GESTÃO DE RISCOS APLICADA A SISTEMAS DE INFORMAÇÃO: SEGURANÇA ESTRATÉGICA DA INFORMAÇÃO

Eduardo Antônio Mello Freitas

2009

UNIVERSIDADE CANDIDO MENDES
PÓS-GRADUAÇÃO "LATO SENSU"
PROJETO A VEZ DO MESTRE

GESTÃO DE RISCOS APLICADA A SISTEMAS DE INFORMAÇÃO: SEGURANÇA ESTRATÉGICA DA INFORMAÇÃO

Por: Eduardo Antônio Mello Freitas

Orientador
Prof. Koffi Djima Amouzou

Brasília
2009

UNIVERSIDADE CANDIDO MENDES
PÓS-GRADUAÇÃO "LATO SENSU"
PROJETO A VEZ DO MESTRE

GESTÃO DE RISCOS
APLICADA A SISTEMAS DE INFORMAÇÃO:
SEGURANÇA ESTRATÉGICA DA INFORMAÇÃO

Apresentação de monografia à Universidade Cândido Mendes como condição prévia para a conclusão do Curso de Pós-Graduação "Lato Sensu" em Gestão Estratégica e Qualidade

Por: . Eduardo Antônio Mello Freitas

AGRADECIMENTOS

Agradeço a Deus e a minha querida esposa que me deram determinação para continuar esta empreitada.

DEDICATÓRIA

Dedico este trabalho a minha esposa e filhos que me apoiaram.

RESUMO

O presente estudo aborda um tema sensível a qualquer empresa inserida em um mercado competitivo: a Segurança da Informação. Neste contexto, a segurança da informação possui posição estratégica tanto para a garantia do presente, naquilo que a empresa já conquistou, como para o futuro, naquilo que ela procura conquistar.

Os sistemas de informação são ferramentas importantes na gestão estratégica do conhecimento das empresas. Eles normalmente dão maior agilidade, versatilidade e disponibilidade da informação, contudo eles também devem garantir que apenas as pessoas autorizadas terão o acesso à informação e saber quem é o responsável pela informação.

Porém segurança implica em custos de manutenção da informação. Sistemas que não levam em conta a segurança são mais simples e mais fáceis de manter, porém quanto custa a perda ou a falta de confiabilidade de suas informações? Podemos dispor de sistemas mais flexíveis, mas sem abrir mão da auditoria destes. Através de modelos como o COBIT e de bibliotecas de melhores práticas como o ITIL, buscaremos identificar o grau de maturidade da empresa e o valor da informação na estrutura gerencial e no poder decisório nos níveis operacional, tático e estratégico.

Finalmente, avaliado o papel estratégico da informação, poderemos mensurar melhor os riscos que estamos dispostos a correr e o quanto devemos investir em prol da segurança e continuidade de negócios da empresa. É a busca por uma posição de maior conforto para a empresa sem deixar de lado a qualidade da informação.

METODOLOGIA

Este estudo foi elaborado com o apoio de pesquisa bibliográfica em livros, revistas, artigos e multimídia, tanto de Tecnologia da Informação como de Administração.

Além dos os recursos apresentados no curso e do material bibliográfico sugerido, fizemos uso de bibliotecas e padrões de melhores práticas que não se limitam à gestão de Tecnologia da informação, visto que a segurança da informação envolve, além da tecnologia, também processos e pessoas. Das bibliotecas ou padrões de melhores práticas destacamos:

- ITIL - biblioteca de infraestrutura de Tecnologia da Informação (TI)
- PMBOK - conjunto de conhecimentos em gerenciamento de projetos
- COBIT – gestão de Tecnologia da Informação (TI)

A ABNT traduziu os documentos ISO 27001 e ISO 27002 e os denominou como NBR ISO 27001 e NBR ISO 27002, respectivamente.

Foram obtidas informações a partir de empresas de consultoria e de pesquisas como o Gartner Group e a Módulo. Algumas fontes de consulta foram recomendações advindas da participação de congressos, tais como o Congresso Nacional de Auditoria de Sistemas e o congresso de Segurança da Informação e Governança.

SUMÁRIO

INTRODUÇÃO

Inicialmente o conhecimento ficava restrito a pessoas ou grupo de pessoas. Em muitos casos o conhecimento ficou perdido na história. Atualmente, temos de filtrar o que é relevante, útil e realmente necessário nesta enxurrada de informações a que somos submetidos. Com tecnologias e sistemas cada vez mais versáteis, nossos dados, informações e conhecimento são mediados pela Tecnologia da Informação. Se por um lado a grande gama de recursos e a flexibilidade que a tecnologia nos fornece é um atrativo, por outro ficamos cada vez mais dependentes dela.

Igualmente as organizações estão cada vez mais dependentes da Tecnologia da Informação. A informação é um ativo não tangível da organização e assim como os ativos tangíveis e financeiros, a organização deve dedicar sua atenção à segurança deste ativo que é a informação que possuem. Falhas e desastres em sistemas de informação podem levar a grandes prejuízos e até à falência de uma empresa.

Cartões de crédito, Internet e globalização potencializaram as relações comerciais entre empresas por meio eletrônico, de forma que a segurança não é apenas uma preocupação da empresa, mas também do cliente ou consumidor. De forma que a própria segurança pode agregar valor ao negócio e a segurança da informação passou a ser parte da estratégia do negócio ou serviço, podendo se traduzir em lucro, aumento de competitividade e fator de redução de perdas. A segurança da informação não pode mais se ater apenas ao nível operacional, mas deve passar para os níveis estratégicos e táticos.

A informação, no sentido geral, é insumo e produto, material de consumo e produto, isto porque ela não deve nunca estar desassociada do todo da atividade do negocio. Esta participação se faz refletir nos sistemas de

informação e devem ser devidamente incluídos no método de custeio da organização. A preocupação com a análise de riscos se fez observar no resultado das pesquisa por segmento, onde as empresas foram solicitadas a escolher as três principais medidas em Segurança da Informação de seu planejamento anual (MÓDULO, 2006):

- **Comércio:** Política de segurança; Análise de riscos no ambiente de TI; Capacitação da equipe técnica.
- **Financeiro:** Adequação às Normas, Regulamentações e Legislação; Análise de riscos no ambiente de TI; Certificado digital.
- **Governo:** Campanha de sensibilização e responsabilização de funcionários; Análise de riscos no ambiente de TI; Adequação a Normas, Regulamentações e Legislação.
- **Indústria:** Análise de vulnerabilidades; Análise de riscos no ambiente de TI; Campanha de sensibilização e responsabilização de funcionários.
- **Serviços:** Análise de riscos no ambiente de TI; Análise de vulnerabilidades; Política de segurança.
- **Telecomunicações:** Adequação às Normas, Regulamentações e Legislação; Análise de riscos no ambiente de TI; Plano de continuidade.

A Tecnologia da Informação deve efetivamente contribuir para minimizar as perdas e potencializar os investimentos. Por outro lado, a Gestão de Riscos e seu planejamento deixou de ser apenas técnica e requer dos demais gestores o compromisso para com a informação. É no trabalho de equipe, com uma cultura de controle de riscos em todos os níveis da organização, que serão encontradas as melhores alternativas para se manter a segurança da informação de forma compatível com seu valor dentro da organização.

CAPÍTULO I - QUANTO VALE A INFORMAÇÃO

"Se você pensa que segurança custa caro, experimente um acidente."
(Stelios Haji-Ioannou)

Quando pensamos em segurança juntamente nos vem a idéia de que algo de valor deve ser guardado ou assegurado. Há algo de valor que não se quer perder e vale a pena investir a fim de se obter esta garantia. Tal qual um seguro de automóvel, podemos selecionar que serviços estamos dispostos a pagar por ele e quanto, assim como podem existir serviços que se colocam como obrigatórios no seguro.

> "Podemos definir Segurança da Informação como uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade" SÊMOLA (2003, p.43)

Trataremos do valor de forma geral, envolvendo a sensibilidade da informação e sua criticidade para as operações do negócio.

1.1. O valor da informação e o tempo

O valor de uma informação ou conhecimento muda com o tempo e possui uma validade. Um manual de um software, por exemplo, pode ser de grande valia e ser bastante utilizado, contudo, em se tornando obsoleto, ele praticamente passa a não ter valor algum. O referido manual pode ter algum valor histórico, mas com certeza o custo operacional e o custo dos recursos despendidos para o seu armazenamento devem ser compensadores. Em alguns casos, a definição do tempo em que a informação deve ser mantida se dá por conta de alguma norma ou dispositivo legal.

A tabela a seguir apresenta alguns prazos em que há a obrigatoriedade de guarda dos documentos por parte da empresa em conformidade com a Lei nº10.406/2002, o Novo Código Civil Brasileiro:

DOCUMENTO	PRAZO
Contratos de seguro em geral	1 ano
Comprovantes de pagamento de aluguéis	3 anos
Dívidas líquidas oriundas da contratação por meio de instrumento público ou particular	5 anos
Documentos comprobatórios do recolhimento de tributos e tarifas	5 anos
Comprovante da prestação de serviços de profissionais liberais	5 anos
Documentação trabalhista relacionada ao vínculo empregatício	5 anos
Documentação trabalhista referente aos encargos da previdência e FGTS	30 anos – seguradas 35 anos - segurados

Tabela I – Prazos de Guarda de Documentos - Lei nº10.406/2002

Pode-se alegar que se tratam de prazos para a guarda dos documentos originais em papel, contudo se faz necessário observar que, de acordo com a Medida Provisória nº 2200/2001, um documento digital ou eletrônico, público ou particular, deve ser considerado para todos os fins legais. Assim sendo, documentos assinados eletronicamente através de Certificados Digitais emitidos pelas Autoridades Certificadoras no âmbito da ICP-Brasil (Infraestrutura de Chaves Públicas Brasileira) possuem a mesma eficácia de uma assinatura de próprio punho. A confirmação da autenticidade assinatura digital no documento é feita pela da informação. O Decreto Federal nº 4.553/2002 define autenticidade como: “asseveração de que o dado ou informação são verdadeiros e fidedignos tanto na origem quanto no destino”.

A falta de planejamento do ciclo de vida da informação irá se refletir em erros na estimativa dos recursos necessários para a segurança e no

armazenamento da informação, o que poderá redundar em desgaste da equipe e prejuízos tanto na aquisição dos equipamentos quanto na manutenção da informação. Esta estratégia reforça ainda mais o ciclo de melhoria continua, também conhecido como ciclo de Deming ou ciclo PDCA (Plan, Do, Check, Action).

É interessante observar que, a depender da arquitetura do sistema de informação o gerenciamento do armazenamento dos dados, conforme a sua utilização, pode vir a ser transparente para os usuários do sistema. Nestes casos, por exemplo, dados com pouca ou nenhuma atualização, ou ainda com utilização mínima, podem ser mantidos em meios preferencialmente pouco voláteis, seguros, porém menos dispendiosos. A recuperação da informação pode ser um pouco mais lenta, porém a periodicidade do acesso justifica a menor desempenho e os menores gastos com manutenção operacional, desde que sua criticidade seja baixa. Há de se considerar, portanto, em termos de tempo, não apenas o custo do processamento da informação, mas também o custo de recuperação da mesma e seu impacto no negócio.

Assim, tanto o tempo passado quanto ao futuro podem influenciar a informação. O tempo passado é o tempo a que se refere a informação e o seu valor no presente. O tempo futuro é o tempo entre a necessidade da informação e a sua obtenção. Se, por exemplo, se um sistema de informação que apresenta cotações atualizadas de produtos no mercado fica for a do ar, a indisponibilidade das informações pode acarretar prejuízos enormes à empresa e perda de clientes. Ao tempo passado se costuma designar de validade da informação; ao futuro, propriamente o valor da informação.

O planejamento da capacidade de armazenamento e gerenciamento do valor da informação no decorrer do tempo deve levar em contar que, com o passar do tempo, maior qualidade é exigida da informação e menores os custos de armazenamento. Por outro lado, um volume cada vez maior de informação e a degradação no acesso por conta da vida útil dos servidores

exigem um acompanhamento constante da performance e da garantia da qualidade dos recursos de suporte (CCTA, 2000) .

1.2. O valor da informação e o público-alvo

Diz um ditado que o conhecimento vem da informação, mas que a sabedoria é o seu correto uso. Nem toda a informação possui o mesmo valor e este valor vai depender de se saber como fazer uso da informação.

O valor da informação também pode variar segundo o seu público-alvo dentro e fora da organização. Dentro da organização podemos considerar os três diferentes níveis de tomada de decisão, quais sejam: operacional, tático e estratégico. Normalmente os dados pontuais do nível operacional serão agrupados, filtrados e analisados como informação do nível tático e que irão evoluir para o conhecimento e aporte à tomada de decisões no nível estratégico (RUD, 2001).

Contudo, a ênfase em processos horizontais com mais decisões sendo delegadas àqueles mais voltados ao nível operacional e tático da organização levou a uma necessidade maior de comprometimento de todas as partes da organização. Seja como for, toda a cadeia de transformação por que passa a informação, de uma forma ou de outra, é responsável por ela. Somos responsáveis tanto pela informação como pelo uso que fazemos dela. Cada nível decisório tem a sua percepção de valor para a informação. Contudo, a informação como qualquer outro ativo da organização deve ter um responsável, um proprietário, conforme expresso na NBR ISO/IEC 17799:2005, no capítulo sobre Gestão de Ativos. Este proprietário, responsável pela informação, é quem irá definir a classificação da informação, quais os controles necessários e quais recursos estão associados à ela.

Uma informação pode ter tal valor estratégico ou papel crítico em uma organização que venha a ser classificada de forma tal que apenas o Presidente, e aqueles que lhe são próximos na organização, podem tomar ciência dela. É a classificação por hierarquia ou autoridade (VACCA, 2005).

Por tudo isto é primordial que as políticas de controle de acesso sejam bem definidas e contem com o aval e apoio da alta direção. Conflitos entre a política de segurança e as operações de manutenção contínua e emergência que zelem pela continuidade do negócio não devem ser ignorados. As políticas de segurança não podem ser incompatíveis com a garantia da disponibilização do serviço.

1.3. Evolução do valor da informação

O Gartner Group, equipe especializada em pesquisas de mercado e consultoria envolvendo a área de Tecnologia da Informação, atribuiu o termo *Business Intelligence* (Inteligência Empresarial ou de Negócios) para designar metodologias e ferramentas de gestão que se fazem através de software com o objetivo de estruturar a cadeia de transformação da informação e sua aplicação nas ações decisórias da empresa.

Relações entre dados outrora desconhecidas, ao surgirem, mostram novas contribuições para o conhecimento. Este conhecimento pode contribuir para diferentes áreas dentro da organização através da aplicação destas ferramentas de gestão. Dentre estas contribuições temos a análise dos níveis de risco, que pode incluir diferentes perspectivas, tais como o risco financeiro na relação com um novo cliente ou na aquisição de uma carteira de ações, bem como o comportamento inesperado de um sistema. Este último, interesse da Gestão de Riscos.

Através de métodos estatísticos, tais como regressão linear e a regressão logística, ou ainda de métodos não-estatísticos ou mistos, tais como árvores de classificação, algoritmos genéticos, redes neurais e árvores de decisão (RUD, 2001), de forma a identificar padrões de comportamento, correlacionar os dados, detectar seqüências e tendências no decorrer do tempo. Uma destas técnicas é conhecida como *Data Mining* (prospecção de dados), extraindo-se comportamentos e conhecimentos do negócio a partir de grandes bases de dados, os quais, de outra forma, provavelmente permaneceriam desconhecidos.

Estas novas relações e comportamentos irão demonstrar a real necessidade da informação e auxiliar na classificação da informação, tanto do valor como dos riscos que envolvem a informação. O valor será maximizado quando a administração for capaz de definir estratégias e objetivos para alcançar a melhor relação entre o seu crescimento, o sucesso qualitativo e a identificação dos riscos relacionados (PRICEWATERHOUSECOOPERS, 2004).

1.4. Segurança da informação agregando valor à informação

Há uma expressão que diz: “Crie uma ratoeira melhor e o mundo achará o caminho até sua porta”. Podemos observar que a Tecnologia da Informação pode, não apenas dar suporte ao processo de transformação da informação, mas pode também lhe agregar valor.

A biblioteca consolidada de melhores práticas ITIL (*Information Technology Infrastructure Library*), em sua segunda versão publicada, teve o seu foco no alinhamento entre a Tecnologia da Informação e os negócios. Já em sua terceira versão, a biblioteca ITIL passou a ter o foco na integração de ambos, visto que a integração da gestão da Tecnologia da Informação e do

negócio da empresa se reflete em mudança nos conceitos das melhores práticas aplicadas à Tecnologia da Informação.

Um dos mais novos conceitos é o de Ciclo de Vida de um serviço, que passa desde a sua necessidade, a estratégia e projeto do serviço, até a extinção do serviço. O investimento e a manutenção da segurança da informação se justifica a partir da identificação de sua real da necessidade estratégica. Os sistemas de informação devem contribuir para que a informação traga segurança ao próprio negócio.

No modelo tradicional da publicação da ITIL v.2, representado na figura a seguir, o Gerenciamento da Segurança, fica posicionado entre o Gerenciamento do Serviço, o Gerenciamento da Infraestrutura de Tecnologia da Informação e Comunicação e o Gerenciamento da Aplicação (BON, 2006).

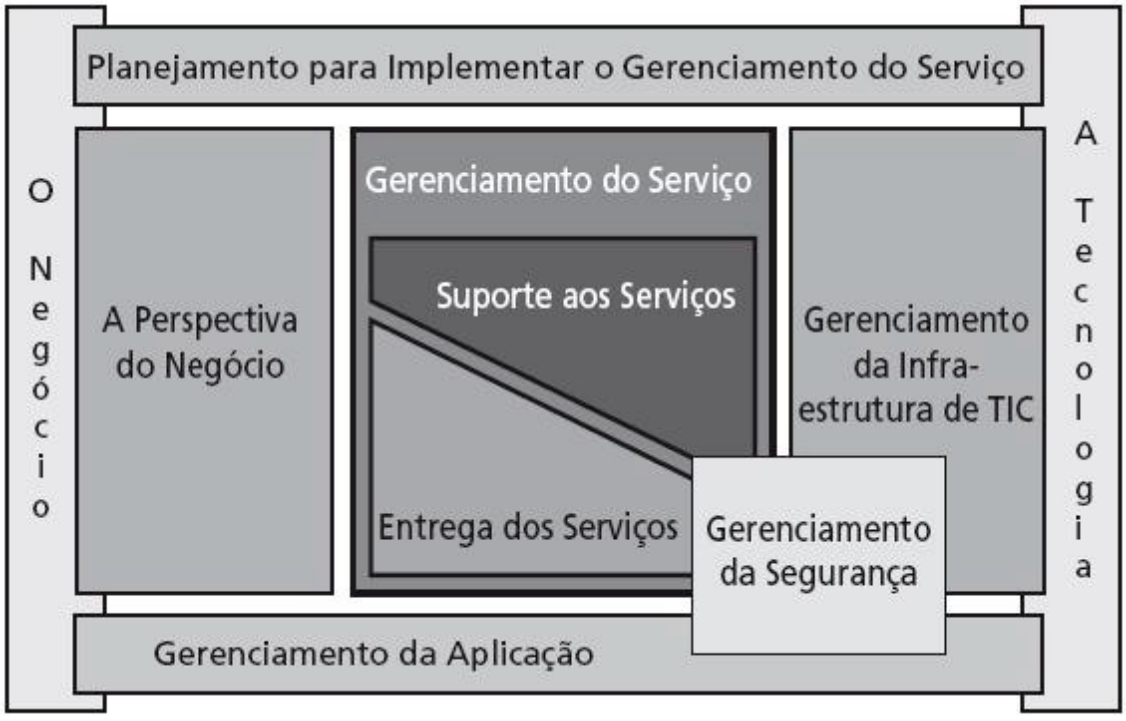

Figura 1 – Modelo ITIL versão 2
Fonte: Citação de Jan Van Bon ao modelo da biblioteca ITIL, 2006

Em termos estratégicos, a segurança da informação pode agregar valor ao dar maior confiabilidade ao próprio processo de transformação. A integração entre o negócio e a tecnologia empregada pode imprimir maior maturidade e solidez às transações com o cliente. A confiabilidade nas transações vai se traduzir na idéia de maior confiabilidade nos negócios.

Faz-se necessário que os executivos de negócio (*Chief Executive Officers - CEO*) e os de Tecnologia da Informação (*Chief Information Officers - CIO*) tenham uma visão alinhada e integrada para a obtenção dos resultados esperados. Para que haja este alinhamento, o foco da entrega de serviços, incluindo-se a segurança da informação, não deve perder a perspectiva do negócio. O sucesso desta conscientização leva à maximização dos benefícios para o negócio (CARTLIDGE, 2004).

Novas atribuições profissionais surgiram por conta do enfoque em segurança e na precisão da informação e seu impacto nos negócios, tais como o CISO – *Chief Information Security Officer* e o CSO – *Chief Information Officer*.

Para se ter sucesso na integração e alinhamento entre o negócio e a Tecnologia da Informação, deve haver integração e alinhamento a partir do planejamento estratégico e suas metas (CARTLIDGE, 2007, 4). Como nem os negócios, nem a tecnologia da informação são estáticos, um processo de melhoria contínua com gestão integrada das mudanças dos negócios de TI é a forma de se garantir a durabilidade do alinhamento e da integração.

A informática sempre foi vista como ferramenta de melhoria. Porém, quando se fala em Segurança da Informação, alguns aspectos são vistos de forma negativa no processo, tais como aumento de custos, perda de liberdade, aumento de complexidade, perda de desempenho, etc. É primordial que haja medição e controle da eficiência e da eficácia dos serviços de tecnologia da informação. Também não se pode deixar de lado a otimização dos custos na

obtenção do resultado final. Contudo não se pode negar que de fato a proteção dos ativos informacionais custa dinheiro e que a segurança naturalmente traz restrições. Por isso a importância de se classificar a informação, a fim de que não se adote um único nível de segurança no seu patamar mais alto (BEAL, 2008, 61).

Os gestores de TI devem ser capazes de demonstrar o valor agregado com a segurança. De fato, nem sempre é possível demonstrar o retorno do investimento em segurança da informação em termos de lucro, mas através da análise da classificação da informação e da gestão de riscos será possível demonstrar o quanto se deixou de perder caso algum desastre ocorresse, ou alguma informação confidencial fosse revelada ou mesmo um sistema crítico ficasse fora do ar. O custo da segurança da informação nunca deve ser maior do que o valor da própria informação!

A segurança da informação deve, portanto, integrar a estratégia do negócio ou serviço, devendo se traduzir em lucro, ganho de competitividade ou confiabilidade no mercado. Diante da falta de gestão de riscos em TI, deve-se refletir na afirmação de Bob L. Martin, CEO[1] da Divisão Internacional do Wall-Mart, em artigo da Harward Renew de setembro de 1995: “os riscos da Tecnologia da Informação estão cada vez mais entrelaçados com os riscos empresariais”.

1.5. O custeio da Segurança de Informação

A análise de custo em Tecnologia da Informação às vezes não é uma tarefa simples, ainda mais quando se trata da segurança da informação. Nem todos os custos são diretos. Um sistema mais seguro, por exemplo, pode exigir mais passos para o seu acesso, cadastramento, treinamento e

[1] Chief Executive Officer – Gerente Executivo

certificações. Destacamos dois métodos de custeio que têm o seu uso em serviços de Tecnologia da Informação: ABC e TCO.

O método de custeio ABC (*Activity Based Costing*), desenvolvido pelos professores Robert Kaplan e Robin Cooper, é um exemplo de método bastante útil quando se trata de custeio de serviço, levando em conta os custos indiretos de uma atividade. Nele as atividades são as interligações entre os insumos e os produtos (NUNES, 1998, p.14). Identificada a atividade, deve-se quantificar a relação entre as atividades e as informações que servem de insumo. Apesar de que em alguns casos a própria informação é o produto. O ideal é que a os responsáveis e usuários da informação, bem como a intensidade de seu uso sejam quantificados.

A que atividades interessa a entrada de dados, seu armazenamento e a garantia de sua segurança? Pode-se quantificar o custo adicional exigido para prover a segurança da informação, mais o consumo vigente dos recursos de infraestrutura, para certa atividade, seja através de valor determinado ou de valor estimado por período. Já na quantificação da relação entre a atividade e o produto final, serão necessários atributos para a atividade, tais como o tempo de processamento e o volume de transações. De qualquer forma, a identificação dos objetos de custeio e os responsáveis pelas atividades irá proporcionar o detalhamento e o rateio dos custos, o que pode ser aplicado à segurança da informação e dos serviços de TI em geral.

A análise de custos algumas vezes não é fácil, porém quanto mais detalhada puder ser a classificação dos custos, maior será a identificação das relações de valor entre a informação e os agentes do negócio.

Outro modelo, desenvolvido por Bill Kirwin, do Gartner Group, é o *Total Cost of Ownership* (Custo Total de Propriedade), que também leva em conta os custos diretos e indiretos por períodos de tempo O foco não está no rateio, mas no custo total da aquisição de um produto ou serviço, incluindo hardware,

software, treinamento, taxas, imposto, adaptação dos sistemas legados, etc. O seu aspecto mais interessante é o de permitir a avaliação do investimento total de uma solução comparando-o com outras soluções também pelo seu custo total. Para isto é importante munir-se de *benchmarks*[2] fornecidos por empresas de pesquisa e consultoria na busca da solução com melhor desempenho adequado à situação em estudo comparativamente com soluções encontradas em outras empresas de reconhecimento no mercado.

[2] O benchmarking se constitui em identificar, otimizar e utilizar o que deu certo em empresas similares.

CAPÍTULO II – O CONTROLE SOBRE A INFORMAÇÃO

O sucesso de qualquer política é medido pelas catástrofes que não ocorrem. (Parkinson)

Existe um termo que é traduzido por “rastreabilidade” que é definido pela *International Organization for Standardization* em seu padrão ISO 8402/1994 como:

> a habilidade de descrever a história, aplicação, processos ou eventos e localização, de um produto, a uma determinada organização, por meios de registros e identificação

Este conceito se aplica muito bem à informação enquanto produto que advém da coleta e armazenamento de dados em direção à construção do conhecimento. A qualidade da informação irá depender da qualidade dos dados e dos processos e condições definidos em sua transformação. Quem alimentou o sistema de informação com aqueles dados? Por que transformação ele passou? Quem é o responsável pela informação? Posso ter certeza de que esta informação é correta?

2.1. Princípios de Segurança da Informação

Conforme a NBR 17799/2003, os princípios básicos para que uma informação seja considerada segura, são:

- Integridade: propriedade de salvaguarda da exatidão e da totalidade do conjunto de ativos.

- Disponibilidade: propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
- Confidencialidade: propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados.

Além destas características, estão presentes na NBR ISO/IEC 27001:2006 outras, as quais já foram ou serão discutidas no decorrer deste trabalho, tais como:

- Legalidade
- Responsabilidade
- Autenticidade
- Autoridade
- Não-repúdio
- Auditoria

2.2. Qual a origem dos dados?

Para a identificação da origem dos dados deve ser possível identificar o usuário. Sistemas que precisam ser abertos ao público em que o usuário é anônimo devem permitir apenas envio de mensagens ou o acesso necessário à divulgação ou marketing do produto, conforme o caso. Pode-se achar que, nestes casos a segurança seria nula, mas na verdade o acesso é que deve ser mínimo. Um usuário anônimo, por exemplo, não deve ser capaz de alterar a página da sua empresa na Web.

Autenticar é verificar se a pessoa é quem ela afirma ser. A autenticação faz uso de uma informação que se julga que apenas a pessoa correta possui (NIZAMUTDINOV, 2005). Normalmente cada usuário cadastrado possui individualmente um código e uma senha. Esta senha pode ser digitada ou pode vir da captura de algum dado biométrico, tal como voz, digital, etc. No caso do reconhecimento biométrico é possível o uso apenas do dado biométrico para a autenticação, mas a segurança fica a depender mais da capacidade de processamento, qualidade do dado biométrico e do algoritmo usado. Já a autorização é verificar se um usuário tem o direito de executar uma determinada ação ou se tem acesso a determinados dados. A autorização é normalmente precedida por autenticação (NIZAMUTDINOV, 2005).

Identificado ou não o usuário, o sistema de informação deve ser capaz de estabelecer o controle de acesso a este usuário. Esta é a medida mais importante para a proteção da informação (BEAL, 2008). O ideal é que a própria existência do controle de acesso venha a dissuadir o mau uso do sistema.

O controle de acesso é necessário à proteção da confidencialidade, integridade e disponibilidade à informação (STEWART, 2008). Aqui disponibilidade a informação representa o direito de acesso à informação, processo ou recurso. Na ISO 17799 existe a premissa de que “tudo deve ser proibido a menos que expressamente permitido”.

O controle de acesso é algo que deve ser sempre revisto. Seja pelo proprietário da informação, como já dissemos, seja pelos responsáveis pelo sistema de informação. Um funcionário demitido não deve ter mantido seu código de acesso habilitado. Os papéis no sistema devem condizer com os

papéis no negócio. É o que na ISO 17799 se determina de requerimentos do negócio para o controle de acesso.

Ainda que não seja o proprietário da informação que dê a entrada dos dados, ele não deve deixar de existir. Devem haver procedimentos formais previamente definidos que incluam as responsabilidades, o uso devido da informação, a complexidade de senhas e os papéis de cada um (NBR ISO/IEC 27001:2006). Pode ser útil a criação a construção de uma matriz de acesso às operações ou informações. Ela permite visualizar o que um usuário ou grupo de usuários está autorizado a fazer ou acessar.

2.3. Classificando os Níveis de Segurança

O Departamento de Defesa americano criou o modelo Bell-LaPadula voltado à classificação da informação, definindo diferentes níveis na política de segurança. As classificações são similares ao que foi decretado no Brasil, Decreto nº 4.553/2002, quais sejam:

- Ostensivo: sem classificação, cujo acesso pode ser franqueado.
- Ultra-secreto: dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado
- Secreto: dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes,

programas ou instalações estratégicos, cujo conhecimento não autorizado possa acarretar dano grave à segurança da sociedade e do Estado.

- Confidencial: dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
- Reservado (que corresponde ao restrito nos EUA): dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Há de se observar que no Decreto nº 4.553/2002 houve reclamações de que o ex-presidente Fernando Henrique Cardoso aumentara os prazos do sigilo para todos os documentos que exigem segurança em relação ao Decreto nº 2.134/1997. Este fato gerou reclames da sociedade em relação à democratização das informações e se refletiu no Decreto nº 5.301/2004, promulgado pelo então Presidente Luís Inácio Lula da Silva. Este aspecto está definido para os órgãos públicos, mas vale considerar a questão para a organização, ainda que ela não tenha relação com questões de segurança nacional: Por quanto tempo uma informação classificada como secreta deverá manter o seu sigilo?

As *Executive Orders*[3] 12356 e 12958, por Ronald Reagan e Bill Clinton, respectivamente, resumiram, para fins de segurança nacional apenas ultra-secretos, secretos e confidencial. Tanto no que se refere aos decretos supracitados como nas Executive Orders, existe a definição específica de algumas autoridades que tratam dos documentos ultra-secretos reforça o envolvimento da alta direção das organizações na classificação dos níveis gerais de segurança.

O guia de estudo para a certificação CISSP[4] nos apresenta duas regras gerais de controle de acesso e o nível de confidencialidade de uma informação que são obrigatórias no modelo Bell-LaPadula:

- usuário que está em um nível de segurança não pode ter acesso a um nível superior de segurança
- usuário que está em um nível de segurança não gravar informação de seu nível em um nível inferior de segurança

Outros modelos foram criados para instituições não militares com foco na integridade da informação, tal como o modelo Biba, com o foco na integridade da informação, ao invés da confidencialidade. Já o modelo Clark-Wilson é voltado à aplicações comerciais, fazendo uso de um triplo controle de acesso: sujeito (ou usuário), programa e objeto, onde o usuário somente pode ter acesso aos objetos através dos programas e o controle vem a partir desta relação. Não se deve confundir a confidencialidade com a privacidade. Um documento pode ser privativo de pessoa ou grupo de pessoas. A confidencialidade tem mais a ver com o tipo de atividade ou papel hierárquico decisório.

2.4. Segregação de Funções e Redes de Comunicação

Outro modelo de classificação e controle da informação é o de Brewer e Nash, o qual busca identificar as situações e conflitos de interesses, de acordo com os papéis que o usuário pode ter, sendo de mais difícil controle quando a base de dados não é unificada.

---

[3] Ordens o Poder Executivo dos Estados Unidos da América de caráter regulatório.
[4] Certified Information Systems Security Professional

Sobre a questão da segregação de funções o Tribunal de Contas da União o define como “princípio básico do sistema de controle interno que consiste na separação de funções, nomeadamente de autorização, aprovação, execução, controle e contabilização das operações”. O seu propósito é reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional dos ativos da organização.

No Manual de Auditoria de Sistemas do TCU[5] é recomendado que a segregação de funções exista, inclusive, na equipe de Tecnologia da Informação. Aqueles que testam o sistema devem ser diferentes daqueles que o desenvolvem, por exemplo.

Em se tratando dos processos de um órgão público, por exemplo, a liquidação de uma despesa não pode ser feita pelo gestor financeiro ou pelo ordenador da despesa. O Acórdão nº 330/2005 do TCU exige até mesmo que haja segregação entre a fase de habilitação e a fase de avaliação das propostas técnicas em envelopes separados.

A segregação de redes, tal como uma restrição física às informações, contribui no sentido de prevenir o acesso não autorizado a um serviço de rede e melhor monitorar grupos de usuários e sistemas de informação (NBR ISO/IEC 27001:2006).

[5] TCU – Tribunal de Contas da União

2.5. Conscientização da Importância da Segurança da Informação

A classificação de níveis de segurança não é imutável, devendo haver um acompanhamento contínuo dos processos e seus riscos com o passar do tempo. É algo que deve fazer parte da cultura da organização (BEAL, 2008).

As classificações contribuem para a percepção dos riscos e valores envolvidos nos negócios. Aspectos como a criticidade da disponibilização de um serviço ou informação também deve fazer parte da classificação. Sendo importante a representação numérica na classificação a fim de auxiliar a gestão de riscos (WESTERMAN & HUNTER, 2008).

Na ITIL, a definição de quão rápido deve ser ou não a restauração e o efetivo retorno à normalidade de um serviço deve ser definido no Acordo do Nível de Serviço (ANS) que deve ser feito entre o departamento de TI e o cliente. A rapidez da resolução é diretamente proporcional ao custo da solução.

O envolvimento maior de todos os executivos da organização tem se tornado uma exigência graças ao caráter mais normativo que vem assumindo a segurança da informação, deixando de ser apenas uma questão técnica,. O Novo Código Civil traz maior responsabilidade aos administradores das empresas e autoridades do Governo. Os gerentes de segurança e riscos precisam se relacionar cada vez mais com os departamentos de sua organização, não apenas com Tecnologia da Informação e Auditoria. Há cada vez mais aspectos jurídicos e de recursos humanos envolvidos.

Segundo a 10ª Pesquisa Nacional de Segurança da Informação da Módulo, empresa especializada em Gestão de Riscos, publicada em 2008, a falta de conscientização (55%) é citada como o principal obstáculo para a implementação de segurança da informação, seguida da falta de orçamento (28%).

2.6. Auditoria e Monitoramento da Informação

Os sistemas de informação devem guardar a origem da informação. Esta informação pode ser nova, modificada ou vir a ser excluída. Ao histórico destas operações damos o nome de trilhas de auditoria, contendo basicamente o usuário, a data da operação, o objeto da operação e o tipo de operação.

Na fase de testes do sistema é esperado que o sistema contemple os requisitos para os quais foi constituído. Uma boa prática é desde o nascedouro prover informações sobre os processos e o manuseio dos registros de dados.

Trilhas de auditoria pode se fazer necessárias por algumas razões:

- informação relevante ao negócio
- responsabilização
- detecção de comportamento que levante suspeitas

A documentação do sistema e o conhecimento da atividade são de grande relevância para a avaliação dos sistemas de informação e de sua segurança. Contudo o acesso às informações fora dos sistemas também deve

ser avaliado. Uma informação pode ser privativa pelo sistema, contudo podem existir vulnerabilidades na base de dados que permitam o acesso direto com direito de gravação fora da aplicação padrão.

Na definição do conteúdo das trilhas de auditoria deve-se levar em conta o volume de transações, pois a inclusão de dados de auditoria pode significar grande consumo de recursos. O impacto na aplicação deve ser justificável diante do impacto e da relevância do negócio. Porém elas somente possuem valor se podem se não puderem ser corrompidas. Se não houver garantia de que aquele que registra os dados não pode alterar o histórico os eventos de atualização sofridos pela informação, esta trilha não é confiável. O sistema de informação em si é alvo de auditoria. No caso de teste do sistema, de acordo com a norma ISO 17799, deve ser provida cópia da trilha de auditoria do uso das operações do sistema. Inclusive, as concessões e revogações de contas em sistemas deve ser auditada.

Em alguns casos, recomenda-se a gravação de cópias de arquivos de logs ou trilhas de auditoria. As trilhas podem ser replicadas em uma base de dados centralizada ou em um sistema de diretórios centralizado com restrições de acesso.

Freqüentemente se pensa em auditoria com referência a um evento, mas ela pode também dizer respeito a um estado como resultado de um somatório de eventos, como é o caso de medidas de desempenho, ao que comumente se chama de monitoramento. Nestes casos são definidos espaços de tempo para o monitoramento de acordo com as atividades em estudo.

A perda de desempenho de um sistema pode ser o objetivo de uma invasão externa e pode acarretar em prejuízo para a organização.

Temos, também, a necessidade do monitoramento constante da conformidade do serviço de TI com os requisitos do negócio. Auditorias podem ser tanto internas como externas. Seja como for, o uso de *frameworks* (estruturas) padronizadas como o COBIT (Controle para a Informação e Tecnologias Relacionadas) tem sido cada vez mais populares para processos de TI. Organizações que estão iniciando em gestão de riscos normalmente o fazem a partir dos resultados da auditoria (WESTERMAN & HUNTER, 2008). Por conta disso, recomenda-se a utilização das melhores práticas aproveitando o resultado da experiência de outros nesta área, evitando-se também riscos desnecessários.

CAPÍTULO III – AMEAÇAS E VULNERABILIDADES

" Nenhum trabalho de qualidade pode ser feito sem concentração e auto-sacrifício, esforço e dúvida."
(Max Beerbohm)

O executivo de negócios nem sempre entende as ameaças por quais passa a informação em um Sistema de Informação. Este capitulo não se propõe a abordar todos os tipos de ameaças ou vulnerabilidades e seus correspondentes mecanismos de controle, mas intenta sensibilizar os responsáveis pela necessidade da segurança da informação e da gestão de riscos.

A auditoria de sistemas é um grande aliado na análise de ameaças e vulnerabilidades, pois confronta os sistemas de informação com normas técnicas de melhores práticas em segurança da informação e analisa os procedimentos e as trilhas de auditorias dos sistemas.

Os tipos de ameaças e vulnerabilidades irão variar conforme o ambiente interno e externo da organização. A infraestrutura de dados e de comunicação utilizada, a organização dos processos, a cultura de segurança dos usuários, o apoio da direção à política de segurança da informação, a competitividade do mercado, a visibilidade da organização, tudo isso são fatores a serem considerados.

Identificar os riscos importa em identificar as ameaças e as vulnerabilidades que podem ser aproveitadas por estas aos sistemas de informação envolvidos e o impacto que as perdas de confidencialidade, integridade e disponibilidade podem causar aos ativos .

3.1. Identificação das Vulnerabilidades e Ameaças

Não existe ambiente totalmente seguro. Independentemente de todo o aparato tecnológico, sempre haverá o elemento humano. As melhores ferramentas até então conhecidas podem ter sido aplicadas, mas nem todas as vulnerabilidades são conhecidas em um momento específico no tempo.

As vulnerabilidades são pontos em que o sistema é susceptível a ataques. Consideramos aqui também, além das fragilidades do sistema, erros que nele existam. A identificação das vulnerabilidades técnicas nem sempre é trivial, requerendo, em geral, profundo conhecimento de Tecnologia da Informação e de Comunicação.

Houve um período de bastante divulgação da existência de “ovos de páscoa” dentro de programas de prateleira como as ferramentas do Microsoft Office e o sistema operacional Windows 95. Após uma seqüência de comandos era possível ver uma apresentação programa escondida dentro do Windows 95 (TABER, 1998). De fato, normalmente a maioria dos usuários utilizam muito pouco de todas as funcionalidades dos softwares que adquiriram.

Contudo, diversas são as vulnerabilidades associadas a procedimentos ou ao comportamento humano. A questão das senhas é um bom exemplo. É fácil entender que, quanto mais complexas as senhas, mais difícil se torna a descoberta delas. Porém, na mesma proporção, mais difícil se torna decorá-las. Uma única senha igual para todos os sistemas facilita a memorização, mas por outro lado se traduz em uma vulnerabilidade que afeta todos os sistemas em questão. Outra alternativa encontrada por algumas pessoas quando a senha é muito complexa é anotar a senha em algum papel. A vulnerabilidade da senha é acrescida pela vulnerabilidade do acesso ao papel com a senha!

A exigência de atualização de senha, apesar de incômoda, contribui para com a segurança da informação.

Em alguns casos é possível se fazer passar por outro no sistema sem o conhecimento, consentimento ou sem que haja falha de procedimento por parte do usuário, mas sim, por conta da baixa qualidade da segurança do sistema ou da falta de utilização de recursos de segurança disponíveis. Uma transação sensível que não seja através de canal ou protocolo de comunicação seguro é uma vítima fácil.

Na figura a seguir vemos a tela de um *sniffer* executado em meu computador. Trata-se de um programa que "fareja" o que passa pela rede. Com ele é possível interceptar a comunicação "ouvida" pelo dispositivo conexão com a rede, normalmente a placa de rede.

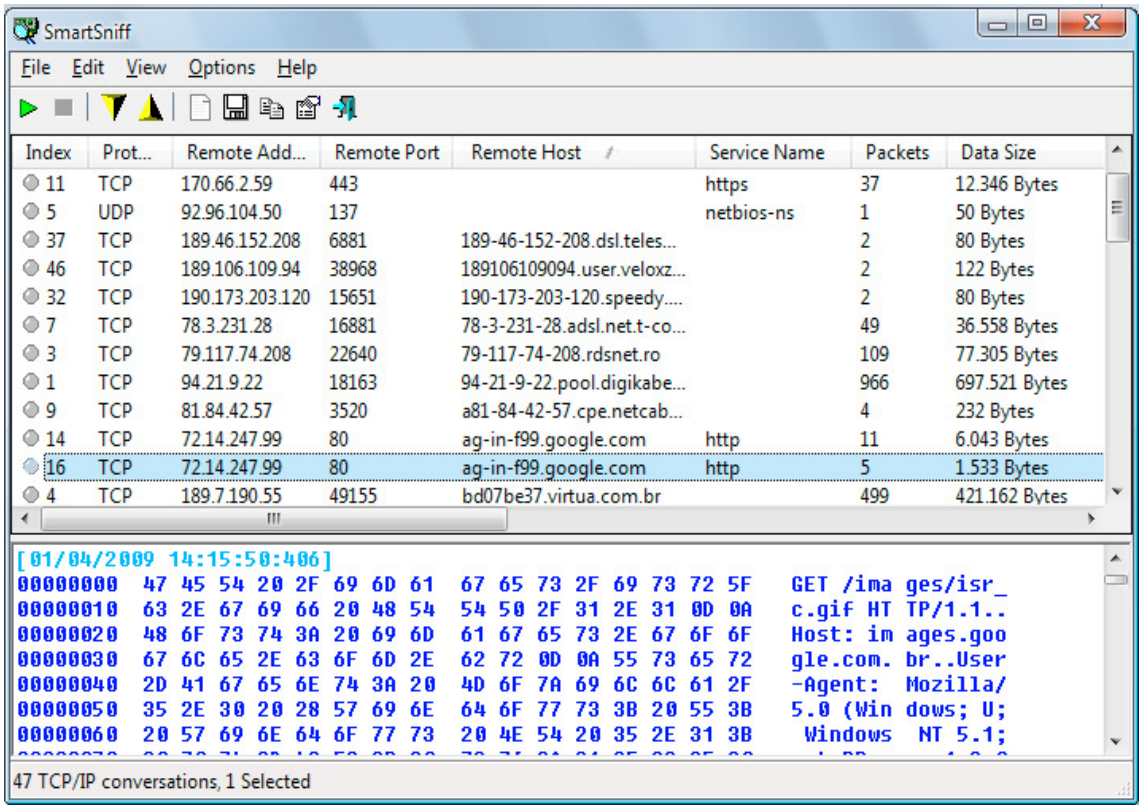

Figura 2 – Tela do programa SmarSniff v.1.4 da Nir Sof apresentando dados de meu computador

Neste exemplo, usei o Firefox para navegar na Internet, que aparece identificado como Mozilla no quadro inferior. Fiz pesquisa de imagem no sítio de buscas do Google (protocolo http) e abri uma conexão segura com o de um banco (protocolo https). Informações como estas podem estar disponíveis a quem possuir o acesso à conexão de rede que se quer analisar ou invadir.

Nas recomendações “Boas Práticas em Segurança da Informação” do TCU, vemos os motivos para o cuidado especial com alguns arquivos. Além dos cuidados já citados, destacamos a preocupação com os seguintes arquivos:

a) Arquivo de Senhas – é um ponto nevrálgico de qualquer sistema. Minha prática tem sido aproveitar a segurança de outros produtos ao sistema a ser desenvolvido. Por exemplo, se for possível que cada usuário possua uma senha no banco de dados, validar este usuário através do banco. Outro exemplo seria aproveitar a validação no sistema operacional para identificar o usuário. Outra alternativa é deixar como senha uma informação biométrica.
b) Arquivos de Log – além de se poder apagar os rastros de um ataque, deve-se cuidar para que os dados de log não comprometam informações sigilosas.
c) Arquivos do Código Fonte – o acesso ao código fonte pode servir para que outros identifiquem vulnerabilidades não percebidas pelos desenvolvedores.

3.2. Programas de Ataque à Segurança da Informação

Quando ocorre o acesso físico ao computador se torna muito mais fácil a quebra de segurança. Programas que atuam de forma ilícita divulgando, alterando ou destruindo informações alheias são denominados de *malwares*, que significa literalmente software malicioso. Neste grupo encontramos:

- vírus - que, como o nome sugere, é um programa que infecta o seu hospedeiro, um ou mais arquivos, e tende a se multiplicar ou a destruir o hospedeiro
- *worm* (verme). eles infesta a rede sobrecarregando recursos, liberando acessos e realizando operações remotas sem que o usuário se dê conta. Colabora com a distribuição de listas de e-mails e mensagens falsas.
- spywares – são os softwares espiões, passando informações do computador infectado.
- cavalo de Tróia – como o nome sugere, é a um programa que debilita as defesas do hospedeiro se fazendo passar por outro um programa inofensivo ou gerando informações falsas. Pode se instalar como um serviço do sistema operacional ou um certificado, por exemplo.
- *keyloggers* – programas que capturam e divulgam o que se tecla. Os alvos usuais são as senhas. Faz parte de uma das categorias anteriores.

Nem sempre à corrupção ou divulgação de informação do usuário do computador é o objetivo de uma invasão. Existem programas cuja intenção é a propaganda de serviços ou produtos, tal como ocorre quando janelas indesejáveis surgem em um navegador Internet sem bloqueador. Tais programas se chamam *adwares*. É comum a presença de *adwares* em programas do tipo *shareware* a fim de incentivar a aquisição da licença.

3.3. *Hackers* e *Crackers*

O jornal “O Estado de São Paulo” apresentou em um artigo a diferença entre *hackers* e *crakers*.

Os hackers são pessoas com bastante conhecimento da tecnologia que, muitas vezes colocam os seus conhecimentos a serviço da sociedade. O

software livre é um exemplo disso. Os hackers em geral atuam como “justiceiros” por causas que entendem como sendo justas, defendendo a liberdade de conhecimento, ainda que nem sempre sejam legais. “Quem não olha com certa simpatia para um 'pichador' de sites de empresas que teimam em pescar baleias?”

Quando se trata de atuação criminosa puramente com o fim de tirar proveito próprio, a denominação usual é a de *crackers*.

O uso de políticas de privacidade, a alteração de senhas de usuários padrões e limpeza de arquivos temporários, podem evitar que informações pessoais fiquem disponíveis a outros usuários. Existem usuários previamente definidos com o controle total do equipamento, são os administradores. No ambiente Microsoft Windows temos o “Administrator” (ou sua versão na língua escolhida para a instalação). No UNIX temos o “root”. Equipamentos de rede configuráveis possuem normalmente um gerente denominado “admin”. O banco de dados Oracle possui um usuário de nome “SYS” que funciona como o gerente do banco e assim segue. Além de usuários padrões existem portas padrões. Estas informações geralmente são de conhecimento dos hackers e são brechas que podem ser facilmente testadas. Mas nem todas as brechas são tão fáceis. O Gerente de Segurança da Informação deve se manter sempre atualizado quanto às vulnerabilidades do parque de equipamentos e programas instalados a fim de minimizar as alternativas de ataques.

3.4. Sistemas de Verificação de Vulnerabilidades

Sistemas operacionais e demais programas de suporte, tais como o navegador da Internet, máquina Java, *frameworks* e *players*, devem ser mantidos sempre atualizados. Normalmente eles possuem algum tipo de

controle interno, que pode ser centralizado, informando ou até mesmo atualizando de vez o programa.

Incluem-se nesta categoria os programas de proteção, tais como antivírus e antispywares. Certificados digitais também devem ser atualizados. Quando vencidos, exigem que o usuário libere exceções de acesso no navegador da Internet. A prática comum pode acabar permitindo com que um certificado falso venha fazer parte da exceção.

A habilitação da atualização automática de programas pode pesar na rede ou no computador e em alguns casos pode-se considerar uma atualização mais espaçada no tempo.

Existem ainda sistemas capazes de verificar se alguma porta do computador está desprotegida e se a configuração do sistema operacional e da rede está compatível com os requisitos de segurança até então conhecidos (VACCA, 2005). A execução destes programas deve ser feita por quem entende as operações por ele propostas.

A integração entre os próprios sistemas da organização podem prover maior segurança ao conjunto. Se, por exemplo, um funcionário está em gozo de férias, não seria normal que ele viesse a acessar um computador de dentro da empresa.

3.5. Principais Ameaças à Segurança da Informação

O ataque deriva de uma ameaça inteligente e é uma ação deliberada contra as políticas de segurança do sistema aproveitando-se de uma vulnerabilidade.

O ataques contra a confidencialidade podem ter por resultado a liberação de informação não autorizada para fins de divulgação ou fraude. Ataques contra a integridade irão contra a confiabilidade da informação. E ataques contra a disponibilidade irão contra o suporte ao serviço ou a destruição da informação. Seja como for, com certeza as maiores ameaças estão dentro da própria organização, de forma que um *firewall*[6] pode não ser suficiente (VACCA, 2005).

Steven M. Bellovin (JAJODIA, 2008), da Universidade de Columbia, lembra que a questão dos ataques internos não é algo novo. Em 1978, Donn Parker, na inauguração de seu livro "O crime por Computador", estimou que 95% de ataques a computadores foram cometidos por usuários autorizados do sistema. Podemos dizer que se tratava de tempos em que o controle de acesso era incipiente. Porém, a realidade de que nem todos os usuários são confiáveis permanece.

Em 2007, o escritório de pesquisas das Forças Armadas dos Estados Unidos da América patrocinou um *workshop* sobre um workshop sobre ataque interno. Participaram convidados incluindo pesquisadores de segurança, acadêmicos, vendedores, técnicos e representantes de outras organizações que perceberam no usuário interno uma grande ameaça. Uma vez que ele já está dentro da organização ele já terá pulado algumas restrições aos serviços.

O mau uso do acesso é um dos ataques mais difíceis de se identificar. Um usuário pode ter se autenticado, estar autorizado, e ainda assim ser uma grande ameaça à segurança da informação. Para o sistema ele é quem afirma ser, contudo basta o descuido para com o sistema aberto e qualquer um pode se fazer passar por aquele usuário, ficando a segurança do sistema fragilizada. Neste caso teria havido cumplicidade, ainda que passiva, do usuário que dispõe da autorização.

---

[6] *Firewall* é um dispositivo ou programa que limita o acesso a certos recursos de rede e pode exigir a autenticação do usuário externo para a liberação do acesso

Como alternativa existe a temporização da inatividade de um sistema aberto ao usuário. Uma vez que o tempo determinado venha a se extinguir, o usuário se verá obrigado a se autenticar novamente. Outra alternativa, quando informações críticas ou mais sensíveis estão para ser acessadas é a confirmação com autenticação biométrica, inviabilizando ou minimizando a troca de usuários.

O preparo da defesa contra ataques ao controle de acesso pode ser mais simples, porém em outros casos, o caminho está primeiramente na detecção do ataque e até mesmo no alerta sobre a situação. A defesa por níveis de acesso pode incluir a necessidade de mais de uma autorização ou tipo de autorização. Em alguns casos a defesa contra os ataques pode significar perda de certa privacidade do usuário, uma vez que seu perfil e ações podem estar sendo armazenadas pelo controle.

Apesar de mais difícil, a utilização de análise de comportamento do usuário ou de alteração de padrões previstos é uma alternativa no caso deste recurso estar disponível, porém somente se presta em situações em que o perfil do usuário ou da utilização dos recursos estão mapeados.

Ataques que se aproveitam de vulnerabilidades técnicas de sistemas de aplicações normalmente precisam de algum tipo de ajuda de dentro. Esta ajuda pode não ser intencional por parte do usuário interno, seja por conta de comportamento impróprio, seja por conta de curiosidade quanto aos limites de seus direitos no sistema. Deve fazer parte da política e dos procedimentos de segurança da informação a atualização constante dos softwares de detecção e tratamento de ameaças como vírus, cavalos-de-tróia, spywares, etc.

Quando é possível para o usuário baixar de programas da Internet, ele deve estar consciente de que pode estar sendo um portal para ataques. Sítios na Internet que não são confiáveis devem fazer parte de lista de bloqueio.

A Módulo apresentou, como resultado de sua pesquisa, quais os problemas que geraram perdas financeiras para governo e empresas. Infelizmente nem todos possuem controle das invasões e conseqüentes perdas. Os vírus possuem posição de destaque, seguidos dos *spams*. SPAM é um termo genérico para mensagens enviadas em massa por alguém que geralmente obteve o e-mail do destinatário sem o seu consentimento. A figura a seguir apresenta o resultado desta pesquisa:

Figura 3 – Problemas que geraram perdas financeiras.
Fonte: Extraído da 10ª Pesquisa da Módulo Nacional de Segurança da Informação

CAPÍTULO IV – INFRAESTRUTURA DE SEGURANÇA DA INFORMAÇÂO

> "*The early bird gets the worm, but it's the second mouse that gets the cheese*". (Steven Wright)

Neste capítulo iremos abordar algumas ferramentas de proteção contra ataques e redução das vulnerabilidades. Tais ferramentas não isentam a preocupação com qualidade das aplicações envolvidas nem a necessária conscientização do uso de práticas mais seguras.

Kenneth J. Knapp e Franklin Morris, examinando as similaridades entre as células biológicas e um sistema de rede de computadores defendeu o que chamou de *defense-in-depth*, que se trata de fazer uso de múltiplas técnicas e camadas a fim de minimizar os riscos quando uma camada fosse comprometida (TIPTON & KRAUSE, 2008).

A segurança deve ser feita em diferentes camadas, com mais de uma alternativa de proteção. Uma vez que uma proteção apresente alguma vulnerabilidade e seja superada, se esta for a única proteção, a informação já fica exposta. A segurança em camadas abrange controles físicos, lógicos e manuais. Diante de restrições orçamentárias, as ações preventivas devem ser as privilegiadas (BEAL, 2008).

Seja como for, a segurança física aos pontos de acesso deve ser uma preocupação básica para a garantia das demais camadas. A segurança física não envolve apenas a garantia dos equipamentos instalados, mas também a prevenção de que nenhum novo ponto de acesso não autorizado seja adicionado à rede (WILES & ROGERS, 2007)

4.1. Criptografia Simétrica e Assimétrica

É um tipo de proteção na codificação da mensagem. Quando um canal de rede não é seguro, informações como senhas e dados financeiros pode ser transmitidos na rede de forma aberta. Programas denominados *sniffers* podem identificar este tráfego.

A criptografia é técnica de se escrever em cifra ou código. Sem a criptografia não existiria comércio eletrônico (BEAL, 2008). A criptografia simétrica exige é feita com uma chave, a qual será usada para a posterior decodificação e leitura da informação. Seu uso se faz quando emissor e receptor possuem uma relação de confiança. Alguns sistemas têm seu código fonte a estrutura de montagem da chave de criptografia, tornando o código um forte ponto de vulnerabilidade do sistema.

A criptografia assimétrica possui uma chave pública e outra privada. Ambas são diferentes, sendo que uma é usada para a codificação da mensagem e a outra para a decodificação. A chave privada deve ser do conhecimento apenas de seu proprietário. A chave pública, por outro lado é de conhecimento de ambos, um documento codificado com a chave pública não pode ser decodificado por ela, como se fosse uma chave simétrica. Assim, na codificação com a chave pública, o proprietário das chaves confirma a confidencialidade da informação e a autenticidade (STAMP, 2008).

A decodificação na criptografia assimétrica requer maior poder de processamento do que na simétrica. Os protocolos TSL e SSL fazem uso dos dois tipos de criptografia. O canal seguro é garantido inicialmente com a criptografia assimétrica, por onde a chave para a criptografia simétrica é enviada. Em seguida a comunicação passa a ser criptografada por esta chave
.

As análises matemáticas em criptografia tem evoluído muito. Muito estudo tem sido feito com geradores de chaves e simuladores de ataques. Um tipo de análise é o de colisão, quando duas partes distintas de um dado produzem o mesmo resultado após a criptografia. Este caminho difere do uso da "força-bruta", onde todas as combinações possíveis dentro de um tamanho e uma faixa determinada de caracteres são testadas.

Em fevereiro de 2005 foi anunciado que Xiaoyun Wang e outros colegas da Shandong University, na China, haviam demonstrado a quebra do algoritmo SHA-1 através da análise de colisões em 2^{69} operações. Com "força–bruta" seriam necessárias 2^{80} operações. É importante que, a depender do uso a quebra era possível em 2^{33} operações! Assim, Xiaoyun Wang observou que um algoritmo pode apresentar importantes vulnerabilidades, ainda que empregue funções não-lineares (que são as mais difíceis de serem descobertas e é o caso do SHA), por conta da forma de sua utilização. O uso adequado das funções reforçam a segurança de um algoritmo criptográfico (PRENEEL & LOGACHEV, 2008). O tempo esforço consumido irá depender do tamanho da chave utilizada e dos tipos de combinações que se fizer.

As organizações IT Governance Institute e The Office of Government Commerce alertam em seu trabalho sobre o alinhamento entre COBIT 4.1, ITIL v.3 e a ISO/IEC 27002 quanto à importância da gestão de chaves de criptografia de acordo com o seu ciclo de vida (ITGI & OGC, 2008)

4.2. Certificados digitais e a Infraestrutura de Chaves Públicas

Na comunicação padrão temos o emissor e o receptor. Quando falamos em PKI (*Public Key Infrastructure*) ou Certificação Digital, temos normalmente uma terceira entidade responsável pela garantia da confiabilidade da mensagem. Alguém em que ambos confiam. O transmissor da mensagem tem sua identidade conferida pela certificadora. O certificado

pode assegurar tanto um usuário, um provedor de informações ou um programa. Existem meios de se fazer uma transação interna nos moldes da certificação digital, porém o normal é a existência de uma entidade certificadora. Este tipo de solução vem alcançando cada vez mais espaço, porém, tem sido questionada quanto aos prazos de validade que as autoridades certificadoras concedem. Outro problema é a possibilidade de que uma autoridade certificadora cesse a sua existência ou se torne indisponível. O negócio ficaria a depender da certificação e a falha indevida pode levar a prejuízos (GLADNEY, 2007).

A infraestrutura de chave pública exige uma hierarquização para otimizar a comunicação em rede. No Brasil, a Medida Provisória nº 2.200/2001 criou um Comitê Gestor vinculado à Casa Civil da Presidência da República, que trata de questões como a validade jurídica e tributária de documento assinados digitalmente. Os produtos e-CPF e e-CNPJ bastante divulgados pela Receita Federal e por certificadoras autorizadas são certificados digitais.

A assinatura digital não dá privacidade a um documento, ela apenas assegura a integridade e o não-repúdio. Para que haja privacidade é necessário que o documento seja criptografado com a chave pública do destinatário e a ele seja enviado, de forma que somente ele poderá decodificar e ler o conteúdo da mensagem com a chave privada dele (STEWART, 2008).

4.3. Redes Privadas Virtuais - VPN

A rede virtual privada permite criar uma espécie de túnel, de um ponto ao outro, dentro de uma rede menos confiável. A maioria das VPNs fazem uso de criptografia. Através da VPN pode-se criar uma conexão entre duas redes distintas ou dois computadores, sendo de grande utilidade no caso de sistemas legados que não possuem confiabilidade na comunicação de dados,

aproveitando o custo mais baixo do acesso à Internet com os potenciais benefícios de uma rede mais segura (FRAHIM & HUANG, 2008).

Este recurso beneficia não apenas os pontos fixos de rede como também os móveis. Através de uma VPN pode-se ter uma conexão segura com o escritório de casa, de um hotel ou aeroporto, por exemplo.

O IPsec é um dos protocolos mais utilizados em VPN. Sua proteção é feita em um nível abaixo do SSL (Secure Socket Layer). Ele foi criado a fim de garantir a integridade dos pacotes de dados, autenticação e criptografia. O protocolo SSL foi desenvolvido pela Netscape a fim de promover o comércio eletrônico na Web e evoluiu para aplicações de correio eletrônico (FRAHIM & HUANG, 2008). A vantagem do SSL para com o IPsec é que o SSL é mais simples e todos os navegadores são compatíveis. O IPsec ainda é dependente do sistema operacional (STAMP, 2008). A figura a seguir mostra estes protocolos em relação às camadas de comunicação de rede.

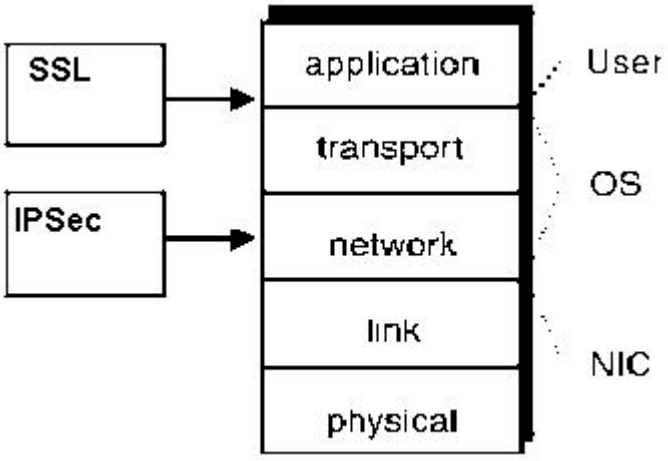

Figura 4 – Protocolos SSL e IPsec
Fonte: Mark Stamp, "Information Security", 2008

4.4. Smartcards

Os *smartcards* são cartões que integram um chip para processamento de operações aritméticas. Eles são uma forma conveniente de se guardar a senha. Os smartcards podem processar dados e tomar decisões inteligentes e mais seguras, como a proteção contra comportamento indesejado. Uma alternativa é armazenar uma representação eletrônica da impressão digital de forma a poder verificar se o usuário do cartão é realmente o seu proprietário, em um leitor ou pelo próprio cartão. O smartcard pode ainda levar informações de certificação ou assinatura digital (BRANDS, 2000).

O acesso à memória do smartcard é garantida contra acesso não autorizado e o cartão pode se desabilitar após tentativas de uso de um código falso. Os cartões também podem ser protegidos contra cópias e é imune a vírus ou *trojans*.

4.5. Firewall

Um *firewall* pode ser instalado através de software no computador que se deseja proteger ou como um hardware a parte protegendo toda uma rede. O firewall funciona como um filtro, podendo determinar o que pode passar de uma rede para outra, por quais portas, quais protocolos e ainda fazer auditoria das conexões (ROGER, 1998).

A funcionalidade de restringir o acesso a rede pode ser feito em conjunto com a configuração de outros dispositivos de rede (roteadores, switches, etc) e deve ser feita de acordo com o planejamento da segmentação da rede, potencializando a segurança da rede (KLOSTERBOER, 2008).

Um firewall não é capaz de detectar todo o tipo de ameaça, contudo cada vez tem sido incorporadas soluções para a prevenção e detecção de invasões (BEAL, 2008).

4.6. Ferramentas de Replicação e Backup

Computadores são equipamentos eletrônicos susceptíveis a falhas. Erros que provoquem a perda da informação necessitam de alternativas de recuperação a fim de promover a restauração do serviço. Como já fora dito, deve haver um planejamento destes serviços baseando-se na classificação da informação e na criticidade do sistema. Pesquisas da Módulo até 2003 apontavam que os sistemas de backup normalmente faziam parte das medidas mais implementadas em termos de segurança por empresas, juntamente com o *firewall*.

É recomendável que a guarda das mídias de backup se situem geograficamente distantes do servidor de origem, tal como deve ocorrer no caso de replicação de recursos para o provimento de um serviço, visto que a indisponibilidade do serviço pode ter causas outras que não um defeito comum em parte do circuito, mas pode ser resultante de desastres como inundações, incêndios e atos de vandalismo ou terrorismo (TCU, 1998). Simulações de recuperação de incidentes devem fazer parte do planejamento da gestão de riscos e de continuidade do negócio.

Em investigação forense a comparação entre backups pode demonstrar o versionamento da informação, a depender do período de retenção do backup. Isso chama a atenção para um erro que pode ser comum: quando a segurança imposta no sistema de informação não é mantida no manuseio do backup, de forma que a confidencialidade do backup venha a se tornar em uma vulnerabilidade (VOLONINO & ANZALDUA, 2008).

CAPÍTULO V – GESTÃO DE RISCOS

Ter sucesso na Gestão de Riscos não significa necessariamente que não haverá riscos, mas que fomos capazes de quantificar o risco e decidir que riscos estamos dispostos a correr. Gestão de riscos é tomar decisões ou mapear os riscos de forma a contribuir para que estas decisões sejam tomadas. Em contrapartida iremos considerar o valor da informação no confronto com os custos da segurança da informação.

Não podemos deixar de considerar na análise de riscos estes três aspectos que devem fazer parte de qualquer porjeto de segurança: Pessoas (cultura, capacitação e conscientização), Processos (metodologias, normas e procedimentos) e Tecnologia (ferramentas que comportam os recursos físicos e lógicos).

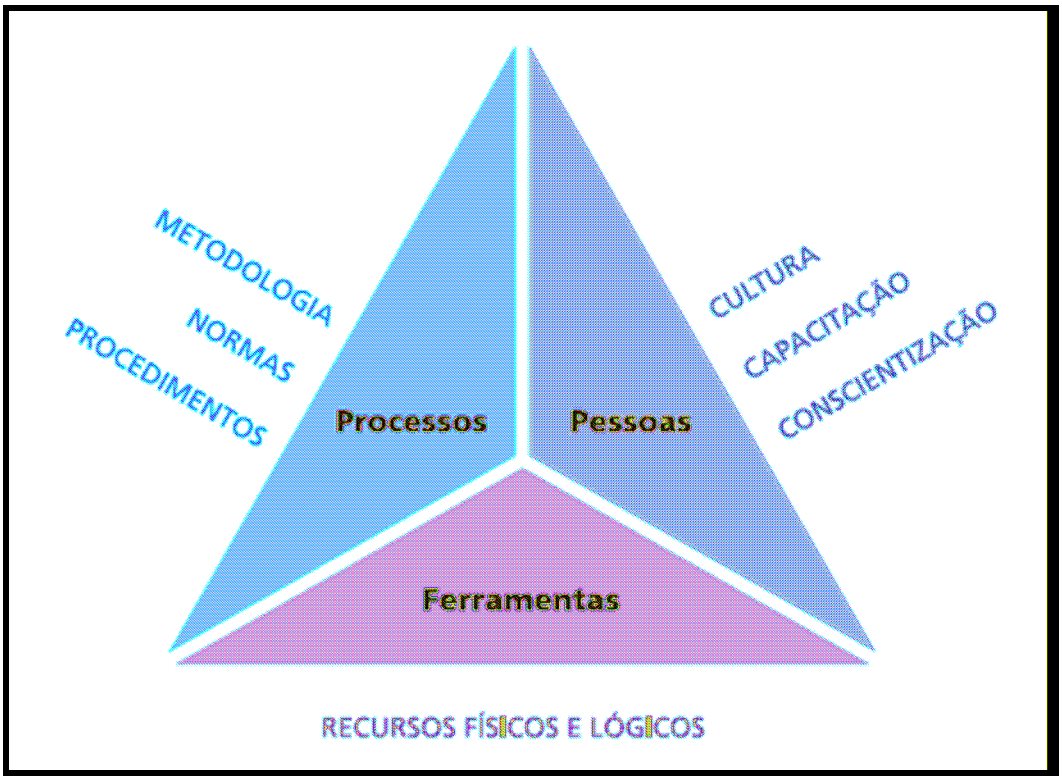

Figura 5 – Aspectos a considerar em projetos de segurança.
Fonte de referência: Portfolio da Módulo Security

Estes três aspectos são o tema da abordagem por disciplinas que se divide em (WESTERMAN & HUNTER, 2008):

- alicerce – base tecnológica: infraestrutura e aplicações
- processo de governança do risco – processo que proporcione visão geral dos riscos nos diferentes níveis da empresa e permita a administração da priorização e do investimento, bem como a administração por níveis.
- Cultura de consciência do risco – conhecimento amplo e aberto a discussões como norma.

Uma análise de riscos que deixe de fora estes aspectos pode ser fadada ao fracasso.

5.1. Maturidade da Gestão de Riscos

De acordo com a definição contida no COBIT 4.0 (2005), a gestão dos riscos requer a conscientização da alta direção executiva da empresa, um claro entendimento do risco que a empresa está disposta a correr, compreender os requisitos normativos envolvidos, transparência quanto aos riscos significativos para a empresa e a inserção das responsabilidades na administração de riscos dentro da organização.

Seguem os níveis de maturidade segundo em gestão de riscos segundo o COBIT 4.1:

0) **Não existente,** quando a avaliação de risco para processos e decisões de negócios não ocorre. A organização não considera os impactos nos negócios associados às vulnerabilidades de segurança e incertezas no desenvolvimento de projetos. A gestão de riscos não é identificada como relevante ao se adquirir soluções em TI e na entrega de seus serviços.

1) **Inicial/Ad Hoc,** quando os riscos de TI são considerados de maneira informal. Avaliações informais de riscos de projetos surgem conforme a situação particular de cada projeto. As estimativas de risco algumas vezes são identificadas em um planejamento de projeto, mas raramente atribuídas a gerentes específicos que sejam responsáveis por elas. Riscos específicos de TI, tais como segurança, disponibilidade e integridade, são considerados ocasionalmente no projeto básico. Riscos de TI que afetem operações do dia-a-dia quase nunca são discutidos nas reuniões gerenciais. Onde os riscos foram considerados, a minimização dos danos é inconsistente. Existe um entendimento emergente de que os riscos em TI são importantes e precisam ser considerados.

2) **Repetitivo mas intuitivo,** quando o desenvolvimento de uma abordagem de avaliação de risco existe e é implementada sob a ponderação dos gerentes de projeto. A gestão de risco é habitualmente tratada em pelos de escalão superior e é tipicamente empregada nos principais projetos ou em caso de ocorrência de problemas. Os processos de minimização de riscos são implementados onde os riscos são definidos.

3) **Definido,** quando uma organização, em uma ampla política de gestão de risco, define quando e como conduzir as estimativas de risco. A administração do risco segue um processo definido e documentado. Treinamento em gestão de risco está disponível para todos os membros da equipe. Decisões para seguir o processo de gestão de risco e receber treinamento se releva como decisão individual. A metodologia de estimativa de risco é convincente e sólida, e garante que os riscos chaves do negócio sejam identificados. Um processo para minimizar os ricos chaves é normalmente instituído assim que os riscos são identificados. As descrições dos cargos consideram as responsabilidades pela gestão dos riscos.

4) **Gerenciado e Monitorado,** quando a estimativa e o gerenciamento do risco é um procedimento padrão. Exceções ao processo de gerenciamento de risco são reportados ao gerente de TI. Gestão de risco de TI é responsabilidade de um gerente sênior. O risco é avaliado e minimizado individualmente no nível de projeto e também regularmente considerado por toda a operação de TI. Os gestores são avisados em caso de mudanças no negócio e no ambiente de TI que possam afetar de forma significativa os cenários de risco. Os gestores estão habilitados a monitorar a situação do risco e a decidir se as condições medidas estão em conformidade com o esperado. Todos os riscos identificados possuem um proprietário designado e tanto a alta direção, como o gerente de TI, determinam os níveis de risco que a organização irá tolerar. Gerentes de TI desenvolvem padrões de medidas para estimativas de risco e definem as relações de risco/retorno. Há o pressuposto de que a gerencia reavalie os risco operacionais regularmente. É criado uma base de dados de gestão de riscos, e parte dos processos de gestão de risco começam a ser automatizados. Os gestores de risco de TI cuidam de estratégias de minimização de riscos.

5) **Otimizado,** quando a gestão de risco evoluiu a um estágio em que um processo estruturado está implantado amplamente na organização e é bem administrado. Boas práticas são aplicadas por toda a organização. A captura, análise e relatório dos dados de gestão de riscos estão bastante automatizados. A orientação é tomada por especialistas da área e a organização de TI toma parte em grupos para troca de experiências. A gestão de riscos é realmente integrada a todos os negócios e às operações de TI, é bem aceita e envolve os usuários dos serviços de TI. A direção detecta e age quando as principais operações de TI e decisões de investimentos são feitas sem considerar o plano de risco. A direção continuamente avalia estratégias de minimização de riscos.

5.2. Atribuindo Responsabilidades para com os Riscos

Segundo o COBIT 4.1 (2007), todo evento que representa um risco deve ser identificado, analisado e estimado, o que, uma vez realizado, deve buscar minimizar os seus e comunicar o risco residual, que é o risco que se sabe estar ainda correndo.

A matriz abaixo, denominada de R.A.C.I. (um acróstico do que identifica) representa uma simplificação do que é definido na estrutura do COBIT 4.1. Ela indica os responsáveis (R), quem deve prestar contas (A), quem deve ser consultado (C) e quem deve ser informado (I). A simplificação está na gerência de Tecnologia da Informação, incluindo arquitetura, desenvolvimento e a gestão de sistemas.

Gestores:

1 – CEO – Chief Executive Officer – Diretor
2 – CFO – Chief Financial Officer – Diretor
3 – Executivos da Empresa
4 – CIO – Diretor
5 – Gerentes Seniores
6 – Gerentes Operacionais
7 – Gerentes de TI (arquitetura, desenvolvimento, administração)
8 – PMO – Gerentes de Processos
9 – Conformidade, Auditoria, Risco e Segurança em geral.

Atividades / Gestores	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
Determinar o alinhamento da gestão de risco	A	R/ A	C	C	R/ A	I			I
Entender estratégias relevantes aos objetivos do negócio		C	C	R/ A	C	C			I
Entender processos relevantes aos objetivos do negócio				C	C	R/ A			I
Identificar objetivos de TI e estabelecer o contexto do risco					R/ A		C		I
Identificar os eventos associados aos objetivos do negócio	I			A/ C	A	R	R		C
Estimar os riscos associados aos eventos				A/ C	A	R	R		C
Avaliar e selecionar os responsáveis pelo risco	I	I		A/ C	A	R	R		C
Priorizar e planejar o controle das atividades	C	C	A	A	R	R	C		C

Aprovar e garantir fundos para os planos de ações de risco		A	A		R	I	I		I
Manter e monitorar os planos de ações de risco	A	C	I	R	R	C	C	C	R

Tabela 2 - Matriz R.A.C.I.

Fonte: Adaptada do COBIT 4.1, Gerenciamento de Riscos

Trata-se de um modelo que deve ser ajustado nas condições e características da organização. É importante observar que no COBIT os gestores de riscos, segurança, auditoria e de conformidade com os requisitos legais participam das outras matrizes RACI como devendo ser consultados. Esta matriz irá orientar o processo de planejamento dos projetos, mudanças, gestão e a classificação dos riscos.

5.3. Gestão de Mudanças e Valor do Negócio

Para se dar início a esta análise é importante dispor de ferramentas que apresentem o impacto dos sistemas de informação no negócio. Toda mudança deve levar em consideração os riscos envolvidos. Não se tratam apenas de riscos em relação ao sistema, mas também as pessoas e o andamento dos processos. De fato o ideal é que as mudanças tenham por base os riscos que cercam o sistema antigo e os ganhos do sistema novo. Lucro, maior produtividade, diferenciação competitiva, redução de riscos e maior agilidade são fatores positivos em prol de mudanças.

Em momentos de mudança e como justificativa para novos investimentos, pode-se associar o risco à performance da aplicação e seu respectivo retorno através da taxa de Sharpe, que é a razão entre o valor esperado de retorno (a diferença entre o retorno atual e um retorno isento de risco), pelo desvio padrão (LAUBSCH, 1999):

$$S = \frac{R - R_f}{\sigma} = \frac{E[R - R_f]}{\sqrt{\mathrm{var}[R - R_f]}},$$

O risco em questão deve ser calculando considerando um período de tempo.

Fatores como adequação do sistema ao número de funcionários, facilidade de aprendizado, melhor suporte são fatores positivos que dizem respeito aos recursos humanos. Tais fatores podem se somar a um processo de melhoria nos procedimentos e de novos requisitos do negócio, fatores que poderiam não alcançar a eficácia esperada se mantido o sistema antigo. A figura a seguir ilustra a argumentação proposta e suas tendências na relação risco X valor (WESTERMAN & HUNTER, 2008):

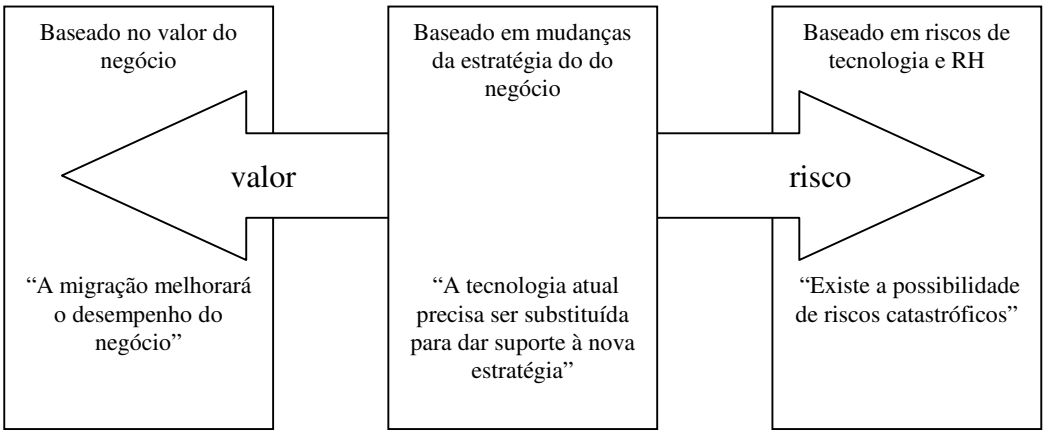

Figura 5 – Alto Valor, Alto Risco. Administrando o Portfolio Legado
Fonte: Richard Hunter e Dave Aron, Gartner Executive Programs, setembro de 2006.

Um catálogo de serviços é um recurso útil na gestão de mudanças e na identificação do valor agregado ao negócio. O ideal é que as informações façam parte de uma base de dados que contenha os itens de configuração de TI de forma a poder relacioná-los aos serviços, ao que se chama de CMDB (Configuration Management Data Base). De posse dos recursos necessários a um serviço, é possível mensurar os custos de cada serviço e posteriormente, com as mudanças, o rateio do investimento (KLOSTERBOER, 2008).

5.4. Estimando os Riscos

A estimativa de riscos está intimamente ligada ao que em Gestão de Riscos, de modo geral, é denominado como “apetite pelo risco”[7], que significa o quanto de risco a alta direção está disposta a correr. As organizações *The Institute of Risk Management* – IRM, *The Association of Insurance and Risk Managers* – AIRMIC e o ALARM, um fórum nacional para Gestão de Riscos no Setor Público do Reino Unido, desenvolveram um padrão de gestão de riscos bastante interessante que é alinhado com a ISO/IEC Guide 73:2002. Neste documento o “apetite pelo risco”, para fins de segurança em sistemas de informação, é melhor situado como “tolerância ao risco”, que é obtido avaliando-se:

- a probabilidade de que o risco venha ocorrer
- a perda potencial ou o impacto financeiro do risco
- o valor do risco

Este valor é obtido através da multiplicação do fator de probabilidade, ou quantificação do risco, pelo fator correspondente à perda potencial ou impacto financeiro (AIRMIC & IRM & ALARM, 2002).

Devemos identificar os s*takeholders*, isto é, aqueles que são os responsáveis pelos investimentos em tecnologia da informação a fim de podermos saber as áreas de interesse de sua participação. Em geral os stakeholder são acionistas da empresa e seus interesses estão em outro nível de exigência, devendo ser traduzidos pela identificação dos *value drivers*, que são os elementos potenciais de valor, cujas medidas de eficiência devem ir ao encontro das demandas dos *stakehoders*. Estes elementos devem ser

detalhados ao ponto de ser possível o seu gerenciamento. O *Balanced Scorecard* - BSC, método desenvolvido por Robert S. Kaplan e Robert D. Norton, é útil na identificação dos *value drivers* ao combinar as medidas de performance e seu alinhamento com os objetivos estabelecidos (SENFT & GALLEGOS, 2009).

Uma vez que temos o arcabouço necessário para identificar as estratégias que criam valor. Identificaremos os aspectos chaves de risco diretamente associados ao risco de fracasso na agregação de valor. Estes elementos de risco deverão ser classificados por faixas (CAREY, 2005).

Definidos todos estes elementos, podemos examinar o exemplo de cálculo de tolerância ao risco apresentado por Mark Carey, CEO da organização DelCreo.

Listemos os *value drivers* e os riscos chaves correspondentes:

Value drivers	**Riscos**
Aumento do rendimento dos investimentos	Interrupção levando à redução nos lucros
Redução de custos	Surgimento de custos não previstos
Prevenção de Perda de Ativos	Desvalorização de ativos

Escolhendo o risco de “Surgimento de custos não previstos”, podemos atribuir pesos para as faixas de valor de custos que não foram previstos:

1) 0 a 50K
2) 51 a 250K
3) 251K a 1M
4) 1M+

Podemos, também, definir os pesos para os itens que indicarão a probabilidade de que o risco ocorra:

1) baixa

[7] Tradução literal de *appetite for risk*.

2) média
3) alta
4) já está ocorrendo

De acordo com o resultado da multiplicação dos dois fatores (cujo valor máximo no exemplo será 4 x 4 = 16), a tolerância ao risco será definida, bem como as ações a serem tomadas:

Entre 1 e 4 - Gerenciar o risco dentro da unidade de negócio ou função.
Entre 5 e 8 - Risco deve ser escalonado para o programa de seguro e financiamento de riscos.
Entre 9 e 11 - Risco deve ser escalonado à tesouraria da corporação.
Entre 12 e 16 - Risco deve ser escalonado à gestão de crises ou à gestão executiva da corporação.

Neste exemplo, significa que, se as operações de investimento implicarem no risco de "surgimento de custos não previstos" na ordem de 60K e probabilidade disto ocorrer for "alta", o valor calculado do "apetite" ou tolerância ao risco será de 2 x 3 = 6, i.é, entre 5 e 8, de forma que o risco deve ir à esfera do programa de seguro e financiamento de riscos, não podendo ser tratado apenas dentro da unidade de negócio.

A classificação deve ser tão detalhada quanto se julgar necessário, podendo ser específica para cada negócio. O peso dos riscos será normalmente definido por valor monetário, percentual de recursos, tempo limite de restauração de serviço, ou seja, o impacto no serviço, bens ou nos lucros.

Geralmente os gerentes de TI e os gerentes operacionais são os mais indicados para mensurar a probabilidade de que um evento ocorra. Contudo, como foi visto na matriz RACI, serão os gestores de negócio que irão identificar

e se responsabilizar pelo peso que irá representar o impacto do risco sobre o negócio.

5.5. Relatórios Gerenciais

Os relatórios fazem parte da gestão de riscos. A existência de uma política que determine a constante avaliação da segurança e dos riscos da informação irá colaborar com informações que darão suporte a novos investimentos ou a identificação de falhas no processo.

No ITIL temos um destaque nos relatórios de auditoria envolvendo: disponibilidade, incidentes, exceções e capacidade de recursos. Variações no consumo de recursos, por exemplo, podem indicar a necessidade de estudo das mudanças que motivaram este comportamento e a necessidade ou não de novos investimentos (itSMF, 2004).

Alcançar um nível maior de maturidade COBIT em gestão de riscos também está associado a aspectos de automação dos relatórios. Os relatórios que mais se destacam são os de log ou incidentes de sistema (monitoramento e resposta a incidentes) e os de métricas de segurança e performance. Porém importa ressaltar que estão incluídos relatórios de testes de novas funcionalidades. Os relatórios devem incluir os pontos chaves de controle tal que sirva de base para a avaliação da conformidade com os requisitos do sistema e o ciclo de vida da informação (TURCATO, 2006).

Tal relatório somente será possível se identificados os fatores que representam um risco para o negócio em questão.

Os relatórios devem conter comparações entre períodos, destacando-se datas em que mudanças ou novas soluções foram implementadas. Estas

mudanças não devem se restringir a mudanças de TI, mas devem incorporar mudanças nos processos e no negócio. O foco é o alinhamento e a integração entre o negócio e TI, em especial, neste caso, os aspectos de segurança e riscos. Os relatórios também devem ser claros e compreensivos (TURCATO, 2006).

Os relatórios de métricas podem ser classificados em operacionais e executivos, de acordo com o público-alvo. Os relatórios operacionais podem incluir informações tais como (BACIK, 2008):

- Número de violações ou tentativas de violações da política de riscos.
- Número de dispositivos fora dos padrões de configuração da corporação.
- Número de contas sem uso ou boqueadas.
- Número de diferentes tipos de ataques contra a corporação de origem externa.
- Número de vírus, *worms* e *Trojans* que foram bloqueados

Relatórios executivos incluem informações tais como as que seguem:

- Montante de tempo de indisponibilidade dos serviço e custos causados por falhas de configurações ou erros de implementação.
- Dinheiro gasto acima ou abaixo do estimado pelos projetos de segurança.
- Lista de riscos suportados ou acordados.

Questionários de conformidade também podem servir de subsídio a avaliação comparativos e histórica da evolução do processo. Os relatórios e questionários de avaliação darão o retorno do ciclo PDCA para o processo contínuo de melhoria.

CONCLUSÃO

Ignorar os riscos não os faz deixar de existir. A informação é um ativo da organização cuja segurança deve fazer parte de sua gestão. Cada vez mais as organizações se tornam dependentes das informações contidas em Sistemas de Informação, mas acabam se esquecendo que equipamentos também estão sujeitos à falhas e deve haver um planejamento para a continuidade do negócio.

O valor da informação, a competitividade da empresa, o alinhamento estratégico irão atuar de forma integrada na justificativa ou não do investimento em segurança da informação. Para este convencimento, em alguns casos, não basta saber o TCO, mas se faz necessário identificar os proprietários da informação e os interessados nela, de forma a poder apresentar o seu impacto nas diferentes áreas da organização.

A normatização contribui para o envolvimento maior dos administradores, de forma que segurança da informação não se trata mais de uma cadeira técnica, mas também requer o conhecimento nos negócios e os reflexos jurídicos envolvidos.

A gestão de riscos em Sistemas de Informação tem a missão de fazer com que os riscos não venham superar aquele que a alta direção está disposta a correr. Os riscos dependem do contexto e envolvem pessoas, processos e tecnologia. As melhores práticas devem ser aplicadas a toda a organização e a manutenção das políticas de segurança devem contar com o apoio da alta direção.

BIBLIOGRAFIA

AIRMIC; ALARM; IRM. **A Risk Management Standard**. London, United Kingdom: The Association of Insurance and Risk Managers; ALARM The National Forum for Risk Management in the Public Sector; Institute of Risk Management, 2002

BACIK, SANDY. **Building an Effective Information Security Policy Architecture**. New York, USA: Auerbach Publications, 2008.

BEAL, Adriana. **Segurança da Informação: Princípios e Melhores Práticas para a Proteção dos Ativos da Informação nas Orgnizações**. São Paulo: Editora Atlas, 2008.

BON, JAN VAN. **Fundamento do Gerenciamento de Serviços em TI baseado na ITIL**. Amersfoort, Holanda: itSMF, Van Haren Publishing, 2006.

BRANDS, STEFAN A. **Rethinking Public Key Infrastructures and Digital Certificates**. London, England: MIT Press, 2000.

BRASIL, ABNT. **NBR ISO/IEC 17799**. Rio de Janeiro: ABNT, 2005.

BRASIL, ABNT. **NBR ISO/IEC 27001:2006**. Rio de Janeiro: ABNT, 2006

BRASIL. **Decreto nº2.134 de 24 de janeiro de 1997**. Brasília: Diário Oficial da União, 1997.

BRASIL. **Decreto nº4.553 de 27 de dezembro de 2002**. Brasília: Diário Oficial da União de 06/01/2003.

BRASIL. **Decreto nº5.301 de 9 de dezembro de 2004**. Brasília: Diário Oficial da União de 10/12/2004.

BRASIL. **Lei Federal nº10.406 de 10 de janeiro de 2002- Institui o Código Civil**. Brasília: Diário Oficial da União, 11/01/2002.

BRASIL. **Medida Provisória nº2.200 de 24 de agosto de 2001 - Institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil**. Brasília: Diário Oficial da União de 27/08/2001.

BRASIL, TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Boas Práticas em Segurança da Informação**. Brasília: Tribunal de Contas da União, 2007.

BRASIL, TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Licitações e Contratos: Orientações Básicas**. Brasília: Tribunal de Contas da União, 2006.

BRASIL, TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Manual de Auditoria de Sistemas**. Brasília: Tribunal de Contas da União, 1998.

BRASIL, TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Técnica de Auditoria: Marco Lógico**. Brasília: Tribunal de Contas da União, 2001.

BRASIL, TRIBUNAL DE CONTAS DA UNIÃO (TCU). **Técnica de Auditoria: Benchmarking**. Brasília: Tribunal de Contas da União, 2000.

CAREY, MARK. 2005. **Determining Risk Apetite**. Artigo do sítio Continuity Central Em: < http://www.continuitycentral.com/feature0170.htm >. Acessado em abril de 2009.

CARTLIDGE, ALISON. **The IT Infrastructure Library: An Introductory Overview of ITIL - Version 2**. Wokingham, United Kingdom: IT Service Management Forum, 2004.

CARTLIDGE, ALISON; LILLYCROP, MARK. **The IT Infrastructure Library: An Introductory Overview of ITIL - Version 3**. Wokingham, United Kingdom: IT Service Management Forum, 2007.

CHEN, NONG. **Personalized Information Retrieval and Access: Concepts, Methods and Practices**. Pennsylvania, USA: Information Science Reference, 2008.

ERBSCHLOE, MICHAEL. **Information Warfare: How to Survive Cyber Attacks**. USA: McGraw-Hill, 2001.

ESTADOS UNIDOS DA AMÉRICA. **Executive Order 12356 of April 2, 1982 – National Security Information**. Washingtn, DC, USA: The White House, 1982.

ESTADOS UNIDOS DA AMÉRICA. **Executive Order 12958 of April 17, 1995 – Classified National Security Information**. Washingtn, DC, USA: The White House, 1995.

FARNSWORTH, ROGER. **CISCO Systems: Introduction to Information Security**. Apresentação de Palestra 302 da CISCO, 1998.

FRAHIM, JAZIB; HUANG, QIANG. **SSL Remote Access VPNs.** Indianapolis, USA: CISCO Press, 2008.

GLADNEY, HENRY M. **Preserving Digital Information**. Heidelberg: Springer, 2007.

INGLATERRA, CENTRAL COMPUTER AND TELECOMMUNICATIONS AGENCY (CCTA). **IT Infrastructure Library: Service Support**. Her Majesty's Stationery Office, 2000.

ITGI. **COBIT 4.0: Objetivos de Control, Directrices Gerenciales, Modelos de Madurez**. Illinois, USA: IT Governance Institute, 2005.

ITGI. **COBIT 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models**. Illinois, USA: Information Tecnology Governance Institute, 2007.

ITGI; OFFICE OF GOVERNMENT COMMERCE**. Aligning CobiT 4.1, ITIL V3 and ISO/IEC 27002 for Business Benefit**. Illinois,USA: IT Governance Institute, 2008.

JAJODIA, SUSHIL. **Insider Attack and Cyber Security: Beyond the Hacker**. Virgínia, USA: Springer Science+Business Media, 2008

KARDEC, Alan; LAFRAIA, João. **Gestão Estratégica e Confiabilidade**. Rio de Janeiro: QualityMark: ABRAMAN, 2002.

KLOSTERBOER, LARRY. **Implementing ITIL Configuration Management**. Massachusetts, USA: IBM Press, 2008.

LAUBSCH, ALAN J. **Risk Management: A Pratical Guide**. USA: RiskMetrics Group, 1999.

LAUREANO, MARCOS AURELIO PCHEK; MORAES, PAULO EDUARDO SOBREIRA. **Segurança como Estratégia de Gestão da Informação**. Artigo de Revista Economia & Tecnologia, v. 8, fascículo 3, pp. 38-44. 2005.

MANDARINI, MARCOS. **Segurança Corporativa Estratégica**. Barueri-SP: Editora Monole, 2005.

NIZAMUTDINOV, MARSEL. **Hacker Web Exploitation Uncovered**. Pennsylvania, USA: A-LIST Publishing, 2005.

NUNES, MARCOS ALONSO. **Custos no Serviço Público**. Brasília: ENAP, 1998.

PRENEEL, BART; LOGACHEV, OLEG A. **Boolean Functions in Cryptology and Information Security**. NATO Science for Peace and Security Sub-Series D: Information and Comunication Security - v.18**.** Amsterdam, Netherlands: IOS Press, 2008.

PRICEWATERHOUSECOOPERS. **Enterprise Risk Management - Integrated Framework: Executive Summary**. Committee of Sponsoring Organizations of the Treadway Commission: COSO, 2004.

RANCE, STUART; HANNA, ASHLEY. **ITIL 3: Glossary of Terms,Definitions and Acronyms**. OGC-Office of Government Commerce, 2007

RUD, OLIVIA PARR. **Data Mining Cookbook: Modeling Data for Marketing, Risk, and Customer Relationship Management**. New York, USA: Wiley Computer Publishing, 2001.

SALTZER, J. H. 1975. **The Protection of Information in Computer Systems**. Em: <http://web.mit.edu/Saltzer/www/publications/protection/index.html> . Acessado em fevereiro de 2009.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: Uma visão Executiva**. Rio de Janeiro: Ed. Campus, 2003.

SENFT, SANDRA; GALLEGOS, FREDERICK. **Information Technology Control and Audit**. New York, USA: Auerbach Publications, 2009

SIMÃO, NUNO. 2008. **As Ferramentas de Inteligência Empresarial**. Em: <http://www.facil.com.br/website/int-bra/noticias.asp?show=4> . Acessado em fevereiro de 2009.

STAMP, MARK. **Information Security: Principles and Practice**. Indianapolis, USA: Wiley Publishing, 2008.

STEWART, JAMES MICHAEL; TITTEL, ED; CHAPPLE, MIKE. **Certified Information Systems Security Professional Study Guide**. New Jersey, USA: John Wiley & Sons Publication, 2008.

TABER, MARK. **Maximum Security: Hacker's Guide to Protecting Your Internet Site and Network**. Kansas, USA: SAMS Publishing, 1998.

TIPTON, HAROLD F; KRAUSE, MICKI. **Information Security Management Handbook**. New York, USA: Auerbach Publications, v.2, 2008.

TURCATO, LANCE M. **Presentation: Integrating COBIT into the IT Audit Process**. San Francisco, USA: ISACA, 2006

VACCA, JOHN R. **Computer Forensics: Computer Crime Scene Investigation**. Massachusetts, USA: Charles River Media, 2005.

VOLONINO, LINDA; ANZALDUA, REYNALDO. **Computer Forensics for Dummies**. New Jersey, USA: Wiley Publishing, 2008.

WESTERMAN, George; HUNTER, Richard. **O Risco de TI. Convertendo Ameaças aos Negócios em Vantagem Competitiva**. Harvard Business School Press, 2007. São Paulo: Ed. M.Books do Brasil, 2008.

WILES, JACK; ROGERS, RUSS. **Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigators**. USA: Syngress Publishing, 2007.

ÍNDICE

FOLHA DE AVALIAÇÃO

Nome da Instituição: Universidade Cândido Mendes – Projeto A Vez do Mestre

Título da Monografia: Gestão de Riscos Aplicada a Sistemas de Informação: Segurança Estratégica da Informação

Autor: Eduardo Antônio Mello Freitas

Data da entrega:

Avaliado por: **Conceito:**