ARTIGO / ARTICLE

LATIN AMERICAN JOURNAL OF BUSINESS MANAGEMENT

Impactos dos procedimentos dos usuários na segurança da informação em ambientes de rede de computadores

Paulo César Ribeiro Quintairos[1]
Edson Aparecida de Araújo Querido Oliveira[2]
Mônica Gonçalves de Mendonça[3]

Resumo

Os Sistemas de Informações — SIs são continuamente afetados pela evolução dos elementos da Tecnologia da Informação — TI. A conexão em rede dos computadores que integram um SI acarretou sérios problemas quanto à segurança da informação. Assim, a gestão da segurança da informação passou a ter importante papel na estratégia de conhecer riscos e definir controles adequados para os SIs. Neste trabalho é apresentado um estudo de caso, realizado em uma instituição federal de pesquisa e desenvolvimento, sobre os impactos do comportamento dos usuários na segurança de um SI. A partir da análise dos *logs* de acesso a internet dos usuários dos sistemas da empresa, foi construída uma tabela de probabilidade e impacto desses logs para a segurança do sistema. Assim foram identificados os riscos potencialmente danosos à segurança do sistema provenientes desses acessos. Os resultados obtidos não apontaram alta significância de risco nos *logs* dos usuários. Entretanto, mostram a necessidade de adotar uma política de segurança, aliada a monitoração e conscientização dos usuários quanto aos riscos que o uso da internet acarreta ao SI da organização.

Palavras-chave: Tecnologia da Informação; Rede de Computadores; Segurança da Informação e Registro de Logs

Recebimento: 30/11/2011 – Aceite: 12/12/2011

[1] Doutor em Física pelo CBPF. Docente do Mestrado em Gestão e Desenvolvimento Regional. End: Rua Expedicionário Ernesto Pereira, 225, Centro, Taubaté – SP, Brasil. E-mail: paulo.quintairos@unitau.com.br

[2] Doutor em Engenharia Aeronâutica e Mecânica pelo Instituto Tecnológico de Aeronáutica. Docente do Mestrado em Gestão e Desenvolvimento Regional. E-mail: edson@unitau.br

[3] Mestre em Desenvolvimento Regional pela Universidade de Taubaté. E-mail: monica@ita.br

Security information in network computer environments: a study on the impact of the user's procedures

Abstract

The Information Systems - SI´s are continuously affected by the evolution of the elements of Information Technology - IT. Nowadays, the IS involves computers connected in a networking. This fact is a source of problems with regard to information security. Thus, the management of information security has to play an important role in the strategy to meet risks and set appropriate controls for the IS´s. This paper presents a case study, carried out in a brazilian federal research and development organization, about the impacts of the users behavior in an IS security. From the analysis of access logs of Internet users of enterprise systems, we built up a table of likelihood and impact of these logs to system security. Once the risks have been identified potentially harmful to the security system from these attacks. The results did not show highly significant risk in the logs of users. However, show the need to adopt a security policy, coupled with monitoring and awareness of users about the risks that the use of the Internet brings to the SI of the organization.

Keywords: Information Technology; Computer Networking; Security Information and Registration Logs

Introdução

O uso disseminado da Tecnologia da Informação nos Sistemas de Informações acarretou o aumento contínuo da dependência das empresas no funcionamento de sistemas integrados de Informática e Telecomunicações. Isso acarretou o aumento com as preocupações relativas à integridade e a segurança dos sistemas. A informação sempre foi um dos bens mais importantes de uma organização. Entretanto, antes do uso dos sistemas de informação baseados em TI, as informações mais críticas para as empresas podiam ser guardadas e trancadas dentro de gavetas e cofres. Atualmente, independente do grau de tecnologia da organização, a proteção da informação é uma das preocupações dos executivos e proprietários das empresas (FONTES, 2008).

No âmbito da Tecnologia da Informação (TI), o sistema de segurança é responsável pela integridade, disponibilidade e confidencialidade das informações armazenadas nos Sistemas de Informações (SIs). O sistema precisa disponibilizar as informações, sempre que solicitadas pelos usuários autorizados, de forma suficientemente completa e precisa, a fim de satisfazer as necessidades da organização (SÊMOLA, 2003).

Nakamura e Geus (2007) descrevem que, enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e a falta de novas oportunidades de negócios.

No âmbito da informação, deve-se ter em mente que o aprimoramento dos sistemas de segurança tem de ser contínuo, pois a tecnologia e os sistemas evoluem rapidamente. A segurança de redes deve ser considerada como parte essencial para a proteção da informação. Entretanto, uma boa estratégia de segurança que deve levar em consideração os aspectos humanos e processuais da organização (NAKAMURA, GEUS, 2007).

Neste artigo é apresentado um estudo sobre como comportamento dos usuários, em relação aos procedimentos de segurança pode influenciar o grau de exposição de uma rede de computadores a problemas de segurança. O trabalho apresentado é um estudo de caso realizado em uma instituição de pesquisa e desenvolvimento do governo federal brasileiro.

A análise apresentada neste trabalho foi realizada a partir dos *logs* de acesso ao ambiente de rede de computadores da organização estudada. O método adotado foi identificar padrões de comportamento dos usuários potencialmente danosos à segurança do sistema. Isso permitiu estabelecer uma relação entre o comportamento dos usuários e o grau de exposição a

riscos que a rede está sujeita. A partir da identificação dos riscos encontrados.

Observa-se que a análise apresentada neste trabalho não envolveu a identificação dos funcionários e usuários do sistema estudado, nem qualquer tipo de avaliação do desempenho da rede de computadores estudada. A finalidade deste trabalho é contribuir com o diagnóstico e aperfeiçoamento das políticas de segurança da informação no ambiente de rede de computadores da instituição em estudo, podendo ser utilizada como referência em outras organizações da região.

Revisão da literatura

A tecnologia da informação (TI) atualmente é apontada como a espinha dorsal dos negócios. Essa mudança exige a aproximação da área de tecnologia aos negócios corporativos e também o alinhamento das estratégias de TI com as estratégias corporativas (SALLÉ, 2004).

O termo informática, como citado por Albertin (1999), é bastante genérico e acaba por englobar alguns componentes para o tratamento da informação, dentre eles a Tecnologia da Informação e Sistema de Informação (SI). Para Cash, McFarlan e Mckenney (1992, *apud* ALBERTIN) Tecnologia da Informação é um termo amplo, e engloba as tecnologias de computadores, telecomunicações e automação de escritório.

Balloni (2006, p.10) define TI como o "conjunto dos recursos tecnológicos e computacionais cuja função é a geração e o uso da informação visando criar, armazenar, difundir dados e informação, no processo de criação de conhecimentos".

Segundo Tapscott (1997), a adoção de TI possibilita aumentar a produtividade, de modo que a eficiência resulte em economia de tempo que, por sua vez, pode ser reinvestida na eficácia. O autor acrescenta ainda que não é mais possível elaborar uma estratégia ou um projeto de negócio sem considerar a importância da tecnologia.

Foina (2009) aponta que a Tecnologia da Informação como abordagem integrada para os problemas mantém como paradigma o fato de que qualquer solução deve considerar as vertentes de tecnologia, a cultura empresarial e as necessidades dos recursos humanos envolvidos.

Martens (2001, *apud* ALTER, 1996) conceitua TI como sendo um conjunto de hardware e software que possibilitam o funcionamento dos SIs, que por sua vez influenciam os processos de negócios. Estes processos podem ser vistos como etapas que utilizam pessoas, informações e outros recursos, para criar valor aos clientes.

Balloni (2006) descreve SI como sendo um conjunto de componentes, que estabelece uma relação com objetivo de coletar dados como entrada, armazenar e transformar esses dados em informação e após isso, divulgar a informação como saída para apoiar a tomada de decisão gerencial, e também apoiar a coordenação, controle, análise e visualização na organização.

Lucas (1986 *apud* ALBERTIN, 1999, p.18) define Sistema de Informação (SI) como um conjunto de procedimentos organizados que, quando executados, proveem informação para suportar a tomada de decisão e o controle numa organização, este termo enfatiza o lado aplicativo da tecnologia de informática utilizado nos procedimentos para tratar as informações existentes.

O'Brien (2004, p. 6) é mais abrangente na sua descrição, pois , ele conceitua SI como "um conjunto organizado de pessoas, hardware, software, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização."

O autor relata ainda (2001, p.20) que os SIs e as TIs devem apoiar as estratégias e processos empresariais, bem como a estrutura e a cultura organizacional de uma empresa, com objetivo de aumentar o valor dos negócios e proporcionar um ambiente dinâmico. Para que haja o efetivo funcionamento, os SIs requerem cinco requisitos básicos: pessoas, hardware, Software, dados e redes.

Segundo Freitas *et al*. (1997, p.24), "a importância da informação dentro das organizações aumenta de acordo com o crescimento da complexidade da sociedade e das organizações. Em todos os níveis organizacionais (operacional, tático e estratégico), a informação é um recurso fundamental".

Albertin (1999) destaca que o tratamento das informações por meio de Sistemas de Informações (SIs) é parte integrante das organizações que oferecem produtos e ou serviços. Os SIs partem por englobar desde a concepção, o planejamento e a produção até a comercialização, distribuição e suporte. Assim sendo, os SIs são atualmente um componente crítico do planejamento estratégico, sendo elemento essencial para que a TI propicie vantagens competitivas às organizações.

Segundo Laudon e Laudon (2004), Tecnologia de Informação e Organizações influenciam-se mutuamente, sendo que a TI deve estar alinhada aos negócios da organização. Somente assim poderá fornecer as informações de que seus importantes grupos internos precisam. Entretanto, os autores destacam que a interação entre Tecnologia de Informação e Organizações é complexa e influenciada por diversos fatores intervenientes, entre eles a estrutura da Organização.

A TI pode proporcionar mudanças diversas, desde uma simples automatização de processos até uma profunda alteração na maneira de conduzir os negócios. Cabe, portanto, à organização avaliar e planejar suas expectativas e necessidades perante o mercado, qual a estratégia a ser adotada e o papel da TI frente aos objetivos organizacionais.

Laurindo (2002) descreve o papel da TI como uma estratégia competitiva, principalmente pelas novas possibilidades de negócios que a TI proporciona. Dada a importância dos SIs e da TI para as organizações, é necessário aprimorar a administração desses sistemas.

Atualmente o planejamento dos recursos de Tecnologia da Informação se encontra mais estruturado e tomando vida própria, como exemplo pode-se citar o Plano Diretor de Informática e o Planejamento Estratégico da Tecnologia da Informação, levando ainda em consideração que os recursos de tecnologia da informação devam estar a serviço do negócio da organização (FONTES, 2008).

Da mesma forma o processo de segurança e proteção da informação necessita de um planejamento, devendo estar adequado ao negócio.

Mas o que considerar em um planejamento de segurança da Informação? Segundo Fontes (2008) alguns aspectos devem ser considerados:

- Características do negócio – pois todo processo de segurança deve estar alinhado com as características do negócio da organização.
- Estrutura do negócio – Disso irá depender como a organização tratará sua informação, de forma centralizada ou descentralizada, pois a maneira como a organização trata suas informações influenciará na gestão dessas informações.
- Plano estratégico da Segurança – a partir da definição da estrutura da organização deve-se elaborar um planejamento estratégico de segurança para a organização, definindo-se políticas, responsabilidades e escopo dos recursos a serem protegidos.
- Mapear as vulnerabilidades e priorizações – com o envolvimento de diversos recursos e diversas tecnologias se torna fundamental fazer o mapeamento para identificar vulnerabilidades existentes e então definir prioridades para implementação de controles.
- Identificar recursos necessários – Além da aquisição de softwares e equipamentos, se faz necessário a aquisição de tempo para os usuários, conscientizando-os na proteção das informações.
- Definir níveis de segurança – Cada organização deve definir o seu patamar de segurança, devendo estar compatível com seu negócio.

Não existe solução certa ou errada, existe sim a solução mais adequada e menos adequada a cada organização. Como qualquer outro

planejamento o planejamento de segurança deve ser feito, pois ele é o rumo a ser seguindo com objetivos bem definidos.

Em um mundo globalizado e com rápidos avanços tecnológicos, faz com que as organizações busquem o mais alto nível de competitividade, no qual a conquista por novos mercados torna-se uma é disputa acirrada (NAKAMURA, GEUS 2007).

Os autores supracitados descrevem que a propriedade determinante nos ambientes corporativos é a complexidade que envolve a comunicação entre diferentes tecnologias, diferentes usuários, diferentes culturas e diferentes políticas internas. Diante dessa complexidade a segurança necessária a ser implementada é igualmente complexa, onde se envolve aspectos de negócio, humanos, tecnológicos, processuais e jurídicos.

De fato, a tecnologia faz parte de um pilar que inclui ainda os processos e as pessoas, que também são considerados para a elaboração de uma estratégia de segurança coerente, de acordo com os aspectos dos negócios da organização. A segurança em ambientes cooperativos será o resultado do conjunto de esforços para atender ao ambiente e as tecnologias, saber como as utilizar e implemantar de modo correto.

Fernandes e Abreu (2008) relatam que a Política de Segurança da Informação está associada ao risco que a TI representa para a continuidade dos negócios da organização.

Descrevem ainda que a dimensão dessa política será tanto maior quanto mais interconectada estiver à organização e mais estratégico for o papel que a TI representa para o negócio, uma vez que eventos de risco estão relacionados com a segurança de dados e informações podendo trazer grandes prejuízos para a organização.

O *NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY* - NIST (2002) relata que os requerimentos de segurança são baseados em padrões sistemáticos, evolutivos e que identificam as vulnerabilidades dos ativos (pessoas, hardware, software, informação), dos processos e das informações associados aos sistemas de TI distribuídos nas áreas de segurança gerencial, operacional e técnica.

O NIST (2005, p.1) recomenda que, ao se definir o modelo de segurança, algumas perguntas consideradas essenciais devam ser respondidas, como: Quais controles de segurança são adequados para proteger os sistemas de informação e garantir a operacionalização da organização? O plano de implementação dos controles está adequado à realidade? Quais níveis de segurança são requeridos para garantir a confidencialidade das informações?

O NIST (2005) aponta que a segurança da informação está associada à gestão de riscos, pois a avaliação de riscos recomenda os controles

mínimos, os documentos e o plano de segurança para os sistemas de informação.

Na abordagem da *Organization for Economic Co-Operation and Development* a segurança da informação ganha uma abrangência estratégica, requerendo ações efetivas do Estado, interagindo com o setor privado e a sociedade. Esses pilares que a OECD defende, devem integrar cada um com sua responsabilidade específica, e construir uma cultura de segurança da informação (OECD, 2005).

Na prática, a definição de um modelo para a segurança da informação tem como objetivo assegurar o negócio da empresa, alicerçado nos aspectos da confidencialidade, integridade e disponibilidade, conforme observado por Pfleeger (1997, *apud* Mendonça, 2007).

Ao utilizar um conjunto de controles será possível conhecer e gerir riscos, orientar ações de continuidade do negócio, níveis de responsabilidade e conformidade com diretrizes, legislações e acordos contratuais, como recomendado pelo NIST (2005, p.1).

A responsabilidade pelo nível correto de segurança da informação deve estar apoiada em uma decisão estratégica de negócios, tomando como base um modelo de Governança da Segurança da Informação que seja capaz de contemplar a análise de risco (MOREIRA, BERNARDES 2005).

Uma administração eficiente da segurança da informação deve prover a proteção de todos os elos da corrente, ou seja, todos os ativos que compõem um negócio sejam eles tecnológicos, de infraestrutura física, informações e pessoas.

Todos em uma organização são responsáveis pela segurança da informação, portanto sé faz necessário haver o envolvimento de todos aqueles que a manipulam dentro da organização – funcionários, estagiários, parceiros e prestadores de serviço. Porém isto só é alcançado através de uma solução corporativa de segurança da informação, implementada com a criação de uma estrutura corporativa adequadamente posicionada no organograma da organização (Sêmola, 2003).

Completando ainda, segundo ENTRUST (2004) para que as organizações obtenham sucesso no processo de segurança da informação, os gestores precisam tornar a segurança computacional uma parte integrante da operação do negócio da organização.

Nesta era digital, como as organizações usam a automatização da Tecnologia da Informação de Sistemas para processar suas informações, para um melhor suporte as suas missões, a Gestão de riscos desempenha um papel fundamental para proteger os ativos de informação da organização. Segundo Brandão e Fraga (2008 apud Swanson e Guttman, 1996) a Gestão de

riscos está baseada em princípios e boas práticas de gerenciamento e segurança, para auxiliar a tomada de decisões.

A gestão de riscos passa a ser então um processo utilizado em todos os tipos de empreendimentos com objetivo de identificar oportunidades e ameaças ao negócio. No ambiente de segurança da informação um processo eficaz de gerenciamento de risco é um componente importante para se alcançar o sucesso.

O principal objetivo de uma eficiente gestão de risco é o de proteger a organização e sua capacidade de desempenhar sua missão, e não devendo ser tratado apenas como uma função tática, mas sim como função essencial da gestão da organização. O risco não pode ser completamente eliminado, o gerenciamento do risco permite aos gestores informações sobre o programa de segurança, visando equilibrar os custos operacionais e econômicos das medidas de proteção e obter ganhos na capacidade de sua missão (NIST SP800-100).

No que diz respeito à segurança da informação, a gestão de risco está focada na prevenção e mitigação dos danos, e as ações dependem do tipo do negócio e das ameaças às quais estão submetidas ABNT ISO/IEC (Guia 73:2005, p.1).

Para Soler et al. (2006) Gestão de risco é o processo de identificação, análise, desenvolvimento de respostas e monitoramento dos riscos em projetos, com objetivo de diminuir a probabilidade e o impacto de eventos negativos e de aumentar a probabilidade e o impacto de eventos positivos.

"Gerenciar riscos envolve a tomada de decisões em ambiente incerto, complexo e dinâmico" (SOLER et al. 2006, pag. 26) percebe-se que a palavra risco está direta ou indiretamente ligada à incerteza, pois trata-se de eventos que podem ocorrer ou não. E mesmo ocorrendo o grau de precisão em que poderão ocorrer é impreciso.

Para que haja uma eficiente Gestão de Riscos temos que ter a noção correta dos riscos, que permitirá que se definam e ferramentas para mitigá-los. Infelizmente os riscos podem ser identificados e reduzidos, mas nunca totalmente eliminados Brandão e Fraga (2008, apud Garfinkel et al. 2003).

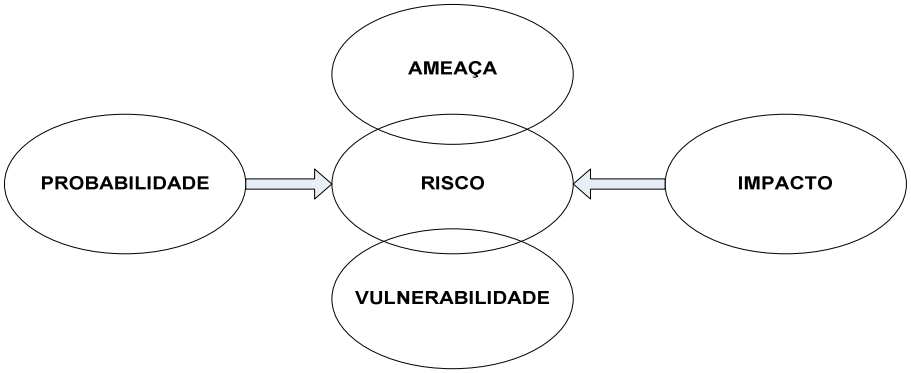
Brandão e Fraga (2008, apud Stoneburner et al. 2002) define o risco como o impacto negativo da exploração de uma vulnerabilidade, considerando a probabilidade do uso do mesmo e o impacto da violação. Ou seja, o risco é uma tentativa de quantificar as possibilidades de violação e os prejuízos decorrentes do impacto do mesmo.

A ABNT, em sua guia 73 (2005, p.2), conceitua Risco como a combinação da probabilidade de um evento e de suas consequências, onde: probabilidade é o grau de possibilidade de que um evento ocorra; evento é a

ocorrência de um conjunto específico de circunstâncias; consequências são resultados de um evento.

O NIST, em seu documento 800-100 (2006, p.85), trata o risco como a probabilidade de que uma fonte de ameaça e uma potencial vulnerabilidade resultem em um evento que cause um impacto adverso à organização, ou seja, acontecendo o cruzamento de uma ameaça com uma vulnerabilidade, o risco estará presente. A Figura 1 apresenta um esquema do processo de análise de risco.

Figura 1: Processo de risco



Fonte: NIST, 800-100, 2006, p.85

O gerenciamento de riscos aplicado aos Sistemas de Informação é tratado pelo *Technology Administration* do (NIST), órgão do Governo americano responsável pela segurança computacional e gerenciamento de TI das organizações públicas, como sendo composto essencialmente pelos processos de: Análise de Risco (Identificação, avaliação e impactos); Mitigação do Risco (priorização, implementação e manutenção das medidas de proteção) e Avaliação do Risco (contínua revisão dos processos chaves para implementar o gerenciamento de risco).

Uma abordagem sistêmica da Gestão de Riscos de Segurança da Informação se faz necessário para identificar as necessidades da organização em relação aos requisitos da segurança da informação e para criar um sistema de gestão de segurança da informação (SGSI), que seja eficaz. Esta abordagem deve estar adequada ao ambiente da organização e em particular deve estar alinhada com o processo maior de gestão de riscos corporativos. A gestão de riscos de segurança da informação deve ser parte integrante das atividades de gestão de segurança da informação e aplicada

tanto à implementação quanto a operação cotidiana de um SGSI (NBR ISO/IEC 27005:2008).

A gestão de riscos deve analisar os possíveis acontecimentos e suas conseqüências, antes de decidir o que será feito e quando será feito, com o objetivo de reduzir os riscos a um nível aceitável (NBR ISO/IEC 27005:2008).

A Norma Brasileira ISO/IEC 27005 (2008) descreve que a Gestão de riscos compreende um conjunto de atividades coordenadas para direcionar e controlar uma organização no que se refere aos riscos. A gestão de riscos inclui as seguintes macro atividades principais:

a) Análise de riscos – uso sistemático de informações para identificar fontes de ameaças, a fim de estimar os riscos;
b) Avaliação de riscos – processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco; e
c) Tratamento de riscos – processo de seleção e implementação de medidas para modificar um risco.

E que a necessidade da gestão de riscos é unanime em todos os empreendimentos.

Toda Organização, independente do setor (público, privado ou terceiro setor), deve investir no negócio baseado na análise e avaliação dos riscos, contribuindo para o sucesso do empreendimento.

O risco é inerente a qualquer atividade, podendo envolver perdas e oportunidades. No que diz respeito à governança, o risco está associado a vários setores, mas o importante é conhecer e ter a capacidade de administrá-lo.

O Instituto Brasileiro de Governança Corporativa (IBGC) lançou o "Guia de Orientação para o Gerenciamento de Riscos Corporativos", contendo recomendações sobre o Gerenciamento de Riscos Corporativos (Instituto Brasileiro de Governança Corporativa, 2007 p.6).

O IBGC (2007, p.7) apresenta que o "conceito atual de riscos envolve a quantificação e qualificação da incerteza, tanto no que diz respeito a perdas como aos ganhos, com relação ao rumo dos acontecimentos planejados, seja por indivíduos ou por organizações".

A implantação de um modelo de Gestão de Risco Corporativo (GRC), segundo o Instituto Brasileiro de Governança Corporativa (IBGC, 2007, p.8), traz alguns benefícios para a organização:

- Preserva e aumenta o valor da organização, mediante a redução da probabilidade de impacto de eventos de perdas no mercado;
- Promove maior transparência ao informar aos investidores e ao público, os riscos aos quais a organização está sujeita e ações adotadas para mitigar;

- Melhora o padrão de governança mediante a explicitação dos riscos em consonância com o posicionamento com os acionistas e a cultura da organização.

A Gestão de Riscos está baseada em princípios e boas práticas de gerenciamento e segurança, para auxiliar a tomada de decisões.

Existem métodos através dos quais o processo de gerenciamento de riscos pode ser implementado com sucesso em uma organização. É necessário que a organização use o método que melhor se adéque as suas circunstâncias, para cada aplicação específica do processo (NBR ISO/IEC 2005:2008).

Entre as ferramentas metodológicas disponíveis para o desenvolvimento da gestão de risco, destaca-se o modelo PDCA, adotado pela ISO/IEC 27001, este modelo é aplicado para estruturar todos os processos do Sistema de Gestão de Segurança da Informação (SGSI).

Para a ABNT, em sua norma NBR ISO/IEC 27001:2006, a adoção do modelo PDCA (PLAN, DO, CHECK, ACT) refletirá os princípios para a governança da segurança de sistemas de informação e redes.

Em um SGSI, a definição do contexto, a análise/avaliação de riscos, o desenvolvimento do plano de tratamento do risco e a aceitação do risco, fazem parte da fase **"Planejar"**. Na fase **"Executar"** do SGSI, as ações e controles necessários para reduzir os riscos para um nível aceitável não implementado, de acordo com o plano de tratamento do risco. Na fase **"Verificar"** do SGSI, os gestores determinarão a necessidade de revisão da avaliação e tratamento do risco à luz dos incidentes e mudanças nas circunstâncias. Na fase **"Agir"** as ações necessárias são executadas, incluindo a reaplicação do processo de gestão de riscos de segurança da informação. O Quadro 1 resume este alinhamento:

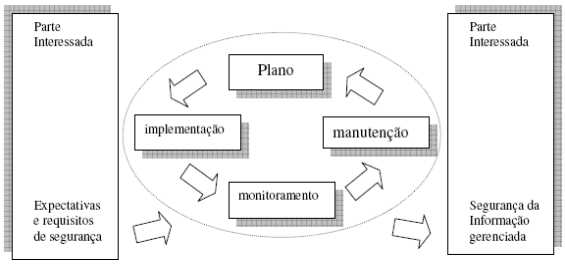
Quadro 1: Processos de gestão de risco

Processo do SGSI	**Processo de Gestão de Riscos de Segurança da Informação**
Planejar	Definição do contexto; Analise/avaliação de riscos; Definição do Plano de Tratamento de risco; Aceitação do risco.
Executar	Implementação do Plano de Tratamento de Risco.
Verificar	Monitoramento contínuo e Análise crítica de riscos.
Agir	Manter e melhorar o processo de Gestão de riscos de Segurança da Informação.

Fonte: ABNT NBR ISO/IEC 27005:2008

A Figura 2 ilustra como um Sistema de Gestão de Segurança da Informação (SGSI) considera as entradas de requisitos de segurança da informação, expectativas das partes interessadas e as ações necessárias e processos resultam no atendimento.

Figura 2: Modelo PDCA



Fonte: ABNT NBR ISO/IEC 27001:2006

Segundo a norma NBR ISO/IEC 27005 (2008) o processo de avaliar os riscos e selecionar os controles pode precisar ser realizado várias vezes, de forma a cobrir diferentes partes da organização ou de sistemas de informação específicos.

Complementando ainda, é conveniente que a análise/avaliações de riscos inclua um enfoque sistemático de estimar a magnitude do risco (análise do risco) e o processo de comparar os riscos estimados contra

critérios de risco para determinar a significância do risco (avaliação do risco).

Essas atividades devem ser realizadas periodicamente, para contemplar as mudanças significativas que ocorrem no ambiente de negócio, e conseqüentemente nos requisitos de segurança da informação, no que se refere aos ativos informacionais, levando em consideração as ameaças, vulnerabilidades e impactos diante de uma situação de riscos.

Durante todo o processo de gestão de riscos de segurança da informação, é importante que os riscos e a forma com que são tratados sejam comunicados ao pessoal das áreas operacionais e gestores apropriados.

Mesmo antes do tratamento do risco, informações sobre o que foi identificado como sendo um risco podem ser úteis para um gerenciamento de incidentes e ajudar a reduzir possíveis prejuízos.

Por meio de uma plena conscientização por parte dos Gestores e todo o efetivo da organização, no que diz respeito aos riscos, à natureza dos controles aplicados para mitigá-los e as áreas definidas como de interesse pela organização auxilia a lidar com os incidentes e eventos não previstos de maneira mais efetiva.Toda atividade de análise e avaliação de riscos deve ser realizada de forma metódica, capaz de gerar resultados comparáveis e reproduzíveis (NBR ISO/IEC 27001:2006).

Wack, at al. (NIST SP800-42, 2001) descreve alguns testes de segurança que são adotados no modelo NIST, considerando este fator uma atividade fundamental. Os testes podem ser abordados de maneira diferenciada, podendo ou não ser executados de acordo com o Sistema. Cada teste possui diferentes ferramentas que podem auxiliar na sua automatização. Os tipos de testes de segurança são: mapeamento da rede; rastreamento de vulnerabilidades; teste de penetração; avaliação de segurança; quebra de senhas; revisão de *logs*; conferência de integridade e detecção de vírus.

Método

O método científico, de acordo com Cervo e Bervian (1996), é o ordenamento que deve ser utilizado para organizar e criar uma dinâmica aos processos necessários para alcançar os resultados e respostas procurados. Assim, o método utilizado no presente artigo foi o estudo de caso, tomando como cenário um ambiente de rede de dados em uma Instituição Pública Federal de P&D.

Do ponto de vista dos objetivos, esta é uma pesquisa descritiva, pois procurou com certa precisão descrever a frequência com que o fenômeno

ocorreu. Já do ponto de vista dos procedimentos técnicos, é documental, pois foram analisados arquivos disponibilizados pela Instituição Pública, com o objetivo de descrever e comparar hábitos e costumes dos servidores que utilizam a rede de computadores, baseando-se na análise de *logs* do sistema de rede e na documentação normativa utilizada pela Organização estudada.

Os dados utilizados como base para esta pesquisa foram extraídos dos arquivos de *logs* registrados na máquina que hospeda o serviço de Proxy da instituição, por onde trafega todo acesso interno e externo ao sistema da rede estudada. Os *logs* registram quem acessou os recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram efetuadas. A população em estudo consta de 300 servidores que utilizam a rede de computadores, e tendo como amostra os registros de *logs* de acesso a rede de computadores.

Segundo o Tribunal de Contas da União – TCU (2007) arquivos de *logs* são usados para registrar ações dos usuários, constituindo-se em ótimas fontes de informação para auditorias futuras, o que na maioria das vezes é o único recurso que um administrador possui para descobrir as causas de um problema ou um comportamento anômalo.

Foi desenvolvido um programa de computador que executou a leitura dos arquivos de *log*, registrados no serviço de Proxy, tomando como base os meses de Abril, Junho e Agosto. Os dados foram ajustados a uma planilha, que permitiu a leitura e a estratificação das ocorrências.

Utilizando o complemento *WOT* que funciona em anexo ao navegador *Firefox*, foi realizada a classificação dos endereços acessados através do protocolo http (*hiper text transfer protocol*), tomando como critério a tabela 1 representada a abaixo.

Após esse processo, as informações foram classificadas por níveis de risco, como mostrado no Quadro 2.

Quadro 2: Classificação em níveis de acesso

NÍVEL DE RISCO		TIPOS DE ACESSO
NULO	0	Internos; Instituições de Ensino e Pesquisa; Governamentais.
MUITO BAIXO	1	Portais de busca; Notícias nacionais; Bancos.
BAIXO	2	Comércio empresas renomadas; Notícias internacionais.
ALTO	3	Comércio empresa pouco conhecido
MUITO ALTO	4	Relacionamentos; Bate-papo; Sites pornográficos.

Fonte: Quintairos, 2010

Os dados coletados e analisados foram utilizados para preencher a tabela de Probabilidade e Impacto (P-I), a qual é caracterizada em uma matriz. Trata-se de uma ferramenta para realizar a priorização dos fatores de risco. Essa tabela possui como colunas a expectativa de ocorrência de um fator de risco e como linhas a expectativa do impacto caso o fator de risco ocorra. As expectativas são informadas através de categorias, conforme mostrado no Quadro 3.

Quadro 3: Probabilidade x Impacto

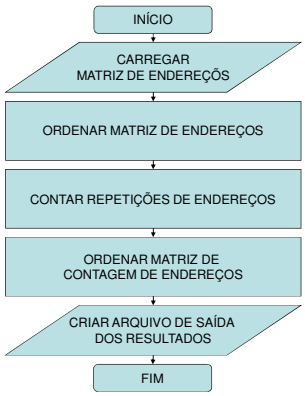
Probabilidade de ocorrência	Impacto sobre o projeto				
	Muito alto	Alto	Baixo	Muito baixo	Nulo
Muito alto					
Alto					
Baixo					
Muito baixo					
Nulo					

Fonte: Schmitz, Alencar e Vilar (2006, pág. 39)

Resultados

Nesta seção são apresentados os resultados obtidos por meio da análise estatística dos *logs* dos usuários no sistema estudado. O procedimento para a análise do nível de risco, tomando como ponto de partida o software que fez a leitura dos logs, é mostrado na Figura 3. O objetivo dessa análise foi apontar que tipos de acesso são os mais danosos a rede de dados analisada. Isso poderá ser usado a fim de nortear medidas que podem ser adotadas por parte dos administradores da rede no que diz respeito ao estabelecimento de políticas de segurança de uso aceitável por parte dos usuários.

Figura 3: Fluxograma para leitura e ordenação dos logs



Fonte: Mendonça, 2010

A Tabela 1 mostra os dados do número de acessos para os meses de abril, junho e agosto de 2010, classificados quanto ao risco oferecido à segurança do sistema. A comparação dos valores de abril e junho, abril e agosto e junho e agosto foi realizada por meio do teste T de Student, considerando 5% de significância. Os resultados obtidos apontam que a variação no número de acessos analisados para os meses de abril, junho e agosto não é estatisticamente significativa.

Tabela 1: Classificação dos acessos quanto ao nível de risco para a amostra de abril, junho e agosto de 2010

NÍVEL DE RISCO	ABRIL		JUNHO		AGOSTO		ACUMULADO	
NULO	26.755,0	12,4%	34.965,0	14,4%	28.162,0	12,3%	89.882,0	13,1%
MUITO BAIXO	66.185,0	30,6%	83.336,0	34,2%	73.243,0	32,1%	222.764,0	32,4%
BAIXO	51.975,0	24,0%	61.388,0	25,2%	64.098,0	28,1%	177.461,0	25,8%
ALTO	40.536,0	18,7%	35.404,0	14,5%	41.346,0	18,1%	117.286,0	17,0%
MUITO ALTO	30.780,0	14,2%	28.406,0	11,7%	21.463,0	9,4%	80.649,0	11,7%
TOTAL	**216.231,0**		**243.499,0**		**228.312,0**		**688.042,0**	

A partir dos dados da coluna "Acumulado" da Tabela 1 — número de acessos classificados quanto ao nível de risco — foi possível estimar os valores esperados para os meses de abril, junho e agosto, supondo não haver diferença na distribuição mensal.

A Tabela 2 mostra os resultados esperados para o mês de abril. Os valores observados e esperados foram comparados por meio do teste do x2 (qui-quadrado), considerando 5% de significância. Os resultados obtidos

foram p ~ 1,0, x2 ~ 0,0 e para um valor crítico de 9,49. Assim sendo, as diferenças entre os valores observados e esperados são mera flutuação estatística.

Tabela 2: Resultados esperados para a classificação de risco dos acessos analisados para o mês de abril

ABRIL				
NÍVEL DE RISCO	**OBSERVADOS**		**ESPERADOS**	
NULO	26.755,0	12,4%	29.029,6	13,4%
MUITO BAIXO	66.185,0	30,6%	70.326,2	32,5%
BAIXO	51.975,0	24,0%	53.319,5	24,7%
ALTO	40.536,0	18,7%	35.717,9	16,5%
MUITO ALTO	30.780,0	14,2%	27.837,7	12,9%
TOTAL	216.231,0		216.231,0	

A Tabela 3 mostra os resultados esperados para o mês de junho. Os valores observados e esperados foram comparados por meio do teste do x2 (qui-quadrado), considerando 5% de significância. Os resultados obtidos foram os mesmos obtidos para os dados de abril, ou seja, p ~ 1,0, x2 ~ 0,0 e valor crítico de 9,49. Assim sendo, as diferenças entre os valores observados e esperados são mera flutuação estatística.

Tabela 3: Resultados esperados para a classificação de risco dos acessos analisados para o mês de junho

JUNHO				
NÍVEL DE RISCO	**OBSERVADOS**		**ESPERADOS**	
NULO	34.965,0	14,4%	32.690,4	13,4%
MUITO BAIXO	83.336,0	34,2%	79.194,8	32,5%
BAIXO	61.388,0	25,2%	60.043,5	24,7%
ALTO	35.404,0	14,5%	40.222,1	16,5%
MUITO ALTO	28.406,0	11,7%	31.348,3	12,9%
	243.499,0		243.499,0	

A Tabela 4 mostra os resultados esperados para o mês de agosto. Os valores observados e esperados foram comparados por meio do teste do x2 (qui-quadrado), considerando 5% de significância. Os resultados obtidos foram os mesmos obtidos para os dados de abril, ou seja, p ~ 1,0, x2 ~ 0,0 e

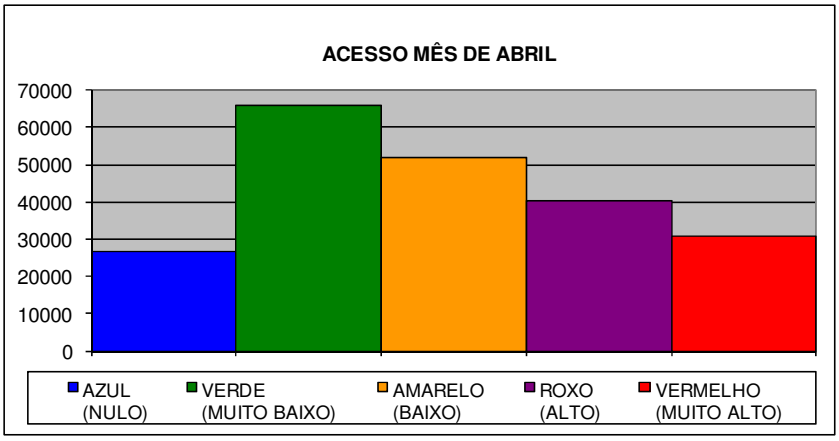
valor crítico de 9,49. Assim sendo, as diferenças entre os valores observados e esperados são mera flutuação estatística.

Tabela 4: Resultados esperados para a classificação de risco dos acessos analisados para o mês de agosto

AGOSTO				
NÍVEL DE RISCO	**OBSERVADOS**		**ESPERADOS**	
NULO	28.162,0	12,3%	29.825,4	12,2%
MUITO BAIXO	73.243,0	32,1%	73.919,5	30,4%
BAIXO	64.098,0	28,1%	58.886,6	24,2%
ALTO	41.346,0	18,1%	38.918,8	16,0%
MUITO ALTO	21.463,0	9,4%	26.761,6	11,0%
TOTAL	228.312,0		228.312,0	

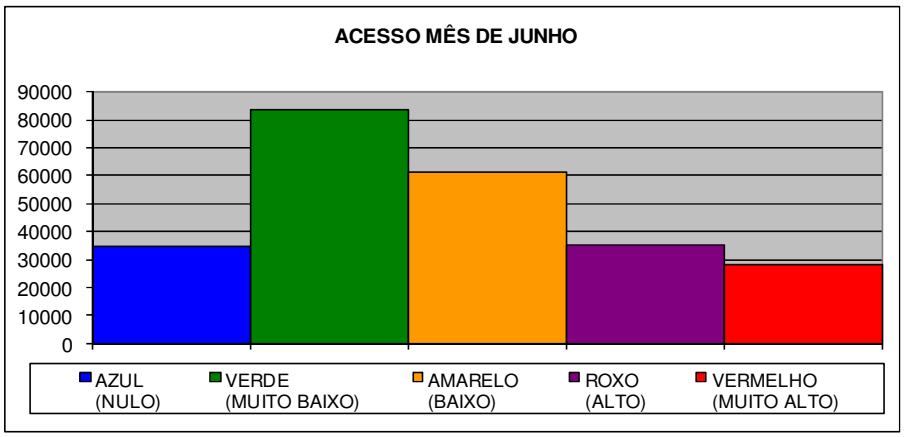
O Gráfico 1 monstra o total de acessos realizados no mês de Abril. Observa-se que os acessos com nível de risco muito baixo se apresentam de maneira predominante, já os níveis baixo, alto e muito alto mantém praticamente a mesma equidistância.

Gráfico 1: Acessos do mês de abril de 2010



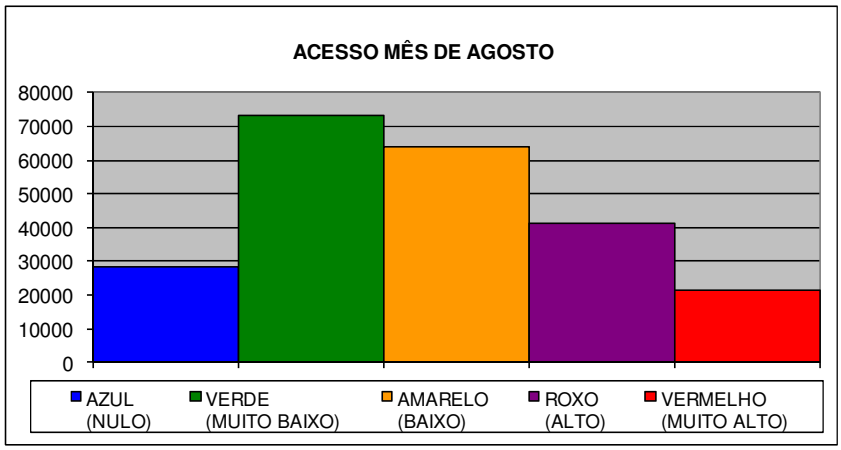
O Gráfico 2 a mostra o total de acessos no mês de Junho. O nível de acesso com risco muito baixo continua predominante, mas a diferença entre o nível de risco baixo para o nível alto se apresenta em uma faixa maior do que no Gráfico 1; percebe-se também que a proporção entre os níveis de risco alto e muito alto diminuiu em relação ao mês anterior.

Gráfico 2: Acessos realizados no mês de Junho



O Gráfico 3 ilustra o total de acessos no mês de agosto, onde é demonstrado que os acessos com nível de risco muito baixo diminuiu em relação aos meses anteriores, com isto houve um aumento de acessos com nível baixo e alto, já os acessos com nível muito alto diminuiu em relação aos meses anteriores.

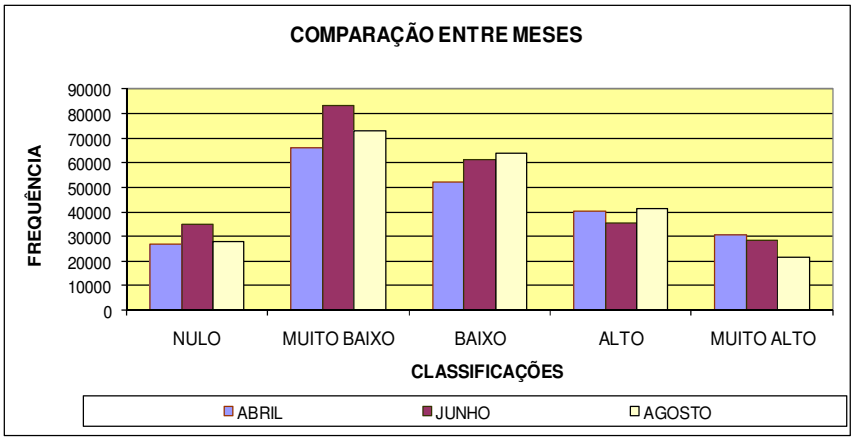
Gráfico 3: Acessos realizados no mês de Agosto



O Gráfico 4 apresenta a comparação dos acessos de abril, junho e agosto. Observa-se que os acessos mais recorrentes foram os de nível de risco muito baixo. Porém percebe-se que nos níveis nulo e muito alto há uma

equiparação. É recomendando a NBR ISO/IEC 27002 que seja feito um controle mais efetivo, de forma a gerenciar esses possíveis riscos.

Gráfico 4: Comparativo de acessos nos meses abril, junho e agosto



Quanto ao impacto e a probabilidade de ocorrência dos eventos, Schmitz et al (2006) citam que uma característica importante em um processo eficiente de priorização dos fatores de risco deve estar baseada na sua probabilidade de ocorrência e no impacto dos critérios de sucesso. Neste trabalho isso é feito através da tabela probabilidade e impacto (PI). Nela é apresentada a intersecção da probabilidade de ocorrência de um evento, bem como o impacto que esse evento pode causar sobre o projeto.

Para a construção dessas tabelas, foi tomado como base o total de endereços acessados a cada mês. Objetivando definir sua amplitude, utilizou-se o intervalo entre o menor e o maior número de acessos realizados em cada endereço. Após o cálculo do valor médio que representa o intervalo de classificação, foi realizada a classificação dos níveis segundo a probabilidade de ocorrência, isto é, quanto mais baixo o número de acessos menor a probabilidade de ocorrência e quanto mais alto os acessos, maior a probabilidade de ocorrência.

Após essa etapa foi realizada a intersecção com o impacto sobre a rede, resultando no número de endereços acessados em cada nível de intersecção, montando assim a tabela probabilidade x impacto (PI),Tabela 5: Matriz de risco para o mês de abril.

Tabela 5: Matriz de risco para o mês de abril

ABRIL					
PROB. OCORRÊNCIA	IMPACTO SOBRE A REDE				
	MUITO ALTO	ALTO	BAIXO	MUITO BAIXO	NULO
MUITO ALTO	0	0	0	2	0
ALTO	0	0	0	0	0
BAIXO	0	0	0	1	0
MUITO BAIXO	0	1	2	3	0
NULO	198	345	428	109	175

A matriz PI — Tabela 5: Matriz de risco para o mês de abril e Tabela 6: Matriz de risco para o mês de junho— representa a intersecção entre a probabilidade de ocorrência e o impacto sobre a rede no mês de abril. É possível verificar que a região onde apresenta o maior fator de risco não conta com endereços a serem monitorados, já a região com fator de risco médio apresenta dois endereços na intersecção muito baixos e muito altos, e um endereço na intersecção alto e muito baixo, significando, portanto que essa área deverá contar com uma efetiva monitoração. Na região de fator de risco que não demanda monitoramento efetivo representa todo o restante dos endereços acessados.

De acordo com a matriz PI que representa a intersecção entre a probabilidade de ocorrência e o impacto sobre a rede no mês de junho (Tabela 6), a região onde apresenta o maior fator de risco, assim como na tabela anterior (Tabela 5) não conta com endereços a serem monitorados. Já a região com fator de risco médio apresenta três endereços na intersecção muito baixos e muito altos, e um endereço na intersecção alto e muito baixo, significando, portanto que essa área deverá contar com uma efetiva monitoração. Na região onde o fator de risco não demanda monitoramento efetivo representa todo o restante dos endereços acessados.

Tabela 6: Matriz de risco para o mês de junho

JUNHO					
PROB. OCORRÊNCIA	IMPACTO SOBRE A REDE				
	MUITO ALTO	ALTO	BAIXO	MUITO BAIXO	NULO
MUITO ALTO	0	0	0	3	0
ALTO	0	0	0	0	0
BAIXO	0	0	0	1	2
MUITO BAIXO	0	1	1	3	0
NULO	196	344	729	133	194

De acordo com a matriz PI que representa a intersecção entre a probabilidade de ocorrência e o impacto sobre a rede no mês de agosto, Tabela 7, verifica-se que tanto na região que apresenta maior fator de risco como na região onde o fator de risco é médio não conta com nenhum endereço acessado, ficando assim todos os acessos classificados na região onde não se demanda nenhum monitoramento efetivo.

Tabela 7: Matriz de risco para o mês de agosto

AGOSTO					
PROB. OCORRÊNCIA	IMPACTO SOBRE A REDE				
	MUITO ALTO	ALTO	BAIXO	MUITO BAIXO	NULO
MUITO ALTO	0	0	0	0	0
ALTO	0	0	0	0	0
BAIXO	0	0	0	0	0
MUITO BAIXO	0	0	0	0	0
NULO	144	441	660	128	234

O Quadro 4 apresenta as médias de todos os acessos realizados nos meses analisados. Nota-se que a região onde o fator de risco é alto não conta com acessos cuja probabilidade de ocorrência seja muito alta ou alta, nem com impacto muito alto ou alto sobre a rede.

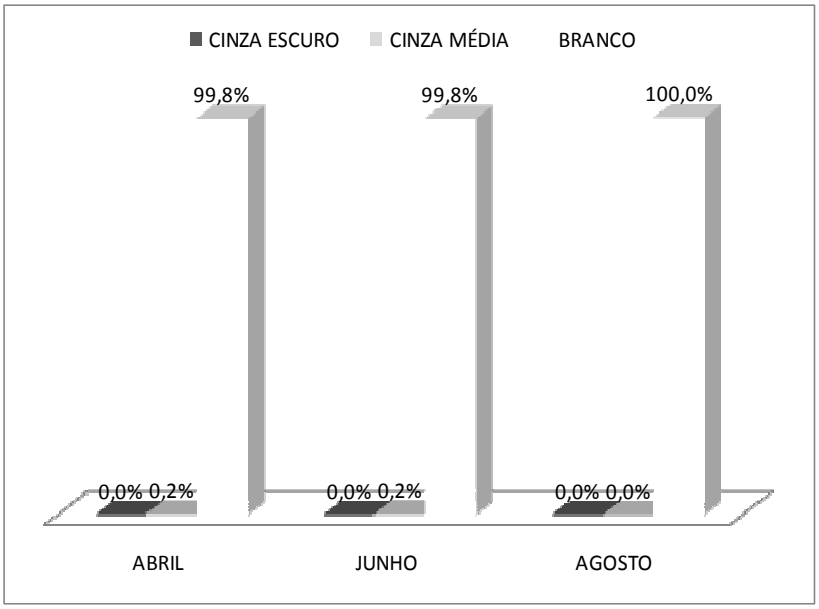
Entretanto, a região onde o fator de risco é baixo está representada pela probabilidade de ocorrência baixa ou muito baixa com impacto baixo e muito baixo. Os eventos dessa região requerem um monitoramento, pois foram identificados riscos. Apesar da probabilidade de ocorrência ser muito baixa, eventos de tal natureza podem acarretar um impacto alto negativo na segurança do sistema estudado. O restante da matriz está representado pela região onde a probabilidade de ocorrência e impacto não requerem nenhuma ação de monitoramento.

Quadro 4: Matriz de risco, comparativo dos meses abril, junho e agosto

PROB. OCORRÊNCIA	IMPACTO SOBRE A REDE - MÉDIA MESES ABRIL, JUNHO E AGOSTO				
	MUITO ALTO	ALTO	BAIXO	MUITO BAIXO	NULO
MUITO ALTO	0	0	0	2	0
ALTO	0	0	0	0	0
BAIXO	0	0	0	1	1
MUITO BAIXO	0	1	1	2	0
NULO	179	377	606	123	201

O Gráfico 5 aponta os fatores de risco existentes na rede em estudo. Nota-se que não há fatores de risco que necessitem ser mitigados. Entretanto, nos meses abril e junho, apesar de existir um percentual de risco de dois por cento da análise, há necessidade que seja realizado um monitoramento, e a região onde o fator de risco é nulo estão representados pelo restante dos acessos.

Gráfico 5: Riscos apresentados nos meses abril, junho e agosto



		ABRIL		JUNHO		AGOSTO	
CINZA ESCURO		0	0,0%	0	0,0%	0	0,0%
CINZA MÉDIA		3	0,2%	4	0,2%	0	0,0%
BRANCO		1261	99,8%	1603	99,8%	1607	100,0%

Considerações finais

A análise apresentada neste trabalho mostrou que o número de acessos potencialmente danosos à segurança do sistema estudado é baixo, o que torna a probabilidade de ocorrência de incidentes pequena. Entretanto, sabe-se que um único acesso a um sítio indevido pode colocar em risco a integridade dos sistemas e a segurança das informações. É digno de nota que o sistema estudado conta com proteções como firewall e antivírus, além da realização periódica de *back up* das informações e dos sistemas. Entretanto, não foi objetivo deste estudo avaliar as proteções do SI estudado, mas apenas a questão dos riscos provenientes do comportamento dos usuários.

Uma dos procedimentos usualmente adotados pelos gestores de TI para prevenir possíveis incidentes e invasões dos sistemas é o bloqueio do acesso aos sítios considerados impróprios ou perigosos. Entretanto, como alertam Nakamura e Geus (2007), a dinâmica da internet e das técnicas de invasão de sistemas torna esse procedimento pouco eficaz. Além disso, esse

procedimento é reativo e prescinde de algum sistema ter sido vítima de um incidente.

Os resultados deste estudo de caso mostram que além de todas as proteções e cuidados com a segurança dos SIs, é imperativo conscientizar os usuários quanto aos riscos que a navegação pela internet pode trazer ao sistema de TI. A combinação das ferramentas de defesa de TI com a o uso criterioso da navegação pela internet é a melhor forma de prevenção de incidentes e da redução dos riscos à segurança e à integridade dos sistemas de informações das organizações.

Referências

ABNT. **ISO/IEC Guia 73:2009**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2009.

ABNT. **NBR ISO/IEC 17799: Tecnologia da Informação – Código de Prática para Gestão da Segurança da Informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2001.

ABNT. **NBR ISO/IEC 27001:2006 Tecnologia da Informação – Técnicas de Sistema de Gestão de Segurança da Informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2006.

ABNT. **NBR ISO/IEC 27005:2008 Tecnologia da Informação – Técnicas de Sistema de Gestão de Riscos da Segurança da Informação.** Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2008.

ALBERTIN, A. L.. **Administração da Informática**: funções e fatores críticos de sucesso. São Paulo: Atlas, 2009.

BALLONI, A. J.. **Por que Gestão de Sistemas e Tecnologia de Informação?** Campinas: Editora Komedi, 2006.

BRANDÃO, J. E. M. S.; FRAGA, J. S. VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais. Gramado, 2008.

CERVO, A. L.; BERVIAN, P. A. **Metodologia Científica**. 4ª ed. São Paulo: Makron *Books*, 1996.

ENTRUST. **Information Security Governance (ISG): An Essential Element of Corporate Governance**. April, 2004. Disponível em: <http://www.entrust.com/ governance>. Acesso em 27 de abril de 2010.

FERNANDES, A. A., ABREU, V. F. **Implantando a Governança de TI: da Estratégia à Gestão dos Processos e Serviços**. Rio de Janeiro: Brasport, 2008.

FOINA, P. R. **Tecnologia de Informação: Planejamento e Gestão.** São Paulo: Atlas, 2009.

FONTES, E. L. G. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

FREITAS, H.; BECKER, J. L.; KLADIS, C. M. e HOPEN, N. Informação e Decisão: Sistemas de Apoio e seu impacto. Porto Alegre: Ortiz, 1997.

LAUDON, Kenneth C.; LAUDON, Janet P. **Sistemas de Informações Gerenciais**. Rio de Janeiro: *Prentice Hall*, 2004.

MARTENS, C. D. P. **A Tecnologia de Informação (TI) em Pequenas Empresas Industriais do Vale doTaquari/RS**. Universidade Federal do Rio Grande do Sul. 2001. Disponível em <http:www.lume.ufrgs.br>. Acesso em 04 de abril de 2010.

MENDONÇA, M. C. S. **A Percepção Gerencial sobre o modelo de gestão da segurança da informação de uma empresa pública de TIC:** perspectiva **de evolução para um modelo de governança.** Universidade Católica de Brasília, 2007. Disponível em < http://bdtd.ibict.br>. Acesso em 06 de abril de 2010.

MOREIRA, E. S.; BERNARDES, M. C. Um modelo para inclusão da Governança da Segurança da Informação no escopo da Governança organizacional. São Paulo 2005. Disponível em <http://www.neoreader.com.br>. Acesso em maio de 2010.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes de Computadores em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

NIST. **Information Security Handbook. A Guide for managers.** Nist Special Publication, 800-100. Disponível em:< http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-mar07-2007.pdf>. Acesso em 23 de set de 2010.

OECD, Organization for Economic Co-operation and Development. **Principles of Corporate Governance.** 2004. Disponível em: <http://www.oecd.org>. Acesso em 05 de abril de 2010.

QUINTAIROS, P. C. R.; et. al. **IT Governance in States Entreprises: A Study about the adoption of the ITIL Methodology in a Institution of higher Education.** In: 7º CONTECSI – International Conference on Information Systems and Technology Management: São Paulo, 2010.

SOLER, A. M. et al. **Gerenciamento de Risco em Projetos**. Rio de Janeiro: FGV, 2006.

SALLÉ, M. **IT Service Management and IT Governance**: Review, Comparative Analysis and their Impact on Utility Computing. HP Research Labs – Trusted. Disponível em <http://www.hpl.hp.com/techreports/2004/hpl-2004-98.pdf>. Acesso em 15 de abril de 2010.

SÊMOLA, M. **Gestão da Segurança da Informação** - Uma visão executiva. Rio de Janeiro: Elsevier, 2003.

TAPSCOTT, D. **ECONOMIA DIGITAL**. São Paulo: Makron *Books* do Brasil Editora Ltda., 1997.

WACK, J.; TRACEY, M.; SOUPPAYA, M.. **Guideline on Network Security Testing**. US Government Printing Office, 2001. NIST, Special Publication, 800-42. Disponível em <http://csrc.nist.gov/publications/nistpubs/800-42-SP800-42.pdf>. Acesso em 23 de set de 2010.