para o tratamento da Estratégia de Proteção. Ela apresenta os principais aspectos relacionados a tais estratégias e solicita, por meio de um "workshop", que sejam listadas as práticas atuais e futuras que se deseja manter ou implementar. Cabe destacar que a OCTAVE também fornece no volume 15, denominado "OCTAVE Catalog of Practices" um conjunto de melhores práticas estratégicas e operacionais, relacionadas à segurança da informação, o que permite que o usuário da metodologia tenha uma base de comparação de onde a organização está, e onde ela deve chegar.

Os Planos de Mitigação são criados a partir das ameaças mapeadas nas etapas anteriores de condução da OCTAVE. Para tal são sugeridos alguns questionamentos a serem feitos visando identificar quais ações são aplicáveis, por exemplo: (1) quais ações poderiam ser feitas para reconhecer ou detectar esse tipo de ameaça? (2) Quais ações poderiam ser adotadas para resistir ou evitar esse tipo de ameaça? (3) Quais ações podem ser feitas para recuperação do ambiente após a ameaça ter se materializado? (4) Quais outras ações são recomendadas? e (5) Como será testado o plano de mitigação para esse ativo?.

Durante o desenvolvimento dos Planos de Mitigação, a Lista de ação de curto prazo já começa a ser elaborada, como um processo natural, visto que, caso a ação a ser feita seja extremamente pontual não será requerida a elaboração de um Plano de Mitigação. Eexemplo: configuração do período de expiração de 1 ano para 90 dias.

Um aspecto extremamente positivo identificado nessa metodologia é que tanto a elaboração da Estratégia de Proteção, quanto os Planos de Mitigação e a Lista de Ações, todos são elaborados em conjunto por um grupo multidisciplinar de profissionais, por meio de "workshops". Isso permite que visões distintas de um mesmo problema sejam consideradas durante a construção da solução. Outro aspecto relevante é que, após a elaboração de tais documentos, eles são

submetidos a análise e aprovação da alta administração, assegurando dessa forma que eles não se transformem apenas em "letras mortas" e sim em ações efetivas para aprimoramento da segurança do ambiente.

Comentário geral:

Com exceção da metodologia FIRM, que não trata a questão da elaboração de uma estratégia de mitigação, as demais metodologias abordam o tema, porém de modos distintos. Como podemos observar a NIST SP 800-30 trata de forma micro a questão da análise de controles a serem implementados, enquanto que a OCTAVE já aborda a questão de modo macro, corporativo.

O fato da NIST SP 800-30 tratar o tema de modo micro não compromete o valor agregado deste material, muito pelo contrário: a análise proposta pela NIST permite que qualquer profissional consiga fazer uma análise apropriada da eficácia dos controles empregados, e principalmente do custo benefício de se manter ou implementar novos controles, considerando não apenas aspectos financeiros, mas também a facilidade de implementação, atendimento a requisitos legais, o que não é tratado pela OCTAVE. O único cuidado a ser tomado nesse caso é que, muitas vezes ações corporativas, em um âmbito maior, resolvem (ou minimizam) diversas vulnerabilidades simultaneamente, sem que seja necessário o tratamento individual de cada uma delas. Por exemplo, caso seja detectado pela organização que um dos grandes problemas é o compartilhamento de senhas, as quais em geral são gravadas em arquivos ou anexadas em "post-it" ao lado do computador. Não basta apenas que se instrua os usuários finais para não gravarem em arquivos ou colarem "post-it", ou diminuir o período de expiração. É necessário que seja feita uma campanha de conscientização, no qual os usuários entendam a gravidade desse procedimento, ou seja, que a organização não está tentando impedir que ele "seja legal" com o companheiro, mas que , toda ação efetuada ficará gravada em "logs" e ele poderá ser responsabilizado posteriormente, ainda que não tenha executado; poderá haver problemas legais referentes ao licenciamento de software (visto que para um único "userID" existe mais de um usuário utilizando); etc. Assim, observamos que diversos outros problemas poderão ser minimizados por meio de uma ação de caráter corporativo.

A metodologia OCTAVE tenta abordar o risco de forma micro (Plano de Mitigação) e macro por meio da (Estratégia de Segurança). Entretanto no caso dos Planos de Mitigação não são feitas análises de custo benefício das ações, sendo apenas listadas as ações que os envolvidos julgam pertinentes. Assim, podemos considerar que a abordagem possui maior valor agregado no tratamento macro dos riscos por meio das Estratégias de Segurança, o que a metodologia do NIST deixa a desejar.

3.2.12 Continuidade do processo de Gerenciamento de Risco de TI

Esse item busca avaliar como cada uma das metodologias trata a continuidade do processo de Gerenciamento de Risco de TI.

FIRM

A metodologia FIRM reconhece claramente que o processo de Gerenciamento de Risco de TI é uma atividade contínua e cíclica a ser executado pelas organizações. Um ciclo completo da FIRM leva em torno de doze meses, sendo que durante esse período são realizadas duas avaliações, de modo que se tenha uma base de comparação para verificação da eficácia dos controles empregados após a primeira análise.

NIST SP 800-30

A metodologia NIST SP 800-30 também propõe que processo de Gerenciamento de Risco de TI seja uma atividade contínua. Essa necessidade decorre do fato de o ambiente tecnológico estar em contínua mudança e atualização. Dessa forma, riscos que foram eliminados no passado podem novamente tornar-se iminentes, e novos riscos conseqüentemente surgirão, decorrentes de tais mudanças. Assim a continuidade do processo é extremamente necessária.

A NIST SP 800-30 propõe que o processo de Gerenciamento de Risco de TI seja repetido, pelo menos, a cada três anos, porém não existe uma periodicidade fixa a ser obedecida. De modo geral, o mapeamento dos riscos deve ocorrer de forma que as novas tecnologias inseridas e as mudanças nas empregadas atualmente, sejam refletidas e tenham seus riscos corretamente mapeados.

OCTAVE

A metodologia OCTAVE possui um volume inteiro destinado à continuidade do processo de análise de risco, esse capítulo é denominado “Volume 13: After Evaluation”. Nesse documento são fornecidos diversos "checklists" e exemplos de resultados esperados para as atividades posteriores a conclusão da análise.

Assim como o NIST SP 800-30, a metodologia OCTAVE considera que o ambiente tecnológico está em constante e rápida mudança, e os “hackers” a cada dia procuram novas formas de explorar as brechas de segurança existentes. Dessa forma, a busca pelo aprimoramento da segurança deverá ser algo contínuo.

A metodologia OCTAVE considera que as organizações devem:

- monitorar o progresso da estratégia de proteção e dos planos de mitigação; e
- monitorar os riscos relacionados à segurança das informações, buscando identificar novos riscos e mudanças nos riscos existentes.

Comentário geral:

É possível observar que as três metodologias concordam entre si sobre a necessidade do processo de Gerenciamento de Risco de TI ser efetuado continuamente. Muitas empresas realizam o mapeamento dos riscos de TI uma única vez, e acreditam que somente com esse resultado têm uma visão substancial de seus riscos e isso acaba gerando uma “falsa sensação de segurança”. Superestimar a eficácia dos controles e a segurança do ambiente, faz com que

muitas brechas de segurança passem desapercebidas, podendo fazer com que a organização tenha surpresas desagradáveis.

A periodicidade com a qual irão se repetir as análises de risco poderá variar de organização para organização, estando diretamente ligada com a dinâmica em que ocorrem mudanças no ambiente de TI, não só no aspecto hardware e software, mas também em relação às pessoas. Diversas vezes, o ambiente tecnológico se torna vulnerável, pois as pessoas que executavam os procedimentos de rotina foram substituídas. Embora o sucesso na execução de procedimentos específicos não deva ser dependente de pessoas, na prática, sabemos que isso não ocorre, e que mudanças no quadro de pessoal, podem refletir em novas vulnerabilidades.

Além da execução periódica do processo de análise de risco, a organização deve possuir métricas que auxiliem na avaliação da eficácia dos controles de mitigação, já empregados.

Adicionalmente, algumas empresas sujeitas a regulamentações externas, por exemplo, Sarbanes Oxley, devem executá-lo numa freqüência menor, atendendo ao que é requerido pela legislação.

3.2.13 Tratamento do risco residual

Esse aspecto visa avaliar como as metodologias abordam o tratamento do risco residual.

FIRM

A metodologia FIRM não trata especificamente a questão do risco residual. No principal documento utilizado para mapeamento das informações referentes ao processo de risco, o "Information Risk Scorecard" não é feito nenhum questionamento visando identificar, direta ou indiretamente, a existência de riscos residuais.

A metodologia menciona que um segundo formulário, denominado "Brief Incident Pro Forma" utilizado somente para documentação dos incidentes de segurança ocorridos, tem como um dos objetivos mapear os possíveis riscos residuais, porém isso não é evidente para a pessoa que está conduzindo o processo.

NIST SP 800-30

A NIST SP 800-30 é a única metodologia, dentre as três analisadas que trata a questão do risco residual.

A NIST SP 800-30 coloca claramente que nenhum sistema de TI pode ter seus riscos completamente eliminados. Dessa forma sempre haverá um risco residual o qual deverá ser tratado de forma que alcance um nível aceitável. Caso existam riscos remanescentes, cuja gravidade não esteja em um nível aceitável, todo o processo de Gerenciamento de Risco de TI deverá ser repetido de forma a buscar estratégias alternativas para eliminação completa ou redução a níveis aceitáveis.

OCTAVE

Esta metodologia não faz referência ao tratamento do risco residual. Ela propõe que para os ativos críticos **todas** as ameaças e vulnerabilidades sejam tratadas. Assim, em teoria não haveria espaço para a existência de riscos residuais para tais ativos (e*mbora saibamos que a eliminação de todos os riscos não é viável).*

Comentário geral:

Os riscos residuais recebem essa denominação por se tratarem de riscos potenciais que, mesmo após a implementação de estratégias para mitigação das vulnerabilidades e ameaças, ou seja controles, estes permanecem ativos. Com exceção da metodologia do NIST, todas as demais não tratam adequadamente a questão do risco residual, fazendo pouca, ou nenhuma, menção ao

tema. O correto entendimento do conceito de risco residual é de extrema importância para as organizações, visto que todos os envolvidos devem ter em mente que nem todos os riscos serão eliminados em sua plenitude e que sempre haverá riscos residuais, os quais devem ser de conhecimento da alta administração, e formalmente aceitos pelos mesmos, evitando assim surpresas futuras.

3.2.14 Nível de utilização internacional da metodologia

Este item tem por objetivo buscar informações que sinalizem qual das três metodologias tem sido mais adotada, no Brasil e no exterior.

Até a data de conclusão dessa dissertação não obtivemos informações emitidas por órgãos independentes, as quais nos permitissem identificar o grau de utilização das metodologias contempladas nessa análise.

Entretanto, em pesquisas realizadas, identificamos por meio de artigos que a IBM utiliza a metodologia OCTAVE para prestação de seus serviços de segurança, e a consultoria KPMG possui sua metodologia de trabalho baseada na FIRM.

Outro ponto a destacar é que a empresa CITICUS, desenvolveu o software de gerenciamento de riscos "CITICUS ONE" totalmente baseado na metodologia FIRM.

Em relação à NIST SP 800-30 não identificamos "cases" públicos de empresas que empregam tal metodologia.

3.2.15 Nível de aderência a requisitos legais

Este aspecto busca avaliar se as metodologias estão aderentes às boas práticas de mercado.

Não foram encontradas muitas evidências referente ao nível de aderência dessas metodologias a requisitos legais. Algumas das informações apresentadas aqui foram inferidas a partir do conteúdo das metodologias e da referência bibliográfica das mesmas.

FIRM

A FIRM não menciona claramente estar aderente a padrões de mercados comumente aceitos. Nela é possível encontrar referências para diversas outras publicações do próprio Information Security Fórum – ISF:

- *The Forum's Standard of Good Practice*
- *IT Could Happen to You: A Profile of Major Incidents*
- *Information Risk Reference Guide*
- *Driving Information Risk Out of the business*

A única referência efetuada a boas práticas de mercado, é em relação a norma BS 7799 – "A Code of Practice for Information Security Management" e que teve como objetivo informar ao leitor que possíveis customizações nas áreas de controles existentes no formulário "Information Risk Scorecard" poderão ser feitas, para assegurar a aderência a outros padrões, como o mencionado acima.

NIST SP 800-30

A NIST SP 800-30 não menciona ao longo do documento estar consistente com outros padrões de mercado relacionados à segurança da informação, como por exemplo a BS7799 ou a ISO:IEC 17799.

Todas a referências mencionadas são feitas a outras publicações do próprio NIST, dentre elas a SP 800-27 –"Engineering Principles for IT Security"; SP 800-14 "Generally Accepted Principles and Practices for Securing Information Technology Systems".

OCTAVE

A metodologia OCTAVE apresenta no "Volume 14: Bibliography and Glossary" uma extensa relação de fontes que foram consultadas para composição do material. Dentre elas é feita menção à "BS7799: Part 1: Code of Practice for Information Security Management of Systems", e à "NIST SP 800-30".

Adicionalmente, no site da OCTAVE é feita uma citação na qual afirma-se que a metodologia atende aos requisitos de Gerenciamento de Risco de TI proposto pela lei Sarbanes Oxley, HIPAA[4] e FISMA[5].

3.3 Consolidação da análise comparativa

De modo geral as três metodologias analisadas (FIRM, NIST SP 800-30 e OCTAVE) fornecem todos os subsídios necessários para condução do processo de Gerenciamento de Risco de TI, porém as características específicas de cada uma fazem com que elas atendam às organizações com diferentes níveis de maturidade e recursos disponíveis. A maturidade refere-se ao conhecimento de Gerenciamento de Risco de TI que a empresa possui e à existência de processos eficazes estabelecidos relacionados a esse assunto. Deve-se entender por recursos a quantidade de profissionais disponíveis nas áreas de negócio e TI, a existência de software

[4] HIPAA: Health Insurance Portability and Accountability Act de 1996 é um padrão que define como as organizações de saúde devem lidar com as informações pessoais referente à saúde.

[5] FISMA: Federal Information Security Management Act (FISMA), parte do Eletronic Government Act de 2002. Legislação americana que fornece um "framework" para assegurar que medidas abrangentes foram tomadas para proteger os ativos e informações federais.

disponível para o mapeamento de vulnerabilidades, disponibilidade de profissionais nas áreas de negócio para tratamento do tema, dentre outros recursos.

A metodologia FIRM é bastante focada no processo de identificação dos riscos e a forma como tais riscos são reportados à alta administração. Sua estruturação permite que seja conduzida de modo descentralizada, com o auxílio das áreas de negócio. Nesse contexto as áreas de Gerenciamento de Riscos / Segurança atuam somente como balizadores do processo, fornecendo o direcionamento necessário. Ela é uma ótima opção principalmente quando os recursos a serem empregados no processo de Gerenciamento de Risco de TI são escassos.

A metodologia NIST SP 800-30 apresenta uma visão geral do processo de Gerenciamento de Risco de TI, possibilitando ao leitor ter uma visão completa, porém superficial do processo. Em poucos momentos o detalhamento apresentado é aprofundado. Dois pontos fortes abordados pela metodologia são: avaliação dos controles já empregados pela empresa e a elaboração da estratégia de mitigação e o tratamento do risco residual. Essa metodologia é mais indicada para as organizações que já possuem um processo de Gerenciamento de Risco de TI estabelecido e que desejam apenas aperfeiçoar aspectos específicos, ou assegurar que todo o ciclo está completo. Ela também é indicada para empresas que necessitam focar na estratégia de mitigação.

A metodologia OCTAVE é a mais completa dentre as três metodologias analisadas. A OCTAVE parte do principio que as pessoas que estão conduzindo o processo, ou que contribuem com o mesmo, não possuem muito conhecimento sobre o tema. Assim, ela busca ao longo dos diversos volumes, exemplificar as atividades a serem executadas, os produtos esperados, como as atividades em grupo devem ser conduzidas, as responsabilidades pela execução das micro atividades, dentre outros aspectos. Se comparada com as demais, esta metodologia é a que envolve um número maior de colaboradores, e de modo recorrente, ou seja, após os levantamentos e elaboração das conclusões, todos os resultados são submetidos a aprovação dos níveis gerenciais. Assim, a quantidade de colaboradores envolvidos é bem elevada, bem como a quantidade de horas disponibilizadas por cada um.

As Figuras 10 e 11, apresentadas abaixo, representam o nível de atendimento de cada uma das metodologias para cada um dos requisitos definidos. Estas figuras permitem ao usuário identificar quais os pontos fortes de cada metodologia, o que contribui na escolha da análise de qual melhor se adapta às necessidades da empresa. A tabela abaixo representa as escalas de medição utilizadas em ambas as figuras:

Símbolo	**Descrição**
	– Não atendido: a metodologia não aborda o tema;
	– Parcialmente, com ressalvas: o requisito foi abordado, porém com alguns aspectos negativos que merecem ser analisados; e
	– Requisito plenamente atendido: o requisito foi atingido completamente, sem ressalvas.

Tabela 07: Legenda utilizada para interpretação das figuras 10 e 11.

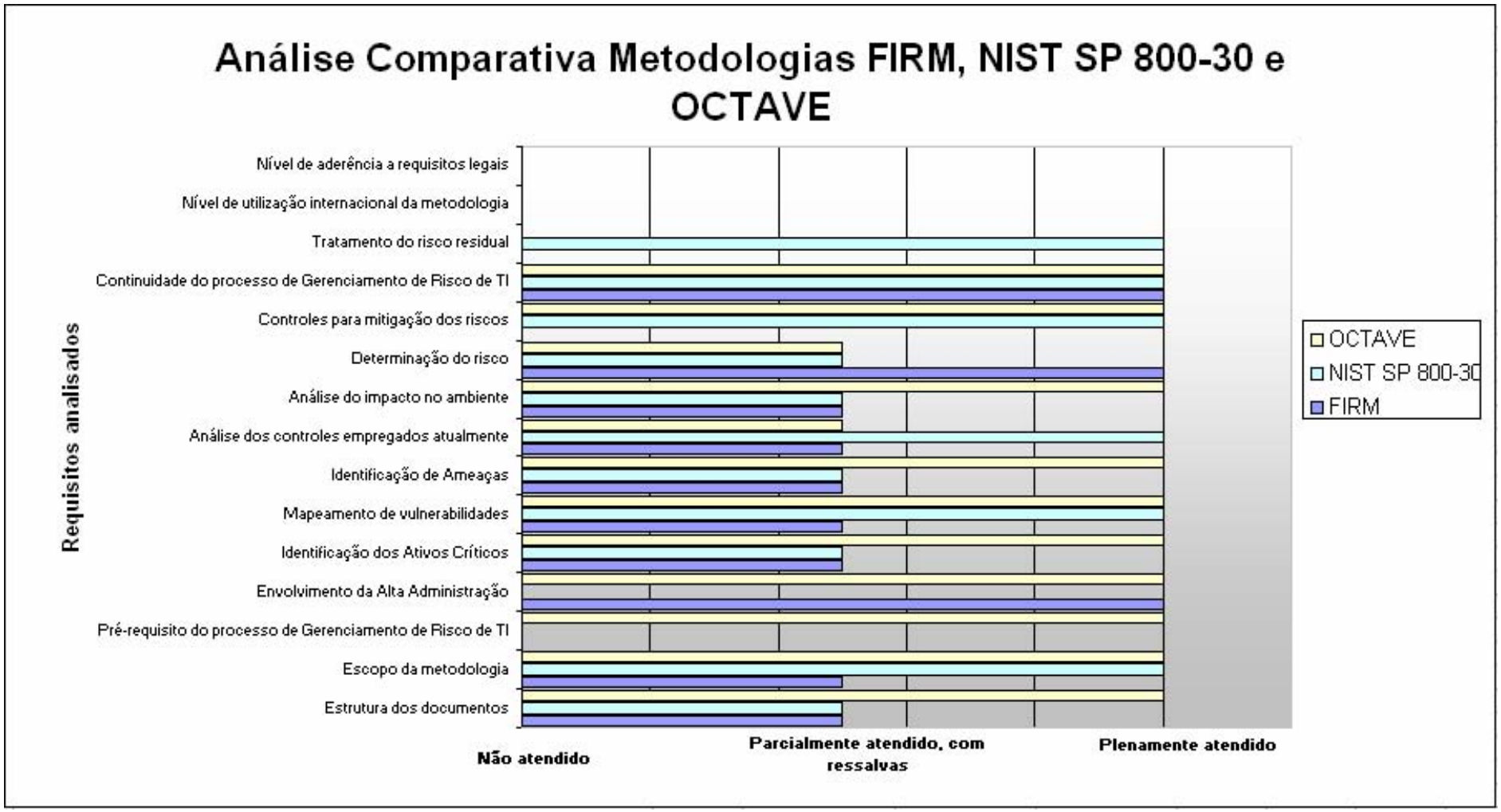

Figura 10: Nível de atendimento aos requisitos analisados

#	Requisitos	FIRM	NIST SP 800-30	OCTAVE
1.	Estrutura dos documentos			
2.	Escopo da metodologia			
3.	Pré-requisito do processo de Gerenciamento de Risco de TI			
4.	Envolvimento da Alta Administração			
5.	Identificação dos Ativos Criticos			
6.	Mapeamento de vulnerabilidades			
7.	Identificação de Ameaças			
8.	Análise dos controles empregados atualmente			
9.	Análise do impacto no ambiente			
10.	Determinação do risco			
11.	Controles para mitigação dos riscos			
12.	Continuidade do processo de Gerenciamento de Risco de TI			
13.	Tratamento do risco residual			
14.	Nível de utilização internacional da metodologia			
15.	Nível de aderência a requisitos legais			

Figura 11: Nível de atendimento aos requisitos analisados utilizando símbolos

Nos gráficos abaixo foram apresentados os níveis de atendimento aos requisitos, individualmente, por metodologia. Adicionalmente, para cada um dos gráficos existe uma tabela associada, a qual justifica sucintamente as situações em que o requisito recebeu a classificação “Parcialmente atendido, com ressalvas”. O detalhamento completo pode ser encontrado no item 3.3 dessa dissertação.

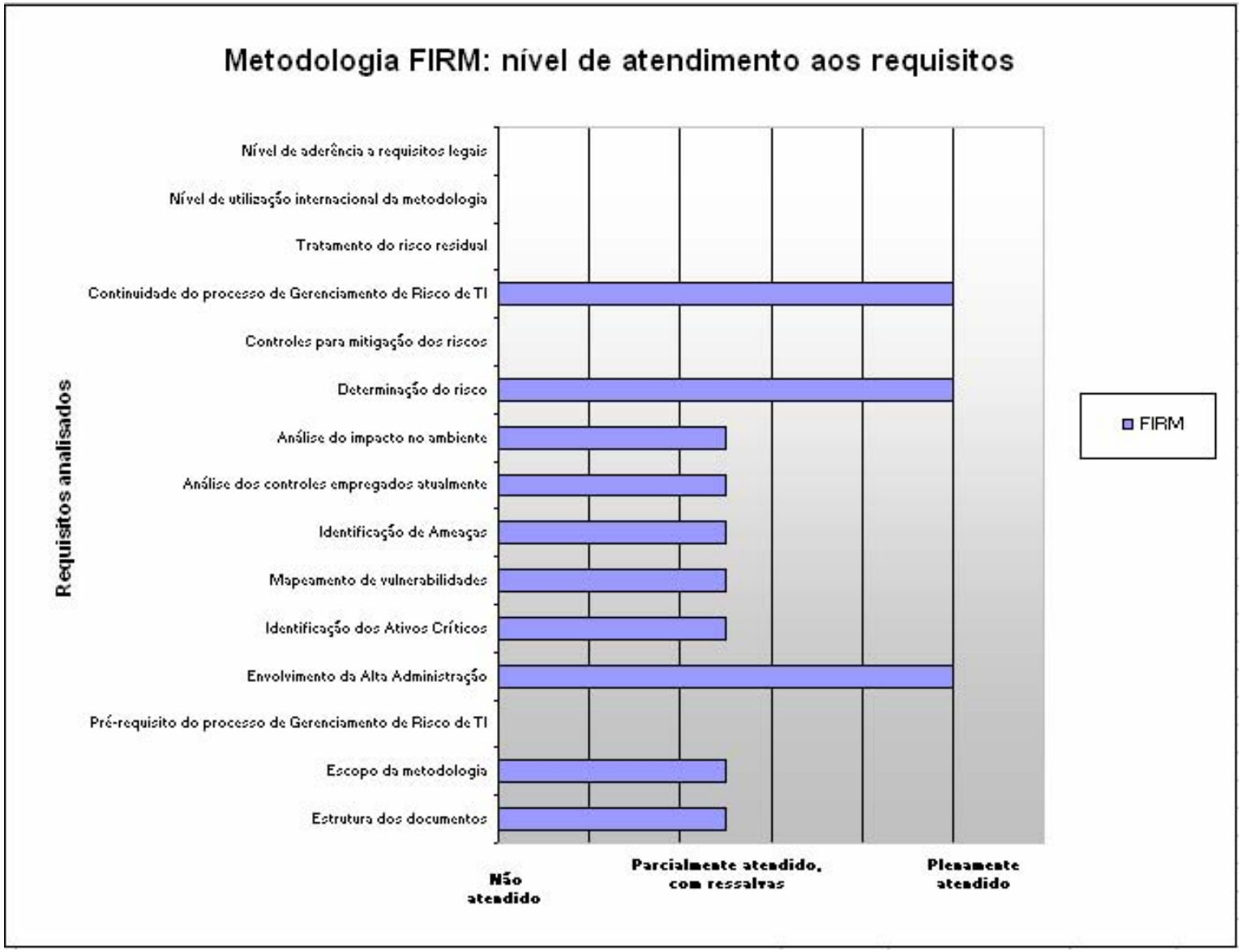

Figura 12: Metodologia FIRM: nível de atendimento aos requisitos

Requisito	FIRM:Pontos de atenção identificados
Estrutura dos documentos	Excesso de simbologia, texto poluído.
Escopo da metodologia	Não aborda a estratégia de mitigação
Pré-requisito do processo de Gerenciamento de Risco de TI	Não aborda esse requisito.
Envolvimento da alta administração	Ok.
Identificação dos ativos críticos	Conceito deturpado em relação a ativo crítico. Não define quais requisitos caracterizam ativo crítico.
Mapeamento de vulnerabilidades	Limita o mapeamento de vulnerabilidades a um escopo reduzido de possibilidades.
Identificação de Ameaças	Utiliza o histórico de eventos para determinar as ameaças.
Análise dos controles empregados atualmente	Limita o mapeamento dos controles a um universo reduzido.
Análise do impacto no ambiente	Possível "mascaramento" das vulnerabilidades por tratá-las de forma agrupadas.
Determinação do risco	Ok.
Controles para mitigação dos riscos	Não aborda esse requisito.
Continuidade do processo de Gerenciamento de Risco de TI	Ok.
Tratamento do risco residual	Não aborda esse requisito.
Nível de utilização internacional da metodologia	Não foram identificadas informações em relação a esse requisito.
Nível de aderência a requisitos legais	Não foram identificadas informações em relação a esse requisito.

Tabela 8: FIRM: Pontos de atenção identificados

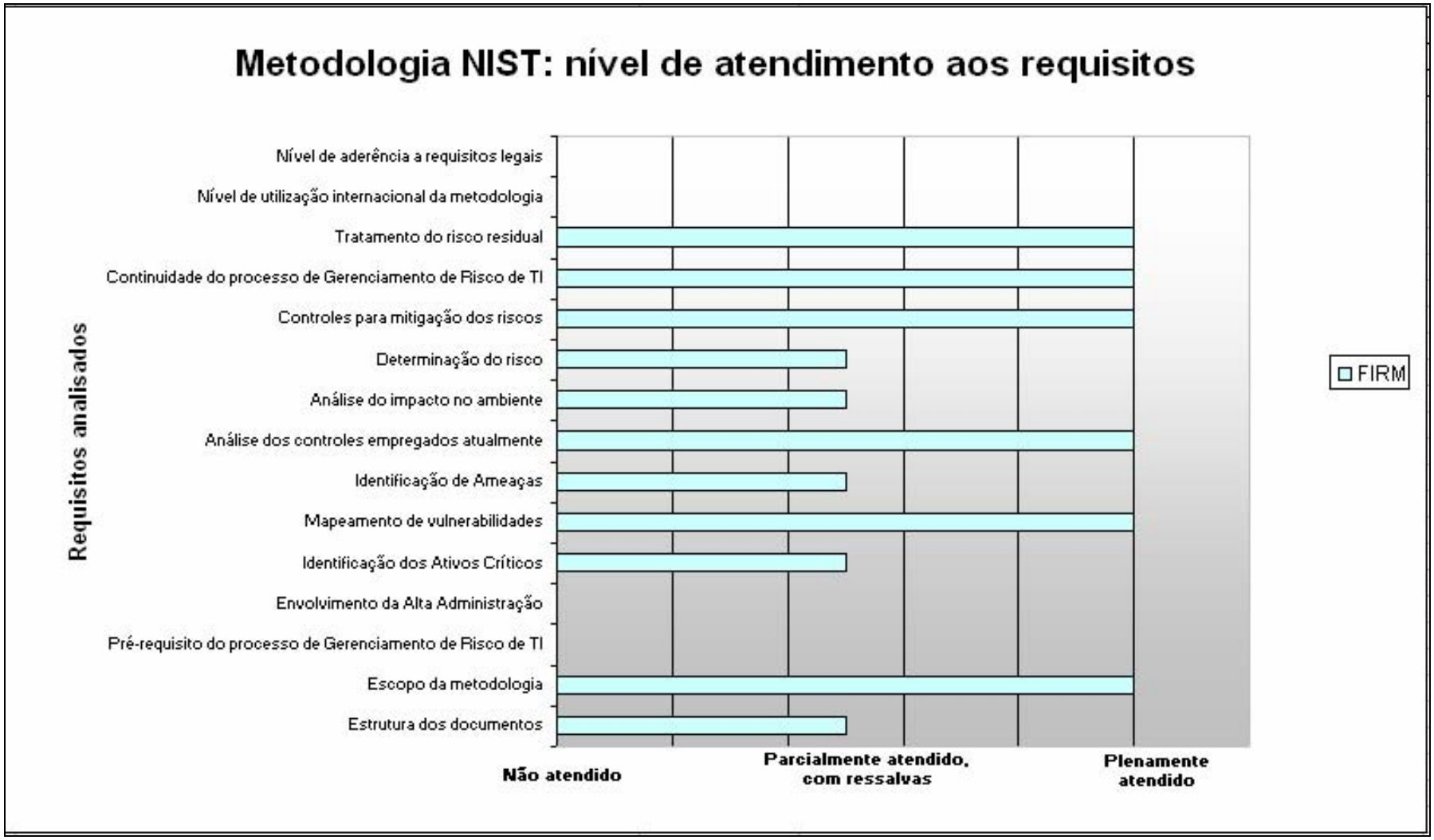

Figura 13: Metodologia NIST SP 800-30: nível de atendimento aos requisitos

Requisito	**NIST SP 800-30:Pontos de atenção identificados**
Estrutura dos documentos	Falta de exemplos práticos.
Escopo da metodologia	Ok.
Pré-requisito do processo de Gerenciamento de Risco de TI	Não aborda esse requisito.
Envolvimento da alta administração	Não há envolvimento da alta administração
Identificação dos ativos críticos	Não define quais requisitos caracterizam ativo crítico.
Mapeamento de vulnerabilidades	Ok.
Identificação de Ameaças	Não propõe lista de ameaça que podem ser consideradas.
Análise dos controles empregados atualmente	Ok.
Análise do impacto no ambiente	Não define em qual escopo deverá ser feito este mapeamento.
Determinação do risco	Não considera diretamente os controles empregados para determinar o risco.
Controles para mitigação dos riscos	Ok.
Continuidade do processo de Gerenciamento de Risco de TI	Ok.
Tratamento do risco residual	Ok.
Nível de utilização internacional da metodologia	Não foram identificadas informações em relação a esse requisito.
Nível de aderência a requisitos legais	Não foram identificadas informações em relação a esse requisito.

Tabela 9: NIST SP 800-30: Pontos de atenção identificados

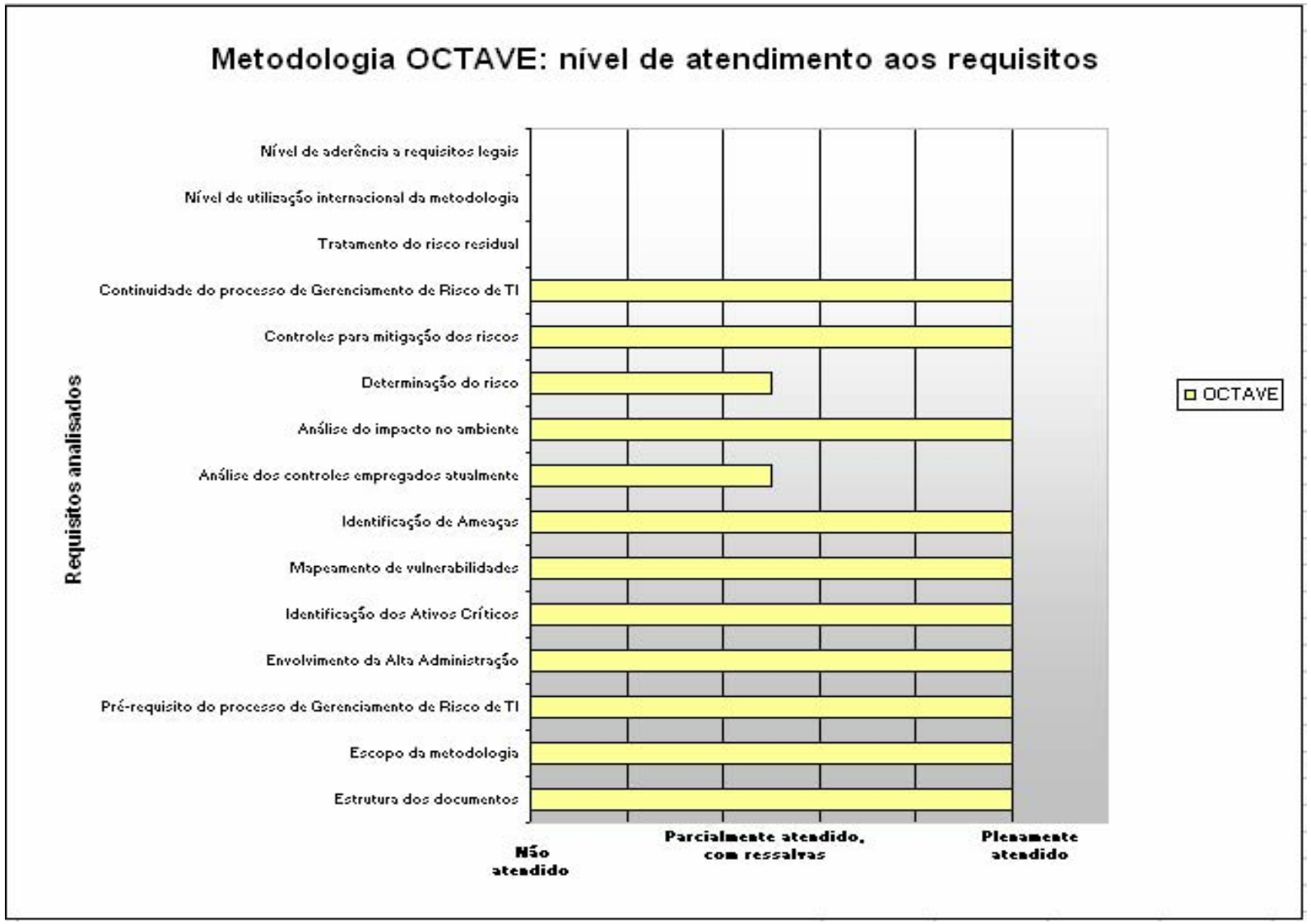

Figura 14: Metodologia OCTAVE: nível de atendimento aos requisitos

Requisito	OCTAVE:Pontos de atenção identificados
Estrutura dos documentos	Ok.
Escopo da metodologia	Ok.
Pré-requisito do processo de Gerenciamento de Risco de TI	Ok.
Envolvimento da alta administração	Ok.
Identificação dos ativos críticos	Ok.
Mapeamento de vulnerabilidades	Ok.
Identificação de Ameaças	Ok.
Análise dos controles empregados atualmente	Não avalia os controles existentes para a determinação do risco, e sim no momento da elaboração da estratégia de segurança a ser empregada.
Análise do impacto no ambiente	Ok.
Determinação do risco	Não considera a probabilidade de ocorrência de uma ameaça para determinar o risco.
Controles para mitigação dos riscos	Ok.
Continuidade do processo de Gerenciamento de Risco de TI	Ok.
Tratamento do risco residual	Não aborda esse requisito.
Nível de utilização internacional da metodologia	Não foram identificadas informações em relação a esse requisito.
Nível de aderência a requisitos legais	Não foram identificadas informações em relação a esse requisito.

Tabela 10: OCTAVE: Pontos de atenção identificados

Na Figura 14 abaixo, o objetivo é demonstrar como cada uma das metodologias se posicionam, considerando o nível de maturidade em relação ao processo de Gerenciamento de Risco de TI que as empresas possuem.

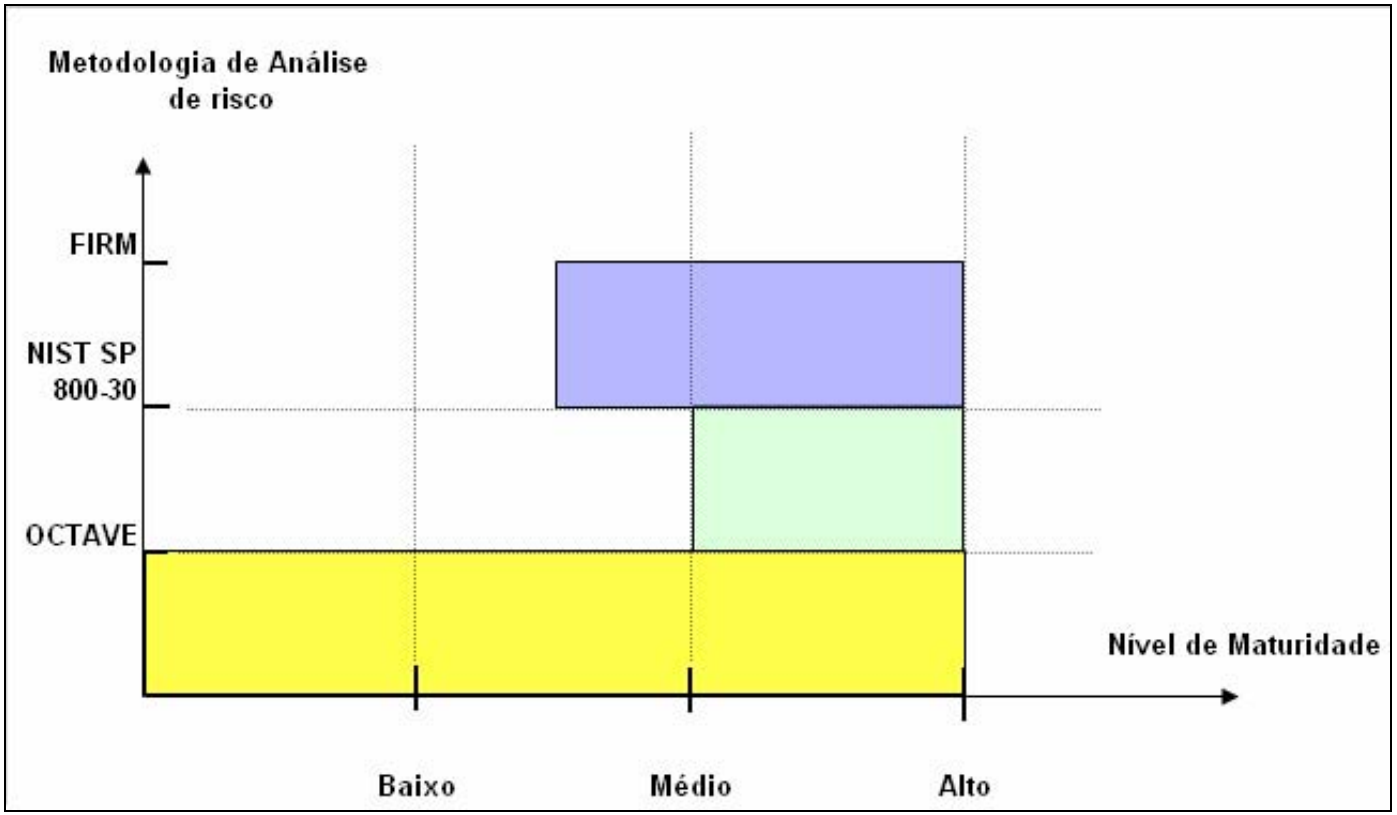

Figura 15: Relacionamento nível de maturidade x metodologias

De acordo com o gráfico, a metodologia FIRM atende melhor às necessidades das empresas que se encontram em um nível de maturidade médio para alto. Isso decorre do fato de ela ter uma deficiência importante: ela não aborda nenhuma informação em relação à elaboração da estratégia de mitigação, aspecto crucial para uma empresa que está iniciando o estabelecimento do processo de análise de risco.

A metodologia NIST SP 800-30, em virtude de apresentar uma visão superficial de todo o processo, deve ser aplicada por organizações que já tenham um nível médio de maturidade e que estejam buscando aprimorar apenas seu processo de Gerenciamento de Risco de TI.

Já a metodologia OCTAVE, por possuir um conteúdo extremamente detalhado pode ser utilizado por organizações com qualquer nível de maturidade. Adicionalmente, a universidade Carnegie Mellon possui uma abordagem simplificada da OCTAVE, denominada OCTAVE-S, destinada a organizações menores, com menos de duzentos funcionários.

Capítulo 4 - Conclusão

4.1 Conclusões

Nessa dissertação apresentamos todo o embasamento conceitual do processo de Gerenciamento de Risco de TI, o qual consiste em proporcionar às organizações meios pelos quais elas possam identificar grande parte dos riscos tecnológicos aos quais estão suscetíveis, elaborar estratégias para mitigação de tais riscos e monitorar o ambiente de forma a assegurar a eficácia dos controles empregados por meio das estratégias de mitigação . Ao longo dessa dissertação buscamos enfatizar a importância desse processo para todas as organizações, e as principais dificuldades encontradas em relação à implementação do mesmo.

Um segundo propósito dessa dissertação foi analisar três metodologias distintas de Gerenciamento de Risco de TI, visando identificar como cada uma delas aborda os principais conceitos relacionados ao tema, ressaltando os seus aspectos positivos e negativos. As metodologias escolhidas foram: FIRM, NIST SP 800-30 e OCTAVE, em virtude de serem conhecidas entre os profissionais de TI, e pela facilidade de obtenção de material sobre as mesmas. Para sistematizar o processo de análise, foram selecionados quinze requisitos que entendemos essenciais em relação ao tema Gerenciamento de Risco de TI:

1. Estrutura dos documentos
2. Escopo da metodologia
3. Pré-requisito do processo de Gerenciamento de Risco de TI
4. Envolvimento da alta administração
5. Identificação dos ativos críticos
6. Mapeamento de vulnerabilidades
7. Identificação de ameaças
8. Análise dos controles empregados atualmente
9. Análise do impacto no ambiente
10. Determinação do risco
11. Controles para mitigação dos riscos
12. Continuidade do processo de Gerenciamento de Risco de TI
13. Tratamento do risco residual
14. Nível de utilização internacional da metodologia
15. Nível de aderência a requisitos legais

As três metodologias analisadas atendem em grande parte aos requisitos listados acima. O não atendimento a algum dos requisitos, ou atendimento parcial aos mesmos não inviabiliza a adoção de nenhuma das metodologias, apenas geram alertas de pontos de atenção a serem considerados durante a implementação, para que não haja o entendimento equivocado sobre o assunto ou a geração de resultados distorcidos. A mensuração incorreta de um risco pode ter impactos significativos na organização, desde a realização de investimentos desnecessários para proteção do ambiente, ou até mesmo a não adoção de nenhuma medida, o que tornará a empresa suscetível a um incidente de segurança que poderá ter grandes proporções, visto que estará sujeita ao fator surpresa.

Cada uma das metodologias possui uma característica peculiar que a diferencia em relação às demais. A metodologia FIRM possui como principal característica ser altamente "fechada". Todos os levantamentos e questionamentos a serem feitos já estão definidos e possuem valores pré-definidos a serem obtidos como retorno, o que permite a fácil tabulação dos resultados e ao mesmo tempo permite que ela seja aplicada de forma descentralizada, por diversas frentes de trabalho. Ao mesmo tempo, ela pode não se adequar totalmente à organização caso esta possua um cenário diferenciado.

A metodologia do NIST possui um conteúdo bem abrangente, porém em poucos tópicos há um aprofundamento do assunto que está sendo discutido. Uma das exceções observadas é em relação ao processo de escolha dos controles de mitigação, para os quais é apresentada passo a passo a análise a ser feita. Outro diferencial é a ênfase dada à adoção do processo de Gerenciamento de Risco de TI durante o ciclo de desenvolvimento de sistemas.

A metodologia OCTAVE prima pelo detalhamento das atividades a serem conduzidas e busca efetuar a identificação dos riscos não somente nos dispositivos tecnológicos, mas também nos processos de TI. Um aspecto deficiente em relação desta metodologia, quando comparada às demais, é a não utilização da probabilidade de materialização das ameaças durante a determinação do risco.

Ao longo da dissertação, a preocupação foi tornar o tema mais acessível, desfazendo o mito de que o processo de Gerenciamento de Risco de TI somente poderá ser conduzido por especialistas no assunto, situação amplamente percebida em diversas organizações. Ao mesmo tempo buscamos reforçar sua relevância para as empresas, e as vantagens obtidas pela condução adequada de um processo de Gerenciamento de Risco de TI, algo que também muitas vezes não é corretamente interpretado, visto que as empresas não obtêm um retorno financeiro imediato decorrente da implementação desse processo.

Visando facilitar a execução do processo, também elaboramos um questionário, o qual contempla os principais aspectos de TI a serem verificados durante a identificação dos riscos. Esse questionário pode ser encontrado no Apêndice A dessa dissertação.

4.2 Trabalhos Futuros

Basicamente existem quatro aspectos que entendo serem relevantes para extensão deste trabalho:

- avaliação de estudo de casos de empresas que tenham adotado cada uma das metodologias mencionadas, permitindo a obtenção da percepção dos gestores dessas empresas sobre as dificuldades encontradas e resultados obtidos;

- mapeamento de outros requisitos relevantes a serem utilizados na comparação das metodologias;

- inclusão da norma ISO/IEC TR 13335-1 “Information technology — Security techniques — Management of information and communications technology security — Part 1: Concepts and models for information and communications technology security management” a qual não foi analisada em função de possuirmos apenas uma versão desatualizada da norma e o custo da nova versão ser extremamente elevado; e

- aprofundamento dos levantamentos quanto aos requisitos “14. Nível de utilização internacional da metodologia” e “15. Nível de aderência a requisitos legais”, para os quais não foi possível obtermos muitas informações.

Capítulo 5 - Bibliografia

ALBERTS, Christopher J.; DOROFEE, Audrey J. Octave Method Implementation Guide v2.0. USA: Carnegie Mellon University, 2001.

BROCK, Jack L. Information Security Risk Assessment – Practices of Leading Organizations. USA: General Accounting Office, 1999.

CCCURE, 1999. Handbook of Information Security Management:Risk Management and Business Continuity Planning. Dísponível em: http://www.cccure.org/Documents/HISM/. Acesso em: 05/06/2004.

COHEN, Fred. Risk Management: Concepts and Frameworks. USA: Burton Group, 2003. 45 p.

COMPUTERWORLD – Análises de risco auxiliam na gestão de segurança. Disponível em: http://computerworld.uol.com.br. Acesso em: 17/01/2006.

D'ANDREA, Edgar et al. Segurança em Banco Eletrônico. São Paulo: Febraban, 2000. 134 p.

EVANS, John. Risk Management Process. USA: PricewaterhouseCoopers, 1999.

FUNDAMENTAL RISK MANAGEMENT, Disponível em: http://searchsecurity.techtarget.com/expert. Acesso em: 17/01/2006.

GEUS, Paulo Lício de; NAKAMURA, Emílio Tissato. Segurança de Redes em Ambientes Cooperativos. São Paulo: Futura 2003. 472 p. ISBN: 8574131792

GORDON, Lawrence A. 2004 CSI/FBI Computer Crime and Security Survey. USA: CSI, 2004. 18 p.

INFORMATION SECURITY FORUM; Fundamental Information Risk Management – Implementation guide. USA: ISF, 2000. 93 p.

INFORMATION SECURITY FORUM; Fundamental Information Risk Management – Supporting Material. USA: ISF, 2000. 123 p.

INFORMATION SECURITY FORUM; Information Risk Reference Guide. USA: ISF, 1999. 89 p.

ISO IEC TR 13335-1 Information technology – Guidelines for the management of IT Security : Part 1 – Concepts and models for IT Security. EUA: ISO/IEC, 1997. 23 p.

ISO IEC TR 13335-2 Information technology – Guidelines for the management of IT Security: Part 2 – Managing and planning IT Security. EUA: ISO/IEC, 1996. 19 p.

MANAGING INFORMATION RISK IS A CORPORATE GOVERNANCE. Disponível em: http://www.itweb.co.za/office/kpmg/0408050815.htm. Acesso em: 17/01/2006.

NBR ISO/IEC 17799 - Tecnologia da informação - Código de prática para a gestão da segurança da informação. São Paulo: ABNT, 2001. 56 p

OIC, 2005. Octave Information Center. Disponível em: http://oattool.aticorp.org/aboutOctave4a.html/ . Acesso em : 17/01/2006.

PRICEWATERHOUSECOOPERS. Information Risk Assessment Concepts and Methodology. USA: PwC, 2003. 67 p.

STONEBURNER, Gary et al. Risk Management Guide for Information Technology Systems – NIST SP 800-30. USA: NIST – National Institute of Standards and Technology, 2002. 55 p.

VALLABHAENI, S. Rao; VALLABHAENI, Devi. CISSP Examination Textbooks. 2°. Edição, Volume . USA: SRV Professional Publications, 2000. 475 p.

WHITMAN, Michael E.; MATTORD, Hebert J.; Principles of Information Security. EUA: Course Technology, 2003. 560 p. ISBN: 0619216255

Apêndice A – Matriz de Avaliação de Riscos

Este questionário foi elaborado a partir da minha experiência pessoal em projetos de mapeamento dos riscos relativos à Tecnologia da Informação. O questionário abaixo contém diretrizes para o mapeamento dos controles implementados e vulnerabilidades existentes nos principais processos que suportam o ambiente tecnológico. Aqui, não estão contidos questionamentos para mapeamento das vulnerabilidades técnicas, as quais deverão ser identificadas com o auxílio de ferramentas de diagnóstico apropriadas.

Recomendamos que o usuário que esteja aplicando o questionário atribua pesos específicos para cada uma das combinações de respostas possíveis.

A.	Contratos e Acordos de Nível de Serviço																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
1	Como são avaliados os prestadores de serviço quanto a capacidade e qualidade para entrega dos serviços acordados?														
2	Existe uma área ou funcionário responsável pela elaboração / revisão dos contratos?														
3	Nos contratos estão inseridas cláusulas referentes a confidencialidade das informações manipuladas?														
4	Os contratos estabelecidos possuem os níveis mínimos aceitáveis estipulados quanto aos serviços prestados?														
5	São definidos responsáveis para monitorar o acordo de nível de serviço?														
6	São realizadas revisões periódicas no acordo de nível de serviço e nos contratos firmados com terceiros?														

A.	Contratos e Acordos de Nível de Serviço																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
7	Existe interação entre usuários / terceiros e os responsáveis pelo acordo de nível de serviço a fim de realizar melhorias no acordo?														
8	Está estabelecida nos acordos firmada a possibilidade da organização auditar as atividades do prestador de serviços?														
9	São claramente definidos aspectos referentes a direitos de propriedade intelectual e direito autoral?														
10	Os acordos prevêem as ações a serem tomadas em caso de descontinuidade do prestador de serviço?														
11	Os contratos contemplam os aspectos relacionados ao Gerenciamento de Mudanças? Ex.: quando e sob quais condições poderão ser feitas intervenções no ambiente.														
12	Os contratos impõem restrições em relação ao envolvimento do prestador de serviços com subcontratados?														

B.	Inventário de Hardware e Software															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
13	A responsabilidade pelo inventário está atribuída a algum funcionário?														
14	São realizados inventários de todos os hardware e software utilizado pela empresa?														
15	Qual o procedimento para realização do inventário? São utilizadas ferramentas automatizadas?														
16	Quais informações são registradas no inventário?														
17	Como são refletidas no inventário as alterações de equipamentos entre áreas, a desinstalação de aplicativos, o descarte de equipamentos?														
18	Como é feito o controle das licenças dos software? Quem é responsável pelo controle das licenças?														
19	Como é detectada a existência de software não autorizado no ambiente de rede da empresa?														
20	Quais os recursos são utilizados para impedir a instalação de software não autorizado?														
21	Existem restrições em relação ao uso de disquetes? Existem controles sobre os gravadores de CD existentes?														

C.	Classificação das Informações															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
22	As informações manuseadas pela empresa são classificadas?														
23	Quais os critérios utilizados para classificação das informações?														
24	A quem foi atribuída a responsabilidade pela classificação das informações?														
25	A classificação atribuída é revisada periodicamente? Qual periodicidade?														
26	São adotados controles condizentes com a classificação atribuída a informação?														
27	Existem níveis de segurança definidos que representem o mínimo de segurança necessário para cada categoria de informação?														
28	Os usuários estão cientes da existência de procedimentos para classificação da informação?														

D.	Resposta à Incidentes															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
29	Existem procedimentos definidos para reporte dos incidentes?														
30	Os incidentes de segurança comunicados são registrados?														
31	Os incidentes de segurança ocorridos são reportados a alguma área da organização?														
32	São adotadas medidas pró-ativas para contenção dos incidentes conhecidos?														
33	Já ocorreram incidentes em função do não cumprimento de normas e / ou procedimentos instituídos pela organização? Quais as medidas adotadas pela empresa neste caso?														
34	As medidas adotadas para solução dos problemas são documentadas?														
35	Os incidentes ocorridos são investigados?														
36	Existem procedimentos definidos para gerenciamento dos problemas?														
37	As trilhas de auditoria dos sistemas operacionais e aplicativos estão habilitadas, facilitando dessa forma a resolução dos problemas?														
38	Os acessos / privilégios concedidos em situações emergenciais são documentados e aprovados pelos gerentes responsáveis?														

D.	Resposta à Incidentes																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
39	Foram estabelecidas as atividades prioritárias a serem executadas em situações de emergência?														

E.	**Segurança física do CPD e áreas críticas**															
#	**Tópico Avaliado**	**Processo estabelecido, nenhuma vulnerabilidade identificada**	**Nenhuma vulnerabilidade conhecida ou suspeita**	**Suspeita de vulnerabilidades significativas**	**Existência de vulnerabilidades significativas**	**Informações insuficientes para a análise**	**Risco de perda financeira**			**Risco de perda de produtividade**			**Risco de perda de confiança do consumidor**		
							A	**M**	**B**	**A**	**M**	**B**	**A**	**M**	**B**
40	Quais os procedimentos adotados para entrada de visitantes?														
41	Estão mapeadas as áreas são críticas na organização?														
42	Como é feito o controle de acesso ao CPD e dependências onde se encontram equipamentos críticos? Como é feito o controle de acesso ao "backup site"?														
43	Os acessos realizados ao CPD são registrados?														
44	Existem procedimentos para concessão de acesso as localidades críticas?														
45	Os prestadores de serviço têm acesso às dependências da empresa que são classificadas como áreas críticas?														
46	Existem sistemas de detecção de intrusão instalados nas áreas consideradas críticas?														
47	Existem extintores de incêndio e detectores de fumaça instalados nas dependências onde estão localizados os equipamentos de informática?														
48	Existem dispositivos para controle de umidade e temperatura nas dependências da empresa onde estão localizados os equipamentos críticos?														

E.	Segurança física do CPD e áreas críticas															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
49	Existem "no-breaks" instalados para todos os equipamentos considerados críticos? Quais os recursos utilizados caso haja interrupção no fornecimento de energia?														
50	Existe um "backup-site" preparado caso ocorra algum desastre que impossibilite o funcionamento do CPD principal?														
51	Existem câmeras instaladas nas dependências onde se localizam os equipamentos considerados críticos para a empresa?														
52	Existem restrições em relação ao consumo de comidas ou bebidas nas dependências onde se localizam os equipamentos críticos?														
53	Está sendo adotada alguma política específica para o armazenamento e manuseio de documentos considerados críticos?														
54	O cabeamento de rede é certificado?														
55	Existem trituradores de papel para destruição dos relatórios considerados confidenciais? Qual prática é adotada para descarte de relatórios considerados confidenciais?														
56	A empresa possui gerador de energia?														

G.	**Política de mesa limpa**															
#	**Tópico Avaliado**	**Processo estabelecido, nenhuma vulnerabilidade identificada**	**Nenhuma vulnerabilidade conhecida ou suspeita**	**Suspeita de vulnerabilidades significativas**	**Existência de vulnerabilidades significativas**	**Informações insuficientes para a análise**	**Risco de perda financeira**			**Risco de perda de produtividade**			**Risco de perda de confiança do consumidor**		
							A	**M**	**B**	**A**	**M**	**B**	**A**	**M**	**B**
62	Foi adotada a Política de Mesa limpa na organização?														
63	Os usuários receberam alguma instrução em relação a: - não deixar papéis sobre as mesas; - não deixar as estações de trabalho logadas, enquanto estiverem ausentes. - cuidados em relação aos locais de transferência e recepção de faxes; e - cuidados em relação aos locais de impressão.														

F.	Segurança dos equipamentos															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
57	Qual o procedimento para remoção de equipamentos para outras áreas / unidades?														
58	Quais os procedimentos para remoção de um equipamento para manutenção externa?														
59	Os equipamentos considerados críticos possuem seguro com roubo, furto e desastres físicos?														
60	Como é feito o controle sobre os equipamentos portáteis? Existe um “pool” de equipamentos para empréstimo?														
61	Como é feito o descarte de equipamento? E de mídias? Quais cuidados são tomados?														

H.	Gerenciamento de mudanças																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
64	Existe uma Área/funcionário responsável pelo gerenciamento de mudanças na empresa?														
65	Existe um procedimento definido para gerenciamento das mudanças nos sistemas?														
66	Quando possível, as mudanças realizadas são testadas em ambiente apropriado (ambiente de homologação)?														
67	São realizadas avaliações dos possíveis riscos e impactos causados pela mudança?														
68	Existe uma metodologia específica para gerenciamento de mudanças?														
69	Toda mudança implementada possui uma documentação correspondente?														
70	As áreas afetadas pela mudança participam do processo de gerenciamento de mudanças? Em que momento elas são envolvidas?														
71	Qual o critério utilizado para priorização das mudanças a serem realizadas?														
72	Em caso de atualização de software como é feito o controle das versões?														
73	Existem procedimentos definidos em caso de mudanças emergenciais?														
74	As mudanças emergenciais são submetidas a aprovação da gerência de TI?														

H.	Gerenciamento de mudanças																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
75	As mudanças emergenciais realizadas são documentadas após a realização das mesmas?														
76	As atividades dos funcionários responsáveis pela manutenção são monitoradas?														

I.	Desenvolvimento de sistemas															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
77	Como são definidos os requisitos dos projetos?														
78	A empresa possui uma metodologia de desenvolvimento?														
79	Quem são os responsáveis pela realização de testes?														
80	Existem ambientes segregados para realização de testes?														
81	Como é elaborada a base de dados que será utilizada nos testes dos sistemas?														
82	Os desenvolvedores possuem acesso ao ambiente de produção?														
83	Como é feita a migração dos sistemas entre os ambientes (desenvolvimento, teste e produção)?														
84	Quem possui autorização para realizar a migração dos sistemas para o ambiente de produção?														
85	Os testes realizados com os sistemas são documentados?														
86	Como são realizadas as manutenções no sistema?														
87	Os sistemas desenvolvidos possuem documentação técnica e manual de utilização para os usuários?														

I.	**Desenvolvimento de sistemas**																
#	**Tópico Avaliado**	**Processo estabelecido, nenhuma vulnerabilidade identificada**	**Nenhuma vulnerabilidade conhecida ou suspeita**	**Suspeita de vulnerabilidades significativas**	**Existência de vulnerabilidades significativas**	**Informações insuficientes para a análise**	**Risco de perda financeira**			**Risco de perda de produtividade**			**Risco de perda de confiança do consumidor**		
							A	**M**	**B**	**A**	**M**	**B**	**A**	**M**	**B**
88	Os prestadores de serviço, responsáveis pelo desenvolvimento dos sistemas, têm acesso a réplicas de bases de dados de produção?														
89	São fornecidos treinamentos aos usuários dos sistemas desenvolvidos?														
90	Como é feito o controle das versões dos sistemas?														
91	Existem procedimentos de codificação segura aos quais os desenvolvedores devem estar cientes durante o processo de desenvolvimento?														
92	São realizadas revisões de código-fonte que assegurem contra "inconsistências" deixadas durante o desenvolvimento (comentários, senhas, etc)?														
93	A metodologia de desenvolvimento de sistema trata dos requisitos necessários para a contratação de terceiros?														
94	Quais medidas são adotadas para garantir a propriedade da organização sobre os sistemas desenvolvidos por terceiros?														
95	Os desenvolvedores recebem diretrizes referentes aos requisitos mínimos de segurança que o sistema deve contemplar? Ex.: controle de acesso, trilha de auditoria, critérios para validação de campos.														

J.	Capacity Planning																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
96	Foram desenvolvidos “capacity planning” para os principais servidores?														
97	Foi designado um responsável pelo “capacity planning”?														
98	Como são feitas as atualizações no “capacity planning”?														
99	Existe um funcionário responsável pela definição de quais recursos devem possuir “capacity planning”"?														
100	A operação da empresa já prejudicada ou indisponibilizada em função da inexistência de “capacity planning”?														
101	O “capacity planning” é constantemente atualizado?														
102	Como é monitorada a capacidade dos recursos/serviços que possuem “capacity planning”? E dos demais recursos/sistemas?														
103	São realizadas previsões, quanto ao crescimento do volume de operações que envolvam determinados recursos e a capacidade máxima suportada por este?														
104	Como é feito o monitoramento da performance dos dispositivos?														

K.	**Backup**															
#	**Tópico Avaliado**	**Processo estabelecido, nenhuma vulnerabilidade identificada**	**Nenhuma vulnerabilidade conhecida ou suspeita**	**Suspeita de vulnerabilidades significativas**	**Existência de vulnerabilidades significativas**	**Informações insuficientes para a análise**	**Risco de perda financeira**			**Risco de perda de produtividade**			**Risco de perda de confiança do consumidor**		
							A	**M**	**B**	**A**	**M**	**B**	**A**	**M**	**B**
105	Existem funcionários / áreas responsáveis pela execução do “backup”?														
106	Qual a freqüência em que são realizados os “backups” (diário, semanal, mensal, anual)?														
107	Quais controles são utilizados para assegurar que o “backup” foi concluído corretamente?														
108	São realizados testes de restauração com as fitas de “backup”?														
109	Os procedimentos de “backup” estão formalmente documentados?														
110	As mídias de “backup” são devidamente identificadas?														
111	Como é feito o controle das fitas de “backup”?														
112	Quais funcionários possuem autorização para terem acesso às fitas de “backup”?														
113	A movimentação das fitas de “backup” (entradas e saídas) ficam registradas em algum documento?														
114	Como é o processo de restauração das fitas de “backup”?														
115	Quais funcionários podem solicitar a restauração das fitas de “backup”?														
116	Em quais situações são solicitadas restaurações de fitas de “backup”?														

K.	Backup															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
117	Existe um ambiente separado para teste das restaurações antes destas serem implementadas no ambiente de produção?														
118	Os procedimentos para restauração das fitas de “backup” estão formalmente documentados?														
119	Onde ficam armazenadas as fitas de “backup”?														
120	Existe armazenamento “off-site” das fitas de “backup”?														
121	Quem é responsável pela definição dos itens que devem ser feitos “backups”?														
122	Já ocorreu algum incidente onde foi necessária a restauração das fitas de “backup”?														
123	Os “backups” realizados atendem a legislação vigente?														
124	Quais é a periodicidade para substituição das fitas de “backup”?														
125	São realizados inventários das fitas armazenadas "off-site"?														
126	As fitas de “backup” estão adequadamente identificadas?														
127	Como é feito o transporte das fitas para armazenamento "off-site"?														

L.	Segurança do ambiente de rede															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
128	Como está estruturada a rede da organização?														
129	É possível realizar conexões remotas na rede interna da empresa?														
130	É utilizado o sistema de "dial-back" para confirmar a origem das chamadas?														
131	Como é feito o processo de concessão de acesso para discagem remota?														
132	Quais as formas de acesso remoto possíveis ao ambiente?														
133	São concedidos acessos remotos a prestadores de serviço?														
134	Como são feitas as alterações nas regras do firewall? Quem possui esse privilégio hoje?														
135	Existem restrições quanto a conexão de equipamentos na rede														
136	Existem conexões de outras empresas no ambiente? Quais? Qual o tipo de Conexão?														

M.	Internet e correio eletrônico															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
137	Como é processo de concessão de acesso à Internet?														
138	Os funcionários podem acessar suas contas de "email" existentes em "sites" da Internet ("webmail")?														
139	Os funcionários estão autorizados a realizar "downloads" de arquivos da Internet em suas máquinas?														
140	Existem modens instalados nas estações de trabalho dos usuários?														
141	É possível realizar conexão via "dial-up"?														
142	Como é feito o controle sob a instalação de "modems" nas estações de trabalho?														
143	Existe uma política definida para uso do e-mail e da Internet? Os usuários têm conhecimento dessa política?														
144	Os e-mails pessoais dos funcionários podem ser abertos pela Área de Segurança? Os funcionários estão conscientes dessa possibilidade?														
145	As mensagens enviadas e recebidas são monitoradas?														
146	Existem restrições quanto ao conteúdo e tamanho das mensagens enviadas e recebidas?														

M.	Internet e correio eletrônico															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
147	A política de utilização da Internet (se existir) controla o acesso a "sites" com conteúdos específicos ("sites" pornográficos, "hackers", drogas, etc) que possam causar danos legais / imagem à empresa?														
148	A rede interna da empresa é protegida por um firewall?														

N.	Plano de contingência e continuidade de negócios																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
149	A empresa possui um plano de contingência formalizado?														
150	No momento da elaboração do plano de contingência foram identificados quais recursos tecnológicos possuíam maior criticidade para a empresa?														
151	O plano de contingência é testado periodicamente?														
152	Foi designado um responsável, ou responsáveis, pelo plano de contingência?														
153	Como são feitas as atualizações no plano de contingência?														
154	Os envolvidos na recuperação do ambiente de tecnologia receberam treinamentos adequados?														
155	Quais os funcionários acionados em caso de problemas?														
156	Qualquer funcionário da empresa possui acesso ao plano de contingência?														
157	As medidas adotadas são documentadas?														
158	Existe contingência para os equipamentos? Foi criado um “backup site”?														
159	Existe um funcionário responsável pela definição de quais equipamentos devem possuir contingência?														

N.	Plano de contingência e continuidade de negócios															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
160	A operação da empresa já foi indisponibilizada em função da inexistência de um plano de contingência?														
161	Foram definidas as medidas prioritárias a serem tomadas caso ocorra um incidente?														
162	A configuração dos equipamentos considerados críticos para a operação da empresa está documentada?														

O.	Antivírus															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
163	Como é feita a instalação e atualização do software de antivírus na empresa?														
164	Quais controles asseguram que o antivírus não foi desinstalado ou está desabilitado?														
165	Os e-mails recebidos são verificados com relação a existência de vírus?														
166	Os incidentes de segurança ocorridos envolvendo a existência de vírus são registrados e reportados?														
167	Existe algum documento da empresa que trate sobre a introdução de disquetes e arquivos no ambiente tecnológico?														
168	Existem procedimentos definidos para remoção de vírus?														

P.	Aquisição de hardware e software															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
170	Como é feita a aquisição e distribuição de software e hardware na empresa?														
171	Os fornecedores são submetidos a um processo de aprovação?														
172	É realizado um estudo do impacto causado por novos hardware e software no sistema como um todo?														
173	Existem ferramentas para distribuição de software?														
174	Os software de sistema são testados antes de serem colocados em ambiente de produção?														
175	Quais controles asseguram a inexistência de software pirata na empresa?														
176	É permitida a utilização de softwares “shareware” e “freeware”?														
177	Existe segregação de funções para atividades como administrador da rede, administrador da base de dados, operador, analista de sistemas, desenvolvedor, dentre outros.														
178	Como são feitas as atualizações dos sistemas operacionais?														

Q.	Suporte técnico																	
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
179	Existe uma área responsável pela prestação de suporte técnico aos usuários da empresa?														
180	As solicitações de suporte técnico são documentadas?														
181	A partir dos problemas documentados são tomadas medidas pró-ativas para resolução do problema?														
182	Como são tratadas as situações em que a solução do problema não é conhecida? Elas são escaladas dentro da Área de TI?														
183	As medidas adotadas para solução dos problemas são documentadas?														
184	São gerados relatórios periódicos com os problemas que ocorreram e o tempo gasto em cada um dos problemas, e a reincidência dos mesmos?														
185	Há um acompanhamento das solicitações de suporte que não são imediatamente resolvidas?														
186	São gerados relatórios com o percentual dos problemas resolvidos?														
187	Existe identificação de chamados de suporte técnico que garantam que sua execução será realizada por pessoal autorizado?														

R.	Processamento em lote																	
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
188	Quais controles são adotados para assegurar que o arquivo de lote foi transmitido / recebido corretamente?														
189	Quais controles foram adotados para assegurar que o arquivo de lote foi processado corretamente?														
190	Os procedimentos de processamento de lote estão documentados?														
191	Quais os responsáveis pelo acompanhamento do processamento do arquivo de lote?														
192	São registrados os erros ocorridos durante o processo de transmissão e processamento dos arquivos?														
193	Os arquivos de lotes rejeitados são notificados ao operador? Neste caso quais os procedimentos para re-execução do arquivo?														

S.	Treinamento																	
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
194	Como são identificadas as necessidades de treinamento dos usuários e funcionários da área de tecnologia?														
195	A empresa possui uma estrutura interna para treinamento de pessoal? Como são fornecidos os treinamentos necessários?														
196	São fornecidos treinamentos referentes a aspectos de segurança (como por exemplo, conduta ética, práticas de segurança, falhas que afetam disponibilidade, confidencialidade e integridade)?														
197	Existe algum programa de conscientização sobre ética profissional e comportamento na organização?														
198	Já foram realizadas campanhas de conscientização?														

T.	Administração da base de dados															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
199	A responsabilidade pela segurança do banco de dados foi designada a algum funcionário?														
200	Existem ambientes segregados para realização de testes com a base de dados?														
201	Existem ferramentas instaladas no ambiente de tecnologia que possibilitam o acesso direto ao banco de dados?														
202	As senhas das contas padrão criadas pela fabricante foram alteradas?														
203	Existem senhas do banco de dados armazenadas em “scripts”, códigos fontes ou em outro formato qualquer?														
204	Quantos usuários possuem conhecimento da senha de administração do banco de dados?														
205	Os acessos concedidos ao banco de dados são revisados periodicamente?														
206	As tarefas de manutenção do banco de dados executadas pelo DBA são realizadas com contas que possuem perfis diferenciados?														
207	São criadas contas únicas e individuais para os usuários do banco de dados?														

T.	Administração da base de dados															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
208	Existe um padrão para convenção dos "logins" criados no banco de dados?														
209	Existe alguma política de contas e senhas adotada para o banco de dados?														
210	Existem prestadores de serviço com acesso a base de dados?														
211	As bases de dados da organização podem ser acessadas remotamente?														
212	A trilha de auditoria do banco de dados está habilitada?														
213	As contas criadas no banco de dados pelos próprios fornecedores foram removidas após implementação?														
214	Como é calculado o espaço necessário para o banco de dados?														
215	As alterações realizadas pelo banco de dados são registradas em “logs”?														
216	Como é feita a criptografia de acesso ao banco de dados? Existe uma política de troca das chaves criptográficas?														
217	Quando do cálculo de tamanho necessário? São consideradas futuras inclusões ou modificações que criem maior necessidade de espaço?														

V.	Concessão de acesso																	
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
218	Como é o processo para concessão de acesso à rede para os funcionários da empresa?														
219	Como é o processo para concessão de acesso à rede para os prestadores de serviço?														
220	As solicitações de acesso são documentadas, possibilitando a verificação periódica?														
221	Todos os usuários possuem ID's únicos? Existem usuários genéricos?														
222	Como é o processo para remoção dos usuários em cada plataforma, em casos de transferências ou desligamentos?														
223	Os usuários "default" criados no momento da instalação foram mantidos?														
224	Existem controles que permitam a identificação de contas inativas?														
225	Os perfis de acesso concedidos aos usuários são revisados periodicamente?														
226	Todas as contas do sistema solicitam a utilização de senhas?														
227	Como são criadas e fornecidas as senhas de acesso?														

V.	Concessão de acesso																
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
228	Existe uma política pré-definida para as contas e senhas? (Esta política deve estipular por exemplo o tamanho mínimo da senha, período para expiração das senhas, caracteres que a compõem, etc.)														
229	São armazenadas senhas em arquivos digitais em formato "clear-text" ou em documentos impressos?														
230	São exibidas mensagens de advertência no momento do “login” para dissuadir o acesso não autorizado ao ambiente?														
231	São exibidas mensagens informando a data e hora do último “logon” do usuário?														
232	O acesso do usuário é bloqueado após inúmeras tentativas de acesso utilizando uma senha inválida?														
233	Existem restrições com relação a realização de “logins” simultâneos pelo mesmo usuário?														
234	Existem restrições com relação ao dia/semana em que os usuários podem realizar “logon”?														
235	As estações de trabalho ativam o protetor de tela com senha após um período de inatividade?														

V.	Concessão de acesso															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
236	A utilização de "logins" com perfis privilegiados são monitorados e registrados?														
237	Quantas pessoas têm conhecimento da senha do usuário de administração das plataformas existentes?														
238	As senhas dos "logins" privilegiados são trocadas após sua utilização?														
239	Os administradores das plataformas utilizam um "login" distinto do "login" de administrador para execução das suas atividades rotineiras?														
240	Os funcionários assinam um termo de confidencialidade/responsabilidade no momento da contratação?														
241	Existem situações em que a senha é fornecida a outros funcionários?														
242	As mensagens de erro exibidas no momento do "login" informam ao usuário onde está o problema?														
243	Existe segregação de funções entre o funcionário que concede o acesso e o funcionário que criará efetivamente os usuários nos sistemas?														
244	Como é o processo para remoção de um usuário da rede?														
245	Existem controles/políticas que garantam que os usuários não fornecerão suas senhas de acesso a terceiros sem prévia autorização?														

V.	Concessão de acesso															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
246	Como é feito o monitoramento das plataformas?														
247	A gravação da trilha de auditoria dos sistemas está habilitada?														
248	Qual a periodicidade em que os arquivos de "log" são removidos ou sobrescritos?														

X.	Gerenciamento de Segurança															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
249	Como é feito o planejamento de longo e curto prazo para as atividades da área de segurança e tecnologia?														
250	Os planejamentos são acompanhados ao longo do ano?														
251	Todos os funcionários da empresa estão cientes dos seus papéis e responsabilidades em relação aos sistemas de informação, controle interno e segurança?														
252	Existem situações em que um único indivíduo seja responsável ou controle todas as etapas de uma atividade crítica? Há segregação de funções dentro da empresa?														
253	Todos os ativos de informação possuem um proprietário, responsável pela sua classificação e seus direitos de acesso?														
254	A área TI/segurança da informação possui um quadro de funcionários adequado para as funções que necessita desempenhar?														
255	Como é feito o planejamento de pessoal para as áreas de TI e segurança da informação?														

X.	Gerenciamento de Segurança															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
256	Existem procedimentos e políticas definidos para controlar as atividades dos terceiros na área de IT/segurança da informação a fim de assegurar a proteção dos ativos de informação da organização?														
257	Qual área é responsável por definir ações disciplinares e punições para casos em que a política de segurança não seja cumprida?														

Z.	Monitoramento do ambiente (avaliação de log)															
#	Tópico Avaliado	Processo estabelecido, nenhuma vulnerabilidade identificada	Nenhuma vulnerabilidade conhecida ou suspeita	Suspeita de vulnerabilidades significativas	Existência de vulnerabilidades significativas	Informações insuficientes para a análise	Risco de perda financeira			Risco de perda de produtividade			Risco de perda de confiança do consumidor		
							A	M	B	A	M	B	A	M	B
258	Os logs dos servidores críticos estão ativos?														
259	Os logs dos bancos de dados críticos estão ativos?														
260	Os logs são armazenados adequadamente?														
261	O acesso ao diretório onde estão armazenados os logs é restrito?														
262	Os privilégios de acesso a tais diretórios são apenas de leitura?														
263	Como é controlada a acuracidade da data/hora das trilhas de auditoria?														
264	A integridade dos arquivos de logs é periodicamente checada?														
265	Foi definida junto a área de negócio o período de geração e armazenamento dos logs?														
266	O período de substituição dos logs está adequadamente configurado?														
267	A responsabilidade pela avaliação dos logs está formalmente atribuída?														
268	Está definida a periodicidade de preservação dos logs?														