ELEMENTOS NECESSÁRIOS PARA O DESENVOLVIMENTO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA UMA INSTITUIÇÃO DE ENSINO SUPERIOR (IES) PÚBLICA

Mariana Vazquez Miano[1]

RESUMO
Este artigo apresenta a construção de uma política de segurança de tecnologia de informação para uma IES pública, com os principais elementos necessários para o seu desenvolvimento, visando à implantação de uma cultura de segurança, contextualizada nos interesses e possibilidades de gestão pública. Como parte principal do desenvolvimento, são apresentadas as melhores práticas para a proteção e controle da informação, com a utilização de COBIT (*Commom Objectives for Information and Related Technology*), ITIL (*Information Technology Infastructure Library*) e a Norma NBR ISO/IEC 27002, interligadas. Considerou-se o ambiente físico e virtual institucional, assim como o organograma institucional para regimentar os controles de acessos.
Palavras-chave: política de segurança; COBIT; ITIL; Norma NBR ISO/IEC 27002.

ABSTRACT
This article presents the construction of an information technology security policy to a public HEI, with the key elements needed for its development for the implementation of a safety culture, contextualized the interests and public management possibilities. As the main development of the best practices for the protection and control of information are displayed, with the use of COBIT (Commom Objectives for Information and Related Technology), ITIL (Information Technology infrastructure Library) and NBR ISO / IEC 27002, interconnected. It considered the physical environment and virtual institutional as well as institutional flow chart for the access control regiment.
Keywords: *security policy; COBIT; ITIL; NBR ISO/IEC 27002.*

1 INTRODUÇÃO

Nenhuma organização nasce com uma cultura pronta. Ela se constrói ao longo do tempo, direcionada pelo que foi desejado como cultura, desde que as ações executadas no dia-a-dia sejam coerentes com essa cultura definida. Isto significa que não basta apenas formalizar uma cultura se as pessoas formadoras de opinião na organização simplesmente não cumprem o que foi determinado. Um exemplo simples é a determinação de que todos devem utilizar crachás de identificação, porém o presidente não utiliza.

Sendo assim, é imprescindível formar a cultura de segurança da informação em todos os usuários que acessam informação, através de processos de conscientização e de treinamento. No processo de conscientização, deve-se alertar o usuário sobre os riscos que a organização sofre e no processo de treinamento, difundir a política de segurança da informação, ensinando-se ao usuário boas práticas para que este saiba como agir nas diversas situações do dia-a-dia, mesmo naquelas não previstas explicitamente nos procedimentos (FERREIRA, ARAÚJO, 2008).

Portanto, é preciso estar atento para que a proteção da informação contemple tanto o ambiente de tecnologia como o ambiente convencional. O controle para não colocar no lixo informação confidencial é tão importante para a proteção quanto o controle de acesso às transações em tempo real.

A inexistência de um processo de formação e manutenção de cultura em segurança da informação enfraquece a cadeia de valores para a obtenção do nível adequado de proteção. Agindo deste modo, não há proatividade para que se estabeleça a segurança. Os gestores que não implementarem esse processo serão relapsos em suas obrigações profissionais.

2 O PROCESSO DE SEGURANÇA DA INFORMAÇÃO

2.1 Políticas e normas

Para comunicar aos usuários os fundamentos da cultura e indicar como as pessoas devem agir é necessário elaborar políticas, normas e procedimentos. Além das tarefas e ações, é preciso explicitar os critérios considerados em sua elaboração, facilitando o seu entendimento e a sua incorporação aos hábitos individuais.

[1] Professora da Fatec Americana. E-mail: vazques.prof@hotmail.com

Uma política é uma diretriz que descreve os requisitos básicos, indicando a filosofia da organização. Todas as ações a serem realizadas pelas pessoas precisam seguir e estar alinhadas a essa política.

Uma norma é um regulamento que define como a política será operacionalizada. Um procedimento é o detalhamento de como uma atividade deve ser realizada.

Todos esses elementos precisam ser escritos em uma linguagem simples, direta e de forma a serem entendidos por cada usuário da informação. É necessário explicitar o que é obrigatório e o que é desejável/opcional (FONTES, 2008).

Políticas, normas e procedimentos precisam ser divulgados e constantemente lembrados, possibilitando que os usuários de todas as áreas da organização não tenham dúvidas de como tratar a informação.

2.2 Padrões e melhores práticas

O profissional de segurança precisa desenvolver ações alinhadas com as melhores práticas para a proteção e controle da informação. Como padrões de mercado aceitos e seguidos pela grande maioria das organizações e governos encontram-se o COBIT (*Commom Objectives for Information and Related Technology*), o ITIL (*Information Technology Infastructure Library*) e a Norma NBR ISO/IEC 27002.

Essas práticas recomendam a existência de processo formal de conscientização em segurança da informação e enfatizam que o elo mais fraco da segurança é o ser humano (FERREIRA, ARAÚJO, 2008). São elas:

2.2.1 COBIT

Possui uma abordagem de controle e é bastante utilizado para a realização de auditorias nos ambientes de informação e de tecnologia da informação. Foi criado pela ISACA (*Information Systems Audit & Control Association*), entidade de profissionais de segurança, auditoria e controle. Também é empregado com a finalidade de Governança de TI, patrocinado pelo ITGI – *IT Governance Institute*, coligado à ISACA (SAHIBUDIN et al, 2008).

O COBIT está dividido em 4 domínios, nos quais 34 processos estabelecem os objetivos de controle necessários para a manutenção de uma estrutura de controles internos que possibilitem à organização atingir seus objetivos de negócio de maneira confiável (do ponto de vista de TI). Os quatro domínios são:

- Planejamento e Organização (*Plan and Organize*);
- Aquisição e Implementação (*Acquire and Implement*);
- Entrega e Suporte (*Delivery and Support*);
- Monitoração e Avaliação (*Monitor and Evaluate*).

2.2.2 ITIL

Possui como objetivo a gestão da tecnologia da informação e seus recursos através da execução dos processos e serviços que precisam ser considerados para uma efetiva execução da tecnologia da informação alinhada ao negócio da organização. Consequentemente, é um guia direcionado para a Governança de TI. O aspecto da segurança da informação é um pequeno segmento do conjunto dessa biblioteca de boas práticas. Foi elaborado pelo *Office of Government Commerce/UK* com o objetivo de que as organizações que se relacionassem com o governo britânico seguissem esse padrão.

A filosofia ITIL adota uma estratégia orientada a processos para atender qualquer tipo de organização. Ela considera o Gerenciamento de Serviços em TI como um conjunto de processos estreitamente relacionados e altamente integrados. Para atingir os objetivos chaves do Gerenciamento de Serviços em TI, devem ser utilizados: pessoas, processos e tecnologias.

Desta forma, as organizações poderão estar seguras da entrega de serviços de TI inovadores e de alta qualidade, alinhados com os processos de negócio. Um grande número de países adotou a ITIL como um padrão para o Gerenciamento de Serviços. Pode-se ousar dizer que a ITIL é o padrão mundial no Gerenciamento de Serviços.

A ITIL era uma série de cerca de 60 livros que foram desenvolvidos no final da década de 80, como um conjunto de melhores práticas para TI. Atualmente, ela é considerada mais do que um conjunto de livros, pois se tornou amplamente aceita para operação dos negócios de TI.

Desde o início, a ITIL foi disponibilizada sem restrições, ou seja, qualquer organização pode utilizar a estrutura descrita nos livros (SUHAIRI, GAOL, 2013). Por este motivo, a ITIL tem sido utilizada por uma grande quantidade de organizações, como os órgãos públicos e entidades privadas (manufatura, instituições financeiras e etc.).

A biblioteca contempla os seguintes assuntos: Gerenciamento da Configuração, Central de Serviços, Gerenciamento de Incidentes, de Problemas, de Mudanças, de Liberações, da Capacidade, da Disponibilidade, da

Continuidade dos Serviços de TI, Gerenciamento Financeiro para Serviços de TI, Gerenciamento do Nível de Serviço, da Infraestrutura e de Aplicações.

Os processos da ITIL podem ser utilizados como base para alcançar conformidade com as normas BS 15000 (*British Standard for IT Service Management*) e ISO/IEC 20000.

2.2.3 Norma NBR ISO/IEC 27002

É baseada na Norma Britânica BS-7799/1 e se apresenta como um código de prática para a gestão da segurança da informação. Seu objetivo direto é a Governança da Segurança da Informação (ABNT, 2005).

Essa norma tem como objetivo "estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização". Anteriormente esta norma era conhecida como NBR ISO/IEC 17799, mas a partir de 2007 a nova edição da ISO/IEC 17799 foi incorporada ao novo esquema de numeração como ISO/IEC 27002.

A parte principal da norma se encontra distribuída em 11 seções, que correspondem a controles de segurança da informação. De acordo com o interesse do presente trabalho, serão abordadas apenas as seções 5 a 9 da Norma supracitada.

Seção 5 – Política de Segurança da Informação

É necessária a criação de um documento sobre a política de segurança da informação da organização, que deveria conter, entre outros, os conceitos de segurança da informação, o comprometimento da direção com a política, uma estrutura para estabelecer os objetivos de controle e os controles, a estrutura de análise e avaliação e gerenciamento de riscos, as políticas, princípios, normas e requisitos de conformidade de segurança da informação específicos para a organização. Essa política também necessita ser comunicada a todos, bem como analisada e revisada criticamente, em intervalos regulares ou quando mudanças se fizerem necessárias.

Seção 6 – Organizando a Segurança da Informação

Para implementar a SI em uma organização, é necessário que seja estabelecida uma estrutura para gerenciá-la. Para isso, as atividades de segurança da informação devem ser coordenadas por representantes de diversas partes da organização, com funções e papéis relevantes. Todas as responsabilidades pela segurança da informação também precisam estar claramente definidas. É importante ainda que sejam estabelecidos acordos de confidencialidade para proteger as informações de caráter sigiloso, bem como as informações que são acessadas, comunicadas, processadas ou gerenciadas por partes externas, tais como terceiros e clientes.

Seção 7 – Gestão de Ativos

Ativo, de acordo com a norma, "*é qualquer coisa que tenha valor para a organização*". Gestão de Ativos, portanto, significa proteger e manter os ativos da organização. Para que eles sejam devidamente protegidos, necessitam ser primeiramente identificados e levantados, com proprietários também identificados e designados, de tal forma que um inventário de ativos possa ser estruturado e posteriormente mantido. As informações e os ativos ainda precisam ser classificados, conforme o nível de proteção recomendado para cada um deles, e seguir regras documentadas, que definem qual o tipo de uso é permitido fazer com esses ativos.

Seção 8 – Segurança em Recursos Humanos

Antes de realizar a contratação de um funcionário ou mesmo de fornecedores e terceiros, é importante que cada um deles entenda suas responsabilidades e esteja de acordo com o papel que desempenhará. Portanto, as descrições de cargo e os termos e condições de contratação precisam estar explícitos, especialmente no que tange às responsabilidades de segurança da informação. É importante também que quaisquer candidatos sejam devidamente analisados, principalmente se o trabalho envolve o manuseio de informações de caráter sigiloso. A intenção é diminuir o risco de roubo, fraude ou mau uso dos recursos.

Durante todo o tempo em que funcionários, fornecedores e terceiros estiverem trabalhando na empresa, eles precisam estar conscientes sobre as ameaças relativas à segurança da informação, bem como de suas responsabilidades e obrigações, de tal maneira que estejam preparados para apoiar a política de segurança da informação da organização. Também precisa ocorrer o processo de treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação. É fundamental ainda que um processo disciplinar formal seja estabelecido para tratar das violações de segurança da informação.

No momento em que ocorrer o encerramento ou uma mudança na contratação, a saída de funcionários, fornecedores e terceiros, é preciso que tudo seja feito de modo ordenado e controlado, para que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso seja concluída.

Seção 9 – Segurança Física e do Ambiente

As instalações de processamento de informação críticas ou sensíveis devem ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física. Essa proteção precisa ser

compatível com os riscos previamente identificados. Os equipamentos também precisam de proteção contra ameaças físicas e ambientais, incluindo aqueles utilizados fora do local.

O uso pela organização dessas práticas identifica que ela está alinhada com padrões internacionais e facilitará qualquer auditoria ou avaliação da organização no que se refere à proteção da informação.

2.3 Programas de conscientização em segurança da informação

Indica-se que os programas de conscientização de usuários em segurança da informação se desenvolvam em conjunto com a área de recursos humanos e com pessoal especializado em comunicação (LYRA, 2008).

A mensagem a ser transmitida deve ser definida pelo profissional se segurança, sendo que a forma de como será comunicada é de responsabilidade dos profissionais de comunicação.

Ao desenvolver seu programa de conscientização, cada organização considerará suas características culturais, seu tipo de negócio e sua disponibilidade de gasto de recursos nesse programa de conscientização, que pode variar desde um simples selo adesivo até uma campanha com peças de teatro, filmes, cartazes e outras ações de grande impacto.

Qualquer que seja a forma de comunicação é necessário estar atento para a continuidade da ação de conscientização, mesmo que de uma forma mais simples. Portanto, mais do que uma campanha, a conscientização precisa ser tratada como um programa contínuo e vivo dentro da organização.

2.3.1 Tratamentos dos ambientes físico e virtual

O ambiente físico precisa ser contemplado no processo de conscientização do usuário. Para um tipo de organização onde já existe fortemente a segurança patrimonial, fica mais fácil a conscientização para a segurança do ambiente virtual. Comparações podem e devem ser feitas para facilitar o entendimento.

As informações que demandam medidas de proteção estão em toda parte. Nos sistemas, anotações, arquivos, CD´s, rascunhos de documentos, *pendrive´s*, versões preliminares de planos e projetos, cestos de lixo, quadros de anotações de reuniões, notebooks e desktops utilizados para projeções em convenções e palestras e, principalmente, na cabeça das pessoas.

Para a conscientização, podem ser divididos os tipos de ambientes a serem protegidos, porém o mais importante é transmitir para o usuário que o objetivo é proteger a informação independentemente de onde ela esteja: ambiente físico, ambiente virtual ou na mente das pessoas.

Portanto, pode-se afirmar que:

a) Considerar o usuário e desenvolver ações para que ele seja conscientizado e treinado é responsabilidade do gestor de segurança. Conscientização e treinamento fazem parte da cadeia de valores para o processo de segurança da informação de forma que o nível adequado de proteção, coerente com o tipo de negócio e com o porte da organização, seja alcançado.

b) O gestor de segurança precisa envolver e comprometer as áreas jurídicas e de recursos humanos, para que as ações a serem implementadas sejam legais e estejam alinhadas com a política de pessoas na organização.

c) Contudo, é importante que tudo isso faça parte do planejamento estratégico em segurança da informação. A abordagem estruturada é um fator crítico para o sucesso da proteção da informação da organização.

2.4 Validação, autenticação e certificação

O uso da Internet para aplicações comerciais e de negócio exige que as informações que circulam pelo mundo virtual sejam cada vez mais protegidas e mereçam confiança. A complexidade da solução dependerá do nível de segurança exigido como consequência da sensibilidade dos dados. Algoritmos de Criptografia, serviços de certificação e procedimentos e autenticação são elementos que cercam aqueles que buscam proteger a informação. De forma geral, esses conceitos não estão explícitos para todos (STALLINGS, 2008). Tomemos um exemplo em que o usuário A envia uma mensagem para o usuário B.

1) Validação da integridade: Quando o usuário A envia uma mensagem para o usuário B, deve-se ter a garantia de que essas informações não são alteradas. Para garantir esse aspecto, é enviado junto com o corpo da mensagem um resumo de mensagem que é o resultado da aplicação de um algoritmo nesse corpo da mensagem. Esse algoritmo (tipo função *hash*) trata uma mensagem de comprimento arbitrário e calcula um valor resultante de tamanho fixo de tal forma que, caso ocorra alguma modificação na mensagem, esse valor resultante não será o mesmo. Essas funções de *hash* são muito eficientes e garantem a integridade da mensagem enviada.

2) Autenticação e assinatura sem manter o sigilo da mensagem: Se o usuário B deseja ter a certeza que foi o usuário A quem enviou a mensagem, este deve assiná-la. A assinatura de uma mensagem por um usuário acontece

utilizando um algoritmo de criptografia assimétrica, onde cada usuário possui uma chave privada (de conhecimento restrito ao próprio usuário) e uma chave pública (divulgada para todos). Para assinar a mensagem, o usuário A criptografa o resumo da mensagem com sua chave privada e envia a mensagem para o usuário B. Ao receber, o usuário B descriptografa o resumo da mensagem com a chave pública de A e guarda esse resultado. Depois aplica a função *hash* no corpo da mensagem e encontra um segundo valor. Caso os dois valores sejam iguais, a mensagem está íntegra e o usuário A foi autenticado.

2.5 O acesso autorizado

Uma das questões básicas quando de um processo de segurança é o acesso à informação. A informação somente deve ser acessada pelos usuários que necessitam da informação para o desempenho das suas funções profissionais dentro da organização e estão autorizados para ter esse acesso, que também precisa ser individual (LYRA, 2008).

Ainda existem organizações que não estão adequadas a este requisito de segurança, porém, a maioria das organizações segue essa orientação. Todavia, estando nesse patamar, a organização se defronta com novos requisitos de controles. Se um usuário (autorizado) vai poder realizar determinada função, como pode ser evitada ou minimizada uma ação de má-fé desse usuário? Sempre alguém vai ter acesso à informação e, nesse caso, ações fraudulentas podem acontecer. Para a diminuição de riscos, podem-se destacar algumas regras, procedimentos e controles:

1) A autorização de acesso não é para sempre. Periodicamente é necessário rever a situação dos acessos de cada usuário. Se o usuário mudar de função ou de área é preciso reavaliar seus acessos à informação. Outro controle que pode ser implementado é o limite de tempo para cada autorização.

2) Considere os diversos níveis de acesso. Existe acesso de leitura, alteração, remoção e criação de informação. Além de ter acesso à informação, o usuário precisa ter o nível adequado de acesso.

3) Restrição de horário e localização. Informações críticas e de grande valor devem ter restrições de horário e de localização do usuário para serem acessadas. Evidentemente esta restrição necessita ser avaliada junto com o impacto operacional que ela acarreta.

4) Trilha de auditoria sempre. Todas as ações realizadas devem ser registradas em arquivo de auditoria. O custo da existência e guarda dessa trilha precisa ser coerente com a criticidade e o valor da informação (NG, 2007).

5) Relatórios de ocorrências têm que ser revisados. Relatórios inteligentes de ocorrências relativas ao negócio/aplicação devem ser verificados por outras áreas que serão afetadas pelo uso da informação. Por exemplo, uma redução maior do que 10% (ou outro percentual acordado) de uma dívida precisa ser analisada por outra área.

6) Segregação de função. Quem faz não confere; quem confere não pode fazer; são algumas das máximas de segregação de função. Quanto maior o valor e o impacto para o negócio da organização, mais é necessário segregar função e assumir o custo dessa segregação.

7) Auditoria periódica. São necessárias auditorias constantes sobre os controles existentes no sistema de informação. Isto inclui auditorias externas e internas.

8) Sistema de controle de acesso à informação não é tudo. Um bom sistema de controle de acesso permite evitar situações de erro e de fraudes em relação à autorização de acesso, mas o sistema de informação faz parte de um processo. Todos os pontos/elementos desse processo devem ser analisados em relação às possíveis fragilidades. O que vai valer é o nível de robustez da segurança desse processo. Se essa organização possuir outras situações específicas é importante que os controles considerem todas essas fraquezas e tudo seja considerado para alcançarmos uma adequada proteção à informação do negócio.

2.6 Acessando a Internet

Muitas organizações ainda possuem dificuldades em relação à liberação do uso da Internet por funcionários e colaboradores. Algumas permitem um acesso amplo, geral e irrestrito, enquanto outras fazem muitas restrições e controle. Porém, quando uma organização tiver definido que tipo de acesso seus funcionários e colaboradores terão na Internet, os seguintes aspectos devem ser considerados (LUCIANO; TESTA, 2011):

1) A singularidade da organização. Cada organização é única e possui características e objetivos que lhes são peculiares. Evidente que organizações do mesmo segmento podem ser consideradas como exemplos. Mas são apenas bons exemplos e nunca um padrão obrigatório a ser adotado. O porte da organização e seus recursos computacionais permitirão uma maior ou menor facilidade técnica no acesso à Internet. Velocidade de transmissão e quantidade de usuários simultâneos são exemplos de limitações.

2) Funções profissionais têm necessidades diferentes. Dentro de uma mesma organização pessoas exercem funções profissionais que possuem necessidades diferentes de uso da Internet. Tipos de serviço e tempos de acesso necessitam ser compatíveis com as necessidades de cada função dentro da organização.

3) Responsabilidade no acesso. Os funcionários e colaboradores devem estar cientes que são responsáveis pelos acessos e uso de serviços realizados na Internet através dos recursos da organização. As informações e facilidades que acessarem serão utilizadas para o desempenho das atividades profissionais dentro da organização. Deve-se lembrar de que a responsabilidade de uso vale para qualquer recurso da organização. Sendo assim, se as pessoas já são educadas e praticam o uso responsável de outros recursos da organização, o uso da Internet provavelmente será feito com tranquilidade, de maneira profissional, com parcimônia e responsabilidade.
4) Política de Segurança – Aspectos de internet. A organização deve explicitar para os funcionários e colaboradores qual a sua política em relação ao acesso à Internet. Principalmente, precisa definir:

- Existência do registro de acessos realizados e funções utilizadas.
- Acesso pela organização a estes registros de acesso.

É interessante que a organização registre os acessos realizados por funcionários e colaboradores, porém, a quebra do sigilo desses acessos somente acontece em função de alguma argumentação forte de fraude ou de baixo desempenho profissional por uso indevido de recursos de acesso à Internet. E nestes casos, com um registro para a auditoria e gerência de nível superior à chefia do funcionário.

3 DESENVOLVIMENTO DE UM MODELO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

O processo de desenvolvimento da política de segurança da informação institucional foi desenvolvido dentro do contexto de uma IES pública, de acordo com seu organograma e com suas possibilidades de exequibilidade e limitações. Para tal objetivo, realizaram-se reuniões com: responsáveis técnicos do CPD (Centro de Processamento de Dados), chefia do CPD, chefias administrativas e a Direção e Coordenações de Cursos.

Todas as instâncias hierárquicas opinaram e receberam cópias da documentação da política de segurança proposta, tendo havido muitas contribuições relevantes oriundas da maioria das chefias. Vale ressaltar que toda Política de Segurança é dinâmica e pode ser alterada de acordo com necessidades que venham a surgir, mediante mudanças de contexto.
Quanto à sua implantação, cabe apenas à Direção da IES esta decisão, assim como os mecanismos que utilizará para tal, pois toda política de segurança é um mecanismo de controle dentro da organização institucional, e sendo um mecanismo de controle, é uma ferramenta de gestão.

3.1 Política de segurança para Instituição de Ensino

Quando se fala em uma Instituição de Ensino, é preciso lembrar que existem algumas particularidades em comparação a uma empresa (NAKAMURA; GEUS, 2007), principalmente relacionada às pessoas que fazem parte da IES.

Em uma IES além do funcionário (administrativo e docente), há também a pessoa do aluno que frequenta as dependências da Instituição, assistindo aulas, e durante estes momentos utiliza os recursos disponíveis e acessa informações da IES a qual pertence. Em algumas Instituições pode existir a pessoa do aluno estagiário ou ainda, aluno funcionário, aquele aluno que estuda na Instituição, porém no período em que não está em sala de aula ele trabalha em algum departamento da própria Instituição.

Uma Política de Segurança voltada para Instituições de Ensino precisa ser criada de forma a estabelecer regras a serem seguidas por todos os usuários dos recursos de informática de maneira que todos sejam envolvidos e conscientizados da importância da segurança das informações da Instituição.

Para a criação do modelo de política de segurança aqui apresentado, foram utilizadas algumas informações como:
- A norma NBR ISO 17799 como referência, sendo que esta norma é o código de prática para a gestão da segurança da informação;
- Informações sobre a estrutura de informática da IES e necessidades de abrangência da política foram buscadas junto à equipe do CPD da IES, em reuniões específicas.

Alguns modelos de política de segurança consultados:

- Modelo da Política de segurança e utilização dos recursos de rede da UNICAMP (Universidade Estadual de Campinas);
- Modelo de Política de Segurança NIC BR Security Office, entre outros.

Atualmente na IES desta pesquisa, não existe nenhuma política de segurança que esteja implantada e seguida por todos os funcionários, existe apenas um procedimento para utilização de Notebooks e *Palm-Tops* particulares na rede IES e um termo de compromisso (elaborado pela equipe do CPD da IES) que a pessoa que estiver utilizando estes equipamentos preenche. De acordo com a figura 1, têm-se elencadas as principais ameaças para a segurança da informação de uma instituição:

Figura 1: Principais ameaças à segurança da informação de uma instituição

Fonte: http://slideplayer.com.br/slide/14021

A pesquisa apresentada na figura 1 foi divulgada na 9ª. edição da Pesquisa Nacional de Segurança da Informação da Módulo Security – encomendada pela Procuradoria da Prefeitura do Rio de Janeiro.

3.2 Objetivos da política de segurança

O objetivo é garantir que os recursos de informática e a informação estarão sendo usados de maneira adequada. O usuário deve conhecer regras para utilização da informação de maneira segura, evitando expor qualquer informação que possa prejudicar a Instituição de Ensino, os funcionários ou alunos.

Tem por objetivo, também, prestar aos funcionários serviços de rede de alta qualidade e ao mesmo tempo desenvolver um comportamento extremamente ético e profissional, de forma a evitar falhas de segurança que possam impossibilitar o acesso às informações, sendo que as ações da equipe de TI no que diz respeito a manutenção de recursos de informática possam ser justificadas com as regras estabelecidas na política (LUCIANO; TESTA, 2011). Ex.: a desativação de uma conta que tenha violado as regras da política de utilização de contas.

É necessário fornecer ao funcionário informações suficientes para saber se os procedimentos descritos na política são aplicáveis a ele ou não, utilizando linguagem simples e de fácil entendimento por todos (NAKAMURA; GEUS, 2007). Assim, para assegurar os altos padrões de qualidade na prestação desses serviços, faz-se necessária a especificação de uma política de segurança da informação, visando esclarecer aos usuários a importância da proteção da informação e definindo normas e procedimentos para a utilização da rede, e consequentemente da informação que nela trafega.

A Política necessita da implementação de controles (LUCIANO; TESTA, 2011) para preservar os interesses dos funcionários, clientes e demais parceiros contra danos que possam acontecer devido à falha de segurança. As normas de utilização e atividades que possam ser consideradas como violação ao uso dos serviços e recursos, os quais são considerados proibidos, precisam estar bem descritas. Podem-se definir como serviços e recursos os equipamentos utilizados pelos funcionários e alunos tais como: computadores, *e-mails*, acesso a Internet, informação em diretórios da rede e afins.

As normas descritas no decorrer podem sofrer alterações sempre que necessário, sendo que qualquer modificação precisa ser registrada e divulgada. Se existir necessidade de mudança no ambiente é preciso fazer a solicitação em tempo hábil para que as providências sejam tomadas.

Tais normas são fornecidas, a título de orientação dos funcionários, alunos e demais envolvidos. Em caso de dúvida o usuário deverá procurar a equipe de segurança visando esclarecimentos. Caso os procedimentos ou normas aqui estabelecidos sejam violados os usuários poderão sofrer punições que serão esclarecidas e

detalhadas durante este documento. Esta política aplica-se a todos os usuários dos sistemas ou computadores da rede Institucional, sendo eles: alunos, funcionários, estagiários, alunos colaboradores, terceiros ou visitantes.

Todos os usuários dos sistemas ou computadores desempenham um papel essencial de apoio efetivo para que a política de segurança possa ser adotada por toda a organização (FERREIRA;ARAÚJO, 2008). É imprescindível assegurar que todos os usuários estejam conscientes da importância de cumprir as definições estabelecidas na política para garantir a segurança das informações acessadas por todos.

Todos devem estar cientes dos procedimentos de segurança, ter conhecimento da política, e se necessário, receber treinamentos de como fazer uso correto das informações que nela estão definidas. Se existirem regras especificas para funcionários, alunos ou alunos colaboradores tem que haver divisões para estas regras.

Sugere-se que a política de segurança seja dividida em políticas de segurança da estrutura de informática (rede, e-mail, Internet, senhas, etc...) e política de segurança física (acesso a laboratórios, departamentos, segurança de equipamentos, documentos armazenados fisicamente, entre outros).

A seguir, apresentam-se alguns tópicos da política de segurança desenvolvida.

3.3 Política de segurança e uso da estrutura de informática

A Política de Segurança da estrutura de informática abrange itens relacionados à segurança da informação relacionada à utilização desta estrutura e contemplará (FONTES, 2008): política de utilização da rede, administração de contas, senhas, e-mail, acesso a Internet, uso das estações de trabalho, utilização de impressoras.

3.3.1 Política de utilização da rede

Esse tópico visa definir as normas de utilização da rede que abrange o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Estes itens serão abordados para todos os usuários dos sistemas e da rede de computadores da IES. Para fins de segurança e desempenho, há a necessidade de separação dos links de acesso: um link exclusivo para o ambiente administrativo e outro para o ambiente acadêmico.

3.3.1.1 Regras gerais

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta (também conhecido como *cracking*). Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se a servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes;

- Não são permitidas tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques, tentativas de provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de invadir um servidor;

- Antes de ausentar-se do seu local de trabalho, o usuário precisa fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas; sempre que possível deve efetuar o *logout/logoff* da rede ou bloqueio do computador através de senha;

- O usuário deve fazer manutenção no diretório pessoal, evitando acúmulo de arquivos desnecessários;

- Material de natureza pornográfica e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;

- Jogos ou qualquer tipo de software/aplicativo não pode ser gravado ou instalado no diretório pessoal do usuário, no computador local e em qualquer outro diretório da rede, podem ser utilizados apenas os softwares previamente instalados no computador;

- Não é permitido criar e/ou remover arquivos fora da área alocada ao usuário e/ou que venham a comprometer o desempenho e funcionamento dos sistemas.

- Haverá limpeza semestral dos arquivos armazenados nestas pastas, para que não haja acúmulo desnecessário de arquivos;

- É proibida a instalação ou remoção de softwares que não forem devidamente acompanhadas pelo CPD, através de solicitação escrita que será disponibilizada, e com a autorização do coordenador da área do solicitante;

- Não são permitidas alterações das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro.

3.3.1.2 Regras para funcionários

- É obrigatório armazenar os arquivos inerentes à IES no servidor de arquivos para garantir a cópia de segurança dos mesmos;

- É proibida a abertura de computadores para qualquer tipo de reparo, caso seja necessário o reparo, este precisa ser solicitado ao CPD;

- Quando um funcionário é transferido entre departamentos, o coordenador que transferiu precisa certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança ainda serão necessários na sua nova função e informar a equipe de TI qualquer modificação necessária;

- Quando ocorrer a demissão do funcionário, o coordenador responsável deve informar a equipe técnica para providenciar a desativação dos acessos do usuário a qualquer recurso da rede. Precisa-se verificar a necessidade de troca de senhas de contas de uso comum ao departamento, evitando o acesso às informações.

3.3.1.3 Regras para alunos

No ingresso do aluno à IES, este receberá uma conta e senha para que possa usufruir da infraestrutura de TI. Essa conta é de responsabilidade do aluno e não deve ser acessada por outra pessoa que não seja o próprio aluno.

É apagado o conteúdo das contas de usuário do domínio Ad (*Active Directory*) semestralmente, portanto o aluno ou professor que desejar manter suas informações precisa providenciar a cópia dos arquivos sempre ao final do semestre. A Secretaria Acadêmica deverá informar ao CPD, semestralmente, o RA dos alunos que tiverem suas matrículas canceladas ou que tiverem concluído o Curso.

3.3.1.4 Regras para alunos estagiários/funcionários

O acesso às informações é feito através da conta criada pela equipe de segurança através de solicitação do coordenador responsável. Se não existir necessidade o aluno estagiário/funcionário pode não ter conta de acesso à rede de computadores. O acesso a diretórios ou compartilhamentos dos departamentos será fornecido somente em caso de necessidade de acesso.

3.3.2 Política de sdministração de contas

Este tópico visa definir as normas de administração das contas que abrange: criação, manutenção e desativação da conta. Esta política será dividida por usuários para facilitar a compreensão.

3.3.2.1 Regras gerais

Desativação da conta:

É reservado o direito de desativar uma conta de usuário, por parte da equipe do CPD da IES, caso verifique-se a ocorrência de algum dos critérios abaixo especificados:

- Incidentes suspeitos de quebra de segurança nas contas dos usuários;
- Reincidência na quebra de senhas por programas utilizados pela equipe do CPD;
- Uso indevido dos recursos acadêmicos.

3.3.2.2 Regras para funcionários

Todo funcionário da IES poderá ter uma conta para acesso aos recursos da rede de computadores da IES. Os acessos a demais sistemas devem ser informados pelo coordenador da área no momento da solicitação da conta do usuário. Para solicitação da conta para novos funcionários os coordenadores devem proceder da maneira descrita abaixo.

Criação de contas:

Todo funcionário pode obter uma conta de acesso à rede de computadores da IES, para isto:

- O coordenador de departamento a que o funcionário pertence faz uma solicitação da criação da conta pessoalmente ou por *e-mail*;
- Esta solicitação é realizada através de e- mail para a equipe do CPD;
- Deve-se informar o número da matrícula do funcionário, assim como os acessos que serão necessários para este usuário;
- Os principais itens a serem informados referentes aos acessos permitidos aos usuários são: se a conta é para acesso ao domínio Ad; se precisará de acesso ao domínio ensino; se precisará de acesso ao sistema acadêmico e a criação da conta de *e-mail*;
- A equipe do CPD retornará para a coordenação de departamento as informações sobre a conta criada.

Manutenção da conta:

- Cada funcionário que tiver sua conta criada terá um espaço no servidor para gravar seus arquivos pessoais; é feita cópia de segurança dos arquivos do servidor do domínio IES semanalmente;

- A manutenção dos arquivos na conta pessoal é de responsabilidade do usuário, sendo que o mesmo deve evitar acumulo de arquivos desnecessários e sempre que possível verificar o que pode ser eliminado;

- As contas podem ser monitoradas pela equipe do CPD com o objetivo de verificar possíveis irregularidades no armazenamento ou manutenção dos arquivos nos diretórios pessoais.

3.3.2.3 Regras para alunos

Todo aluno da IES poderá ter uma conta para acesso aos recursos da rede de computadores, sendo que estará usando o domínio Ad, porém não é possível o armazenamento.

Criação de contas:

- A criação da conta do aluno é feita através do envio das informações de matrícula dos alunos pela Secretaria Acadêmica. Alunos que não possuírem conta de acesso à rede de computadores precisam solicitar à equipe do CPD a criação da mesma, portando documento de identificação acadêmica.

- A senha dos alunos é criada pela equipe do CPD no momento da criação da conta, e poderá ser alterada quando o usuário utilizar sua conta.

3.3.2.4 Alunos estagiários/funcionários

A criação de conta para acesso à rede de computadores da IES para aluno estagiário/funcionário dependerá da necessidade de utilização. Se existir necessidade, o procedimento será o mesmo utilizado para criação de contas para funcionários. O coordenador da área responsável informará ao CPD os dados necessários para criação da conta.

3.3.3 Política de senhas

As senhas são utilizadas pela grande maioria dos sistemas de autenticação e são consideradas necessárias como meio de autenticação. Porém, elas são consideradas perigosas, pois dependem do usuário, que pode, por exemplo, escolher senhas óbvias e fáceis de serem descobertas, ou ainda compartilhá-las com outras pessoas.

3.3.4 Política de utilização de e-mail

Esse tópico visa definir as normas de utilização de e-mail que engloba o envio, o recebimento e o gerenciamento das contas de e-mail (COSTA el al, 2012). Todos os usuários de e-mail precisam tomar ciência de que a Internet opera em domínio público que foge do controle do CPD da IES. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis.

Grande parte da comunicação do dia-a-dia se passa através de e-mails. Mas é importante também lembrar que grande parte dos vírus atuais também chega por esse meio. Esses vírus são enviados automaticamente, isso significa que um e-mail de um cliente, parceiro ou amigo não foi mandado necessariamente pelo mesmo. Os servidores de e-mail encontram-se protegidos contra vírus e códigos maliciosos, mas algumas atitudes do usuário final são importantes. Para isto é fundamental que algumas regras sejam obedecidas.

3.3.4.1 Regras para funcionários

- Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito a IES, não podendo tornar-se público;

- O e-mail da IES não deve ser utilizado para fins pessoais;

- É obrigatória a utilização de assinatura nos e-mails, seguindo padrão a ser estabelecido pela IES.

3.3.5 Política de acesso à Internet

Esse tópico visa definir as normas de utilização da Internet que engloba desde a navegação a sites, downloads e uploads de arquivos (COSTA et al, 2012). A Internet é uma ferramenta de trabalho e deve ser usada para este fim pelos funcionários e alunos da IES, não sendo permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

3.3.5.1 Regras gerais

- Somente navegação de sites é permitida. Casos específicos que exijam outros tipos de serviços como *download* de arquivos, serão solicitados diretamente à equipe do CPD, com autorização do supervisor do usuário que deseja este acesso;

- É proibida a divulgação de informações confidenciais da IES em grupos de discussão, listas ou bate-papo, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei;

- Caso a IES julgue necessário haverá bloqueios de acesso à:

1. Arquivos que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos;
2. Domínios que comprometam o uso de banda ou perturbe o bom andamento dos trabalhos;

3.3.5.2 Regras para funcionários

Poderá ser utilizada a Internet para atividades não relacionadas com a Instituição durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política.

- Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da Instituição e devem providenciar o que for necessário para regularizar a licença e o registro desses programas;

- Funcionários com acesso à Internet não podem efetuar *upload* de qualquer software licenciado para à IES ou de dados de propriedade da IES, sem expressa autorização do responsável pelo software ou pelos dados;

- Se necessário, para fins de averiguação, haverá a geração de relatórios dos sites acessados por usuário, assim como a publicação desse relatório e prestação de contas do usuário dos acessos.

3.3.6 Política de uso das estações de trabalho

Cada estação de trabalho possui códigos internos que permitem que ela seja identificada na rede. Sendo assim, tudo que for executado na estação de trabalho será de responsabilidade do usuário. Por isso, sempre que sair de frente da estação de trabalho o usuário precisa ter certeza que efetuou o *logoff* ou bloqueou a estação de trabalho.

3.3.6.1 Regras gerais

- Não deve ser utilizado nenhum tipo de software/hardware sem autorização do CPD;
- Não é permitido gravar nas estações de trabalho MP3, filmes, fotos, jogos (diversão) e software com direitos autorais ou qualquer outro tipo que possa ser considerado pirataria;
- Nas estações de trabalho deve ser mantido somente o que for supérfluo ou pessoal. Todos os dados relativos à IES precisam ser mantidos no servidor, onde existe sistema de backup diário e confiável;
- Os arquivos gravados em diretórios temporários das estações de trabalho podem ser acessados por todos os usuários que utilizarem a mesma, portanto não se pode garantir sua integridade e disponibilidade.

Poderão ser alterados ou excluídos sem prévio aviso e por qualquer usuário que acessar a estação.

3.3.7 Política de uso de impressoras

Esse tópico visa definir as normas de utilização de impressoras disponíveis nos departamentos da IES. Esta política é aplicada somente a funcionários e alunos/funcionários que utilizam impressoras em seus departamentos, sendo que, nos laboratórios de ensino (utilizados pelos alunos), não existem impressoras instaladas.

A IES contará com uma política de cotas por departamento e usuário.

3.4 Política de segurança física

O objetivo desta política é prevenir o acesso não autorizado, dano e interferência às informações e instalações físicas da Instituição. A segurança física dos equipamentos de informática e das informações da IES deve ser protegida de possíveis danos. Será abordada a segurança física dos laboratórios de informática, das instalações de TI, dos equipamentos no geral e procedimentos para garantir a segurança física.

3.4.1 Política de controle de acesso

Existem áreas que merecem maior atenção quanto ao controle da entrada de pessoas. Estas áreas são departamentos que contêm informações ou equipamentos que precisam ser protegidos, como por exemplo: sala de servidores, departamento financeiro, setor de documentação, departamento de recursos humanos, sala de coordenadores e diretores, entre outras (FONTES, 2008). Convém que estas áreas sejam protegidas por controles

de entrada apropriados para assegurar que apenas pessoas autorizadas tenham acesso liberado. Instalações desenvolvidas para fins especiais que abrigam equipamentos importantes exigem maior proteção que o nível normalmente oferecido. As instalações da equipe de TI devem ser localizadas e construídas buscando minimizar: acesso público direto, riscos ao fornecimento de energia e serviços de telecomunicações.

Para um bom funcionamento dos serviços de TI, os servidores precisam estar em ambientes devidamente refrigerados (ar condicionado) e as fitas de backup em locais seguros e replicadas em outros setores/departamentos da Instituição.

3.4.1.1 Regras gerais

Apenas pessoas autorizadas podem acessar as instalações do CPD, sendo que os funcionários devem usar crachás de identificação. Departamentos que possuem informações confidenciais de alunos, como por exemplo, documentação e informações acadêmicas e financeiras, terão o acesso permitido somente para pessoas autorizadas.

É necessário que a temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações estejam de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

Se ocorrer a perda de chaves de departamentos ou laboratórios, a coordenação responsável deve ser informada imediatamente para que possa providenciar a troca da fechadura e de outras cópias da chave perdida.

3.4.2 Política de mesa limpa e tela limpa

A política de mesa limpa precisa ser considerada para os departamentos e utilizada pelos funcionários da IES, de modo que papéis e mídias removíveis não fiquem expostos aos acessos não autorizados. A política de tela limpa considera que se o usuário não estiver utilizando a informação, ela não deve ficar exposta, reduzindo o risco de acesso não autorizado, perda e danos à informação.

3.4.3 Política de utilização de laboratórios de informática

Para a utilização de laboratórios e equipamentos de informática, algumas regras precisam ser cumpridas para que possa ser feito o uso correto das instalações, evitando qualquer tipo de dano a equipamentos em laboratórios que possam prejudicar a utilização dos mesmos. A manutenção preventiva será realizada semanalmente e a reparação dos laboratórios, semestralmente.

3.4.3.1 Regras gerais

- Haverá controle quanto ao acesso dos laboratórios de informática, somente sendo permitido o uso dos mesmos com um funcionário/professor responsável. É de responsabilidade do professor/funcionário que utilizou o laboratório zelar pela ordem das instalações, sendo que se necessária qualquer tipo de manutenção, a equipe do CPD deve ser informada;

- No momento em que entrar no laboratório, o funcionário responsável verifica se todos os computadores estão funcionando corretamente. Após a utilização, esta verificação precisa ser repetida. Se houver algum problema, a equipe técnica do CPD deve ser informada, para que a solução possa ser providenciada o mais rápido possível. Os equipamentos ficarão trancados e em segurança quando deixados sem supervisão, não sendo permitida a utilização de laboratórios sem supervisão;

- Nenhum equipamento pode ser conectado aos sistemas ou rede sem aprovação prévia e, se necessário, sob supervisão. O consumo de alimentos e bebidas é proibido nos laboratórios. As chaves de acesso aos laboratórios devem ficar guardadas em locais que o acesso seja controlado, que não seja permitida a entrada de pessoas não autorizadas, evitando assim o acesso às chaves;

- Se a utilização do laboratório não estiver prevista no horário do laboratório, esta utilização somente ocorrerá mediante a reserva do laboratório, garantindo assim que exista um registro de utilização dos laboratórios;

- Os laboratórios não poderão ser utilizados em aulas que não têm em seu Plano de Aula a necessidade de utilização de laboratório de informática. A justificativa de uso de laboratórios de informática por "conforto térmico" não será aceita.

3.5 Termo de compromisso

O termo de compromisso é utilizado para que os funcionários, alunos, alunos funcionários/estagiários se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não

cumprimento. No termo de compromisso podem ser reforçados os principais pontos da política de segurança, que deve ser assinado por todos os funcionários e estagiários e renovado sempre que necessário.

3.6 Violação da política, advertência e punições

Ao detectar uma violação da política, é necessário determinar a sua razão, ou seja, a violação pode ter ocorrido por negligência, acidente ou erro; por desconhecimento da política ou por ação previamente determinada, ignorando a política estabelecida. Um processo de investigação/sindicância determina as circunstâncias da violação, como e porque ela ocorreu.

Nos termos da Política, a IES procederá ao bloqueio do acesso ou o cancelamento do usuário, caso seja detectado uso em desconformidade com o que foi estabelecido ou de forma prejudicial à Rede, além de instaurar uma sindicância, para as devidas responsabilizações. É recomendado o treinamento dos usuários em segurança da informação, como forma de conscientização e divulgação da política de segurança a ser seguida por todos.

O programa de treinamento em segurança deve fazer parte do programa de integração de novos funcionários e do programa de integração de novos alunos (ao início de cada ano letivo), com a realização de treinamentos de atualização para os funcionários mais antigos.

4 CONSIDERAÇÕES FINAIS

A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante nas organizações. Para o desenvolvimento do modelo de política de segurança foi utilizada a norma NRB ISO 17799, que é a tradução da norma BS 7799 homologada em setembro de 2001 pela ABNT. Esta norma trata da Gestão de segurança da informação e abrange os mais diversos tópicos da área de segurança, possuindo assim um grande número de controles e requerimentos que devem ser atendidos para garantir a segurança das informações de uma empresa ou instituição (LUCIANO, 2011).

É importante a definição, para usuários da rede de computadores da IES, de regras existentes a ser seguidas para a utilização de maneira adequada dos recursos de informática, assim como para a garantia da segurança física. O modelo de política de segurança desenvolvido visa à descrição destas regras de modo acessível ao entendimento dos usuários.

A política de segurança pode ser definida em três níveis: estratégico, tático e operacional (FONTES, 2008). No nível estratégico, definem-se diretrizes mais genéricas de modo que os executivos possam entender o que está sendo definido; no nível tático, definem-se normas e padronizações, fazendo que todos os pontos da empresa tenham o mesmo nível de segurança; no nível operacional, são definidos procedimentos e intrusões, de modo que se a configuração está no papel não há como ser realizada de forma diferente, independente de quem a estiver realizando.

O modelo desenvolvido se aplica ao nível tático, pois foram definidas regras com o objetivo que todos sigam um padrão de utilização dos recursos, garantindo a segurança das informações. Este estudo procurou abranger a segurança da informação, tendo seu objetivo voltado para a construção de uma política de segurança da informação.

Durante a implementação da política de segurança toda a organização deve ser envolvida. É indicada a realização de treinamentos conscientizando a importância da segurança da informação e do envolvimento de cada um na utilização e divulgação da política de segurança.

5 REFERÊNCIAS

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação.** ABNT, 2005.

COSTA, J. S, SILVA, J., CRUZ, M.A.P.(2012). Segurança de redes de computadores na Internet. **Inova Ação**. P.77-88, v.1. n.2.

FERREIRA, F. N. G, ARAÚJO, M. T. **Política de Segurança da Informação – Guia Prático para Elaboração e Implementação**. 2ed. Rio de Janeiro, Edit. Ciência Moderna, 2008.

FONTES, E. L. G. **Praticando a segurança da informação**. Rio de Janeiro, Brasport, 2008.

LUCIANO, E. M.,TESTA, M. G.(2011). Controles de governança de tecnologia da informação para a terceirização de processos de negócio: uma proposta a partir do COBIT. **JISTEM Revista de Gestão da Tecnologia e Sistemas de Informação.** P. 237-262, v.8, n.1.

LYRA, M. R. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro, Edit. Ciência Moderna, 2008.

NAKAMURA, E. T., GEUS, P. L. **Segurança de redes em ambientes corporativos**. São Paulo, Novatec, 2007.

NG, R. **Forense computacional corporativa**. Rio de Janeiro, Brasport, 2007.

SAHIBUDIN, S., SHARIFI, M., AYAT, M. "*Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations", in Modeling & Simulation*. **AICMS 08**. **Second Asia International Conference on**, 2008.

STALLINGS, W. **Criptografia e segurança de redes**. 4ed. São Paulo: Pearson Prentice Hall, 2008.

SUHAIRI, K., GAOL, F. L. (2013) *The Measurement of Optimization Performance of Managed Service Division with ITIL Framework using Statistical Process Control.* **Journal of Networks**, P.518-529, v. 8, n. 3.