APLICAÇÃO DA METODOLOGIA DE AVALIAÇÃO DE RISCOS PARA O GERENCIAMENTO ESTRATÉGICO DA SEGURANÇA DA INFORMAÇÃO

Josiane Kroll
Programa de Pós-Graduação em Engenharia de Produção (PPGEP)
Universidade Federal de Santa Maria (UFSM)
Santa Maria, RS – Brasil
josi.unc@gmail.com

Marcos Cordeiro D'Ornellas
Laboratório de Computação Aplicada (LaCA)
Universidade Federal de Santa Maria (UFSM)
Santa Maria, RS – Brasil
marcosdornellas@gmail.com

RESUMO

O número de incidentes de segurança contra as informações das organizações tem aumentado durante os últimos anos. As informações estão se tornando a cada dia mais vulneráveis devido à ausência de ações que impeçam a ocorrência de falhas de segurança. Este artigo mostra como a metodologia de avaliação de riscos reforça o gerenciamento estratégico da tecnologia da informação e aumenta o nível da segurança da informação.

PALAVRAS-CHAVE. Metodologia de riscos. Gestão da segurança. Planejamento estratégico.

ABSTRACT

The number of security incidents against organizations has increased during the last years. Information is becoming more vulnerable every day due to the absence of actions that prevent the occurrence of security failures. This article shows how the risk assessment methodology enhances the information technology strategic management, increasing protection against attacks, and raising the level for information security.

KEYWORDS. Methodologies of risks. Security management. Strategic planning.

1. Introdução

A segurança das informações tem sido a principal preocupação das organizações atualmente. Com a popularização dos recursos de informática, os problemas relacionados a ameaças, tentativas de ataques e invasões afetam os requisitos básicos dos sistemas computacionais (PINHEIRO, 2007). Sem a implementação de medidas adequadas de segurança as informações das organizações estão tornando-se cada vez mais vulneráveis. A falta de segurança dos sistemas de informação causa o descontentamento tanto dos clientes como dos próprios funcionários da organização. Para o desenvolvimento das organizações e de suas soluções, a gestão da segurança é um elemento fundamental para o sucesso (BEZERRA; NAKAMURA; RIBEIRO, 2006).

O aumento de danos causados por falhas de segurança tem feito com que, as organizações implementem mecanismos de proteção de diversas maneiras. Há organizações que implementam a segurança adotando mecanismos de proteção complexos interligados de diferentes formas no contexto de segurança dos sistemas de informação (BEZERRA; NAKAMURA; RIBEIRO, 2006). Porém, outras implementam programas de segurança informais que não atendem todos os requisitos de proteção e protegem parcialmente os as informações. Outras ainda, só implementam a segurança quando sofrem um dano. Esse tipo de organização é aquela que só efetua ações para reparar o dano, mas não planeja ações futuras. E por fim, há organizações melhor estruturadas que estabelecem programas de segurança com mecanismos e procedimentos avançados de proteção, mas que mesmo assim não estão livres da ocorrência de uma falha de segurança.

Embora qualquer mecanismo de proteção implementado pela organização possa ser benéfico e traga resultados positivos, é necessário estabelecer medidas de segurança eficazes que dêem tranqüilidade aos gestores e maiores garantias de proteção. Uma organização que possui um bom programa de segurança precisa planejar e estabelecer medidas de segurança conforme os objetivos da organização. Com a avaliação de riscos é possível prever situações futuras que estimulam a implementação de medidas de segurança. Além do mais, a avaliação de riscos fornece subsídios para se estabelecer o planejamento estratégico da segurança e das informações. O processo de avaliação de riscos também é uma das premissas cada vez mais adotada pelas organizações, sendo muitas vezes obrigatória devido a leis e regulamentações (BEZERRA; NAKAMURA; RIBEIRO, 2006).

Este artigo analisa o processo de avaliação de riscos para o gerenciamento estratégico da segurança da informação, buscando indícios de melhorias nas medidas de segurança tomadas pelas organizações. O objetivo é verificar como metodologia de avaliação riscos pode contribuir para o gerenciamento estratégico da segurança da informação. Também é discutido cada item encontrado que favorece o gerenciamento estratégico e promove possíveis garantias de segurança. As organizações podem se beneficiar desse estudo verificando como a avaliação de riscos pode útil para implementação da segurança. Ainda será possível verificar como a avaliação de riscos pode influenciar a tomada de decisões e minimizar possíveis falhas de segurança.

Este artigo está organizado da seguinte forma: na seção 2, são apresentados os trabalhos relacionados com a metodologia de avaliação de riscos e a gestão da segurança. Na seção 3, é apresentado o conceito de metodologia de avaliação de riscos e como ela pode ser implementada por uma organização. Na seção 4 são apresentadas as estratégias de segurança adotadas pelas organizações na busca por segurança. Na seção 5, é discutido como a avaliação de riscos contribui para o gerenciamento estratégico da segurança. Por fim, a seção 6 traz as conclusões do trabalho apresentado.

2. Trabalhos relacionados

Surgiram muitos trabalhos que indicam a metodologia de avaliação de riscos para a implementação da gestão da segurança da informação. Um exemplo disso é o trabalho proposto por Bezerra, Nakamura e Ribeiro (2006) que propõem a metodologia de avaliação de riscos para maximizar as oportunidades e minimizar os potencias de perdas nas organizações. A implementação do processo de avaliação dos riscos pode ser um instrumento para a tomada de

decisões pelas organizações, sejam elas para decisões técnicas, operacionais, gerenciais ou estratégicas (BEZERRA; NAKAMURA; RIBEIRO, 2006). Nesse trabalho o autor indica como o gerenciamento de riscos deve ser modelado, discutido e seguido pelas organizações na execução dos seus projetos.

Vellani (2006) também descreve a metodologia de avaliação de riscos como um guia para tomada de decisões e ainda discute a utilização de métricas de segurança para avaliar e gerenciar os processos de segurança implementados. O processo de análise da segurança fornece evidências para aplicar conceitos de segurança em cenários específicos ainda desconhecidos (VELLANI, 2006).

Outro trabalho realizado por Pinheiro (2007) cita os benefícios que a política de segurança pode adquirir se estiver baseada na avaliação de riscos e na integração de ferramentas. A segurança baseada na integração de soluções pode permitir a melhoria da postura da segurança e tratar dos aspectos críticos de proteção (PINHEIRO, 2007).

Hampshire e Tomimura (2004) propõem a implementação da análise de riscos para o projeto de implantação da segurança, onde eles citam a avaliação de riscos como uma ferramenta importante no processo de identificação e tratamento das vulnerabilidades encontradas na organização. O bom entendimento dos requisitos de segurança, a avaliação de riscos e o seu gerenciamento, além do envolvimento e comprometimento da direção da organização, são imprescindíveis no estabelecimento de uma política de segurança adequada (HAMPSHIRE; TOMIMURA, 2004).

Outros trabalhos citam a metodologia de avaliação de riscos como uma ferramenta que pode apoiar a implementação da segurança nas organizações, mas não relatam como este processo pode aumentar as garantias de proteção das informações. O trabalho proposto nesse artigo se difere dos demais por analisar a metodologia de avaliação de riscos como uma ferramenta para o gerenciamento estratégico da segurança da informação. É importante verificar a influência da metodologia de avaliação de riscos para estabelecer estratégias de segurança. O presente estudo procura verificar como os dados obtidos através da avaliação de riscos contribuem para implementar medidas eficazes de segurança. O resultado do bom gerenciamento da segurança fornece maiores garantias de proteção.

3. A metodologia de avaliação de riscos

O risco é a probabilidade de ameaças explorarem vulnerabilidades, gerando perdas de confidencialidade, integridade e disponibilidade das informações, causando impactos nos negócios (MAYER; FAGUNDES, 2008). Para identificar o risco é necessário especificar todas as ameaças e vulnerabilidades que podem afetar a segurança dos sistemas de informação em todo o seu ciclo de vida (HAMPSHIRE ; TOMIMURA, 2004).

Com a metodologia de avaliação de riscos é possível fazer a análise das vulnerabilidades e das ameaças que podem causar riscos à segurança as informações (VELLANI, 2006).

A metodologia de avaliação de riscos é definida como um processo que confirma as decisões de tecnologia da informação usadas para balancear os custos econômicos e operacionais das medidas preventivas para proteger os sistemas de tecnologia da informação e os dados que suportam a missão da organização (VELLANI, 2006).

A implementação da metodologia de avaliação dos riscos envolve a identificação dos ativos, das ameaças, das vulnerabilidades e dos riscos, avaliando e selecionando medidas de segurança para reduzir os riscos e para implementar medidas que assegurem a segurança (VELLANI, 2006).

Com a implementação da metodologia de avaliação de riscos é possível aumentar a eficiência operacional reduzindo assim as perdas, fraudes, falhas, acidentes, conduzindo a organização à melhoria dos seus processos (MAYER; FAGUNDES, 2008).

A avaliação de riscos é principalmente usada na indústria da segurança para dar visão do risco que está relacionado com a capacidade de enxergar o futuro, de modo a tomar as ações mais indicadas e necessárias para minimizar possíveis danos (BEZERRA; NAKAMURA; RIBEIRO, 2006).

Com a implementação da metodologia de avaliação de riscos focada na área de Tecnologia da Informação (TI) pode-se observar que a avaliação de riscos é uma forma de atender aos requisitos impostos pelas leis, normas e regulamentações relacionadas com a segurança da informação (MAYER; FAGUNDES, 2008, *apud* MÓDULO SECURITY, 2007).

3.1 Aplicação da metodologia de avaliação de riscos nas organizações

As organizações estão buscando identificar o que pode ocorrer e dessa forma propor ações preventivas que podem ser adotadas para impedir possíveis ataques. A avaliação de riscos procura identificar os riscos de segurança envolvidos com a confiança em um sistema definido (VELLANI, 2006). Com base no entendimento de alguns fatores como os ativos, as ameaças e as vulnerabilidades, é possível identificar a exposição a um risco.

Há diferentes metodologias para a avaliação de riscos (*TAG's Risk Assesment Process* (VELLANI, 2006); *OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation* (ALBERTS et. al, 2003)*; AS/NZS* 4360:2004 (HART, 2006); entre outras) e elas variam de acordo com os métodos de mitigação dos riscos aplicados. Embora a implementação dessas metodologias seja diferente, todas possuem o mesmo objetivo que é mitigar e avaliar exposição ao risco.

A metodologia de avaliação de riscos *TAG's Risk Assesment Process* (VELLANI, 2006) que possui o mesmo princípio das outras metodologias pode ser implementada por qualquer organização. Essa metodologia pode ser implementada como mostra a figura 01:

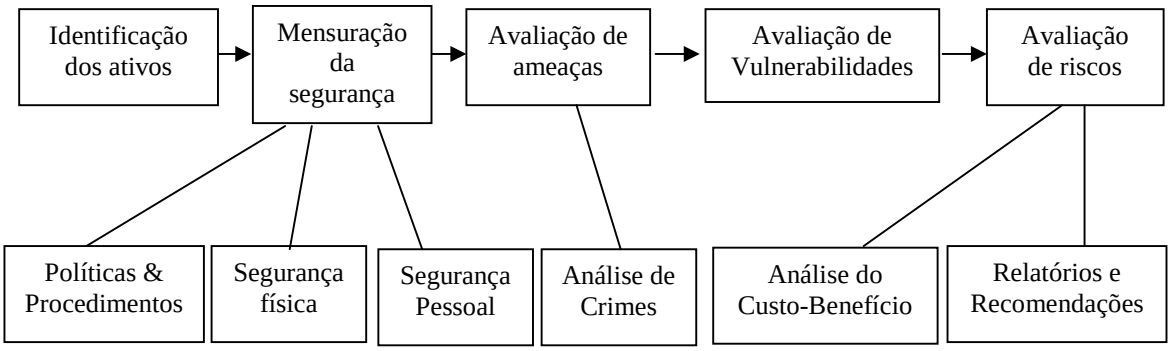

FIGURA 1 – TAG's - Processo de avaliação de riscos estratégico.
Fonte: Adaptado de Vellani (2006).

As atividades propostas na *TAG's Risk Assesment Process* são descritas a seguir:

1. *Identificação dos ativos:* a organização deve identificar quais ativos são críticos e devem ser protegidos. Esses ativos podem ser propriedades, pessoas e informações.

2. *Mensuração de segurança corrente:* é designada para a proteção dos ativos. A mensuração da segurança inclui a avaliação dos procedimentos, políticas, equipamentos de segurança física, segurança pessoal ou alguma outra combinação. A mensuração da segurança corrente pode ser realizada com a utilização de métricas e de testes.

3. *Avaliação das ameaças*: o processo de avaliação das ameaças inclui:
   - Identificação da ameaça: identifica o adversário em potencial e suas características;
   - Classificação da ameaça: identifica o objetivo e determina a sua criticabilidade;
   - Análise da Conseqüência/ Criticabilidade: analisa o efeito comprometimento de um ativo. A organização deve identificar as ameaças, analisá-las e colocá-las em uma escala que determina qual pode trazer mais dano a organização. Uma sub atividade do processo de avaliação de ameaças é a análise de crimes. Com a análise de crimes é realizada a identificação das ameaças sobre a perspectiva de proteção responsável determinada pela prática forense. A análise de crimes é composta por três fases:

- O exame lógico de crimes que tem motivado na mensuração preventiva;
- A identificação da freqüência de crimes específicos com o detalhamento de incidentes temporais (dia e hora) e o risco colocado para o proprietário da informação e;
- A revisão da aplicação de padrões de segurança e a mensuração preventiva.

4. *Avaliação das vulnerabilidades:* consiste da identificação das fraquezas dos programas de segurança que possibilitam uma ameaça explorar uma vulnerabilidade. Os passos para a avaliação das vulnerabilidades são:
   - Identificação dos recursos que necessitam de proteção;
   - Revisão do histórico de segurança e informações de incidentes se avaliável;
   - Preparação de uma pesquisa de segurança;
   - Identificação das mensurações de segurança existentes para cada propriedade e a determinação da efetividade de cada medida individual ou a combinação com outra.
   - Designação de uma classificação para cada propriedade baseada na escala de classificação das vulnerabilidades quantitativas ou qualitativas;
   - Preparação de um relatório com recomendações para mensurações individuais ou mudanças no programa de segurança.

5. *Avaliação dos riscos:* este processo é realizado através da identificação dos riscos sobre os ativos encontrados, da mensuração da segurança corrente e da avaliação das vulnerabilidades e ameaças. Na avaliação de riscos é realizada a análise do custo - beneficio da proteção contra cada risco. Essa avaliação fornece um relatório de dados e recomendações a serem seguidas pela organização.

Através dos dados obtidos com a metodologia de avaliação de riscos pode-se avaliar o real impacto das ameaças, medir as brechas de segurança e direcionar os investimentos em segurança (VELLANI, 2006). Isso fornece a organização mais confiança na tomada de decisões.

4. Estratégias de segurança adotadas pelas organizações

Uma estratégia pode ser definida como a elaboração de um plano com a determinação de objetivos de longo prazo e de ações adequadas para atingi-los. A estratégia de uma organização envolve a situação atual e planeja a situação futura com um conjunto de objetivos e ações para torná-los concretos (NICOLAU, 2001). Ainda, para as organizações uma estratégia define planos da alta administração para alcançar resultados consistentes com a missão e os objetivos gerais da organização (WRIGHT; KROLL; PARNELL, 2000).

As estratégias de segurança buscam planejar ações futuras definindo tarefas, atitudes e providências para eliminar e reduzir as causas das ameaças ou minimizar as conseqüências de ameaças que venham a se consumar. A estratégia de segurança deve estar alinhada aos recursos organizacionais com as ameaças e as oportunidades do ambiente (BENZ, 2008).

As estratégias de segurança para a proteção das informações na maioria das organizações são definidas basicamente através da implementação de políticas e procedimentos de segurança aliados a equipamentos de proteção física.

As políticas de segurança são estabelecidas para definir os direitos de acesso à informação dos usuários, suas obrigações de proteger e manter os dados proprietários da organização e a implantação de medidas a serem tomadas no caso da violação da segurança (GOMES; CARDOSO, 2008). Além disso, as políticas de segurança são desenvolvidas para assegurar que as organizações cumpram com as leis e regulamentações de segurança (BENZ, 2008).

Os procedimentos de segurança são implementados para cumprir com as exigências da política de segurança (VELLANI, 2006). De acordo com a política de segurança estabelecida são adotados ou não mecanismos de prevenção e identificação de ameaças, vulnerabilidades e riscos.

Os procedimentos de segurança também podem ser implementados pelas organizações sem que exista uma política de segurança definida.

As organizações também se preocupam com a segurança física além da lógica. A utilização de câmeras, sensores de presença, alarmes entre outros equipamentos fazem parte dos procedimentos de segurança adotados pelas organizações.

As organizações que desconhecem meios de planejar a segurança corretamente implementam mecanismos de proteção baseados em pesquisas de mercado verificando o que as outras organizações do meio fazem ou então, depois de sofrerem um ataque implementam uma medida de proteção mais eficiente que a anterior.

Sem uma estratégia de segurança estabelecida, os mecanismos de proteção são implementados pelas organizações sem serem gerenciados e sem uma perspectiva de até quando eles estarão trazendo o retorno esperado. A busca pela segurança faz com que as organizações tentem se proteger de todas as formas até mesmo implementando mais mecanismos de proteção que o necessário (PINHEIRO, 2007). Isso pode acarretar na sobrecarga de serviços de segurança sendo executados nas estações de trabalho e na alocação de recursos financeiros desnecessários.

As estratégias de segurança adotadas pelas organizações se diferem, mas todas buscam os mesmos objetivos, que são a garantia da continuidade dos negócios, a proteção das informações e o fortalecimento organizacional.

5. A avaliação de riscos e o gerenciamento estratégico da segurança

Estabelecer o gerenciamento da segurança das informações é um grande desafio para as organizações que crescem em complexidade de mecanismos de segurança e em incertezas de proteção (CARALLI; WILSON, 2004). Desenvolver além de um plano de segurança pode ser muito difícil para as organizações que procuram um modelo de gestão de segurança.

A metodologia de avaliação de riscos aplicada ao gerenciamento estratégico da segurança contribui para aumentar as garantias de proteção das informações das organizações. Isso pode ser observado pelos seguintes fatores:

a) A tomada de decisões reflete no conhecimento prévio dos riscos de segurança: com os dados obtidos pela avaliação de riscos é possível verificar quais são as ameaças e as vulnerabilidades que podem resultar riscos para a organização. A tomada de decisões então, é realizada baseada em fatores de segurança. Isso pode trazer mais confiança as organizações e reduzir erros de planejamento.
b) A política de segurança é bem estruturada: ao estabelecer uma política de segurança é necessário ter conhecimento das necessidades de proteção da organização. A avaliação de riscos fornece um panorama da segurança que contribui para o estabelecimento de procedimentos e métodos adequados.
c) O plano de segurança focaliza ações futuras: planejar a segurança envolve estabelecer ações de curto e longo prazo que garantam a progressão gradual da segurança. O plano de segurança pode ser mais bem estruturado e direcionado aos objetivos da organização.
d) Os investimentos em segurança são devidamente planejados: os investimentos em segurança podem ser reduzidos se bem planejados. Uma melhor distribuição dos recursos financeiros destinados à segurança pode ser realizada através da definição das urgências e prioridades.
e) São tomadas ações preventivas e não corretivas: se gasta muito tempo tentando reparar danos ocorridos pela falta segurança que poderiam ser evitados com simples medidas de proteção. A avaliação de riscos fornece informações necessárias para que sejam tomadas ações de prevenção a ataques.
f) Os recursos de segurança são gerenciados: com a avaliação de riscos é verificada a necessidade de proteção de cada recurso e então são implementados mecanismos de segurança com uma finalidade específica. O gerenciamento dos recursos de segurança é realizado através do planejamento e da correta distribuição da segurança. Assim, não há uma sobrecarga de processos de segurança sendo executados e nem de mecanismos de

segurança sendo implementados desnecessariamente. Com isso, ganha-se mais desempenho de máquina e se reduz custos.

g) A sensibilização da segurança está focada na realidade da organização: conscientizar os funcionários e os clientes baseando-se em dados obtidos pela avaliação de riscos é expor fatos reais da organização que realmente necessitam de medidas de proteção. Dessa forma a organização pode melhor elaborar a documentação de normas e regulamentações de segurança para os usuários.
h) A organização tem mais credibilidade dos clientes: uma organização que possui uma boa reputação e fornece garantias de segurança das informações dos seus clientes, consegue ampliar seus negócios.
i) O custo–beneficio da implementação da segurança é relatado: a avaliação de riscos fornece evidências dos benefícios que a organização pode ter se protegendo e dos custos decorrentes de não se prevenir. A avaliação de riscos fornece uma perspectiva futura de possíveis danos e cabe a cada organização decidir que medidas devem ser tomadas.

A metodologia de avaliação de riscos influência diretamente no estabelecimento de estratégias de segurança. As decisões de segurança são guiadas pelos dados obtidos como a avaliação de riscos. A identificação das ameaças, vulnerabilidades e dos riscos fornece indícios para implementação de estratégias. O planejamento financeiro destinado à segurança deve estar alinhado aos objetivos de proteção da organização. Com a definição de prioridades de proteção a organização pode gerenciar a estrutura de segurança e garantir que a segurança acompanha o crescimento da organização.

6. Conclusão

Com a metodologia de avaliação de riscos associada ao gerenciamento estratégico da segurança da informação, as organizações podem estabelecer medidas preventivas de segurança que podem tanto tratar de riscos emergenciais como prevenir futuros riscos. A segurança pode ser planejada para garantir que não ocorram incidentes de segurança e ainda para definir prioridades de proteção.

O gerenciamento estratégico da segurança pode trazer maiores garantias de proteção para organização através da implementação de métodos e de procedimentos apropriados ao ambiente de exposição das informações. Além da diminuição dos custos relacionados aos investimentos em segurança e reparos ocasionados falhas ou ausência de procedimentos de segurança.

Com o conhecimento das ameaças, vulnerabilidades e riscos, as organizações podem estabelecer estratégias que acompanham a evolução das mudanças e as alterações das características dos riscos. O entendimento da segurança pode apoiar as decisões relacionadas ao desenvolvimento, manutenção ou operação dos procedimentos de segurança.

Além dos fatores que contribuem para o aumento da segurança das informações, a metodologia de avaliação de riscos pode revelar fatos ainda desconhecidos pelas organizações. Essa premissa determina que não é possível estabelecer uma boa estratégia de segurança sem conhecer os riscos. Dessa forma a metodologia de avaliação de riscos influência diretamente no planejamento estratégico da segurança.

Com a metodologia de avaliação de riscos aliada ao gerenciamento estratégico da segurança das informações, as organizações podem estabelecer metas de proteção e ir aperfeiçoando os mecanismos de segurança conforme suas necessidades.

A metodologia de avaliação de riscos também promove a avaliação dos procedimentos de segurança que são executados pela organização. É possível verificar a eficácia desses procedimentos e melhor estruturar a segurança. Isso evita que políticas de segurança defasadas permanecem regentes nas organizações.

Referências

Alberts, C.; Dorofee, A.; Stevens, J.; Woody, C.; *Introduction to the OCTAVE Approach.* Carnegie Mellon University - Software Engineering Institute. Pittsburgh, 2003.

Benz, K. H. *Alinhamento estratégico entre as políticas de segurança da informação e as estratégias e práticas adotadas na TI: Estudos de casos em instituições financeiras.* 200f. Dissertação (Mestrado em Administração) – Universidade Federal do Rio Grande do Sul– UFRGS, Porto Alegre, 2008.

Bezerra, E. K.; Nakamura, E. T.; Ribeiro, S. L. *Maximizando Oportunidades com Gestão de Segurança e Gerenciamento de Riscos*. [S.I.:s.n.] [2006?].

Caralli, R. A.; Wilson, W. R. *The Challenges of Security Management.* Networked Systems Survivability Program Software Engineering Institute, 2004.

Gomes, O. H.; Cardoso, A. L. S. *Um olhar epistemológico sobre segurança digital nas organizações.* Universidade Federal da Bahia, Salvador-BA, 2008.

Hampshire, M. C. S.; Tomimura, C. T. *Proposta de implementação da Análise de Risco em um Projeto de implantação da Segurança da Informação.* Centro Tecnológico da Marinha em São Paulo (CTMSP), São Paulo – SP, [2004?].

Hart, Barry. *AS/NZS 4360 SET Risk Management Set.* SAI Global, 2006.

Mayer, J.; Fagundes, L. L. *Proposta de um Modelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação.* VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais, São Leopoldo-RS, 2008.

Nicolau, I. *O conceito de estratégia.* INDEG/ISCTE - Instituto para o desenvolvimento da Gestão Empresarial: Campo Grande, 2001.

Pinheiro, J. M. S. *Os benefícios da política de segurança baseada na avaliação de riscos e na integração de ferramentas.* Revista Científica do Centro Universitário de Volta Redonda, 2007.

Vellani, K. H. *Strategic Security Management: A Risk Assessment Guide for Decision Makers.* [S.I.] USA: Elsevier, 2006. 416 p.

Wright, P.; Kroll, M.J.; Parnell, J. *Administração Estratégica. Conceitos.* São Paulo: Atlas, 2000. 433p.