INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia associada à Universidade de São Paulo

ANÁLISE DE RISCO PARA INVESTIMENTO DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

NELSON NOVAES NETO

São Paulo
2005

INSTITUTO DE PESQUISAS ENERGÉTICAS E NUCLEARES
Autarquia associada à Universidade de São Paulo

ANÁLISE DE RISCO PARA INVESTIMENTO DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

NELSON NOVAES NETO

Monografia apresentada como parte dos requisitos para obtenção do certificado de conclusão do Curso de Especialização em **Gestão da Segurança da Informação**

Orientador:
Celso Hamilton Leite

São Paulo
2005

Banca examinadora:

_____

_____

_____

Aos meus pais, à minha irmã e aos meus avós.

ANÁLISE DE RISCO PARA INVESTIMENTO DE SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

Nelson Novaes Neto

RESUMO

Neste trabalho, foi desenvolvido um modelo de análise de risco, destinado aos profissionais da área de Tecnologia da Informação, com o objetivo de auxiliar o processo de investimento em segurança e garantir a implementação das melhores práticas de segurança, com o menor custo para o negócio. Essas medidas visam à proteção dos ativos e à mitigação dos riscos, sejam elas a aquisição de ferramentas ou a implementação de processos, sem deixar de observar as recomendações nacionais e internacionais, bem como a norma NBR ISO/IEC 17799 que cobre vários tópicos da área de segurança da informação e possui um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações. Por meio de uma metodologia, procura-se introduzir o profissional de tecnologia da informação na dinâmica dos riscos e orientar a preparação e formação de um time que conduza à identificação dos principais ativos da organização. Uma vez conhecidos os ativos da organização, uma análise de ameaças e vulnerabilidades é executada, por meio do mapeamento de arquitetura e decomposição dos aplicativos. Com os resultados dessa análise, uma matriz de risco é desenvolvida para estabelecer os níveis de severidade, criticidade, impacto e controles existentes e necessários. Posteriormente, as informações fornecidas pela matriz de risco servirão de fonte para a seleção das medidas de segurança que indicam as proteções efetivas para os riscos e o desenvolvimento de um relatório para o setor estratégico da organização.

RISK ANALYSES FOR SECURITY INVESTMENT IN INFORMATION TECHNOLOGY

Nelson Novaes Neto

ABSTRACT

In this work was developed a risk analysis model, destined to Information Technology professionals, aimed to help in security investment process and to guarantee the implementation of best security practices with low costs for the company/business. These measures intents are to protect the asset, and don't matter if it's by tools acquisitions or by process implementation, observing the national and international recommendations, as well as NBR ISO/IEC 17799 pattern, which covers many topics of Information Security area and has a large number of controls and requirements that must be attended in order to guarantee the information security. By using a methodology, we can try to introduce the information technology on the risks dynamic, which helps in preparing and building up a team that guide the identification of the organization main assets. Once we know the organization assets, we start an analyze of vulnerabilities and threats, by mapping architecture and decomposing the applications. With this analyze results, a risk matrix is developed in order to establish the severity, criticism, impact and control levels existing and needed. At last, the information given by the risk matrix will be used as font to select security measures that bring the effective protection to the risks and the development of a report to the strategy organization department.

SUMÁRIO

Página

Lista de Figuras

Página

Lista de Tabelas

Página

1. INTRODUÇÃO

O setor da Tecnologia da Informação é gerido por processos cíclicos de investimentos, mudanças, processos, desenvolvimento de novos ativos para a organização. Esse setor depende de um alinhamento estratégico com os principais objetivos da organização, deve acompanhar as tendências mercadológicas e precisa estar preparado para garantir a competitividade, a qualidade, a segurança, o diferencial de mercado e a continuidade nos negócios.

Para alcançar e manter esses objetivos, os processos cíclicos devem suportar novas tecnologias, processos, desenvolvimento, requisitos legais, normativos e controles que forneçam a proteção ideal para os ativos, que são classificados como algo de valor para a organização.

O desenvolvimento de novos ativos ou as mudanças na organização podem difundir novas vulnerabilidades que favoreçam a concretização de ameaças novas ou já conhecidas, podendo, conseqüentemente, ocasionar um impacto e um possível dano potencial aos negócios da organização.

Conhecer os pontos de vulnerabilidade e identificar a proteção ideal para os ativos da organização é um bem necessário para garantir competitividade e continuidade, pois quanto mais entendemos das origens, ameaças, vulnerabilidades, ativos, impactos e medidas de seguranças, maiores são as chances de controlar o fator de exposição e risco, podendo minimizar o impacto caso uma ameaça seja concretizada. Não assumir e não tratar o risco de forma consciente, de acordo com a estratégia de negócio, é o maior risco que existe.

Conhecer e gerir um processo de análise de risco corretamente é o melhor caminho para identificar os principais ativos, as vulnerabilidades e ameaças existentes e recomendar os controles para fornecer a proteção ideal aos ativos da organização.

O processo de análise de risco pode ser utilizado para auxiliar nos investimentos de segurança da informação, pois a correta identificação das fragilidades existentes permite determinar o balanceamento dos investimentos em medidas de segurança. Nessas medidas, os controles devem garantir a preservação de confidencialidade, integridade e disponibilidade e o investimento tem de estar alinhado com os objetivos de negócio e o valor do ativo para a

organização, seja ele tangível ou intangível. Assim, o processo de análise de risco é um investimento benéfico, atual e futuro que favorece a todos.

2. OBJETIVO

Demonstrar a importância e os benefícios de um processo de análise de risco, bem como seu conceito e uma metodologia para auxiliar no desenvolvimento de um processo que defina o correto investimento em controles de segurança para o setor de tecnologia da informação.

3. REVISÃO BIBLIOGRÁFICA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001. (NBR ISO/IEC 17799). Demonstra a importância de implementar os requisitos de segurança necessários em uma organização, pois a confidencialidade, integridade e disponibilidade da informação podem ser essenciais para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização. Esses requisitos podem ser estabelecidos por meio da legislação vigente, objetivos e requisitos para o processamento da informação e avaliação de risco nos ativos da organização. É explícito que os requisitos de segurança são identificados mediante uma avaliação sistemática dos riscos de segurança, em que são identificadas as ameaças aos ativos, as vulnerabilidades e sua probabilidade de ocorrência e impacto potencial estimado. Com base nos resultados da avaliação, os gastos com controles para a mitigação dos riscos devem ser balanceados de acordo com os danos ocasionados pelas potenciais falhas de segurança. Não é objetivo da NBR ISO/IEC 17799, 2001, apresentar um modelo de análise de risco.

BRASILIANO, ANTONIO CELSO RIBEIRO. Manual de análise de risco para a segurança empresarial. São Paulo: Sicurezza, 2003. Define uma ameaça ou risco como um evento capaz de produzir perdas reais e mensuráveis por um padrão comum, classifica-os como especulativos ou dinâmicos e riscos puros ou estáticos. Riscos especulativos podem apresentar probabilidade de ganho ou perda e o risco puro envolve somente a chance de perda. Caracteriza os riscos como humanos, técnicos e incontroláveis. O processo de análise de risco é determinado por uma metodologia própria e define que a identificação dos riscos, sua origem, é necessária para a eficácia no tipo de tratamento e proteção que será atribuído ao ativo. Demonstra que o processo de análise de risco pode pertencer a duas categorias: métodos objetivos e métodos subjetivos, porém declara que o método subjetivo tende a ser mais difundido no decorrer do tempo. Quando existe um histórico consistente de eventos ocorridos, recomenda-se utilizar o método objetivo; com a ausência dos eventos devem-se estabelecer critérios para determinar o grau de criticidade de cada risco. Uma matriz de impactos cruzados é utilizada para verificar a interdependência entre todos os

riscos, verificando como a ocorrência ou não de um risco pode aumentar ou diminuir a probabilidade de outro risco, e uma matriz de monitoramento, que tem como objetivo acompanhar a mitigação ou elevação dos riscos.

BRASILIANO, ANTONIO CELSO RIBEIRO. Manual de planejamento. Gestão de riscos corporativos. São Paulo: Sicurezza, 2003. Descreve o processo de gestão de riscos corporativos que é contemplado como parte de um planejamento estratégico empresarial. O principal objetivo é levantar os riscos corporativos na área legal e de operação para reduzir as ameaças que podem impactar nas metas definidas pela corporação. O plano estratégico em gestão de riscos é elaborado seguindo uma metodologia própria denominada Método Brasiliano, que é uma adaptação do Método Grumbach desenvolvido pelo brasileiro Raul Grumbach, idealizado para ser aplicado em planejamento estratégico. O Método Brasiliano mensura todo e qualquer risco e realiza a respectiva análise do investimento, visando mitigar os próprios prejuízos. A conclusão das 11 fases do método gera automaticamente um plano de gerenciamento de riscos corporativos. O processo de análise de risco é dividido entre duas categorias: métodos objetivos e subjetivos. Recomenda-se o uso do método objetivo quando a empresa possui histórico consistente de eventos ocorridos para determinar estatísticas, probabilidades e médias que possam ser úteis para embasar o plano diretor de gestão de riscos corporativos. São apresentados diversos métodos para o cálculo de probabilidade, média aritmética, desvio-padrão, coeficiente de variação, eventos independentes. Quando não existem dados consistentes, a metodologia utilizada é a subjetiva, em que os cálculos seguem critérios preestabelecidos, com uma escala de valor, na qual uma equipe disciplinar poderá arbitrar e avaliar o grau de criticidade de cada risco da empresa. Para o método subjetivo são apresentados o Método de Mosler, que serve de base para a identificação, análise e evolução dos fatores que podem influir na manifestação e concretização da ameaça, projetando qual será o impacto de concretização pela classe e dimensão de cada risco, e o Método de Willian T. Fine, que tem como objetivo estabelecer prioridade, integrando grau de risco com a limitação econômica.

CARUSO, CARLOS A. A. Segurança em informática e de informações. São Paulo: Senac, 1999. Sistematiza uma metodologia de análise de risco

simples para auxiliar na decisão de investimentos de segurança: análise dos riscos e suas conseqüências; estimativa das probabilidades de ocorrência; estimativa do dano causado pela ocorrência do incidente; cálculo de exposição, em que a exposição é proporcional à vulnerabilidade ou dano financeiro; probabilidade de ocorrência em vezes ao ano e correlação dos resultados para determinar as medidas de proteção aos ativos. É definido que o ativo de informação deve ser protegido como qualquer ativo tangível e que o ativo de informação é composto de três fatores de produção: capital, mão-de-obra e processo. Os processos de análise de risco recebem uma crítica quanto ao grau de subjetividade que o ativo avaliado apresenta para o proprietário do mesmo, porém determinam que a avaliação do ativo deve ser conduzida pelo responsável e assessorada por um especialista de segurança, e, mesmo apresentando subjetividade excessiva, o processo não altera o fato de que existem riscos e que os mesmos devem ser avaliados.

GREY, STEPHEN. Risk analysis for IT projects. England: Wiley, 1995. Descreve a importância do processo de análise de risco para minimizar os impactos no gerenciamento de projetos, nos quais os principais riscos estão associados ao correto gerenciamento dos gastos, ao cumprimento dos prazos de desenvolvimento e entrega do projeto e à abrangência e previsão de novos recursos ou atividades no decorrer e futuro do projeto. A metodologia para análise de risco no gerenciamento de projetos é definida como quantitativa, pois justifica que é a única capaz de gerenciar corretamente o processo de tempo, prioridades, agregação de decisões e suporte para a correta tomada de decisão. Esse processo de análise de risco só pode ser executado com o histórico de planos existentes, levantamento de custo e tempo em projetos anteriores. Com base nesse histórico é utilizada a ferramenta @RISK que provê capacidade de determinar o custo necessário, tempo, rendimento e outros modelos de risco para obter a melhor tomada de decisão com o menor risco para o projeto.

PELTIER, THOMAS R. Information security analysis. United States of America: Auerbach, 2001. Estabelece um processo de análise de risco denominado Facilitated Risk Analysis Process (FRAP), com objetividade, simplicidade e estabelecendo quatro passos para auxiliar as unidades de negócio no desenvolvimento de um processo de análise de risco. O risco é denominado

por alguém ou algo de qualquer natureza que produz ou induz fraquezas nos ativos da organização. É definido que a análise de risco é essencial para a sobrevivência, competitividade e aplicação de controles sobre as ameaças e vulnerabilidades. Determina que o processo de análise de risco deve ser efetuado quando envolver uso de dinheiro, recursos ou no início de uma tarefa, projeto ou desenvolvimento. A metodologia FRAP foi desenvolvida para simplificar e trazer vantagens sobre qualquer modelo de análise de risco interno. O método é subjetivo, qualitativo e determina que o valor do ativo, controles e análise de vulnerabilidades devem ser obtidos com foco nas propriedades de integridade, confidencialidade e disponibilidade. Os quatro passos que constituem o processo são: seleção de um time responsável pela identificação e principais riscos para a organização; levantamento das ameaças e priorização das vulnerabilidades e questionários e matriz de prioridade; atribuição de controles para proteção e mitigação dos riscos; correlação entre controles, riscos e relatório executivo.

ROPER, CARL A. Risk management for security professionals. Burlington, MA: Butterworth Heinemann, 1999. Apresenta uma metodologia de gerenciamento de análise de risco, com base no processo desenvolvido pelo Risk Management Training Working Group (RMTWG) do U.S. Security Policy, para os profissionais de segurança. Aponta o gerenciamento de risco como o melhor e mais importante processo para determinar a proteção adequada para os principais ativos com um custo aceitável. O processo contém cinco fases seqüenciais que estabelecem os principais ativos que necessitam de proteção, identificação das ameaças, identificação das vulnerabilidades, análise de risco para determinar as prioridades, controles e probabilidade de exploração ocasionada pelas ameaças, seleção dos principais controles para redução das vulnerabilidades, ganho de eficiência, análise de custo/benefício e priorização das recomendações para estabelecer uma eficiente tomada de decisão. A metodologia de análise de risco é definida como um processo que identifica e avalia as ameaças e vulnerabilidades para um ativo apontando a probabilidade de perda, dano e impacto ocasionado pela exploração das vulnerabilidades. É explícita a grande preocupação e importância de um tratamento ideal para os adversários de negócio que podem conduzir atividades e impactar nos ativos da organização, que pode possuir um valor diferenciado para esse adversários. O ativo é definido como qualquer pessoa, material, informação ou atividade que

agregam valor positivo para os proprietários do negócio. A vulnerabilidade é caracterizada por qualquer fraqueza que pode ser explorada por um adversário que deseje obter acesso a um ativo. As ameaças são definidas por qualquer indicação, circunstância ou evento com potencial para causar perda ou dano nos ativos da organização. A classificação das ameaças e vulnerabilidades é conjugada como: Crítica, que indica que a ameaça pode atingir o ativo e um adversário pode obter acesso ao mesmo; Alta, que indica uma credibilidade existente que permite o acesso ao ativo por determinados adversários conhecidos; Média, que indica a existência de uma ameaça potencial e possibilita que um adversário obtenha acesso reduzido a um ativo; Baixa, que indica uma pequena ou nenhuma evidência de acesso ao ativo. O modelo para o processo de análise de risco é subjetivo e qualitativo de acordo com critérios preestabelecidos e informações obtidas por histórico e centros de inteligência como: Agência Central de Inteligência e Departamento de Defesa (CIA/DoD) dos EUA.

SÊMOLA, MARCOS. Gestão da segurança da informação, uma visão executiva. Rio de Janeiro: Campus, 2002. Apresenta de forma superficial e estratégica a análise de risco, sem apontar uma metodologia. Demonstra que o fator crítico de sucesso para o processo é mapear os relacionamentos dos processos com os ativos de informação. Define que um ativo é todo elemento que compõe os processos que manipulam e processam a informação, a própria informação ou qualquer meio que armazene, transporte, descarte ou manuseie. Trata as ameaças como agentes ou condições que exploram vulnerabilidades provocando perda de confidencialidade, integridade e disponibilidade e classifica-as como naturais, involuntárias e voluntárias. A vulnerabilidade é caracterizada por uma fragilidade presente nos ativos, que explorada por ameaças, agentes externos, afeta negativamente a confidencialidade, integridade e disponibilidade. Os controles de segurança são procedimentos ou mecanismos usados para a proteção dos ativos com a característica de prevenção, detecção ou correção e com o objetivo de minimizar o risco e limitar o impacto indesejável. O risco é definido pela probabilidade das ameaças que exploram as vulnerabilidades ocasionando impactos aos negócios e interpreta o risco como proporcional à vulnerabilidade, ameaça e impacto, e inversamente proporcional às medidas de segurança.

4. METODOLOGIA

4.1. A importância da análise de risco

Alcançar os objetivos de uma organização pode ser um trabalho árduo para aqueles que não conhecem a dinâmica dos riscos e não acreditam na existência dos mesmos, pois torna-se evidente que o maior risco é o desconhecimento e a certeza de que o risco não existe.

Classificando o risco como um evento inerente a qualquer natureza humana, que está associado às leis da probabilidade e que possui o potencial de ocasionar danos aos ativos, resultando em perdas tangíveis e intangíveis, podemos concluir que conhecer a dinâmica dos riscos, suas conseqüências, impactos e também as causas da sua concretização é um fator de importância para atingir e proteger os objetivos da organização. Determinar o risco, avaliá-lo devidamente e principalmente bem administrá-lo podem ensejar decisões cautelares apropriadas e, conseqüentemente, traduzir-se em efeitos positivos para a organização[2].

O processo de gerenciamento de risco é definido como o melhor método ou modelo para determinar o investimento ideal em controles e benefícios para garantir que o risco permaneça em um nível aceitável. Saber identificar os ativos, analisar as probabilidades, avaliar o risco e determinar o tratamento ideal é o melhor e mais importante caminho para manter a competitividade e sobrevivência da organização.

4.2. Análise de risco

A análise de risco está integrada ao processo de gerenciamento de risco, que é considerado um processo cíclico voltado à proteção dos investimentos, ativos e interesses da organização e deve ser agregado às áreas de negócio e estratégicas da organização, podendo ser expandido por todas as áreas, pois é classificado como um investimento necessário e que favorece a todos.

Conceitualmente a análise de risco é definida como um conjunto de atividades para identificar os principais ativos de uma organização, vulnerabilidades e ameaças, riscos e impactos; priorizar as vulnerabilidades e selecionar os controles de segurança. Esse processo é responsável pela correta recomendação dos controles de segurança e monitoramento para garantir a preservação da confidencialidade, integridade e disponibilidade e minimizar o risco e impacto nos ativos e negócios da organização.

A análise de risco é essencial para a tomada de decisão em qualquer organização, deve ser um processo contínuo e executado em qualquer tipo de mudança, sempre relacionado direta ou indiretamente com os ativos, principalmente quando envolver investimento ou alteração estratégica na organização. Pode ser utilizada para classificar o nível de proteção atual e identificar os controles existentes. De preferência, a análise de risco deve recomendar os controles de segurança no estágio de projeto e na especificação dos requisitos, pois os controles são considerados mais baratos e eficientes. Ela deve ser utilizada para tratar e reduzir o risco a um nível aceitável, pois no geral não existe risco “zero”.

Tendo em vista que o fator tempo faz parte da estratégia de novos negócios em uma organização, principalmente no setor de tecnologia da informação, o processo de análise de risco deve ser adaptado ao escopo do projeto. O escopo define os componentes de negócios a serem analisados, a relevância de cada ativo que presta suporte ao negócio, as funções de controles, e deve ser claramente definido quanto a sua finalidade, responsabilidade e abrangência. Esse processo deve ser conduzido por especialistas internos ou consultoria e por aqueles que conhecem, desenvolvem e utilizam as aplicações e sistemas. Um relatório deve apresentar detalhadamente os resultados e as recomendações de controles para a mitigação dos riscos, sendo classificado

como confidencial e disponibilizado somente para os gerentes e os envolvidos no processo de decisão[9].

A análise de risco habilita a organização a manter o foco nos objetivos da segurança da informação e na qualidade para implementação de um efetivo processo de qualidade em segurança, assim assegurando uma arquitetura de soluções para um adequado gerenciamento dos riscos. Essa arquitetura deve dar suporte às políticas de segurança da informação, classificação de informações, normas e requisitos legais.

A organização deve implementar nove objetivos que são suportados pelos princípios de gerenciamento de risco, figura 1:

1. Manter a confiança do cliente na organização;
2. Proteger a confidencialidade para informações sensíveis;
3. Proteger a sensibilidade dos dados de operação contra divulgações não apropriadas;
4. Evitar atos ilegais ou maliciosos nos sistemas da organização;
5. Assegurar que os recursos computacionais estejam bem empregados;
6. Evitar fraudes;
7. Evitar gastos elevados com incidentes;
8. Estar de acordo com a legislação vigente e normas;
9. Evitar um ambiente de trabalho hostil.

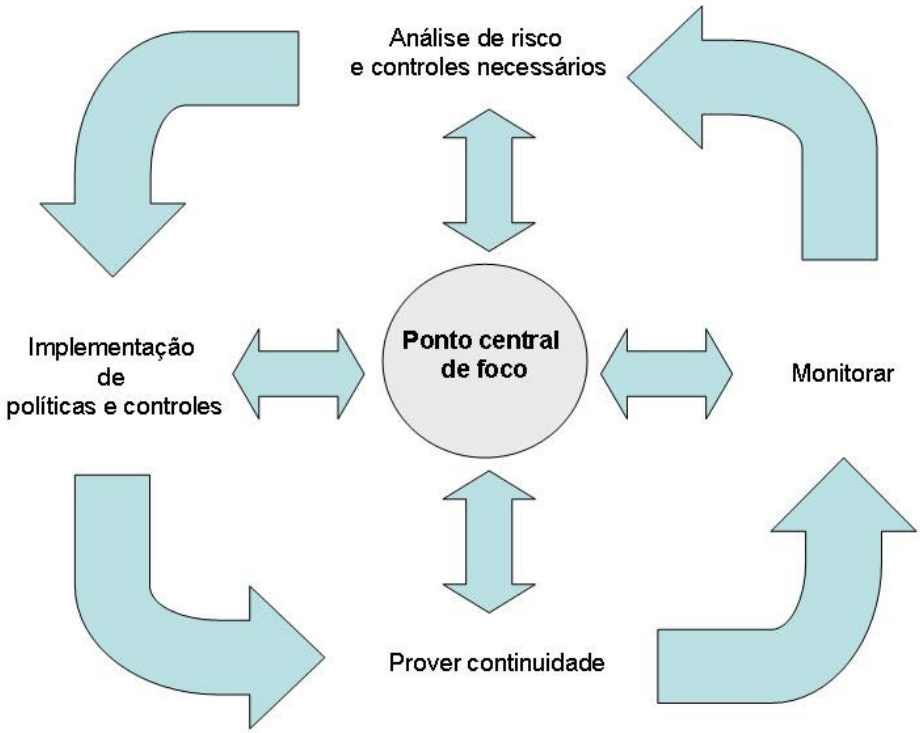

Figura 1. – Princípio de gerenciamento de risco.

Fonte: *EUA Governemment Accounting Office / AIMD – 98-68 – Information Security Management.*

Existem diversos modelos para o processo de análise de risco, automatizados ou não. Cada organização deve selecionar, estabelecer ou criar sua própria metodologia para análise de risco de acordo com seus objetivos, cultura e negócio. Independente do estilo definido, existem duas categorias para a análise de risco: quantitativa ou qualitativa[10].

Análise de risco quantitativa

O objetivo da análise de risco quantitativa é calcular valores numéricos objetivos para cada um dos componentes coletados durante as fases de análise de custo/benefício e de avaliação de risco. Pode-se estimar o valor por meio do histórico consistente de eventos ocorridos, utilizando números dos eventos, valores monetários, custo de substituição, perda de produtividade, freqüência etc. Todos os passos do processo de análise de risco devem ser calculados com a mesma objetividade. Existem alguns pontos fracos que podem dificultar e tornar esse processo extremamente caro. O fato de não haver um método formal e rigoroso de calcular efetivamente o valor dos ativos e controles faz com que os valores financeiros encubram o fato de que os números são baseados em estimativas. Nesse caso, não é possível calcular com precisão o impacto de um incidente em ativos intangíveis, como a marca comercial e imagem da organização.

Um clássico algoritmo utilizado para determinar o valor quantitativo do impacto é a formula de Exposição de Perda Anual (ALE, *Annualized Loss Expectancy),* que é o resultado da Expectativa de Perda Única(SLE, Single Loss Expectancy), multiplicado pela Taxa de Ocorrência Anual(ARO, *Annualized Rate Occurance*)[9].

Exposição de Perda Anual = Expectativa de Perda Única x Taxa de Ocorrência Anual

O valor da Expectativa de Perda Única é calculado pela perda monetária, impacto, da ocorrência de cada ameaça, que é obtida pela multiplicação do Valor do Ativo pelo Fator de Exposição.

Expectativa de Perda Única = Valor do Ativo x Fator de Exposição

O Valor de Exposição é representado pela magnitude da perda ou impacto no valor de um ativo. Esse valor é de 0 a 100%.

O ARO é caracterizado pela freqüência de uma ameaça ser concretizar, em que o valor pode ser obtido pela tabela multiplicadora de perda anual, tabela 1.

Tabela 1. – Tabela multiplicadora de perda anual.

Tabela multiplicadora de perda anual		
Nunca		0,0
Uma vez em 300 anos	1/300	0,00333
Uma vez em 200 anos	1/200	0,005
Uma vez em 100 anos	1/100	0,01
Uma vez em 50 anos	1/50	0,02
Uma vez em 25 anos	1/25	0,04
Uma vez em 5 anos	1/5	0,20
Uma vez em 2 anos	½	0,50
Anualmente	1/1	1,0
Duas vezes ao ano	1/0,5	2,0
Uma vez ao mês	12/1	12,0
Uma vez por semana	52/1	52,0
Diariamente	365/1	365,0

Por meio do resultado de ALE, as organizações podem utilizar esse parâmetro para determinar o valor do prêmio que deverá ser investido para minimizar o fator de exposição e taxa de ocorrência anual.

Por exemplo, observando o risco de um incêndio: Assumindo que o valor do ativo é de R$1.000.000,00, o fator de exposição é de 50% e a taxa de ocorrência anual é de uma vez a cada dez anos, 1/10.:

Exposição de Perda Anual = (1.000.000,00 x 50% = 500.000,00) x 1/10 = R$50.000,00.

Com base em uma análise de custo x beneficio convencional, a organização poderia justificar o investimento de R$50.000,00 por ano para prevenir a ocorrência ou reduzir o impacto de um incêndio.

Exemplo de análise quantitativa:

- Valor geral do ativo para a organização é calculado ou estimado em termos financeiros diretos:

  - ✓ Portal de internet, com atividade 24 horas por dia, sete dias por semana.
  - ✓ Gera uma receita média de R$ 50.000,00 por dia na venda de publicidade on-line.
  - ✓ Valor anual do site em termos de receita de vendas é R$ 18.250.000,00.

- Impacto financeiro imediato da perda do ativo:

  - ✓ Para uma indisponibilidade de 4 horas a exposição é de 0,000456 hora por ano.
  - ✓ Perda direta de R$ 8.333,00 por ano.*

  * O cálculo de perda de receita é complexo para obter precisão e identificar todos os tipos de perda possíveis.

- Impacto indireto nos negócios causado pela perda do ativo:

  - ✓ Gasto estimado em publicidade para contrabalançar a publicidade negativa de um incidente: R$ 15.000,00.
  - ✓ Estimativa de perda de 1 por cento das vendas anuais: R$ 18.250,00.
  - ✓ Despesa extra de publicidade + perda anual da receita de vendas. Total de R$ 33.250,00 em perdas indiretas por ano.

- Perda direta + indireta = R$ 41.583,00 anual.

- Taxa de ocorrência anual do incidente: 1 vez a cada 2 anos = 0,50.

- Expectativa de perda anual: R$ 41.583,00 x 0,50 = R$ 20.791,50.

- Custo para o estabelecimento de controles ou salvaguardas para impedir esse tipo de dado: R$ 20.791,50 ou menos por ano.

Os dados calculados são baseados em estimativas subjetivas. Os principais valores que servem de base para os resultados não resultam de equações objetivas ou conjuntos de dados estatísticos bem definidos, e sim de opinião dos responsáveis pela avaliação.

Análise de risco qualitativa

O objetivo da análise de risco qualitativa é calcular mediante critérios preestabelecidos, modelo subjetivo, com uma escala de valor em que uma equipe multidisciplinar poderá arbitrar determinando graus de criticidade. Esse modelo é simples e não demanda histórico ou valores, freqüências de ameaças etc., não requer conhecimento específico e provê flexibilidade no processo e relatório. Em contrapartida, é um processo subjetivo e pode ser influenciado pelo time selecionado ao processo. O modelo qualitativo é recomendado para avaliar os ativos que são classificados como intangíveis, quando não é possível determinar com precisão o valor dos ativos e impactos e quando não existe histórico de eventos e métricas.

As vantagens e disvantagens de cada tipo de análise pode ser observado na tabela abaixo:

Tabela 2. – Benefícios e desvantagens das análises quantitativa e qualitativa[8].

	Quantitativa	**Qualitativa**
Benefícios	– Os riscos são priorizados de acordo com o impacto financeiro; os ativos são priorizados de acordo com valores financeiros. – Os resultados podem ser expressos usando uma terminologia de gerenciamento (por exemplo, valores monetários e probabilidade expressos como uma porcentagem específica). – A precisão tende a aumentar com o passar do tempo à medida que a organização coleta registros históricos dos dados e ganha experiência.	– Permite a visibilidade e a compreensão da classificação de riscos. – Maior facilidade de chegar a um consenso. – Não é necessário quantificar a freqüência da ameaça. – Não é necessário determinar os valores financeiros dos ativos. – Maior facilidade de envolver pessoas que não sejam especialistas em segurança ou computadores.
Desvantagens	– Os valores do impacto atribuído ao risco são baseados na opinião subjetiva dos participantes. – O processo para atingir resultados confiáveis e um consenso é demorado. – Os cálculos podem ser complexos e demorados. – Os resultados são apresentados em termos monetários e podem ser difíceis de serem interpretados por pessoas sem conhecimento técnico. – O processo exige experiência e conhecimento, portanto pode ser difícil explicá-lo aos participantes.	– Riscos graves podem não ser diferenciados o suficiente. – Dificuldade de justificar o investimento na implementação de controles, pois não há valores básicos para realizar a análise de custo/benefício. – Os resultados dependem da qualidade da equipe de gerenciamento de riscos formada.

4.3. Ativos

O ativo é definido como um elemento de valor para uma organização. Esse elemento compõe os processos que manipulam e processam a informação, incluindo a própria informação, o meio em que ela é armazenada, transportada, descartada ou qualquer outro recurso que a manipule direta ou indiretamente. Mesmo que um ativo seja passível do tratamento físico-contábil, ele pode ser importante para a sobrevivência da organização [11].

O ativo é produzido por meio dos fatores de produção: capital; mão-de-obra e processos, e a junção destes constitui-se em produtos, bens e informações. Por ser considerado um elemento de valor, o ativo deve receber a proteção adequada para garantir a confidencialidade, integridade e disponibilidade e, conseqüentemente, a competitividade e continuidade nos negócios [3].

Os ativos podem ser subdivididos em quatro grandes grupos: pessoas; processos de negócio; tecnologia e infra-estrutura.

> **Pessoas:** são todas as que de maneira direta ou indireta estão envolvidas com as atividades que dizem respeito à organização.
>
> **Processos de negócio:** são definidos como uma série de atividades de negócios que consomem recursos e produzem um bem ou serviço.
>
> **Tecnologia:** constitui-se de *hardware*, *software* ou qualquer outro elemento tecnológico. É um universo criado para ganhar produtividade, mercado e aumentar lucros.
>
> **Infra-estrutura:** suporta os elementos de pessoas, processos de negócio e tecnologia. Pode ser identificada por meio de instalações da organização, estrutura física, mecânica, hidráulica, ambiente físico, instalações elétricas, telefonia, telecomunicações, entre outros.

Em uma organização, existem muitos ativos que possuem valor tangível ou intangível. O processo de análise de risco auxilia na identificação dos ativos críticos e estabelece os fatores e impactos quanto à sua relevância e severidade para a organização. O processo de identificação dos ativos é o primeiro passo no modelo de análise de risco, deve ser estabelecido por todos os envolvidos em sua execução e seguir uma metodologia definida para:

- Determinar os ativos críticos que necessitam de proteção;
- Identificar eventos indesejáveis e expectativas de impacto;
- Priorizar o valor dos ativos relacionados à perda do mesmo;
- Definir o valor de reposição, perda e mercado.

4.4. Risco

O risco é definido pela probabilidade de uma ameaça explorar uma vulnerabilidade, provocando perda de confidencialidade, integridade e/ou disponibilidade com possíveis impactos para os negócios. O risco também está relacionado às questões de severidade que definem o grau do dano causado ao ativo.

Conhecer a dinâmica dos riscos é uma questão essencial para a sobrevivência humana e dos negócios. O risco está presente na natureza humana, é inerente a qualquer atividade e pode representar dimensões e efeitos tanto negativos como positivos [3]. De acordo com a natureza humana, o risco é classificado e resulta em dimensões e efeitos negativos. A diminuição eficaz da sua probabilidade é obtida com o estudo e a compreensão do surgimento do risco, pois todo risco possui uma origem.

Definido como um evento capaz de produzir perdas reais e mensuráveis por um padrão comum, as organizações devem estabelecer métricas para mensurar as perdas reais que podem ser valores financeiros como o desgaste da imagem da empresa.

Os riscos, quando classificados como negativos, representam somente a chance de perda e nenhuma possibilidade de ganho ou lucro. As perdas diretas e indiretas resultantes da materialização dos riscos podem ser agrupadas em:

- Perdas decorrentes de morte, invalidez e desligamento de empregados;
- Perdas por danos à propriedade e aos bens;
- Perdas decorrentes de fraudes e atos criminosos;
- Responsabilidade legal;
- Prestação de serviço ou qualidade do produto;
- Acidentes em geral;
- Catástrofes naturais;
- Colapso estrutural nas instalações físicas.

O risco representa a possibilidade de um acontecimento incerto, fortuito e de conseqüências negativas ou danosas. Em qualquer circunstância, a organização deve evitá-lo ou estar pronta para reduzir as perdas que ele produzirá, se concretizado. A fim de obter a clareza de todos os tipos de eventos negativos, é necessário averiguar as condições, as circunstâncias, as atividades, as relações e os objetos que possam colaborar para a sua ocorrência e concretização. Como o risco sempre existe, os controles e medidas de segurança são os responsáveis por determinar se o risco será de alto ou baixo impacto.

Os riscos podem ser classificados em três categorias:

Riscos humanos: são aqueles provenientes da ação direta, voluntária ou involuntária das pessoas, que podem ser internas ou externas do ambiente da empresa.

Riscos técnicos: são os causados pela falha de equipamentos e sistemas, tendo como conseqüência direta incêndios, explosões, interrupções, oscilações elétricas, falhas de climatização, umidade, gases corrosivos, magnetismo, radiações, poeira e qualquer outro evento que coloque em risco toda a estrutura de informação.

Riscos incontroláveis: são aqueles provenientes da natureza ou impactos indiretos. A natureza, por mais que monitorada, é incontrolável e por meio de chuvas, vendavais, terremotos etc. pode ocasionar danos aos negócios.

Os impactos indiretos são derivados dos riscos humanos e técnicos, porém são classificados como um evento externo e que dificilmente pode ser controlado, por exemplo, incêndio em edificações vizinhas.

O tratamento do risco deve ser orientado por um processo bem definido e atender aos objetivos, à estratégia e aos processos de negócios da organização. Os riscos são encarados de forma diferente por parte das pessoas que podem sofrer suas conseqüências, assim um processo de análise de risco deve determinar os controles, a criticidade e estabelecer as medidas de segurança de forma especial para cada risco. Um dos maiores problemas e risco para a organização é não reconhecê-lo, não tratá-lo ou ignorá-lo de forma inconsciente.

Os tratamentos para o risco podem ser definidos como:

Aceitar/Tolerar: deve ser utilizado quando os riscos forem de baixa gravidade, baixa probabilidade de ocorrência ou quando os custos para a implementação de controles são maiores do que os custos dos impactos ocasionados por uma ameaça.

Contornar/Evitar: estabelecer medidas, mudança de processos, tecnologias, restrições em sistemas ou processos ou qualquer outra alternativa que possa minimizar o risco sem comprometer o objetivo de negócio.

Transferir: atribuir responsabilidade a um meio externo, terceirização, que exerça seguro, melhor qualidade em serviço, ou contratar um seguro para a proteção do ativo.

Reduzir: implementar controles de segurança com um custo aceitável para minimizar a ocorrência de ameaças, redução das vulnerabilidades, controles de detecção e medidas para minimizar o impacto no caso de um evento não desejável.

4.5. Ameaças

As ameaças são eventos capazes de explorar vulnerabilidades existentes causando impactos e possíveis danos aos negócios. Mediante a exploração das fragilidades, os requisitos de confidencialidade, integridade e disponibilidade são comprometidos.

Existem três elementos que estão associados às ameaças [11]:

Agente: é o responsável por conduzir a ameaça, seja ela por meio humano, natural ou máquinas/sistemas.

Ameaças naturais: poluição, ventania, ciclone, erosão, terremoto, tornado, tsunami, partículas de combustão, alagamento, tempestades etc.

Ameaças humanas: concorrentes, ladrões, fornecedores, terceiros, funcionários insatisfeitos, adversários políticos, imprensa, crime organizado, usuários autorizados, *hackers, crackers*, espiões etc.

Ameaças via máquinas/sistemas: *worms*, vírus, *trojan*, bombas lógicas, *scan* etc.

Motivação: são ações que fazem com que o agente explore a vulnerabilidade. Essas ações podem ser acidentais ou intencionais e somente o agente humano pode ser classificado como as duas ações.

Acidental: divulgação de informação, distúrbio e oscilação elétricos, interrupção elétrica, falha em ar-condicionado, umidade, fogo, enchente, falha de *hardware* e *software*, erro de operação, interrupção de telecomunicações etc.

Intencional: alteração de dados, sabotagem, roubo, divulgação de informação, furto, *hacker*, vandalismo, fraude, crime organizado, concorrente etc.

Resultado: acontecimento ocasionado pela exploração de uma vulnerabilidade, podendo ser perda de acesso, modificação, destruição etc.

4.6. Vulnerabilidades

As vulnerabilidades são fraquezas ou fragilidades presentes nos ativos da organização, que por sua vez podem ser exploradas pela ação das ameaças e ocasionar um incidente de segurança que afete negativamente a confidencialidade, integridade e disponibilidade. Por ser um elemento passivo, a vulnerabilidade necessita de um agente causador para que seja explorada e comprometida.

Com o isolamento do agente causador, ameaça, a vulnerabilidade pode ser ilusoriamente considerada como neutra, assim a identificação das ameaças é fundamental para alcançar a correta priorização das vulnerabilidades, gastos em controles e medidas de segurança necessárias para minimizar o risco e deixá-lo em um nível aceitável de acordo com os objetivos da organização.

As vulnerabilidades são classificadas como [4]:

Físicas: localização física em perímetro perigoso, CPDs mal planejados, falta de recursos de combate a incêndio, instalação hidráulica em localização incorreta, vazamentos, falta de ar-condicionado e regulador de umidade em CPDs etc.

Naturais: excesso de temperatura, chuvas e tempestades com possibilidade de alagamento, terremotos, incêndios, umidade, poeira, fumaça etc.

***Hardware*:** defeito ou falhas nos recursos tecnológicos originados por desgastes, falha nos procedimentos de manutenção e instalação, falta de contrato de suporte, obsolescência etc.

***Software*:** erros de programação ou funções de código, erros de configuração e instalação, falta de *backup*, falta de controles nos processos de autenticação, autorização e contabilização de acesso, perda de dados, vazamento de informações etc.

Mídias: falha na destruição de discos, fitas, relatórios e impressão, radiação eletromagnética, falha no armazenamento e transporte, perda ou danificação de mídias etc.

Comunicação: falha ou perda na comunicação, acesso não autorizado, roubo de comunicação e dados, vazamento de dados etc.

Processos: falha no planejamento estratégico, falhas em procedimentos e fluxo de operação, erros em projetos etc.

Exemplos de vulnerabilidades no setor de tecnologia da informação:

- Servidor *Web* desatualizado;
- Falta de documentação atualizada;
- Sistema operacional *linux* com *kernel* desatualizado;
- Roteadores de borda sem controle de listas de acesso;
- Roteadores com *snmp* e permissionamento *rw* habilitado;
- Antivírus não atualizado nos servidores;
- Insatisfação profissional na área de operações;
- Uso de protocolo sem criptografia para acesso administrativo aos servidores;
- Falha nos processos de *backup;*
- Instabilidade no sistema de ar-condicionado;
- Falta de um circuito redundante de energia;

- Inexistência de uma política de segurança e de classificação;
- Transações eletrônicas sem mecanismo de criptografia de dados sigilosos;
- Inexistência de um gerenciamento de mudanças e *patches*;
- Inexistência de controle de acesso físico ao CPD.

A organização deve estabelecer um processo de identificação de vulnerabilidades, que pode ser desenvolvido por checklists de segurança [4], uso de ferramentas de varredura de vulnerabilidades, análise de documentações, análise de processos, análise de diagrama de arquitetura, entrevistas técnicas e gerenciais, análise e visita a ambientes e outros métodos. O processo de identificação de vulnerabilidades tem de ser um contínuo e orientado pela área de segurança da informação, a qual é a responsável pela identificação de novas vulnerabilidades e pelo processo de análise de risco, que deve ser efetuado em conjunto com os responsáveis dos processos de negócio. É fundamental que a organização possua um inventário atualizado de todos os sistemas, serviços, pessoas, processos, documentações, *hardwares*, *softwares* e outros para não comprometer nenhuma análise de vulnerabilidade.

Esse processo pode ser alinhado com algumas metodologias existentes no mercado que apontam as melhores práticas para o gerenciamento de processos, governança corporativa, controles de segurança e que ajustam os serviços de tecnologia da informação aos requisitos de negócios através da gestão de qualidade de seus componentes e serviços.

Exemplos de metodologias que podem auxiliar um processo de identificação de vulnerabilidades:

> **IT Infrastructure Librar (ITIL):** é uma metodologia para o gerenciamento do ambiente de infra-estrutura de empresas de qualquer porte. É um conjunto que consistente de melhores práticas mundiais que objetiva alinhar os serviços de tecnologia de informação aos requisitos de negócios através da gestão de qualidade de seus componentes e serviços.

Control Objectives for Information and related Technology (Cobit): Trata-se de uma estrutura para o gerenciamento dos processos de negócios alinhada a um modelo de governança em tecnologia de informação que permite o entendimento e o gerenciamento dos riscos.

NBT ISO/IEC 17799: Código de prática para a gestão da segurança da informação que dispõe de guias e recomendações sobre as boas práticas de gestão de segurança.

4.7. Medidas de segurança

As medidas de segurança podem ser classificadas como controles, que por sua vez têm o objetivo de reduzir ou eliminar as vulnerabilidades e minimizar ou bloquear as ameaças, bem como reduzir o impacto caso uma vulnerabilidade seja explorada. Esses controles devem ser aplicados e monitorados para garantir a menor taxa de exposição e proteção nos ativos da organização. Os controles podem ser ações, aquisição de equipamentos, novos processos e muitas vezes podem ser ações que não demandam gastos, mas sim a utilização de recursos internos, fatores políticos, leis vigentes etc [1].

Os controles devem ser aplicados após uma análise de custo, segundo a qual os controles são selecionados de acordo com o custo e o benefício que exercem sobre os ativos e objetivos da organização.

Com base nas análises de vulnerabilidade e ameaças, somadas ao cruzamento e priorização das vulnerabilidades, o responsável pelo processo de análise de risco, bem como os responsáveis ou usuários dos ativos e do setor da segurança da informação, devem selecionar os controles e as medidas essenciais para a minimização do risco com o menor custo/benefício. Esses controles não devem engessar o processo de negócio ou impactar nele. Portanto, é extremamente recomendado que um processo de análise de risco e a adoção de medidas de segurança sejam estabelecidos no início de um projeto, garantindo menor custo, continuidade do processo com o menor risco e medidas de segurança para a proteção adequada [5].

Os controles podem ser caracterizados nos seguintes tipos:

Preventivos: têm como objetivo bloquear ou minimizar os impactos ocasionados pela exploração das vulnerabilidades. Essas ações podem ser a implantação de mecanismos de segurança, conscientização de segurança na organização, políticas de segurança, adequação com normas, *checklists*, políticas, leis e modelos de processos, por exemplo, o ITIL. No setor da tecnologia da informação, essas medidas podem ser: configurações de segurança nos servidores e equipamentos de telecomunicações, implementação de filtros de acesso, modelagem de base de dados, processo de atualização de *patches*, políticas de segurança, catracas de acesso, utilização de criptografia, *firewalls*, IDS ativo, antivírus etc.

Detectivos: têm o objetivo de identificar a ocorrência de eventos não desejáveis ou ameaças, a fim de evitar a exploração das vulnerabilidades. Essas medidas também são utilizadas para o gerenciamento de métricas e ocorrências, com o objetivo de servir como base de eventos para futuras análises de risco e processos de decisão. Algumas medidas detectáveis para o setor de tecnologia são: central de monitoramento de *software*, *hardware* e aplicação, *triggers* em banco de dados, alarmes, câmeras de monitoramento, IDS, análise de risco e outros.

Corretivos: são medidas utilizadas para recuperar o ativo atingido ou reduzir o impacto ocasionado pelas ameaças. Essas medidas também são utilizadas para equiparar os processos tecnológicos, pessoas, infra-estrutura, processos de negócios com os objetivos de segurança estabelecidos na organização. Para o setor de tecnologia da informação essas medidas podem ser: plano de continuidade de negócio, restauração de *backups*, plano emergencial para recuperação de desastres, filtros de acesso dinâmicos para proteção de ataques DoS (Denial of Service), servidores *spare*, dispositivos de balanceamento de tráfego etc.

Alguns tipos de controles possuem mais de uma característica: proteger um ou mais ativos e eliminar ou minimizar uma ou mais vulnerabilidades. Portanto, a junção de um processo de priorização e da matriz de vulnerabilidades e a seleção de controles com o menor custo/benefício são o grande objetivo para minimizar os riscos para os ativos da organização [9].

Em função da complexibilidade de permeabilizar todos os ativos, reduzir ou eliminar todas as vulnerabilidades, implementar controles efetivos e reduzir os gastos, a segurança da informação estabelece alguns processos para segregar a adoção desses controles e garantir a melhor redução dos riscos. Essas medidas são definidas como proteção de perímetro e barreiras de segurança.

Proteção de perímetro: é a implementação de controles em profundidade que atribuem a proteção ideal para cada perímetro que uma ameaça pode comprometer até atingir o ativo alvo, vide Figura 2.

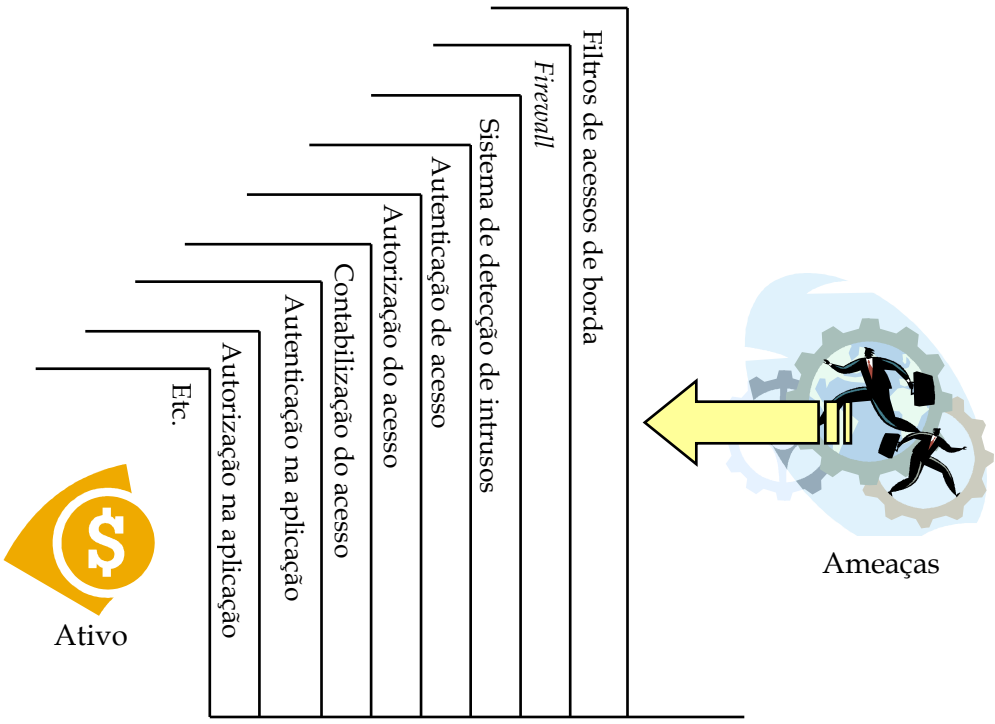

Figura 2. – Proteção de perímetro.

Barreiras de segurança: fornecem a segregação dos controles em seis barreiras para garantir a integração e interação a fim de obter a redução dos riscos. O conceito constitui-se de seis barreiras, sendo que uma auxilia e complementa a anterior, vide figura 3.

1. **Desencorajar:** faz com que os agentes das ameaças percam o interesse ou motivação para explorar uma vulnerabilidade;

2. **Dificultar:** possui controles que dificultam o acesso indevido de um agente da ameaça;

3. **Discriminar:** responsável pela adoção de controles que gerenciam o acesso e definem as autorizações de acesso e manipulação;

4. **Detectar:** possui mecanismos para o monitoramento e dispositivos de alerta para uma situação de risco;

5. **Deter:** possui mecanismos que necessitam de uma ação para impedir que a ameaça atinja os ativos. Esta barreira deve conter a ação da ameaça;

6. **Diagnosticar:** é a barreira responsável por alimentar o processo, torná-lo cíclico e manter a continuidade da gestão de segurança. Esta barreira conduz os processos de análise de risco e alimentação de métricas e eventos para auxiliar nos processos de investimento e investigação.

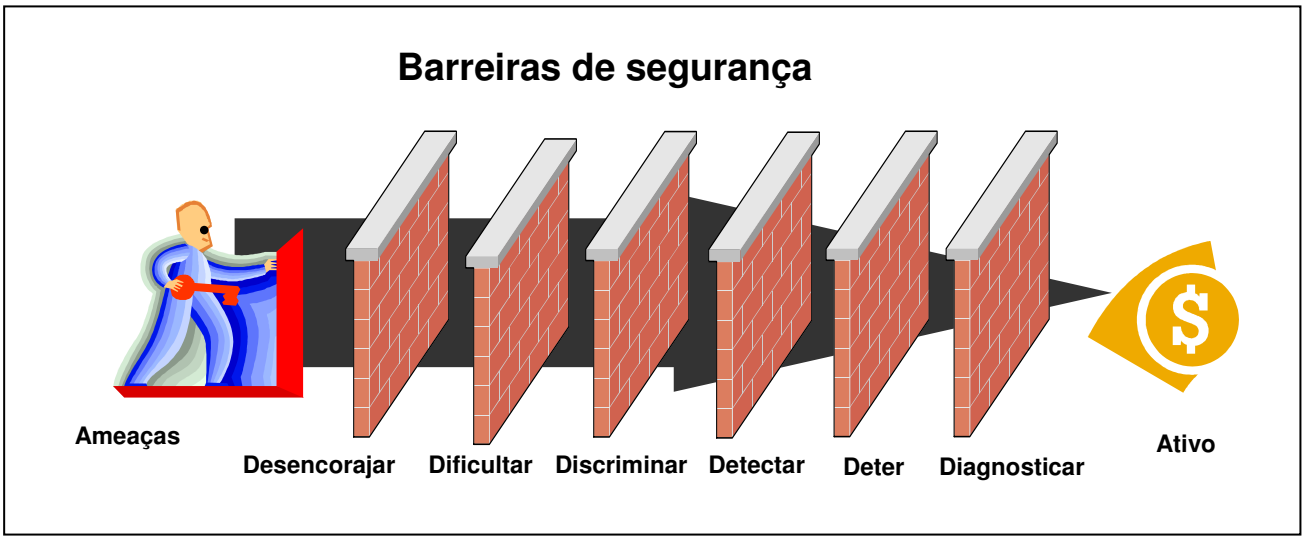

Figura 3. – Barreiras de segurança.

4.8. Análise de risco para o investimento de segurança em tecnologia da informação

O investimento de segurança possui muitas respostas elucidativas que fazem com que a idéia de despesas seja revertida em um ótimo investimento. O ROI ou retorno sobre investimento é uma ferramenta ou modelo que utiliza o cruzamento de dados reais relacionados a custos diretos, indiretos e intangíveis, para apoiar uma tomada de decisão.

Como qualquer outro investimento, o de segurança pode representar a valorização de recursos, tempo e esforço com o objetivo de fortificar o ambiente de controles internos para minimizar os riscos e impactos mais significativos, utilizar capital em determinado processo e fornecer outras idéias para a obtenção de controles que visam a um retorno esperado. Esse investimento deve atribuir os controles de segurança para garantir a confidencialidade, integridade e disponibilidade nos principais ativos da organização e permeabilizar os quatros elementos fundamentais que são a base de tudo: pessoas, processos de negócio, tecnologia e infra-estrutura; esses ativos podem ser tangíveis ou intangíveis, por exemplo, se a preservação imagem da organização for comprometida, gastam-se muito mais recursos tentando reconstruir uma imagem sólida, segura, eficiente e compromissada com o cliente do que os que foram gastos para construí-la.

Para obter a proteção ideal e manter o risco em um nível aceitável os controles devem ser mensurados de acordo com o objetivo do negócio e o valor atribuído ao ativo, sendo que o valor gasto nunca deve ser superior ao do ativo protegido e o valor agregado deve incluir os valores tangíveis e intangíveis.

De acordo com o ciclo de vida do setor de tecnologia da informação, os processos de mudanças e implementação de novas tecnologias podem trazer novas vulnerabilidades e ameaças aos ativos da organização. Neste ponto, a análise de risco deve ser utilizada para identificar os riscos evidentes e auxiliar no correto investimento nos controles de segurança.

A área da segurança da informação, em conjunto com os responsáveis pelo ativo, é responsável por estabelecer os controles necessários para minimizar os danos aos negócios e maximizar o retorno dos investimentos e as oportunidades de negócio. A segurança pode ser obtida com a implementação de uma série de controles, como políticas, práticas, procedimentos, estruturas organizacionais, tecnologias e funções de *software,* ou então projetada para evitar ou transferir o risco para obter a redução de exposição desejada. Como o objetivo é mitigar o risco, o investimento de segurança deve ser um processo contínuo e orientado pela análise de risco. Esse investimento, por muitas vezes, pode não agregar retorno visível quanto à sua função, pois seu objetivo é minimizar o impacto e proteger o ativo de algo incerto, que se comprometido deve possuir os controles necessários para minimizar o dano e garantir a salvaguarda esperada.

Com o foco em tecnologia da informação podemos equiparar o investimento de segurança como um processo sutilmente diferenciado do desenvolvimento ou aquisição de um novo sistema, servidores, software, pessoas, processos ou qualquer outro meio que envolva diretamente a aquisição de recursos. Essa diferença está atrelada à falta de métricas e dados existentes que possam determinar, por meio de números e projeções futuras, a certeza da existência ou ocorrência de um determinado risco.

Para obter o investimento de segurança ideal precisamos conhecer profundamente o que pretendemos investir e proteger, pois simplesmente a correta tomada de decisão pode demonstrar que nem sempre a aquisição de um equipamento de segurança, *firewalls*, detecção de intrusos, equipe de segurança, pessoas, antivírus e isoladamente outros conseguem assegurar a proteção ideal para um ativo de informação e mostrar que somente a mudança de um processo pode garantir a mesma ou melhor proteção para o ativo. Por exemplo, a aquisição

de um *firewall* não garante a proteção completa para os sistemas de informação. Um simples processo de gerenciamento de atualizações de *patches*, configurações de segurança, aplicação e monitoração podem suprir a necessidade de um *firewall* e agregar mais segurança para os ativos com um custo reduzido. A implementação de segurança através de profundidade, proteção de perímetro, políticas de segurança e classificação da informação são alguns dos controles que devem ser caracterizados como importantes para obter a mitigação de qualquer risco, sendo que esses controles devem ser identificados e orientados por meio de uma avaliação sistemática dos riscos de segurança.

4.9. Processo de análise de risco para segurança em tecnologia da informação

4.9.1. O processo e requisitos

Como qualquer outra atividade ou processo, a análise de risco demanda um processo bem definido, alinhado com a estratégia de negócio da companhia e que seja de fácil implementação.

Cada organização deve eleger ou desenvolver seu próprio processo de análise de risco, seja ele por desenvolvimento interno, consultoria externa ou com o auxílio de ferramentas para análise de risco, e ele deve estar adequado à cultura da organização [9].

O processo de análise de risco deve ser conduzido por um líder de projeto, um facilitador para gerenciar as reuniões e pelos representantes das áreas envolvidas no processo.

O facilitador do projeto deve ser uma pessoa neutra e que entenda os objetivos de negócio da companhia e conheça profundamente os sistemas da organização e os participantes. Pode ser membro da área de projetos ou segurança da informação.

Os *skills* para o facilitador são:

Escuta: deve possuir habilidade de escutar bem para responder verbalmente ou não às dúvidas dos participantes, ser subjetivo e claro.

Liderança: deve possuir postura de um líder e conduzir do início ao fim o processo, centralizar discussões e manter o foco no tema envolvido.

Reflexão: deve analisar as idéias e torná-las de fácil interpretação.

Sumarização: possuir habilidade para expor temas e idéias em conjunto e seqüência.

Suporte: criar um clima de confiança e honestidade.

Intervenção: deve possuir habilidade para ajudar os participantes em idéias alternativas que gerem discussão ou corrigir idéias que estejam fora do ponto de ação.

Centralização: deve ajudar o grupo a aceitar outras visões e ser confidente para todos os participantes.

Resolução de problemas: observar aspectos relevantes das idéias e ajudar o time a estabelecer um controle objetivo e na resolução de problemas.

Mudança do time: capacidade para identificar quem não faz parte do processo e providenciar um participante ativo.

O facilitador deve:

1. Observar atentamente e escutar o que todos os participantes dizem e fazem;
2. Reconhecer todas as idéias e incentivar a participação;
3. Observar respostas não verbais;
4. Escutar e manter o time envolvido;
5. Não perder o ponto de vista;
6. Ser neutro;
7. Aprender a honestidade e nunca ser hostil;
8. Evitar ser uma autoridade;

9. Estabelecer espaços de tempo e ser pontual;
10. Utilizar paradas para discussões livres;
11. Servir o time;
12. Parar o processo se o grupo estiver lento ou fora de controle.

O gerente do negócio, o líder do projeto e o facilitador devem identificar os participantes, que serão as pessoas responsáveis por auxiliar na identificação dos riscos, ativos, vulnerabilidades, ameaças e controles existentes ou necessários.

O processo deve incluir integrantes das áreas:

- Proprietário funcional;
- Usuário do sistema;
- Administrador do sistema;
- Analista de sistemas;
- Programadores de sistema;
- Programadores de aplicação;
- Administradores de banco de dados;
- Segurança da informação;
- Segurança física;
- Telecomunicações;
- Administradores de rede;
- Provedores de serviço;
- Setor estratégico;
- Auditor (se necessário);
- Jurídico (se necessário);
- Recursos humanos (se necessário).

O processo envolve a análise de sistemas, aplicações, segmentos de operação de negócios e outros sistemas ou processos identificados pelo gerente de negócio. O líder deve estar familiarizado com os objetivos e a estratégia da organização e necessita de participantes especializados com potencial para identificar as vulnerabilidades, ameaças e controles necessários.

Durante a reunião, orientada pelo facilitador, o time identificará as potenciais ameaças, vulnerabilidades e resultantes de impacto negativo na confidencialidade, integridade e disponibilidade dos ativos. O time analisará os efetivos impactos nos processos de negócio e classificará os riscos de acordo com o nível de criticidade e severidade.

Antes de iniciar uma reunião, todos os integrantes devem conhecer ou ser apresentados às definições básicas para o processo de análise de risco: risco, medidas de segurança, ameaças, vulnerabilidades, confidencialidade, integridade e disponibilidade.

O objetivo final da reunião é identificar os eventos indesejáveis e não autorizados, identificar e priorizar os riscos que podem trazer impacto nos processos de negócio ou missão da organização e estabelecer as medidas de segurança necessárias para mitigar o risco a um nível aceitável ou reduzir o resultado de um impacto.

Após a reunião, o gerente de negócio, o líder do projeto e o facilitador devem correlacionar as informações identificando os controles existentes, o cruzamento de vulnerabilidades e controles, estabelecer os controles efetivos para a mitigação dos riscos de acordo com o objetivos e a estratégia da organização e disponibilizar um relatório final, classificado como confidencial, aos gerentes de negócio e gestores responsáveis pelos processos e estratégia da organização.

4.9.2. Identificação dos ativos

A identificação dos ativos é tarefa fundamental para obter sucesso na análise de risco. Sem conhecer os principais ativos da organização não se pode conhecer o que se deseja proteger, estabelecer controles e identificar o real risco que existe na organização.

Esse processo é orientado com base nos resultados financeiros e estratégicos para a organização. Portanto, os representantes e gerentes de negócios devem estar envolvidos para compartilhar as informações sobre os processos críticos e desmembrá-los em perímetros físicos, humanos, tecnológicos e negócios, com características e funções explicitamente específicas que justifiquem ações sob medida. A identificação do valor do ativo não deve ser

atribuída ao setor de segurança da informação, sistemas de informação ou qualquer outro, pois o valor do ativo deve ser determinado por quem o manipula, cria ou custodia.

A identificação dos ativos consiste em:

- Determinar os ativos críticos;
- Identificar os impactos e os eventos indesejáveis;
- Valorizar e priorizar os ativos em conseqüência a sua perda.

Antes de determinar os ativos da organização, é importante saber que:

- Nem todos os ativos necessitam do mesmo nível de proteção;
- Nem todos os ativos são importantes sobre outros itens;
- Nem todos os ativos têm o mesmo valor para pessoas distintas;
- Nem todos os ativos são essenciais para a organização;
- Nem todos os ativos são identificados em uma organização de grande escala;
- O valor para redução do risco em um ativo deve ser razoável e justificado em relação ao valor do ativo.

A identificação do ativo pode ser conduzida por uma sessão de perguntas e pelo mapeamento de relevância, estudo de impacto e prioridades quanto à gravidade, urgência e tendência do ativo.

Estudo de prioridade GUT: define a prioridade de um ativo em relação à gravidade, urgência e tendência.

Gravidade: define quanto seria grave se um ativo fosse atingido por uma ameaça.

Urgência: define a urgência para solucionar os efeitos ocorridos e em reduzir os riscos no ativo.

Tendência: define a tendência dos riscos de segurança se nenhuma medida de segurança fosse aplicada ao ativo.

Tabela 3. – GUT.

Gravidade	Urgência	Tendência
1 – Sem gravidade	1 – Sem pressa	1 – Não agravará
2 – Baixa gravidade	2 – Tolerante à espera	2 – Agravará a longo prazo
3 – Média gravidade	3 – O mais cedo possível	3 – Agravará em médio prazo
4 – Alta gravidade	4 – Com alguma urgência	4 – Agravará em curto prazo
5 – Altíssima	5 – Imediatamente	5 – Agravará imediatamente

O resultado da prioridade de GUT pode ser definido pela multiplicação dos valores de gravidade, urgência e tendência.

Exemplo de ativo: Gravidade média, Com alguma urgência e Agravará em curto prazo = 3 x 4 x 4 = 48.

O valor do ativo é atribuído por estimativas subjetivas, pois não há ferramentas nem métodos objetivos para determinar o valor concreto de um ativo.

Para ajudar na identificação dos ativos, os integrantes devem responder às perguntas do questionário a seguir:

Questionário estruturado para identificação de ativo [10]

1. Quais são as atividades críticas que ocorrem nesta organização?
2. Descreva as pessoas, clientes, usuários, visitantes.
3. Qual informação crítica ou sensível reside na organização?
4. Identifique os equipamentos e sistemas críticos e valiosos para a organização.
5. Descreva a localização específica dos ativos identificados.

Para cada um dos ativos identificados, responda:

1. Em que medida a obtenção desse ativo ajuda um adversário a atingir seus objetivos?
2. O que a organização perderia? O que o adversário ganharia?
3. Esses ativos são valiosos para a organização antes do adversário obtê-lo?
4. Quanto seria o gasto para desenvolver esses ativos? Quanto seria o tempo de vida e impacto sem esse ativo?
5. Se um ou mais ativos forem comprometidos, qual será o impacto nas pessoas, clientes e imagem da organização?

Com as respostas obtidas pelo questionário, uma avaliação de impacto deve ser efetuada para identificar os ativos com maior criticidade e que mais necessitam de proteção. Devem-se mapear as relevâncias, fazer um estudo de impactos quanto à confidencialidade, integridade e disponibilidade e definir prioridades quanto à gravidade, urgência e tendência.

Mapeamento das relevâncias: define quanto um ativo é relevante para a organização.

Tabela 4. – Mapeamento de relevância.

Escala	Auxílio de interpretação
1 – Não considerável	Envolve o atingimento gerenciável do processo de negócio, podendo provocar impactos praticamente irrelevantes.
2 – Relevante	Envolve o atingimento gerenciável do processo de negócio, podendo provocar impactos apenas consideráveis.
3 – Importante	Envolve o atingimento gerenciável do processo de negócio, podendo provocar impactos parcialmente significativos.
4 – Crítico	Envolve a paralisação do processo de negócio, podendo provocar impactos significativos.
5 – Vital	Envolve o comprometimento do processo de negócio, podendo provocar impactos incalculáveis na recuperação e na continuidade do negócio.

Estudo de impactos de CID: define quanto um ativo é sensível para a organização em relação à confidencialidade, integridade e disponibilidade do mesmo [11].

Tabela 5. – Impactos de CID.

Ativo Escala	**Confidencialidade**	**Integridade**	**Disponibilidade**
1 – Não considerável			
2 – Relevante			
3 – Importante			
4 – Crítico			
5 – Vital			

4.9.3. Análise de ameaças e vulnerabilidades

O passo subseqüente à identificação dos principais ativos da organização é determinar as ameaças e vulnerabilidades relacionadas a esses ativos, bem como os controles de segurança existentes para cada um deles.

No processo de análise de ameaças e vulnerabilidades, devem-se identificar os principais adversários e conhecer quanto eles são críticos e perigosos para os negócios da organização. Esses adversários são caracterizados como os agentes responsáveis por conduzir uma ameaça, seja ela por meio humano, natural ou máquinas/sistemas.

A análise de ameaças e vulnerabilidades para um sistema de tecnologia de informação deve ser efetuada por meio de um diagrama de arquitetura do ativo. Os especialistas envolvidos precisam desenvolvê-lo cobrindo todos os perímetros e dependências do ativo; identificação das tecnologias implementadas; decomposição do sistema; identificação e priorização das ameaças e vulnerabilidades e documentação. Os especialistas têm de conhecer profundamente o funcionamento do ativo, bem como o valor e os resultados do processo.

Diagrama de arquitetura: o diagrama de arquitetura de alto nível deve descrever a composição e a estrutura do ativo, bem como seus subsistemas, suas características de implantação física e lógica e controles existentes. Dependendo da complexidade do sistema, devem-se criar diagramas adicionais que se concentrem em diferentes áreas, por exemplo, um diagrama para modelar a arquitetura de um servidor de aplicativo de camada intermediária ou um para servir de modelo para a interação com um sistema externo.

O diagrama a seguir demonstra a arquitetura de um ativo que é o sistema de vendas on-line de uma organização, na qual é o responsável pelo faturamento de vendas e representa o principal processo de negócio para a organização. Este diagrama foi desenvolvido pelos especialistas da organização, que detalharam o sistema e identificaram os controles de segurança existentes [6].

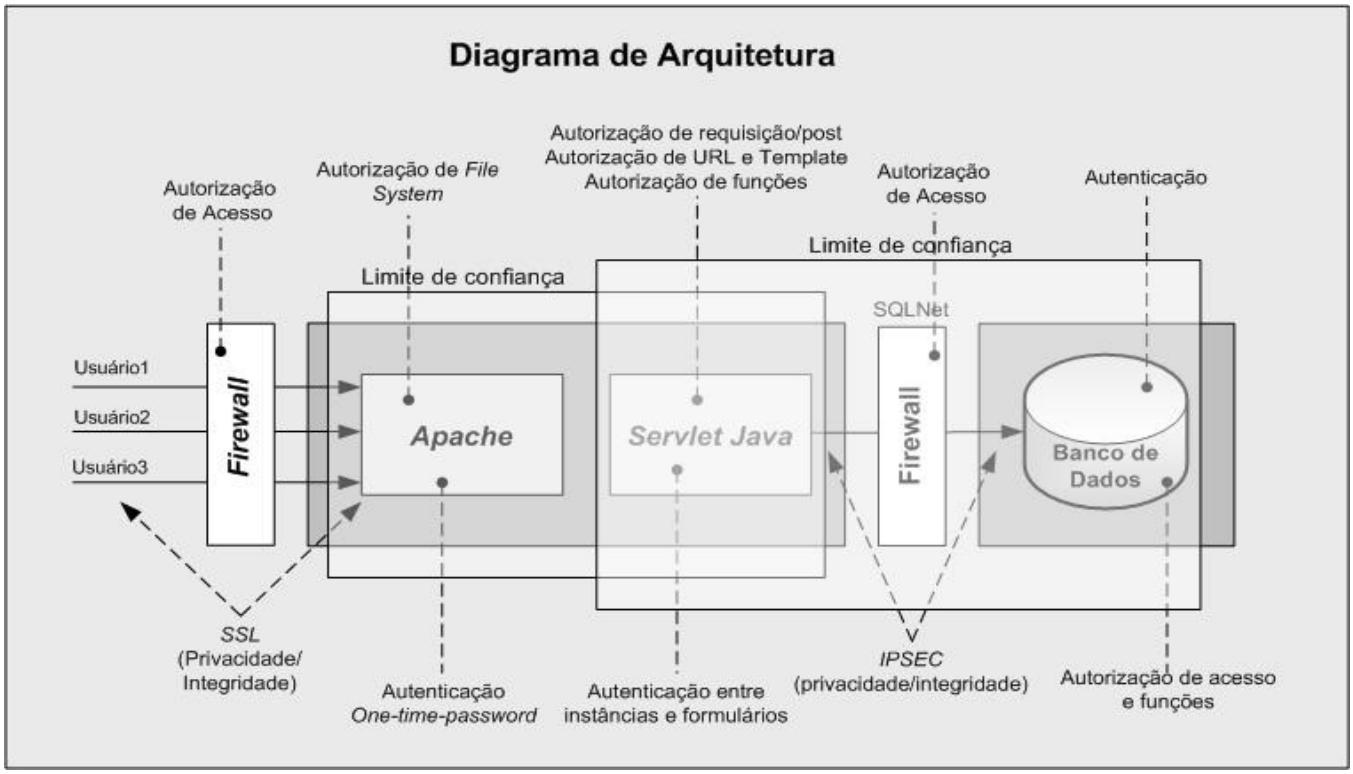

Figura 4. – Mapeamento de arquitetura.

Identificar as tecnologias: as tecnologias utilizadas para implementar o sistema devem ser identificadas para auxiliar na localização de ameaças específicas às tecnologias e ajudar a determinar as técnicas de mitigação corretas e mais apropriadas para o ativo.

Tabela 6. – Identificação de tecnologias.

Tecnologia/Plataforma	Detalhes de implementação
Servidor Linux Suse 9.1	Sistema operacional responsável pelo servidor *web* e instância Java.
Apache 2.0.53	Servidor *web* responsável por prover o acesso à aplicação http e servir como interface para a *servlet.*
Mod_SSL	Utilizado para criptografar o tráfego http.
Jetty	Utilizado para gerenciar a aplicação Java.
Mod_RSA	Utilizado para autenticação forte.
IPSEC	Utilizado para criptografar o tráfego entre o servidor *web* e o banco de dados *Oracle*.
Oracle 9i	Servidor de banco de dados.
Firewall-1 NG	Utilizado para filtrar os acessos externos e internos.

Decomposição do sistema: o sistema ou aplicativo deve ser dividido em partes para criar um perfil de segurança para o aplicativo, tomando por base as áreas tradicionais de vulnerabilidade. Neste processo, devem-se identificar os limites de segurança, o fluxo de dados, pontos de entrada e códigos privilegiados e documentar os perfis de segurança [7].

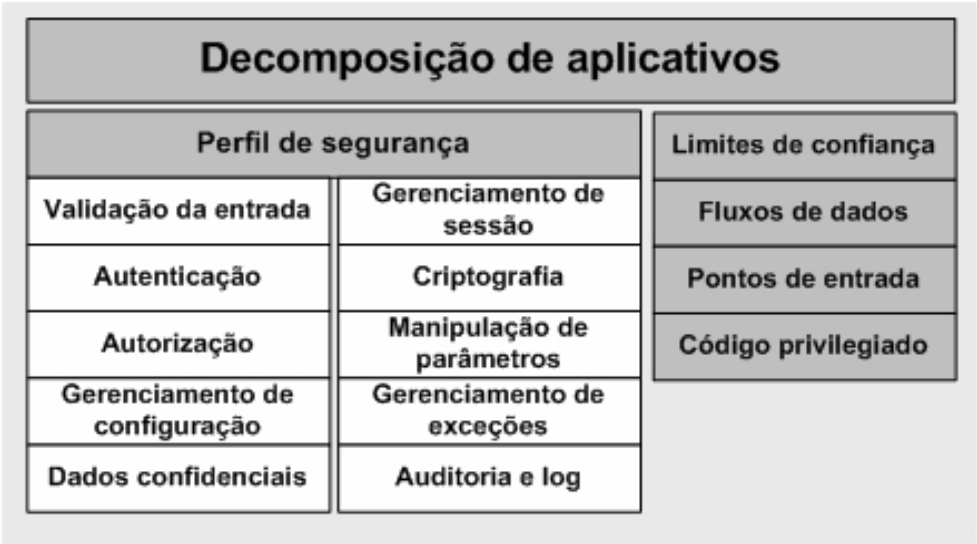

Figura 5. – Decomposição de aplicativos.

Fonte: http://www.microsoft.com/brasil/security/guidance/topics/devsec/secmod76.mspx

O processo de decomposição possui as seguintes tarefas:

Identificar os limites de confiança: identifica os limites de segurança que cercam cada bem tangível do sistema. Esses bens são determinados pelo projeto do aplicativo. Para cada subsistema, deve-se considerar se os fluxos de dados *upstream* ou se a entrada do usuário é confiável, levando em conta que o fluxo de dados e as entradas podem ser autenticados e autorizados. O código de chamada também dever ser confiável e pode ser autenticado e autorizado. Devem-se definir os *gatekeepers* adequados para proteger todos os pontos de entrada de um determinado limite de segurança e que o ponto de entrada do destinatário

valide totalmente os dados que passem por um limite de confiança, bem como conjuntos que confiam em outros conjuntos.

Identificar o fluxo de dados: identifica o fluxo de dados entre os subsistemas individuais pelo nível mais alto e segrega-os em camadas. O fluxo de dados entre os limites de confiança é extremamente importante, pois o código que recebe os dados externos ao seu próprio limite de segurança deve presumir dados mal-intencionados e realizar a validação dos dados.

Identificar os pontos de entrada: os pontos de entrada do sistema ou aplicativo devem ser identificados por servirem como pontos de entrada para ataques. Os pontos de entrada devem ser identificados e os tipos de entrada que transitam por ele precisam ser conhecidos, pois por meio da entrada um invasor pode obter acesso e atacar diretamente um ponto de entrada interno. Para cada entrada devem-se determinar os tipos de *gatekeepers* que forneçam autorização e o grau de validação.

Identificar o código privilegiado: os códigos privilegiados acessam tipos específicos de recursos seguros e realizam outras operações privilegiadas. As diretivas de segurança de acesso ao código devem conceder ao código privilegiado as permissões de segurança de acesso ao código apropriado. O código privilegiado deve garantir que os recursos e as operações que ele encapsula não sejam expostas a um código não confiável e possivelmente mal-intencionado.

Documentar o perfil de segurança: identifica as abordagens do projeto e da implementação utilizadas para a validação de entrada, autenticação, autorização, gerenciamento de configuração e as áreas restantes em que os aplicativos são mais suscetíveis à vulnerabilidade [7].

Tabela 7. – Perfil de segurança.

Categoria	Considerações
Validação de entrada	Todos os dados de entrada são validados? Um invasor poderia incluir comandos ou dados mal-intencionados no aplicativo? Os dados são validados à medida que passam entre limites de confiança separados (pelo ponto de entrada do destinatário)? Os dados no banco de dados são confiáveis?
Autenticação	Ao serem passadas pela rede, as credenciais são protegidas? São utilizadas diretivas de conta de alta segurança? As senhas de alta segurança são obrigatórias? O sistema está utilizando certificado? Os verificadores de senha (utilizando *hashes* unilaterais) são utilizados para senhas do usuário?
Autorização	Quais *gatekeepers* são utilizados nos pontos de entrada do aplicativo? Como a autorização é imposta no banco de dados? A estratégia de defesa utilizada é abrangente? O sistema falha com segurança e somente permite o acesso com a confirmação bem-sucedida de credenciais?
Gerenciamento de configuração	Quais interfaces de administração o aplicativo suporta? Como elas são protegidas? Como a administração remota é protegida? Quais armazenamentos de configuração são utilizados e como eles são protegidos?
Dados confidenciais	Quais dados confidenciais são manipulados pelo aplicativo? Como eles são protegidos na rede e em armazenamentos persistentes? Qual o tipo de criptografia utilizado e como as chaves de criptografia são protegidas?
Gerenciamento da sessão	Como os *cookies* de sessão são gerados? Como eles são protegidos para evitar o seqüestro da sessão?

Categoria	Considerações
	Como o estado persistente de sessão é protegido? Como o estado de sessão é protegido à medida que ela atravessa a rede? Como o aplicativo é autenticado com o armazenamento de sessão? As credenciais são passadas pelo fio e mantidas pelo aplicativo? Se sim, como elas são protegidas?
Criptografia	Quais algoritmos e técnicas criptográficas são utilizados? Qual o tamanho das chaves de criptografia e como elas são protegidas? O aplicativo coloca sua própria criptografia em ação? Com que freqüência as chaves são recicladas?
Manipulação de parâmetros	O aplicativo detecta os parâmetros violados? Ele valida todos os parâmetros em campos de formulário, estado da exibição, dados do *cookie* e cabeçalhos http?
Gerenciamento de exceções	Como o aplicativo manipula as condições de erro? As exceções sempre têm permissão para propagar de volta ao cliente? São utilizadas mensagens de erro genéricas que não contenham informações exploráveis?
Auditoria e log	O aplicativo audita as atividades em todas as camadas em todos os servidores? Como os arquivos de log são protegidos?

Identificação das ameaças e vulnerabilidades: o processo de identificação das ameaças deve ser desenvolvido pelos especialistas responsáveis pelos sistemas e subsistemas do ativo. A identificação pode ser efetuada por meio de uma base de categoria de ameaças que é agrupada por categoria de rede, *host* e aplicativo, ou com base em determinados pontos que são os fatores objetivos de um invasor.

Ameaças de rede: os principais componentes que formam a infra-estrutra são roteadores, *firewalls* e *switches*. Eles agem como *gatekeepers* que protegem os servidores e aplicativos de ataques e invasões. As vulnerabilidades comuns incluem configurações de instalação-padrão, controles de acesso abertos e dispositivos sem as correções de segurança mais recentes. As ameaças de nível de rede mais importantes incluem [6]:

Coleta de informações: os dispositivos de rede podem ser descobertos e ter seu perfil traçado do mesmo modo que outros sistemas.

Ação de *sniffers*: ato de espionagem para monitorar o tráfego da rede e obter informações sensíveis.

***Spoofing*:** meio de ocultar a verdadeira identidade de alguém na rede.

Seqüestro de sessão: conhecido como ataque de interceptação, o seqüestro de sessão convence o servidor ou um cliente a aceitar o *host upstream* como um *host* legítimo real.

Negação de serviço: tipo de ataque que não permite que um usuário legítimo acesse um servidor ou serviços.

Ameaças de *host*: as ameaças do *host* são direcionadas ao software do sistema no qual os aplicativos são criados. As ameaças no nível do *host* mais importantes incluem:

Vírus, cavalos de tróia e *worms*: vírus é um programa criado para realizar atos mal-intencionados e causar interrupção do sistema operacional ou aplicativos. Um cavalo de tróia é parecido com um vírus, exceto pelo fato de que o código mal-intencionado fica dentro do que parece ser um arquivo de dados inofensivo ou um programa executável. Um *worm* é parecido com um cavalo de tróia, exceto pelo fato de que ele se prolifera sozinho de um servidor para outros.

Scan: efetua varredura de portas, sistemas e arquitetura da aplicação para obter informações valiosas para auxiliar ataques mais significativos.

Quebra de senha: utiliza métodos para decifrar a combinação de nome de usuário e senha válida.

Negação de serviço: um invasor interrompe o serviço de um sistema por meio de força bruta ou exploração de uma vulnerabilidade existente no serviço ou aplicativo.

Execução arbitrária do código: quando um invasor pode executar um código mal-intencionado no servidor, ocasionando outros ataques ou paralisação do serviço.

Acesso não autorizado: controles de acesso inadequados que podem permitir acesso não autorizado às informações restritas ou realização de operações restritas.

Ameaças de aplicativos: as ameaças dos aplicativos são direcionadas à manipulação da funcionalidade da aplicação, fazendo com que a mesma seja manipulada por um atacante. As ameaças no nível de aplicativos mais importantes incluem:

Validação da entrada: estouro de *buffer*; XSS (*cross-site scripting*); injeção de código SQL; canonização.

Autenticação: espionagem de rede; ataques de força bruta; ataques de dicionário; repetição de *cookie*, roubo de credencial.

Autorização: elevação de privilégio; divulgação de dados confidenciais e violação de dados.

Gerenciamento de configuração: acesso não autorizado a interfaces de administração; acesso não autorizado a armazenamentos de configuração; recuperação de dados de configuração em texto não criptografado; falta de responsabilidade individual; contas de processo e serviço muito privilegiadas.

Dados confidenciais: acessar dados confidenciais em armazenamento; espionagem na rede, violação de dados.

Gerenciamento de sessão: seqüestro de sessão; repetição de sessão, interceptação.

Manipulação de parâmetros: manipulação de seqüência de caracteres para consulta; manipulação de campo de formulário; manipulação de *cookie*, manipulação do cabeçalho http.

Gerenciamento de exceção: divulgação de informações; negação de serviço.

Auditoria e *log*: o usuário nega a realização de uma operação, o invasor explora um aplicativo sem rastreamento; o invasor encobre seus rastros.

Classificação das ameaças e vulnerabilidades: as ameaças devem ser classificadas e priorizadas de acordo com o seu risco e impacto para a organização.

Matriz de prioridade

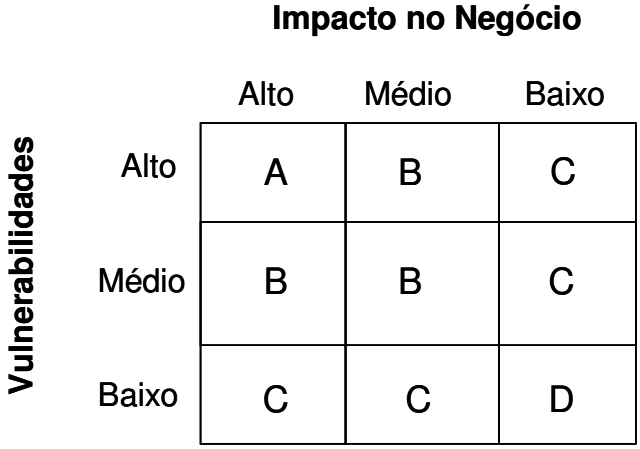

Figura 6. – Matriz de prioridade.

A classificação, figura 6, deve seguir os seguintes critérios:

Alta vulnerabilidade: uma grande fraqueza existe nos sistemas ou nos processos operacionais, o impacto no processo de negócio é severo ou significante e um controle deve ser implementado imediatamente.

Média vulnerabilidade: existem algumas fraquezas e o impacto pode ser severo ou significante, um controle pode e deve ser implementado.

Baixa vulnerabilidade: o sistema está ausente de fraquezas e opera perfeitamente, nenhum controle precisa ser implementado.

Alto impacto: pode resultar em grandes impactos severos e prejudicar ou exterminar as operações da organização.

Médio impacto: poderá resultar em uma perda significante, mas os negócios da organização sobrevivem.

Baixo impacto: poderá resultar em uma pequena perda em algum processo de negócio ou não acarretar nenhum dano.

As prioridades são:

A – Deve-se implementar uma ação corretiva imediatamente;
B – Um controle de correção pode ser implementado;
C – Requer monitoração;
D – Nenhuma ação é requerida.

Documentação das ameaças e vulnerabilidades: o processo de documentação das ameaças deve incluir vários atributos da ameaça e vulnerabilidades. Os atributos são: descrição da ameaça, destino da ameaça, técnicas de ataque, vulnerabilidades exploradas, controles existentes, contramedidas de segurança necessárias para tratar a ameaça e priorização da ameaça e vulnerabilidade [9].

Exemplo de documentação: **Ameaça X**

Descrição da ameaça: invasor obtém acesso à execução de comandos privilegiados no sistema por um ataque *buffer overflow*.
Alvo da ameaça: obter nível privilegiado de execução de comandos para obter acesso ao banco de informações de cartão de crédito.
Técnicas do ataque: envio de dados mal-intencionados para ocasionar o estouro da pilha de memória do servidor *web* e introduzir um *shell code* para a execução de comandos no sistema operacional.
Vulnerabilidades: servidor *web* desatualizado.
Controles atuais: *firewall*, antivírus e autenticação.
Contramedidas: atualizar o servidor *web*, o sistema de detecção de intrusos e manter um processo de gerenciamento de *patches*.
Prioridade: A (alto impacto).

4.9.4. Identificação e tratamento dos riscos

Depois de identificadas as ameaças e vulnerabilidades críticas para os ativos da organização, os riscos devem ser expostos e correlacionados por meio de uma matriz de risco do ativo [9].

Com a matriz, é possível identificar e selecionar qual será o tratamento ideal para o risco, seja ele: aceitar, contornar, transferir ou evitar.

A correlação dessas informações pode demonstrar que a simples implementação de uma medida de segurança é capaz de mitigar vários riscos, bem como reduzir a exposição de confidencialidade, integridade e disponibilidade, proteger outros ativos e priorizar o risco.

Tabela 8. – Exemplo de matriz de risco.

Matriz de risco						
Risco	**Prioridade**	**Tipo**	**Controle atual**	**Controles necessários**	**Severidade GUT**	**Tratamento**
1. Acesso de informação confidencial por usuário não autorizado	**A**	**Integridade Confidencialidade**	**1, 2, 9, 11**	**3, 5, 6, 8**	**100**	**Evitar**
2. *Defacement* do site	**A**	**Integridade Disponibilidade**	**1, 5, 7, 9, 11**	**4, 6, 8, 10**	**125**	**Evitar**
3. Ataque de negação de serviço	**B**	**Disponibilidade**	**3, 11**	**7, 10**	**48**	**Reduzir**

- A severidade é calculada pelo modelo de GUT:

Risco 1. Altíssima gravidade x Com alguma urgência x Agravará em curto prazo.
Risco 2. Altíssima gravidade x Urgência imediata x Agravar imediatamente.
Risco 3. Média gravidade x Com alguma urgência x Agravará em curto prazo.

- A prioridade é calculada pela matriz de prioridade.
- O tipo é definido pelo elemento comprometido: confidencialidade, integridade e disponibilidade.
- Os controles atuais são identificados pela tabela de controles.
- Os controles para mitigação do risco são selecionados pela tabela de controles.
- O tratamento é selecionado após a identificação dos valores da matriz de risco.

Tabela 9. – Exemplo de lista de controles.

Lista de controles		
Número do controle	**Classe**	**Descrição do controle**
1	*Backup*	Sistema de *backup* e *restore*, incluindo processo e gerenciamento de fitas
2	Controle de acesso	*Firewall* para a proteção de acesso entre perímetro interno
3	Monitoramento	Sistema de detecção de intrusos
4	Gerenciamento de mudanças	Processo e sistema para atualização de *patches* e sistemas
5	Controle de aplicação	Aplicação de controle para validação de entrada e modificação de informação
6	Controle de acesso	Sistema de autenticação *one-time-password*
7	Controle de acesso	*Firewall* para proteção de acesso externo
8	Monitoração	Sistema de identificação de vulnerabilidades
9	Antivírus	Sistema de antivírus para servidores e estações
10	Plano de recuperação	Desenvolvimento, documentação e teste de um processo de recuperação de desastres
11	Manutenção	Contrato de suporte para os servidores e equipamentos de rede

4.9.5. Identificação das medidas de segurança

As medidas de segurança devem ser selecionadas após o cruzamento dos resultados da matriz de risco.

Por meio da relação entre prioridade, tipo, severidade, tratamento do risco e relação dos controles, os especialistas devem identificar e selecionar os controles que cobrem os riscos de maior impacto e os controles que, se implementados, garantem uma mitigação geral nos riscos de maior impacto.

De acordo com a análise do exemplo da matriz de risco, os controles 4, 6, 8, 10 devem ser implementados imediatamente na organização para reduzir o risco em um nível aceitável. Os controles selecionados atuam diretamente no risco de maior impacto, 2, e conseqüentemente auxiliam na minimização dos riscos 1 e 3, exercendo uma ótima relação de custo, benefício e retorno de investimento.

4.9.6. Relatório final

Depois de completada a sessão de análise de risco, um documento deve ser desenvolvido para detalhar os resultados do processo e incluir as conclusões e plano de ação para a mitigação dos riscos. Esse documento precisa incluir os seguintes tópicos:

- Descrição dos processos, ativos e pessoas envolvidas;
- Processo de análise de risco, descrevendo os riscos que afetam a confidencialidade, integridade e disponibilidade, bem como o impacto para a organização;
- Descrição dos controles necessários para a mitigação do risco;
- Descrição de como, quando e quem implementará os controles;
- Descrição do tratamento atribuído aos ativos e especialmente os riscos que foram aceitos.

O documento deve ser classificado como confidencial e encaminhado para os gerentes do negócio, setor de segurança da informação, setor de assuntos estratégicos e proprietários representantes.

5. DISCUSSÃO

Os resultados obtidos no processo de análise de risco demonstraram que por meio dela é possível dimensionar o correto investimento nos controles de segurança correlacionados aos riscos existentes nos ativos da organização e que somente com a identificação dos principais ativos e riscos pode-se saber em que, onde e como investir em segurança para minimizar a exploração das vulnerabilidades ou o impacto para o negócio.

Para que o processo seja executado com eficiência e apresente o resultado esperado é necessário que se tenha o apoio do setor estratégico, diretores e principais colaboradores da organização, pois a coleta e o desenvolvimento do processo dependem de informações de outros setores e da utilização de recursos na organização. O resultado também deve ser apresentado para o setor estratégico e responsáveis pela organização, assim é possível eleger o rumo, de acordo com a estratégia, para os principais riscos que podem prejudicar o negócio.

6. CONCLUSÃO

As mudanças mercadológicas exercidas nestes últimos anos, sejam elas oriundas de novos produtos, sistemas, adoção de metodologias, regulamentações e requisitos legais, mostram para as organizações que o setor de segurança da informação é um bem necessário, eficaz, que auxilia no desenvolvimento estratégico e ,em muitos casos, pode agregar produtividade e lucratividade para a organização.

O setor de segurança da informação pode demonstrar que o conhecimento da dinâmica e o gerenciamento dos riscos são fatores relevantes para garantir o correto investimento em controles e processos para proteger a organização das constantes mutações e dos riscos que são inerentes à natureza humana.

Com um processo de análise de risco a área de segurança da informação consegue apresentar para a organização o mapeamento dos seus principais ativos, diminuindo a discrepância entre a ilusão e o valor do ativo, os controles de segurança existentes e a importância do ativo para a organização. Por meio da análise de ameaças e vulnerabilidades, os profissionais envolvidos conhecem profundamente as dependências e processos de cada ativo, bem como os adversários e principais ameaças. A consolidação e a priorização das vulnerabilidades e ativos fazem com que os principais riscos sejam levantados e que uma análise de controles apresente os efetivos controles para garantir a confidencialidade, disponibilidade e integridade. Esse aprendizado é um investimento para o capital humano e um instrumento que pode auxiliar na vitalidade da organização.

Para complementar o processo de análise de risco recomendo a utilização ou o desenvolvimento de um modelo de mapeamento de métricas, para quantificar o histórico de eventos e incidentes, e seguir como suporte para uma consolidação entre as análises de risco subjetiva e objetiva, garantindo um resultado mais sólido para as futuras análises de risco.

Com base neste trabalho acredito que o processo de análise de risco deve ser utilizado nas organizações que desejam investir seguramente ou quando

querem levantar a necessidade de um investimento em segurança da informação, para assim atender e proteger o bem mais valioso da organização.

7. GLOSSÁRIO

Buffer Overflow: condição de erro que consiste na alteração indevida de posições de memória. Quando essa alteração resulta na modificação de endereços de retorno de funções armazenados na pilha, pode ocorrer uma alteração maliciosa do fluxo de execução do programa e a condição recebe o nome específico de *Stack Overflow*. Quando a alteração resulta na modificação de posições de memória contendo informações disponíveis para a aplicação, pode-se alterar o comportamento da aplicação baseado nessas informações e a condição de erro recebe o nome específico de *Heap Overflow*.

Cavalo de Tróia: programa que, além de executar funções para as quais foi aparentemente projetado, executa outras funções normalmente maliciosas e sem o conhecimento do usuário.

Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas, processos e sistemas autorizados.

Cookies: um pequeno arquivo que é armazenado localmente no computador do usuário com propósitos de registro e que contém informações pertinentes ao site sobre o usuário, como preferências do mesmo.

Cracker: termo genérico usado para designar pessoas que acessam sistemas de informação sem autorização, com a finalidade de roubar informações e causar prejuízo.

Criptografia: é a ciência e arte de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações secretas. É usada, dentre outras finalidades, para: autenticar a identidade de usuários; autenticar transações bancárias; proteger a integridade de transferências eletrônicas de fundos e proteger o sigilo de comunicações pessoais e comerciais.

Defacement: caracterizado como pichação cibernética, em que um atacante desconfigura ou altera qualquer informação de um site.

Disponibilidade: garantia de que pessoas, processos e sistemas autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Firewall: uma solução de segurança que segrega uma porção de uma rede a partir de outra porção, permitindo que apenas tráfego autorizado passe, de acordo com regras de filtros especificadas.

Gatekeepers: mecanismo para monitorar e proteger os pontos de entrada de um limite de segurança ou *gateway*.

Gateway: equipamento ou ponto de entrada e saída de uma rede de comunicação. Trata-se de um nó de rede que traduz pacotes de informação entre duas redes incompatíveis.

Hackers: invasores de computadores e sistemas. A quebra de segurança de redes é para o *hacker* apenas um desafio, embora o termo às vezes seja usado com sentido pejorativo, quando o correto seria *cracker*.

Host: é uma máquina conectada à internet ou intranet, na qual pode prover a funcionalidade de cliente ou servidor.

IDS: do inglês *Intrusion Detection System*. Um programa, ou um conjunto de programas, cuja função é detectar atividades incorretas, maliciosas ou anômalas.

Integridade: salvaguarda na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.

IP Spoofing: consiste na troca do endereço IP original por um outro, podendo assim se passar por um outro host.

Kernel: parte central de um sistema operacional; à parte do sistema que gerencia a memória, os arquivos e os dispositivos periféricos, mantém a data e a hora, ativa aplicações e aloca os recursos do sistema.

One-Time Password (Senha de uso único): semelhante ao método de desafio e resposta, este método garante que a autenticação seja protegida contra ataques passivos no reenvio de senhas capturadas, conhecidos como ataques de replay.

Patches: pacote de software para atualização, correção de sistema ou segurança.

RW: leitura e escrita.

Servidor: em uma rede, é o computador que gerencia e fornece recursos de software e informações para os demais computadores da rede.

Servidor Spare: servidor utilizado para redundância do servidor primário.

Shellcode: é um grupo de instruções *assembler* em formato de *opcode* para realizar diversas funções como chamar uma *shell* e estabelecer a execução de comandos.

Site ou Website: é um conjunto de páginas que reúne informações ou sistemas de organizações, entidades, pessoas ou instituições.

Sniffer: analisador de tráfego. Software que inspeciona pacotes de dados que circulam pela rede e extrai informações deles.

SNMP: o *Simple Network Management Protocol* é um protocolo usado para monitorar e controlar serviços e dispositivos de uma rede TCP/IP.

Spoofing: prática em que um computador ou alguém envia comandos ou mensagens a outro se fazendo passar por um terceiro.

Switch: é um equipamento que permite numa LAN interligar dois ou mais computadores. Normalmente funciona na layer 2 (Data-link layer) ou na layer 3 (Network layer) já com algumas capacidades de roteamento do modelo OSI. Ao contrário de um *hub*, o *switch* envia os pacotes de dados exclusivamente para o computador de destino e não efetua o *broadcast* para todos os computadores a ele ligados.

Tojan: vide Cavalo de Tróia.

Triggers: gatilho que consiste em uma *Stored Procedure* que é executado em resposta a uma ação ocorrida com determinados dados, como, por exemplo, uma inserção de novos registros.

Upstream: dados transmitidos do cliente para o servidor.

8. REFERÊNCIAS BIBLIOGRÁFICAS

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação – Código de prática para a gestão da segurança da informação.** Rio de Janeiro: ABNT, 2001. (NBR ISO/IEC 17799)

2. BRASILIANO, ANTONIO CELSO RIBEIRO. **Manual de análise de risco para a segurança empresarial.** São Paulo: Sicurezza, 2003.

3. BRASILIANO, ANTONIO CELSO RIBEIRO. **Manual de planejamento. Gestão de riscos corporativos.** São Paulo: Sicurezza, 2003.

4. CARUSO, CARLOS A. A. **Segurança em informática e de informações.** São Paulo: Senac, 1999.

5. GREY, STEPHEN. **Risk analysis for IT projects.** England: Wiley, 1995.

6. MICROSOFT. **Ameaças e contramedidas.**
   Disponível em:
   http://www.microsoft.com/brasil/security/guidance/topics/devsec/secmod75.mspx
   Acesso em: 20 dez. 2004.

7. MICROSOFT. **Modelagem de ameaças.**
   Disponível em:
   http://www.microsoft.com/brasil/security/guidance/topics/devsec/secmod76.mspx
   Acesso em: 20 dez. 2004.

8. MICROSOFT. **Guia de gerenciamento de riscos de segurança.**
   Disponível em:
   http://www.microsoft.com/brasil/security/guidance/riscos/srsgch02.mspx
   Acesso em: 20 dez. 2004.

9. PELTIER, THOMAS R. **Information security analysis.** United States of America: Auerbach, 2001.

10. ROPER, CARL A. **Risk management for security professionals.** Burlington, MA: Butterworth Heinemann, 1999.

11. SÊMOLA, MARCOS. **Gestão da segurança da informação, uma visão executiva.** Rio de Janeiro: Campus, 2002.