Universidade de Brasília

Faculdade de Tecnologia

Departamento de Engenharia Elétrica

GESTÃO DA SEGURANÇA DA INFORMAÇÃO NA ERA DO CONHECIMENTO E SUA APLICAÇÃO NA ÁREA DE TI

LEONARDO DE PAIVA SOUZA

Orientadora: Profª Msc: ELIANE CARNEIRO SOARES

Monografia de especialização submetida ao Departamento de Engenharia Elétrica da Faculdade de Tecnologia da Universidade de Brasília, como parte dos requisitos necessários para a obtenção do grau de especialista em Sistema de Gestão de Segurança da Informação.

PUBLICAÇÃO: UnBLabRedes MFE. 041/2012

BRASÍLIA/DF: DEZEMBRO /2012

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GESTÃO DA SEGURANÇA DA INFORMAÇÃO NA ERA DO CONHECIMENTO E SUA APLICAÇÃO NA ÁREA DE TI

LEONARDO DE PAIVA SOUZA

MONOGRAFIA DE ESPECIALIZAÇÃO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE ESPECIALISTA.

APROVADA POR:

ELIANE SOARES, Mestre, UnB
(ORIENTADORA)

EDNA DIAS CANEDO, Doutora, UnB/FGA
(EXAMINADOR)

GIOVANNI ALMEIDA SANTOS, Mestre, UnB/FGA

(EXAMINADOR)

DATA: BRASÍLIA/DF, 07 DE DEZEMBRO DE 2012.

FICHA CATALOGRÁFICA

SOUZA, LEONARDO PAIVA
Gestão da Segurança da Informação na Era do Conhecimento e sua aplicação na área de TI. Distrito Federal 2012.
xvi, 63 p., (ENE/FT/UnB, Especialista, Sistemas de Gestão de Segurança da Informação, 2012).

Monografia de Especialização – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Conhecimento 2. Informação
3. Segurança

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

SOUZA, Leonardo de Paiva. (2012). Gestão da Segurança da Informação na Era do Conhecimento e sua aplicação na área de TI. Monografia de Especialização, Publicação: UnBLabRedes MFE. 041/2012, nov/2012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 64 p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Leonardo de Paiva Souza
TÍTULO DA DISSERTAÇÃO: Gestão da Segurança da Informação na Era do Conhecimento e sua aplicação na Área de TI.
Especialista/2012.

_____

Leonardo de Paiva Souza
Endereço: CNB 05 lote 03 Ap. 204 – Taguatinga Norte
CEP 72115- 055 – Brasília – DF - Brasil

Dedico a minha namorada Alline, pelos momentos felizes que sempre me proporciona.

Te amo.

AGRADECIMENTOS

A Deus por iluminar meus caminhos em mais essa jornada.

Aos meus pais, Eudes e Almeí, meu irmão Elton e minha avó Anie pelo carinho e pela presença marcante em todos os momentos de minha vida.

A orientadora Profª.Msc. Eliane Carneiro Soares, pelo apoio, incentivo e profissionalismo com que me conduziu na construção deste trabalho..

Aos colegas de trabalho, lotados no Laboratório de TI, da Gerência Técnica de Tecnologia da Informação, no SG-11, pelas conversas enriquecedoras, ajuda em diversos aspectos, colaboração e amizade. A todos, os meus sinceros agradecimentos.

“A pior coisa para construir futuro é achar que o passado já sustenta (...)
Quando o jogo e a estratégia mudam rapidamente não basta se contentar com o possível.
É preciso fazer seu melhor.”

Mário Sergio Cortella

RESUMO

O presente trabalho tem por escopo um estudo de caso sobre a Gestão da Segurança da Informação na Era do Conhecimento e sua Aplicação na Área de TI, tendo como foco o Laboratório de TI, da Gerência Técnica de Tecnologia do Departamento de Engenharia Elétrica da UnB. Nesse sentido, o presente estudo mostra que a informação se tornou um recurso imprescindível para as organizações e profissionais que buscam o aprimoramento e o êxito em seus campos de atuação, e por isso é importante que se proteja dados e os recursos corporativos, preservando sua confidencialidade, integridade, disponibilidade, autenticidade, contra perdas e danos ou qualquer outro tipo de evento, garantindo, assim a continuidade do negócio. Dentro deste contexto, valendo-se do método dedutivo, o estudo, a partir de um roteiro de observação prévio, no qual se analisa/avalia o nível de conscientização dos funcionários lotados no Laboratório de TI, no SG-11, em relação a diversos aspectos envolvidos na segurança da informação, enfatizando a importância dos controles físicos que limitam o contato ou acesso direto à informação ou à infraestrutura de TI e os controles lógicos que impedem ou limitam o acesso à informação que está em ambiente controlado eletronicamente, pois ambos os controles funcionam como barreiras. Aborda-se ainda, o comportamento do capital humano, posto que é na conduta destes que a proteção da informação é critica. Dentro deste contexto, observou-se, que no âmbito do Laboratório de TI pesquisado os funcionários são capacitados e treinados visando o aprimoramento constante dos processos de resposta a incidentes internos e externos como forma de garantir a manutenção do nível de segurança acordado com a UnB. Eles agem de forma proativa e de acordo com o repertório de normas da família ISO/IEC 27000, bem como, em consonância com as instruções normativas dirigidas a Administração Pública Federal. No que tange aos controles físicos e lógicos, como a área de TI vive em constante inovação, sempre haverá novos equipamentos disponíveis no mercado. Mas, atualmente, o Laboratório de TI carece de um controle de acesso biométrico. A gestão da Segurança da Informação dispõe de inúmeros mecanismos que a suportam, contudo, é primordial a participação e a conscientização do capital humano na condução deste processo, posto que as inovações no setor ocorram de forma acelerada.

Palavras chaves: Segurança da informação, controles físicos e lógicos e capital humano.

ABSTRACT

The scope of this paper is a case study on the Management of Information Security in the Age of Knowledge and Its Application in the Field of IT, focusing on the IT Lab, the Technical Management of Technology Department of Electrical Engineering at UNB. In this sense, the present study shows that information has become an invaluable resource for organizations and professionals seeking improvement and success in their fields, and so it is important to protect corporate data and resources, preserving its confidentiality, integrity, availability, authenticity, against loss or damage or any other type of event, thus ensuring business continuity. Within this context, using the deductive method, the study, from a screenplay by observation prior (Appendix-A) analyzes / evaluates the level of employee awareness in crowded Lab IT, the SG-11, compared the various aspects involved in information security, emphasizing the importance of physical controls that limit contact or direct access to information or to IT infrastructure and logical controls that prevent or limit access to information that is electronically controlled environment, for both controls act as barriers. Covers up yet, the behavior of human capital, since it is the conduct of the protection of information is critical. It was observed that under the IT Lab researched the employees are skilled and trained in order to constantly improve the processes of response to internal and external incidents as a way of maintaining the level of safety agreed with the UnB. They act proactively and in accordance with the standards of the family repertoire of ISO / IEC 27000 and in accordance with regulatory instructions directed the Federal Public Administration. The Management of Information Security have numerous mechanisms that support it, however, is paramount participation and awareness of human capital in driving this process, given that innovations in the sector occur de rapidly.

Keywords: Information security controls, logical and physical and human capital.

SUMÁRIO

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ABNT: Associação Brasileira de Normas Técnicas

BS: *British Standard*

BSI: *British Standard Institute*

DTL: Divisão Técnica Laboratorial

ENE: Departamento de Engenharia Elétrica da Universidade de Brasília

FT: Faculdade de Tecnologia

IEC: International Electrotechnical Commission

ISO: International organization for Standardization

ITGI: *IT Governance Institute*

MEC: Ministério da Educação e Cultura

NBR: Normas Brasileiras

PDCA: *Plan-Do-Check-Act*

SG- 11: Bloco da Divisão Técnica Laboratorial da Universidade de Brasília

SGSI: Sistema de Gestão da Segurança da Informação

SI: Sistemas de Informação

TI: Tecnologia da Informação

UnB: Universidade de Brasília

1 INTRODUÇÃO

O ambiente institucional está mudando continuamente, tornando-se mais complexo e menos previsível, e cada vez mais dependente de informação e de toda a infraestrutura tecnológica que permite o gerenciamento de enormes quantidades de dados. Em qualquer tipo de organização, seja comercial, seja pública, seja prestadora de serviços ou industrial, existirá sempre a necessidade de tomar decisões. São inúmeras as forças que impõem novas concepções e valores à sociedade e às organizações, sendo a mais importante delas a rapidez nas mudanças exigidas.

As novas tecnologias têm exigido mudanças e adaptações das empresas em ritmo sem precedentes. Elas têm exercido forte impacto até mesmo sobre as estruturas empresariais mais conservadoras, como por exemplo, as organizações governamentais que também convivem nesse ambiente competitivo e, também cooperativo, posto que a demanda por eficiência exija interação entre os sistemas de informações das diversas organizações governamentais.

A importância da Área de TI no suporte e viabilização dos processos gerenciais torna imprescindível a disponibilidade de informação na condução dos negócios. Em outras palavras, a informação tornou-se o bem mais precioso para as organizações. Por isso, elas passaram a difundir um novo modelo de gestão que dá ênfase à proteção dos dados, informações e conhecimentos, protegendo-os contra o uso inadequado e possível adulteração ou destruição por agentes adversos.

De acordo com a Norma ABNT ISO/IEC 27002 (2005, p. 2), “a segurança da informação protege a informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os danos, maximizar o retorno dos investimentos e as oportunidades de negócio.”

Assim, a relevância do tema reside na qualidade das informações disponibilizadas pelos avanços tecnológicos e na necessidade de controle sobre elas, haja vista, que as organizações frequentemente se deparam com dificuldades para estabelecer modelos adequados de Sistema de Gestão de Segurança da Informação.

1.1 OBJETIVOS

1.1.1 Objetivo Geral

Analisar/avaliar o nível de conscientização do capital humano lotado no Laboratório de TI, na Gerência Técnica de Tecnologia da Informação, no SG-11, da Engenharia Elétrica da UnB, na condução do Sistema de Gestão da Segurança da Informação - SGSI desta área.

1.1.2 Objetivos Específicos

- Identificar os riscos e vulnerabilidades de dados e informações, considerando os controles físicos e lógicos;

- Avaliar o nível de conscientização do capital humano;

- Conhecer as opções de tratamento de riscos apontadas pela família ISO/IEC 27000;

- Observar a efetividade das ações de segurança da informação desenvolvidas no Laboratório de TI, na Gerência Técnica de Tecnologia da Informação, no SG-11, da Faculdade de Engenharia Elétrica da UnB;

- Sintetizar as recomendações das melhores práticas de segurança que devem ser adotadas pelas organizações.

1.2 JUSTIFICATIVA

A escolha do tema se justifica, para as organizações governamentais, privada e do terceiro Setor, posto que a informação tornou-se um recurso imprescindível para as organizações e profissionais que buscam o aprimoramento e o êxito em seus campos de atuação, pois, o principal objetivo da segurança da informação é estabelecer diretrizes e padrões que permitam garantir a integridade, a confidencialidade e a disponibilidade de dados e informações corporativas.

Para isso, faz-se necessário a definição de uma política eficiente que possua as diretrizes gerais, normas gerais para usuários, normas gerais para técnicos, normas específicas, sanções, termos de sigilo e responsabilidade, além é claro dos investimentos em

divulgação e treinamento de forma a conscientizar seus colaboradores da importância de se adotar as diretrizes previstas na Política estabelecida pela organização. Convém ressaltar que a segurança na área de TI se apoia sobre três pilares: a tecnologia; todos os processos de administração e operação; e, as pessoas que possibilitam a obtenção de uma infraestrutura mais segura que não se restringe apenas a uma boa tecnologia. Portanto, uma Política de Segurança só será efetiva com a participação de todos.

Justifica-se também para a sociedade, que cada dia mais depende da informação e precisa salvaguardar dados e informações sigilosas, evitando fraudes e o acesso de pessoas não autorizadas. Justifica-se ainda para o meio acadêmico que, à luz da segurança da informação, deve estar consciente dos riscos e vulnerabilidades de dados e informações, bem como das opções de tratamento destes riscos preconizadas pela família de normas ISO/IEC 27000 que engloba os controles físicos e lógicos, bem como a conduta do capital humano.

1.3 ORGANIZAÇÃO DO TRABALHO

No que tange à estrutura, o presente estudo encontra-se dividido em três partes. A primeira parte do trabalho traz o texto introdutório onde se contextualiza o tema, definindo os objetivos que norteiam a pesquisa. Num outro momento trata-se da relevância e da justificativa para a escolha do tema, bem como da metodologia da pesquisa.

A segunda parte do estudo traz o referencial teórico onde se traça um breve histórico da Área de TI em estudo, no caso a Gerencia Técnica de Tecnologia da Informação, no SG-11, da Engenharia Elétrica da UnB. Aborda-se, também a importância do conhecimento para as organizações destacando os antecedentes do conhecimento e mostrando que mesmo antes da época da "organização que aprende", das "competências essenciais", dos "sistemas especializados" e do "foco na estratégia", bons gerentes já valorizavam a experiência e o *know-how* de seus funcionários – isto é, seu conhecimento. Procurou-se ainda conceituar conhecimento no âmbito das organizações, mostrando que a literatura consultada o define como: a capacidade de aplicar informação a um trabalho ou a um resultado específico. Neste contexto enfatizou-se a distinção entre dados e informação e conhecimento, mostrando que a literatura não apresenta uma diferenciação clara entre a chamada sociedade da informação e a

sociedade do conhecimento. Contudo, é possível constatar que uma é alicerce da outra e ambas estão interligadas.

Destaca-se, também o papel do gestor na Era do Conhecimento mostrando que gestão é a disciplina que torna produtivos os saberes de vários campos do conhecimento. Aborda-se a organização que dissemina o conhecimento enfatizando a importância do gerente do conhecimento, posto que alguém precise ser responsável pela gerência do conteúdo do conhecimento organizacional, bem como por sua tecnologia.

Dá-se ênfase ao capital intelectual que é a soma do conhecimento de todos em uma organização e sua capacidade de criar continuamente e proporcionar valor de qualidade superior criando diferencial competitivo para as organizações, enfatizando a importância da gestão deste capital, por parte dos gerentes que devem adotar práticas de gestão que propiciem a criação e aprendizado individual, assim como estratégias para conversão do conhecimento individual em coletivo nos mais diversos níveis da organização.

Trata-se, ainda dos pressupostos para a efetividade e eficácia de um Sistema de Gestão da Segurança da Informação – SGSI. Dentro desta realidade procura-se conceituar informação que no contexto deste estudo pode ser definida como: a ação de informar; formação ou moldagem da mente ou do caráter, treinamento, instrução, ensinamento, comunicação de conhecimento instrutivo.

Em se tratando da segurança da informação o estudo se vale da definição dada pela ISO/IEC 27002/2005 que a define como: "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio."

Com escopo nestes argumentos o estudo dá noções gerais sobre as normas da família ISO/IEC 27000 que foram criadas para ordenar as diversas normas de segurança da informação publicadas através da parceria entre a *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC).

No que tange aos princípios básicos da segurança da informação, o estudo destaca a confidencialidade, a integridade e a disponibilidade de informações, aos quais se acrescenta a autenticidade, não repúdio, responsabilidade e confiabilidade, buscando garantir à integridade

da informação, reduzindo ao máximo os riscos de vazamentos, a integridade dos bancos de dados, as fraudes em arquivos, o roubo de informações, a proteção contra erros humanos e operacionais por falta de treinamento, o uso indevido do sistema por pessoas não autorizadas que podem sabotá-lo, ocasionando paralisações de rede ou serviços, ou até mesmo ameaças que visam prejudicar as organizações e, também os equipamentos utilizados.

Daí, a importância da abordagem da análise e avaliação dos riscos, posto que eles determinem as necessidades de segurança adequadas, assim como os processos que estão em funcionamento no momento, facilitando, assim a definição de um processo de segurança adequado para cada organização.

Tratou-se, ainda, da gestão estratégica da segurança da informação mostrando que com o planejamento adequado, as organizações podem lidar com brechas de segurança de forma proativa. Com suporte nestes argumentos, abordou-se a importância da definição da política de segurança da informação como ferramenta importante para combater ameaças e os mecanismos de segurança, enfatizando os controles físicos e os controles lógicos.

A terceira parte dedica-se ao estudo de caso, enfatizando a Segurança da Informação, destacando o cenário atual encontrado no Laboratório de TI, da Gerencia Técnica de Tecnologia da Informação, localizado no SG-11, da Faculdade de engenharia Elétrica da UnB. Os dados coletados na observação participante enfatizam os mecanismos de segurança que apoiam os controles físicos e lógicos no âmbito deste laboratório e, também o comportamento do capital humano alocado nesta área, analisando e avaliando o nível de conscientização dos mesmos.

1.4 METODOLOGIA

A palavra método é de origem grega e significa o conjunto de etapas e processos a serem vencidos ordenadamente na investigação dos fatos ou na procura da verdade. Assim, buscando atingir os objetivos, geral e específicos, propostos para o estudo, o método adotado foi o dedutivo que segundo Marconi e Lakatos (2001) é um método lógico que pressupõe que existam verdades gerais já afirmadas e que sirvam de base para se chegar através dele a conhecimentos novos, ou seja, ele parte do geral para o particular.

Assim, buscando conhecer o nível de conscientização dos servidores do Laboratório de TI, fez-se um diagnóstico da política de segurança adotada para proteger as informações e controlar o risco de revelação ou alteração por pessoas não autorizadas observando se são adotadas as melhores práticas de segurança na manutenção do SGSI, implantado no mencionado laboratório.

Quanto ao tipo de pesquisa, valendo-se da classificação proposta por Vergara (2003), quanto aos fins, à pesquisa foi exploratória e descritiva. Exploratória porque, embora a Universidade de Brasília – UnB seja uma instituição com tradição e alvo de pesquisas em diversas áreas de investigação, não se verificou a existência de estudos que abordem a necessidade de uma avaliação constante dos riscos a que está exposto o Laboratório de TI. Descritiva, porque expõe os dados coletados na observação (Anexo A), feita por este pesquisador que atua no mencionado departamento.

Quanto aos meios a pesquisa foi bibliográfica e de campo. Bibliográfica porque foi feita com base em material publicado em livros, revistas, e sites que forneceram instrumental analítico para a fundamentação teórica do estudo. Já a pesquisa de campo é a investigação empírica realizada onde ocorre o fenômeno e que dispõe de elementos para explicá-lo. No caso o Laboratório de TI, onde foram observados, por um período de aproximadamente quatro meses, os diversos aspectos envolvidos na segurança da informação, como por exemplo: a existência de controles físicos e lógicos, os riscos, vulnerabilidades, e o nível de conscientização do capital humano lotado neste laboratório.

A Amostra foi composta pelos servidores, prestadores de serviços e estagiários lotados no laboratório. São eles: quatro analistas de sistemas de informação, dois técnicos de informática e um estagiário. O instrumento utilizado na pesquisa foi à observação participante feita a partir de um roteiro prévio (anexo A).

No que tange aos procedimentos, vale destacar que os participantes da pesquisa foram observados durante quatro meses, mais especificamente nos meses de março, abril, maio e junho de 2012, em sua rotina dentro do Laboratório, tendo como parâmetro o roteiro de observação (Anexo A). Buscou-se, portanto, diagnosticar os riscos e as vulnerabilidades do SGSI, do mencionado laboratório, na busca de soluções que tornem mais efetiva a proteção das informações dele emanadas, tendo como suporte a literatura consultada e, também as

normas da família ISO/IEC 27000 que tratam da segurança da informação no ambiente corporativo.

As informações coletadas durante a observação foram anotadas e sintetizadas no corpo deste trabalho. Posteriormente, as observações foram confrontadas com o referencial teórico do estudo buscando detectar as lacunas na segurança da informação no âmbito do Laboratório de TI, buscando assim sugerir melhorias na política de segurança a partir da adoção de controles físicos e lógicos eficazes, aliado à conscientização do capital humano.

2 REFERENCIAL TEÓRICO

2.1 IDENTIFICAÇÃO E CARACTERIZAÇÃO DA ORGANIZAÇÃO

Fundado em 1967, o Departamento de Engenharia Elétrica da Universidade de Brasília, está localizado no Campus Universitário Darcy Ribeiro, em Brasília-DF. No início, o ENE funcionou provisoriamente no prédio SG-11. Apenas 5 (cinco) professores foram os pioneiros responsáveis pela implantação do curso de graduação em engenharia elétrica. Os alunos não passavam de algumas dezenas, que ingressavam mediante um vestibular genérico para todas as engenharias. A primeira turma formou-se em 1969 e o curso foi oficialmente reconhecido pelo MEC em 1970.

Desde a sua criação, o Departamento de engenharia Elétrica - ENE da Faculdade de Tecnologia – FT da Universidade de Brasília – UnB demonstra uma expansão sólida, vigorosa e coerente. Como marcos dessa expansão cita-se a criação de novos cursos de graduação: Engenharia de Redes de Comunicação (1997) e Engenharia Mecatrônica (1997); como também a implantação da pós-graduação em nível de mestrado (1979), de mestrado profissionalizante (2000) e de doutorado (2001).

A história do ENE é caracterizada pela busca da excelência na formação de seus alunos e pelo dinamismo em perceber e seguir os avanços da ciência e da tecnologia, por isso, o mencionado Departamento possui uma estrutura física que comporta a maior quantidade e diversificação laboratorial da Universidade de Brasília. Os alunos, na realização de suas atividades didáticas e/ou pesquisa, terão acesso aos diversos Laboratórios do Departamento de Engenharia Elétrica - ENE e a infraestrutura dos Grupos de Pesquisa. Vale ressaltar que o número de laboratórios sofreu um acréscimo de 20% nos últimos dois anos e de 40% nos últimos quatro anos. Neste estudo destaca-se o Laboratório de TI, na Gerência Técnica de Tecnologia da Informação, localizada no SG-11.

A Divisão Técnica Laboratorial - DTL é responsável pela área Técnica e Administrativa dos Laboratórios do Departamento de Engenharia Elétrica da Universidade de Brasília, na qual se inclui o Laboratório de TI, no SG-11, laboratório alvo deste estudo. Entre

outras atribuições, a DTL é responsável pela gestão dos equipamentos científicos do departamento e o suprimento e controle dos materiais de consumo eletroeletrônicos para as aulas de laboratório e projetos de pesquisa desenvolvidos pelo corpo docente e discente deste departamento, compreendendo os três cursos regulares: Engenharia Elétrica, Engenharia de Redes de Comunicação e Engenharia Mecatrônica.

No que tange ao corpo técnico, o diferencial da qualidade dos serviços tem sido pautado na gestão de pessoas, processos e tecnologia com orientação total ao usuário, através de atitudes praticadas no dia-a-dia do Departamento. O quadro de colaboradores alocados no Laboratório é composto por uma equipe técnica altamente qualificada, que tem por compromisso desenvolver os seus serviços sempre adotando um padrão de qualidade e segurança. Entende-se que os colaboradores são o principal ativo, já que é através das pessoas que se torna possível desenvolver todas as competências técnicas necessárias para a concretização de todos os objetivos e compromissos. A Equipe Técnica está inserida em processos contínuos e regulares de capacitação, com o desígnio de sempre estarem atualizados com as tecnologias e conhecimentos vigentes no mercado.

A missão do Departamento de Engenharia Elétrica é prover a melhor composição técnica e serviços para atender as demandas da clientela, buscando sempre a continuidade das soluções implementadas. O Departamento tem como visão ser referência dentro do Serviço Público no contexto da Excelência em Gestão de Pessoas, Processos e Tecnologia com orientação total ao usuário. A ENE tem como princípios: Compromisso e Seriedade; Espírito de Equipe; Melhoria Contínua; E como lema: "Nada está tão bom que não possa ser melhorado."

Após traçar um breve histórico do Departamento de Engenharia Elétrica – ENE, com ênfase na Gerencia Técnica de Tecnologia da Informação, localizada no SG-11, no próximo tópico enfatizar-se-á a importância do conhecimento nas organizações contemporâneas.

2.2 A IMPORTÂNCIA DO CONHECIMENTO PARA AS ORGANIZAÇÕES

É perceptível, no cotidiano das organizações, o súbito interesse pelo conhecimento. Segundo Davenport e Prusak (1998,) inúmeras conferências e centenas de artigos em publicações acadêmicas e de negócios procuram alcançar alguma compreensão desse tema

nebuloso. O avanço da consultoria na área do conhecimento e a mobilização em torno do assunto nos meios empresariais sinalizam a progressiva convicção de que entender o conhecimento é fundamental para o sucesso das empresas – e talvez para a sobrevivência das organizações.

2.2.1 Antecedentes do conhecimento

Segundo Takeuchi e Nonaka (1997), o conhecimento começou a ganhar redobrada atenção. Nesse sentido, gerentes só há pouco se deram conta de que têm recorrido ao conhecimento ao longo de toda sua carreira. Não só teóricos sócio-econômicos como Peter Drucker e Alvin Toffler chamaram a atenção para a importância do conhecimento como recurso e poder gerencial. Também um número crescente de estudiosos nas áreas de organização industrial, gerenciamento da tecnologia, estratégia gerencial e teoria organizacional começaram a teorizar sobre a administração do conhecimento.

Convém lembrar que, mesmo antes da época da "organização que aprende", das "competências essenciais", dos "sistemas especializados" e do "foco na estratégia", bons gerentes já valorizavam a experiência e o *know-how* de seus funcionários – isto é, seu conhecimento. Hoje, porém, muitas empresas perceberam que necessitam de mais do que apenas uma abordagem aleatória (e até mesmo inconsciente) do conhecimento corporativo para vencer na economia atual e futura. A capacidade de agregar conhecimentos a produtos e serviços faz com que as organizações modernas se tornem capazes de criar novos produtos e serviços intensivos em conhecimento (Terra, 2005).

Para Davenport e Prusak (1998), essa percepção coincide com a renovada ênfase, entre estrategistas e economistas, em idéias associadas a uma teoria empresarial baseada em competências ou em recursos. Atualmente, teóricos de muitas disciplinas estão voltando sua atenção para uma das dinâmicas essenciais das empresas: o conhecimento subjacente em rotinas e práticas que a empresa transforma em produtos e serviços valiosos.

Convém salientar que múltiplos fatores levaram à atual "explosão do conhecimento". Esta convergência de causas é um dos motivos pelos quais o ato de identificar claramente o conhecimento ganhou importância fundamental. A percepção e a realidade de um novo mundo competitivo globalizado constituem uma das forças motrizes. As rápidas mudanças e a

crescente competição levaram as empresas a buscarem uma vantagem sustentável para se distinguir em seus mercados (Davenport e Prusak,1998).

O surgimento deste fenômeno se deu com o advento da Era do Conhecimento e estão transformando as relações econômicas, políticas e sociais da civilização humana, como a globalização, os mercados regionais e os avanços tecnológicos, em especial a tecnologia da informação (Terra, 2005). Daí a necessidade de se buscar, quais seriam os principais pontos de consenso entre os diversos tipos de estudos e abordagens que procuram explicar o que é conhecimento e como o novo conhecimento é gerado.

Para Crawford (1994), na perspectiva das organizações, conhecimento é entendimento e *expertise*. É a capacidade de aplicar a informação a um trabalho ou a um resultado específico. Para efeitos deste estudo contemplou-se a definição dada por Davenport e Prusak (1998) que afirmam: conhecimento é a informação valiosa da mente humana, inclui reflexão, síntese e contexto. De difícil estruturação e captura em máquinas, frequentemente tácito e de difícil transferência.

Admite-se, contudo, a existência de muitos tipos de conhecimento que são relevantes para as empresas. Davenport e Prusak (1998) apresentam uma definição funcional de conhecimento, no âmbito das organizações:

O conhecimento é uma mistura fluida de experiência condensada, valores, informação contextual e insight experimentado, a qual proporciona uma estrutura para a avaliação e incorporação de novas experiências e informações. Ele tem origem e é aplicado na mente dos conhecedores. Nas organizações, ele costuma estar embutido não só em documentos ou repositórios, mas também em rotinas, processos, práticas e normas organizacionais (Davenport; Prusak, 1998, p.6).

Para esclarecer tal definição, Davenport e Prusak (1998) afirmam que: o conhecimento deriva da informação da mesma forma que a informação deriva de dados. Essa afirmação vai de encontro à premissa de Crawford (1994) de que somente os seres humanos são capazes de produzir e aplicar os conhecimentos através de seu cérebro ou de suas habilidosas mãos. Por isso, criar e implantar processos que gerem, armazenem, gerenciem,

disseminem e protejam o conhecimento representam o mais novo desafio a ser enfrentado pelas empresas.

2.2.2 Distinção entre dados, informação e conhecimento

É comum verificar, na literatura existente, que alguns autores não fazem distinção entre dados, informação e conhecimento, ou seja, a literatura não apresenta uma diferenciação clara entre a chamada sociedade da informação e a sociedade do conhecimento. Contudo, é possível constatar que uma é alicerce da outra e ambas estão interligadas (Terra, 2005).

> *De acordo com Choo (2003) em um primeiro nível, a organização do conhecimento é aquela que possui informações e conhecimentos que a tornam bem informada e capaz de percepção e discernimento. Num nível mais profundo, a organização do conhecimento possui informações e conhecimentos que lhe conferem uma vantagem, permitindo-lhe agir com inteligência, criatividade e, ocasionalmente, com esperteza. (Choo, 2003, p.17).*

O autor enfatiza ainda que no coração da organização do conhecimento está à administração dos processos de informação, que constituem a base para criar significado, construir conhecimento e tomar decisões. Nesse novo modelo, a informação, o conhecimento e os produtos com base nesses elementos passaram a compor os ativos das organizações. Chamados de ativos intangíveis formam a base para entrada da organização na sociedade do conhecimento e representam parte significativa do patrimônio dessas organizações (Choo, 2003).

Neste contexto, convém explicitar os conceitos de dados e de informação para que se possa fazer tal distinção e, assim, buscar uma melhor compreensão acerca dos termos aqui colocados.

Para Davenport e Prusak (1998), dados é um conjunto de fatos distintos e objetivos, relativos a eventos. Os dados por si só apresentam pouca relevância. Apesar da sua importância para as organizações, os dados não têm significado inerente, pois descrevem apenas parte daquilo que aconteceu. Sendo assim, não oferecem base de sustentação para tomada de ação.

Já a informação é descrita pelos autores como sendo uma mensagem, geralmente na forma de um documento ou uma comunicação audível ou visível. Essa mensagem constituirá uma informação dependendo de como é percebida pelo receptor. A informação movimenta-se pelas organizações por redes *hard* e *soft*, pela *internet*, via *intranet* e outros meios de divulgação. Para eles, diferentemente do dado, a informação tem significado. Ela não só dá forma ao receptor como possui ela própria uma forma: está organizada para alguma finalidade. Dados tornam-se informação quando lhes acrescenta significado (Davenport e Prusak,1998).

2.3 O PAPEL DO GESTOR NA ERA DO CONHECIMENTO

Conforme abordado, o mundo está passando por enormes mudanças. Uma dessas transformações é a globalização, com o crescimento explosivo do comércio global e da competição internacional. A outra força é a mudança tecnológica que proporciona avanços notáveis na disponibilidade de informações e na velocidade das comunicações. Paradoxo é que a globalização e os avanços tecnológicos abrem muitas novas oportunidades, não obstante ameaçarem o *status quo*. Dessa forma, "as empresas passam a operar em um mercado *darwiniano* onde os princípios de seleção natural levam à sobrevivência das mais capacitadas" (Ghoshal, 2000).

Para Stewart (1998), uma fabrica não começa a produzir coisas sozinhas, e a gestão do conhecimento não existe sem gerentes do conhecimento. Desta forma alguém precisa ser responsável pela gerência do conteúdo do conhecimento organizacional, bem como por sua tecnologia. Para aprender a lidar adequadamente com o novo é preciso quebrar pardigmas e até promover mudanças culturais Daí surge em cena um novo tipo de gerente, o gerente do conhecimento que precisa desenvolver diversos papéis.

2.3.1 Papéis gerenciais

Com relação aos papéis gerenciais, Mintzberg (*apud* Robbins, 1999) concluiu que os gerentes desempenham 10 papéis diferentes, altamente inter-relacionados, que podem ser agrupados como sendo, inicialmente, concernentes às relações interpessoais, à transferência de informação e à tomada de decisão, conforme mostra o quadro 1, a seguir:

Quadro 1: Papéis Gerenciais

Papel	Descrição	Exemplo
Interpessoal		
Figura principal	Chefe simbólico: solicitado a desempenhar um número de obrigações rotineiras de natureza legal ou social	Cerimônias requisições de status, solicitações.
Líder	Responsável pela motivação e direção de subordinados	Praticamente todas as atividades gerenciais envolvendo subordinados
Ligação	Mantém uma rede de contatos externos que fornecem favores e informações	Reconhecimento de correspondência trabalho externo no conselho
Informacional		
Monitor	Recebe grande variedade de informação; serve como centro nervoso de informação interna e externa da organização.	Lidar com toda correspondência e contatos classificados como de interesse primário para recebimento de informação.
Disseminador	Transmite informação recebida de fora ou de outros subordinados para os membros da organização	Expedição de correspondência para a organização com propósitos internacionais: contatos verbais envolvendo fluxo de informação para subordinados, assim como sessões de revisão.
Porta-voz	Transmite informação para fora sobre os planos, políticas, ações e resultados da organização; serve como perito na indústria de organização.	Reunião com o Conselho; lidar com contatos envolvendo transmissão de informação para os de fora.
Decisório		
Empreendedor	Busca oportunidades na organização e seus ambientes e inicia projetos que tragam mudanças	Sessões de estratégia e revisão envolvendo iniciação ou planejamento de projetos de aprimoramento.
Administrador de problemas	Responsável por ação corretiva quando a organização enfrenta problemas importantes e inesperados	Sessões de estratégia e revisão envolvendo problemas e crises
Alocador de recursos	Toma ou aprova decisões organizacionais significativas	Programação, requisições para autorizações; orçamentos; a programação de trabalho dos subordinados.
Negociador	Responsável por representar a organização em importantes negociações	Negociações de contratos.

Fonte: Robbins (1999)

O mundo se tornou uma aldeia global, onde as organizações não são mais limitadas por fronteiras nacionais e isso faz com que os gerentes tenham que se tornar capazes de trabalhar com pessoas de diversas culturas. Analisando o quadro 1 contata-se que os gestores, para serem capazes de trabalhar eficazmente com estas pessoas, devem entender suas culturas e como estas se moldaram, e aprender a adaptar seu estilo gerencial, adequadamente. Além disso, eles devem estar preparados para transferir informações e tomar decisões, posto que atualmente, a gestão nas organizações passa, obrigatoriamente, pela compreensão das características e demandas do ambiente competitivo.

De acordo com Nóbrega (2004), é através da gestão que outras inovações produzem seus efeitos. A mentalidade gestão é decisiva numa multiplicidade de circunstâncias. Tudo que implica organizar para alcançar um propósito precisa de gestão, pois ela está ligada à produção de riqueza, no aumento de produtividade e na qualidade de vida de um século para cá.

Se gestão significa gerência, administração pressupõe-se a ideia de dirigir, de tomada de decisão. Esse processo de decisão ocorre em várias esferas da sociedade: em instituições, organizações, empresas, grupos, entre outros. Portanto, gestão é um conjunto de regras, estruturas e ações que modelam a execução das funções de uma organização, ou seja, é a disciplina que torna produtivo os "saberes" de vários campos do conhecimento (Fernandes, 2008).

Dessa forma, cabe aos gerentes adotar práticas de gestão que propiciem a criação e aprendizado individual, assim como estratégias para conversão do conhecimento individual em coletivo nos mais diversos níveis da organização (Crawford, 1994). Tal afirmação vai ao encontro da premissa que as empresas de sucesso são aquelas que criam sistematicamente novos conhecimentos, dissemina-os pela organização inteira e rapidamente os incorporam em novas tecnologias e produtos (Garvin, 2000).

Pelo exposto, e em face das novas exigências da sociedade do conhecimento, percebe-se cada vez mais a urgência das organizações reestruturarem seus modelos de gestão.

2.3.2 A organização que dissemina o conhecimento

É evidente que se vive em um ambiente cada vez mais turbulento, em que vantagens competitivas precisam ser permanentemente, reinventadas e setores de baixa intensidade em tecnologia e conhecimento perdem, inexoravelmente, participação econômica (Fernandes, 2008).

Diante da necessidade de novos padrões de produtividade, eficácia nos custos, qualidade e necessidade de reformar as culturas empresariais com novos valores e estilos gerenciais, empresas com visão de futuro voltam-se cada vez mais para programas internos e personalizados de educação continuada de executivos, gerentes e especialistas, a fim de ajudá-los a alcançar seus objetivos estratégicos e agirem como catalisadores da mudança organizacional (Nóbrega, 2004).

Para Takeuchi e Nonaka (1997), numa economia onde a única certeza é a incerteza, apenas o conhecimento é fonte segura de vantagem competitiva. É possível observar que os mercados mudam, as tecnologias proliferam, os concorrentes se multiplicam e os produtos se tornam obsoletos quase da noite para o dia.

Dentro desta realidade, as organizações de sucesso são aquelas que, de forma consistente, criam novos conhecimentos, dissemina-os profusamente em toda a organização e rapidamente os incorpora em novas tecnologias e produtos. Essas atividades caracterizam a organização “criadora de conhecimento", cujo negócio exclusivo é a inovação contínua (Nóbrega, 2004).

A literatura sobre o tema gestão, é clara quando afirma que se deve aproveitar às intuições dos diferentes empregados, de modo a converter essas contribuições em algo sujeito a testes e possibilitar seu uso em toda a organização. O elemento crítico desse processo é o comprometimento pessoal, o senso de identidade dos empregados com a empresa e sua missão. No entanto, esse compromentimento depende da capacidade do gestor de ouvir as diversas opiniões dentro da organização (Nóbrega, 2004).

Contudo, poucos gerentes apreendem a verdadeira natureza da organização criadora de conhecimento — e muito menos sabem como gerenciá-la. O motivo: entendem de maneira imprópria o que seja conhecimento e o modo como as empresas são capazes de explorá-lo.

Considerando-se este cenário, a possibilidade de se criar mecanismos que se adaptem a realidade da organização é praticamente impossível, haja vista que os colaboradores que convivem diariamente com os problemas não são consultados.

Emerge desta situação, as habilidades humanas do gestor, ou seja, eles necessitam, de boas habilidades para lidar com pessoas. Levando-se em conta que as organizações existem para atingir objetivos cabe a eles definirem estes objetivos, bem como os meios para atingi-los.

Desta forma, os gestores devem estar cientes que os métodos tradicionais de treinamento e desenvolvimento de pessoas não têm conseguido acompanhar o ritmo das frequentes mudanças que vêm ocorrendo no mundo. Daí a necessidade de se buscar novos caminhos, para manter seu corpo gerencial e funcional atualizados, quase em tempo real.

No início do século passado, Fayol escreveu que todos os gerentes executam cinco funções gerenciais: eles planejam, organizam, comandam, coordenam e controlam. Mas segundo Robbins (1999), atualmente, estas funções foram condensadas em quatro funções: planejamento, organização, liderança e controle.

-Função planejamento: compreende definir as metas da organização, estabelecendo uma estratégia global para atingir estas metas e desenvolver uma ampla hierarquia de planos para integrar e coordenar atividades;

-Função organização: incluí a determinação de quais tarefas devem ser feitas, quem vai fazê-las, como as tarefas devem ser agrupadas, quem se reporta a quem e que decisões devem ser tomadas;

-Função liderança: como toda organização contém pessoas, os gerentes devem estar empenhados em liderá-las, pois cabe à gerência dirigi-las e coordená-las. Na função liderança, os gerentes motivam seus subordinados, dirigem as atividades de outros,

selecionam dos canais de comunicação mais eficazes ou resolvem conflitos entre seus membros.

-Função controle: depois que os objetivos são determinados, os planos formulados, os arranjos estruturais delineados e as pessoas contratadas, treinadas e motivadas, ainda existem a possibilidade de algo dar errado. Para assegurar que as coisas estejam indo conforme o desejado faz-se necessário que o gerente passe a exercer a função controle, onde o gerente deve monitorar o desempenho da organização e compará-lo com os objetivos pré-determinados. Em caso de desvio cabe ao gerente, reorganizar as atividades e fazer com que a organização volte aos trilhos (Robbins, 1999).

Como o presente estudo aborda a Gestão da Segurança da Informação na Era do Conhecimento e sua aplicação na área de TI, vale ressaltar que a alta administração, principalmente, nas organizações governamentais, não se responsabilizam pelas políticas de TI; não designam Comitê Gestor de TI; não monitoram o desempenho da Área de TI; não definem objetivos e indicadores , não avaliam o desempenho e, tampouco gerenciam os riscos de TI, conforme preconiza o IT Governance Institute – ITGI.

Sabe-se que as organizações governamentais devem apresentar resultados positivos para os cidadãos, ou seja, elas têm o dever de planejar, controlar e ser eficiente. Por isso, a qualidade da informação e o controle sobre ela é primordial. Contudo, o que se percebe é o descaso. (Fernandes, 2008).

Diante disso, infere-se que cabe aos gestores de TI a iniciativa de integrar o capital humano da organização, os parceiros, os fornecedores e, até mesmo, a sociedade, formando uma cadeia de valor, focada na estratégia, para solucionar os entraves burocráticos que dificultam a implantação de um Sistema de Gestão da Segurança da Informação eficiente e eficaz.

Daí a necessidade de se conhecer a importância do capital intelectual para as empresas, tendo em vista serem eles os principais agentes na criação do conhecimento.

2.3.3 Capital intelectual

Capital intelectual é a soma do conhecimento de todos em uma organização, o que lhe proporciona vantagens competitivas; Trata-se, portanto, da capacidade mental coletiva, a capacidade de criar continuamente e proporcionar valor de qualidade superior. Está nas habilidades dos funcionários; em seus conhecimentos tácitos e nos obtidos nas suas interações profissionais; na busca permanente de atualização do saber; nas informações alcançáveis; nas informações documentadas sobre cliente, concorrentes, parceiros e fornecedores. Portanto, diz respeito às pessoas, seu intelecto, seus conhecimentos e experiências (Fleury; Oliveira, 2001).

Para Bukowitz e Williams (2002) o capital intelectual é composto pelos ativos intangíveis da organização, e pode ser se sinônimo de conhecimento.

A literatura sobre administração e gestão, aponta para a fundamental importância da gestão dos recursos humanos nas organizações, pois segundo Garvin (2000), na nova sociedade do conhecimento, são as pessoas que farão com que as empresas possuam um diferencial e garantam vantagem competitiva no mercado.

No entender de Cavalcanti, Gomes e Pereira (2001),

> *O conceito 'capital intelectual' refere-se tanto à capacidade, habilidade e experiência quanto ao conhecimento formal das pessoas que integram uma organização. O capital intelectual é um ativo intangível que pertence ao próprio indivíduo, mas que pode ser utilizado pela empresa para gerar lucro ou aumentar seu prestígio e reconhecimento (Cavalcanti; Gomes; Pereira, 2001, p. 55).*

Para ilustrar tal afirmação, vale ressaltar a máxima de Weber (*apud* Davenport e Pruzak, 1998) que afirmam: a nova economia não está na tecnologia, seja ele o *microchip* ou a rede mundial de telecomunicações. Está na mente humana. Infere-se, portanto, que capital intelectual diz respeito às pessoas, seu intelecto, seus conhecimentos e experiências.

A constatação de que o conhecimento é o novo recurso competitivo, mostra a necessidade de se administrar o intangível. Portanto, o tema central da gestão do conhecimento é aproveitar os recursos que já existem na organização.

2.3.4 Gestão do capital intelectual

Drucker (2000) descreve a mudança organizacional como uma "viagem sem fim". Assim, qualquer grande iniciativa de mudança deve começar pela descrição do destino da viagem, ou seja, o objetivo da mudança. Dessa forma, cabe ao gestor gerenciar, administrar e dirigir a tomada de decisão.

Na opinião de Nóbrega (2004),

> *A habilidade mais central de um gestor é a mesmíssima do médico, engenheiro ou do físico: é o domínio de critérios que permitam identificar o que é relevante em cada circunstância e discernir quando faz sentido usar certo remédio, pois há sempre fatos relevantes 'escondidos' por trás das coisas que interessam no mundo das organizações. E, o talento é descobrir o que é relevante (Nóbrega, 2004, p. 17).*

No passado, o paradigma de organização era uma coleção de funções bem desenvolvidas e administradas, criando um padrão de excelência operacional. Como consequência, os produtos gerados eram os melhores possíveis, e bastavam manuais funcionais, que deviam ser obedecidos por todos, e durar para sempre. O sucesso dependia apenas de seguir à risca as instruções prescritas, e o trabalho gerencial era zelar pelo fiel cumprimento das prescrições (Drucker, 2000).

Modernamente, as organizações vivem em um ambiente cada vez mais turbulento, em que vantagens competitivas precisam ser permanentemente, reinventadas e setores de baixa intensidade em tecnologia e conhecimento perdem, inexoravelmente, participação econômica (Nóbrega, 2004).

Assim, surgiram inúmeros projetos de reengenharia, que transformaram radicalmente o panorama empresarial. Mas, se por um lado esses projetos de reengenharia abordaram os processos, tornando-os ágeis, flexíveis e mais dinâmicos, por outro, o enfoque restringiu-se aos fluxos de informação, ignorando o conhecimento. Isso justifica a permanência de deficiências até hoje não superadas, posto que a flexibilidade das pessoas, de maneira geral, é próxima a zero (Nóbrega, 2004).

Sobre o assunto, Cury (2000) argumenta:

> *Uma organização é mais do que um conjunto de bens e serviços. É também uma sociedade humana e, como todas as sociedades desenvolvem formas específicas de cultura. Essa cultura aliada à capacitação organizacional são fontes de sucesso cada vez mais importantes. Assim, organizações devem procurar construir relações tanto com os clientes como com os funcionários, pois organizações com cultura forte evitam a rotatividade, pois para preservar e construir capacidade organizacional é necessário reter aqueles que detêm o conhecimento tácito (Cury, 2000, p. 103).*

Nesse contexto, cabe aos gerentes adotar práticas de gestão que propiciem a criação e aprendizado individual, assim como estratégias para conversão do conhecimento individual em coletivo nos mais diversos níveis da organização (Takeuchi; Nonaka, 1997).

Hoje, o êxito das empresas se situa mais em suas capacidades intelectuais e sistêmicas do que nos ativos físicos. O gerenciamento do intelecto humano e, sua conversão em produtos e serviços úteis, transforma-se rapidamente na habilidade executiva crítica da Era do Conhecimento.

As organizações saudáveis geram e usam o conhecimento. À medida que interagem com seus ambientes, elas absorvem informações, transformam-nas em conhecimento e agem com base numa combinação desse conhecimento com suas experiências, valores e regras internas (Davenport e Prusak,1998).

Percebe-se, então que existem várias maneiras de as empresas estimularem o compartilhamento fortuito do conhecimento em seus departamentos ou unidades de negócios, tais como: criar locais e ocasiões para os funcionários interagirem informalmente. Todavia, elas são localizadas e fragmentárias. Dessa forma, é pouco provável o sucesso de empresas que não se preocupem com o tema, gestão do capital intelectual.

2.4 A INFRAESTRUTURA DE TI

Conforme abordado no decorrer deste estudo, o ambiente institucional está mudando continuamente, tornando-se mais complexo e menos previsível, e cada vez mais dependente de informação e de toda a infraestrutura tecnológica que permite o gerenciamento de enormes quantidades de dados.

A maioria das organizações reconhece a importância de uma infraestrutura de TI otimizada e eficiente, haja vista que ela é um ativo estratégico e o alicerce essencial ao qual o software pode oferecer serviços e aplicativos de usuários necessários para que o negócio funcione de modo eficaz e bem-sucedido (Microsoft TechNet, 2006).

A infraestrutura TI é uma das áreas que mais proporcionam valor ao negocio. Para a Microsoft TechNet, a capacidade do cliente em usar a tecnologia para aprimorar a agilidade do negócio e oferecer valor comercial aumenta à medida que passa do estado básico e continua em direção a um estado dinâmico, que dá autonomia aos operadores de informações e gerentes, oferecendo suporte a novas oportunidades comerciais.

Ao sair de um estado básico e caminhar rumo a um estado dinâmico com uma infraestrutura mais madura, a segurança melhora de altamente vulnerável para dinamicamente proativa, pois o gerenciamento de infraestrutura de TI muda de altamente manual e reativo para altamente automatizado e proativo (Microsoft TechNet).

Segundo Soares (2011), as novas realidades de negócios, de modo geral apontam para empresas fortemente suportadas pela TI. A obtenção de informações precisas, ágeis e confiáveis fez com que houvesse um aumento considerável sobre as exigências por serviços da TI com qualidade. Em consequência disto à infraestrutura de TI torna-se cada vez mais complexa para suportar todos os processos de negócio.

Sendo assim, racionalizar a infraestrutura tem sido a meta das organizações que, via de regra, assumem uma visão estratégica de maior prazo com relação à maturidade de infraestrutura de TI, vinculando esses aprimoramentos de capacidade e maturidade às suas necessidades comerciais e à estratégia comercial global (Microsoft TechNet).

Contudo, passar de um ambiente altamente vulnerável, com uma infraestrutura básica, para uma infraestrutura mais madura proativamente dinâmica requer investimentos. O mercado disponibiliza as tecnologias, os processos e os procedimentos para auxiliar as organizações a passar pela jornada de otimização da infraestrutura.

Para compor esta infraestrutura de TI dinamicamente proativa faz-se necessário os seguintes elementos: computadores e equipamentos relacionados, sistemas de armazenamento

e recuperação, *software* básico e aplicações computacionais, sistemas de redes, e instalações prediais.

2.4.1 Instalações prediais

A primeira etapa da infraestrutura de TI, geralmente, é a definição do local onde serão instalados os equipamentos (instalações prediais). A infraestrutura de TI precisa ser alocada em local seguro em um ambiente estável, suprida com energia elétrica suficiente para sua operação. Faz-se necessária também uma adequada climatização do ambiente, com vistas a manter o funcionamento adequado dos equipamentos. É preciso, ainda controlar o acesso a estas instalações, evitando o acesso não autorizado, danos e interferências nos equipamentos e garantia de segurança às informações organizacionais que serão armazenadas. (Araújo, 2010).

2.4.2 Equipamentos de informática

Este termo engloba diversos ativos importantes da infraestrutura de TI, que vão desde computadores desktops, notebooks e servidores, impressoras, entre outros. Trata-se, portanto, de uma infraestrutura ampla, que depende do porte da organização e de suas expectativas em relação ao objetivo que se quer atingir. Entre os principais elementos que compõem uma infraestrutura de TI listam-se os seguintes:

- Servidores: São computadores robustos, geralmente com uma boa capacidade de processamento, de memória e de espaço em discos configurado para oferecer serviços remotos, em geral para várias pessoas, tais como: serviço de email, página Web, banco de dados entre outros. Eles podem ser de três tipos: servidor torre (gabinetes desktops), servidores em *rack* horizontal e servidores *blade*, que são instalados verticalmente em *racks* e abrigam servidores, *storage* e *switches* em um mesmo chassi (Araújo, 2010).

- *Desktops e notebooks:* Os computadores pessoais são ativos importantes da infraestrutura de TI estão presentes, por exemplo, nos laboratórios, secretarias e salas de professores, pois é por meio destes equipamentos que os colaboradores têm acesso aos dados e informações disponibilizados para a organização (Araújo, 2010).

2.4.3 Infraestrutura de redes

Para que a informação trafegue no ambiente organizacional, faz-se necessário a instalação de uma infraestrutura de rede que conta com um conjunto de elementos que facilitam o estabelecimento dessa comunicação. Entre os principais elementos desta infraestrutura destacam-se os seguintes:

- Cabeamento de rede: para que os dispositivos citados possam realizar suas funções, eles precisam estar conectados. Esta é função dos cabos de rede, possibilitar a comunicação entre os dispositivos de redes. São exemplos de cabos de redes: cabo coaxial, cabo de par trançado e cabo de fibra óptica.

- Placas de rede: Permitem que os computadores sejam conectados à rede de uma organização, geralmente utilizando o protocolo tcp/ip.

- *Bridges*: Responsáveis por interligar duas ou mais redes, atuam tanto como regenerador de sinais, quanto como verificador de endereços contidos nos *frames* das mensagens.

- Hubs: Responsáveis pela comunicação entre diferentes redes de computadores permitindo que computadores distantes se comuniquem.

- Switches: Dispositivos responsáveis por reencaminhar módulos (frames) entre os diversos nós de uma rede.

- Repetidores: São equipamentos responsáveis por regenerar o padrão de bits de sinais recebidos, com a finalidade de evitar danos à integridade do sinal transmitido e que o mesmo não chegue muito fraco ao próximo ponto da rede.

- Gateway**:** Responsável por interligar redes que usam protocolos diferentes (Tanenbaum, 2003).

2.4.4 Sistemas de armazenamento e recuperação de dados e informações

O armazenamento dos dados e das informações de uma organização é uma questão crítica de responsabilidade da infraestrutura de TI. Neste contexto, os mecanismos

responsáveis por armazenar e recuperar dados e informações organizacionais devem fazê-lo mantendo a segurança da informação, preservando as características da informação no que diz respeito à sua integridade, disponibilidade e confidencialidade, além de sua autenticidade, conforme dispõe a norma ISO/IEC 27002 (ABNT, 2005).

Neste contexto, o *storage*, que pode ser considerado como um servidor de discos para armazenamento de dados em uma rede, sendo o principal elemento do sistema de armazenamento, garantindo robustez e segurança aos dados armazenados (Castells, 2007).

2.4.5 Software

Software é o programa de computador e toda a documentação e mídia que o acompanha, ou seja, são sistemas baseados em computador e é por meio de sua utilização que são suportados, diretamente ou indiretamente, os processos da organização. Geralmente, um software é classificado em categorias quanto ao grau de associação do mesmo às atividades de controle do computador e às atividades finais do usuário (Tanenbaum, 2003).

De acordo com Araújo (2010), os softwares podem ser softwares de sistema (softwares básicos às rotinas do computador, fazendo com que seus componentes funcionem corretamente e interajam entre si), aplicativo (aqueles utilizados pelos usuários para desempenhar tarefas) ou embarcado (software embutidos que disponibilizam as funções a que se destinam equipamentos que não são computadores, como por exemplo, um micro-ondas. Sintetizando, o software básico é responsável pelo gerenciamento de recursos computacionais, enquanto o software aplicativo está voltado para as necessidades finais do usuário (como, por exemplo, digitar um texto, navegar na internet ou jogar).

2.5 OS PRESSUPOSTOS PARA A EFETIVIDADE E EFICÁCIA DE UM SGSI NAS ORGANIZAÇÕES GOVERNAMENTAIS

A palavra “informação”, sempre foi ambígua e liberalmente empregada para definir diversos conceitos. A palavra tem sua raiz no latim informar, que significa “a ação de formar matéria, tal como pedra, madeira, couro etc. “Segundo Setzer (1999), a definição mais comum é: a ação de informar; formação ou moldagem da mente ou do caráter, treinamento, instrução, ensinamento, comunicação de conhecimento instrutivo.

Em se tratando de segurança da informação, as normas da família ISO/IEC 27000 definem- a como: “a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre investimentos e as oportunidades de negócio.” A *International Organization for Standardization* afirma que a segurança da informação é importante para os negócios, tanto do setor público quanto do privado, para proteger as infraestruturas críticas (ABNT, 2005).

2.5.1 A importância da gestão de segurança da informação

Diariamente as organizações, seus sistemas e redes de computadores são expostos a diversos tipos de ameaças a segurança das informações. Ocorre que, muitos sistemas de informação não foram projetados para serem seguros. Contudo, a segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados (Sêmola, 2003).

Atualmente, numa era onde o conhecimento e a informação são fatores de suma importância para qualquer indivíduo, organização ou nação, a Segurança da Informação é um pré-requisito para todo e qualquer sistema de informações estarem, de certa forma, protegidos. Sendo assim, a segurança da informação pode ser definida como um conjunto de medidas que se constituem basicamente de controles e políticas de segurança, que devem ser implementadas para proteger e defender a informação que está em um ambiente de perigo, risco ou incerteza, tendo como principal objetivo a proteção das informações de clientes e empresa, para assegurar que os riscos sejam reduzidos a um nível aceitável evitando-se a revelação ou alteração por pessoas não autorizadas (Soares, 2011).

2.5.2 Histórico das normas da família ISO/IEC 27000

A série ISO/IEC 27000 foi criada para que pudesse reunir de forma ordenada às diversas normas de segurança da informação, esta série é composta por normas de segurança da informação publicadas através da parceria entre a *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC).

A série ISO 27000 está sendo povoada por várias normas individuais, algumas delas bastante conhecidas e já publicadas. Outras serão definidas, desenvolvidas e publicadas

paulatinamente nos próximos meses e anos. A Figura 1 reflete a posição atual das principais normas operacionais da série 27000, explicitando algumas de suas funções.

Figura 1 – Normas ISO 27000
Fonte: (Correia, 2011)

Essa série não cobre apenas questões técnicas de segurança dentro do setor de tecnologia da informação, sendo propositalmente abrangente para que possa ser aplicável em qualquer organização, não importando seu tamanho ou segmento.

Em se tratando da norma NBR ISO/IEC 27002, antiga NBR ISO/IEC 17799, convém lembrar que ela é derivada da norma britânica BS 7799, que foi a primeira norma com foco em Sistemas de Informação – SI. Esta norma é de muita valia para organizações que almejam a implantação de um processo de segurança da informação efetivo, porém a de se ressaltar que a norma é apenas guia, apenas a vontade e dedicação das organizações poderão determinar o sucesso em se implementar tais mecanismos.

A mencionada norma foi desenvolvida pelo *British Standard Institute* - BSI. A primeira parte dessa norma, BS 7799-1, publicada em 1995, tem como foco um código de melhores práticas de SI. Já a segunda parte, BS 7799-2, publicada em 1998, de forma geral, implementa o sistema de gestão dessas melhores práticas.

Em 2000, a BS 7799-1 foi republicada e atualizada tornando-se uma norma ISO, mais especificamente, a ISO 17799:2000. Sua primeira versão brasileira foi publicada em 2001, com a denominação de NBR ISO 17799. Em 2005 foi publicada a segunda versão da norma no Brasil, a NBR ISO/IEC 17799.

Posteriormente, a segunda parte da norma BS 7799, também se tornou um padrão ISO, a ISO 27001; e a norma ISO 17799:2005 se tornou o padrão ISO 27002, que no Brasil, foi numerada como NBR ISO/IEC 27002. Infere-se, portanto, que estas normas tornaram padrão internacional o que havia sido desenvolvido e publicado pela entidade normativa inglesa *British Standard Institution* – BSI.

Contudo, o universo das normas da família ISO/IEC 27000, não se restringe as normas ISO/IEC 27001 e 27002, que atualmente, são as principais referências para a quem procura tratar a questão da segurança da informação de maneira eficiente e eficaz.

A família ISO/IEC 27000 continua a crescer. Na reunião do Comitê ISO/IEC, em Novembro de 2005, em *Kuala Lumpur*, na Malásia, foram aprovadas as seguintes normas e projetos de norma desta família.

- ISO/IEC 27000/2009 - Sistema de Gerenciamento de Segurança - Explicação da série de normas, objetivos e vocabulários;
- ISO/IEC 27001/2005 - Sistema de Gestão de Segurança da Informação - Especifica requerimentos para estabelecer, implementar, monitorar e rever, além de manter e provisionar um sistema de gerenciamento completo. Utiliza o *Plan-Do-Check-Act* - PDCA (como princípio da norma e é certificável para empresas;
- ISO/IEC 27002/2005 - Código de Melhores Práticas para a Gestão de Segurança da Informação - Mostra o caminho de como alcanças os controles

certificáveis na ISO 27001. Essa ISO é certificável para profissionais e não para empresas;

- ISO/IEC 27003/2010 - Diretrizes para Implantação de um Sistema de Gestão da Segurança da Informação - Segundo a própria ISO/IEC 27003, "o propósito desta norma é fornecer diretrizes práticas para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI), na organização, de acordo com a ABNT NBR ISO/IEC 27001/2005;
- ISO/IEC 27004/2009 - Gerenciamento de Métricas e Relatórios para um Sistema de Gestão de Segurança da Informação - Mostra como medir a eficácia do sistema de gestão de SI na corporação;
- ISO/IEC 27005/2008 - Gestão de Riscos de Segurança da Informação - Essa norma é responsável por todo ciclo de controle de riscos na organização, atuando junto à ISO/IEC 27001 em casos de certificação ou através da ISO/IEC 27002 em casos de somente implantação;
- ISO/IEC 27006/2007 - Requisitos para auditorias externas em um Sistema de Gerenciamento de Segurança da Informação - Especifica como o processo de auditoria de um sistema de gerenciamento de segurança da informação deve ocorrer;
- ISO/IEC 27007 – Referências (*guidelines*) para auditorias em um Sistema de Gerenciamento de Segurança da Informação;
- ISO/IEC 27008 - Auditoria nos controles de um SGSI - O foco são nos controles para implementação da ISO/IEC 27001;
- ISO/IEC 27010 - Gestão de Segurança da Informação para Comunicações Inter Empresariais- Foco nas melhores formas de comunicar, acompanhar, monitorar grandes incidentes e fazer com que isso seja feito de forma transparente entre empresas particulares e governamentais;
- ISO/IEC 27011/2008 - Gestão de Segurança da Informação para empresa de Telecomunicações baseada na ISO/IEC 27002 - Entende-se que toda parte de telecomunicação é vital e essencial para que um SGSI atinja seus objetivos plenos, juntamente com outras áreas, para tanto foi necessário normatizar os processos e procedimentos desta área objetivando a segurança da informação

> corporativa de uma maneira geral. A maneira como isso foi feito, foi tendo como base os controles e indicações da ISO/IEC 27002 (Correia, 2011).

Com a evolução, de forma acelerada, da Tecnologia da Informação aumentou de forma significativa a complexidade deste ambiente, bem como, o seu relacionamento com as demais áreas dentro das organizações. Consequentemente passou-se a exigir dos gestores à aplicação de controles cada vez mais eficientes e eficazes capazes de salvaguardar a informação corporativa, posto que ela carregue em si conhecimento e inteligência.

Dentro desta realidade, as ações de Segurança da Informação tornaram-se organizadas, alinhadas ao negócio e principalmente embasadas por códigos de boas práticas e normas internacionais. Sendo, assim, conforme abordado no decorrer deste estudo a principal referência mundial em norma de Segurança da Informação é a série de normas da família ISO 27000 que evoluíram com o passar dos anos e passaram por inúmeras mudanças até chegarem às normas que modernamente são utilizadas.

As mencionadas normas possuem diferentes funções, como por exemplo: fundamentos e vocabulário; requisitos; e diretrizes, que ajudam a elevar o nível de confiança inter-organizacionais (CERT.br, 2011).

2.5.3 Princípios básicos da segurança da informação

Conforme abordado, a segurança da informação é o bem mais valioso de uma organização, seja ela pública ou privada. A segurança busca garantir à integridade da informação, reduzindo ao máximo os riscos de vazamentos de informações, a integridade dos bancos de dados, as fraudes em arquivos, o roubo de informações, a proteção contra erros humanos e operacionais por falta de treinamento, o uso indevido do sistema por pessoas não autorizadas que podem sabotar o sistema, ocasionando paralisações de rede ou serviços, ou até mesmo ameaças que visam prejudicar as organizações e, também os equipamentos utilizados.

Daí a necessidade de se investir em segurança da informação. Em se tratando dos princípios a ISO/IEC 27002/2005 preconiza que é foco da administração de segurança da informação:

- A confidencialidade: é a garantia de que a informação só poderá ser acessada por pessoas autorizadas, ou seja, é a proteção da informação contra sua revelação, leitura ou cópia por pessoas não autorizadas, tanto interna quanto externamente.

- A integridade: se refere à informação que é exata e completa, ou seja é a proteção contra qualquer modificação que não seja autorizada pelo proprietário daquela informação. Portanto, integridade é a garantia que o dado permanece intacto, não foi corrompido, encontra-se íntegro. Em outras palavras, nada foi acrescentado, retirado ou modificado dos dados originais.

- A disponibilidade: também chamada de continuidade dos serviços, significa que a informação deve estar acessível às pessoas autorizadas no momento em que for necessária. Sintetizando, é a proteção das informações disponíveis no sistema contra a degradação e indisponibilidade (ABNT, 2005).

- A autenticidade: o controle de autenticidade está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo (Stair, 2002).

O autor ressalta ainda que a verificação de autenticidade é necessária após todo processo de identificação, seja de um usuário para um sistema, de um sistema para o usuário ou de um sistema para outro sistema. Ela é a medida de proteção de um serviço/informação contra a personificação por intrusos (Stair, 2002). Contudo, outras propriedades tais como, não repúdio, responsabilidade e confiabilidade também podem estar envolvidas, conforme descrito pela Figura 2.

Figura 2 - Princípios Básicos da Segurança da Informação
Fonte: Soares (2011)

Infere-se, portanto, que qualquer solução de segurança da Informação deve satisfazer os citados princípios. Sendo assim, para garantir a confidencialidade e privacidade esta proteção deve ser estendida a qualquer mídia que a contenha, seja ela impressa ou digital, considerando todos os fragmentos de informação que podem cair em mãos erradas e prejudicar os planos da organização.

É preciso garantir que os dados que estão em trânsito na rede não sejam vistos, alterados ou extraídos por pessoas estranhas ao ambiente corporativo e, até mesmo pelo público interno que não esteja autorizado para tanto. Por isso, é necessário ter controle de acesso, ter *logs* de quem teve acesso, checar permissões, entre outros, para evitar a indisponibilidade destes dados. (CERT.br, 2011).

2.5.4 Análise e avaliação dos riscos

A Tecnologia da Informação - TI tornou-se estratégica para as Organizações governamentais, consequentemente o tema Segurança da Informação tem sido priorizado no ambiente corporativo, posto que as organizações, tanto públicas quanto privadas estão cada vez mais preocupadas com as ameaças que podem comprometer a segurança de suas informações. Elas sabem que é importante proteger seus dados e recursos contra perdas e danos ou qualquer outro tipo de evento (DIAS, 2000).

Tal afirmativa encontra suporte na edição de leis e normativos relacionados à Segurança da Informação, aplicáveis à Administração Pública Federal. Entre os principais normativos cita-se os seguintes:

- Lei Nº 7.232/84, da Casa Civil, da Presidência da República, que "Dispõe sobre a Política Nacional de Informática, e dá outras providências (CASA CIVIL,84);

- Decretos 3.505/2000, 3.996/2001 e 4.553/2002, provenientes da Casa Civil da Presidência da República, Subchefia de Assuntos Jurídicos, que preconizam, respectivamente: "Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal"; "Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal"; e "Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal" (CASA CIVIL, 2000, 2001 e 2002).

- Instrução Normativa GSI/PR, nº 1, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

- Norma Complementar nº 002/DSIC/GSIPR - Metodologia de gestão de SIC. Define a metodologia de gestão de segurança da informação e comunicações utilizada pelos órgãos e entidades da Administração Pública Federal, direta e indireta;

- Norma Complementar nº 003 - Elaboração e manutenção da Política de Segurança. Estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações (POSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta;

- Norma Complementar nº 004 - Gestão de Riscos. Estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

- Norma Complementar nº 005 - Disciplina criação de ETIR (CRI). Disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta;

- Norma Complementar nº 006 - GCN. Estabelece diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

- Norma Complementar nº 07/IN01/DSIC/GSIPR,. Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

- Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

- Norma Complementar nº 09/IN01/DSIC/GSIPR, Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta.

- Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

- Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

- Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

- Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

- Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

- Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

- Instrução Normativa nº 04, de 19 de maio de 2008. Dispõe sobre o processo de contratação de serviços de Tecnologia da Informação pela Administração Pública Federal direta, autárquica e fundacional.

Percebe-se, portanto, que a inserção do Brasil na sociedade da informação fez com que a Administração Pública passasse a se preocupar com a eficiência e efetividade da máquina administrativa, pois o sucesso da política de governo eletrônico depende da definição e publicação de políticas, padrões, normas e métodos para sustentar as ações de implantação e operação do Governo Eletrônico que cubram uma série de fatores críticos para o sucesso das iniciativas governamentais.

Por isso, a segurança da informação passou a fazer parte da agenda governamental, posto que as Organizações Governamentais tem dado grande atenção para a segurança da informação, com o intuito de proteger seus ativos. Mas, além da edição de leis e normativos relacionados à segurança da informação, aplicáveis à Administração Pública Federal, os gestores da área de TI contam ainda com outras medidas que podem ser tomadas para garantir à segurança da informação no âmbito das organizações governamentais, como por exemplo: estudos e capacitações do capital humano e também com as diretrizes para o gerenciamento de riscos fornecidos pela Norma ISO/IEC 27005.

2.5.5 A Gestão de riscos de segurança da informação (ISO/IEC 27005)

Como gerenciar risco de segurança da informação tornou-se prioritário para as áreas de TI, convém destacar que a Norma ISO/IEC 27005 fornece as diretrizes para o gerenciamento dos riscos de – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação, descrevendo o passo a passo, do processo de gestão de riscos, auxiliando as organizações na administração de tais riscos (ABNT, 2008). Segundo a mencionada norma o processo de Gestão de Risco contempla as seguintes etapas:

- Definição do contexto – nesta etapa é feita uma análise da organização definindo suas principais características, o escopo e os limites de atuação, ou seja, antes de iniciar a Análise de Risco é necessário entender a organização e suas capacidades/potencialidades, assim como quais são suas metas, objetivos e estratégias utilizadas para atingi-las. É, portanto, a identificação da área de interesse, identificação e avaliação dos recursos, e identificação dos requisitos de segurança.

- Análise/Avaliação de riscos – esta etapa é composta por três sub-atividades: identificação dos riscos, análise dos riscos e avaliação dos riscos. É onde há a identificação dos riscos, de ameaças e vulnerabilidades dos recursos do sistema.. Os riscos são classificados conforme sua ordem de prioridade e relevância, ou melhor, determina-se o nível, a prioridade e a categoria dos riscos se descreve o critério utilizado para a avaliação de cada um dos riscos a serem classificados, bem como se especifica as condições que deverão ser seguidas para que o sistema se comporte dentro dos parâmetros estabelecidos. Se as informações obtidas forem suficientes para tomar as medidas necessárias para a redução dos riscos a níveis aceitáveis, inicia-se o tratamento dos riscos;

- Tratamento do risco – nesta etapa as medidas para reduzir os riscos previamente identificados são selecionadas e implantadas de modo a manter os níveis de risco em patamares aceitáveis estabelecidos pelo critério de risco. Também são tomadas as medidas para tratar dos aspectos parciais com a diminuição do impacto. Portanto, é a etapa onde os controles para reduzir, evitar, transferir ou prevenir os riscos são definidos ;

- Aceitação do risco - é uma das formas de tratamento de riscos. Quando o custo de proteção contra um determinado risco é superior ao custo do próprio ativo, se aceita o risco.

Esta aceitação também pode ser estendida para os casos em que os riscos já atingiram patamares aceitáveis. A aceitação deve assegurar que os riscos residuais sejam explicitamente entendidos pelos gestores da organização, pois se não há possibilidade de evitar ou tratar o risco, é importante aceitá-lo e registrar a decisão identificando o responsável pela decisão. Essa explicitação é importante nos casos em que ocorre a omissão ou adiamento da aplicação das medidas para tratar os riscos residuais, por exemplo, devido a custos;

- Comunicação do riscos – ela pode ocorrer durante todo o ciclo de gestão de riscos e é nesta atividade que as informações sobre os riscos que foram identificados, tratados ou não, devem ser disseminadas para todos os envolvidos que precisam ter conhecimento a respeito desses riscos. A meta é alcançar o consenso sobre como os riscos devem ser gerenciados entre os tomadores de decisão e as partes interessadas. A comunicação dos riscos inclui a informação sobre a existência, natureza, forma, probabilidade, severidade, tratamento, aceitabilidade dos riscos, entre outros, haja vista que alguns riscos não são tratados por falta de recursos.

- Monitoramento e Análise crítica de riscos – conforme abordado no decorrer deste estudo os riscos, ativos, vulnerabilidades, ameaças e probabilidades de ocorrência devem ser monitorados constantemente a fim de tomar decisões com maior agilidade nas possíveis mudanças no contexto da organização. Os riscos e seus fatores são dinâmicos e podem mudar repentinamente, fazendo surgir novas ameaças e vulnerabilidades que podem alterar a situação dos riscos considerados aceitáveis. O monitoramento constante e a análise crítica podem contribuir para a melhoria do processo de gestão de risco

Neste contexto, a Figura 3 sintetiza as várias etapas do processo de Gestão de Risco, mostrando que o processo se inicia com a Definição do Contexto da organização, onde se identifica e se avalia os riscos, classificando-os conforme sua ordem de prioridade e relevância.

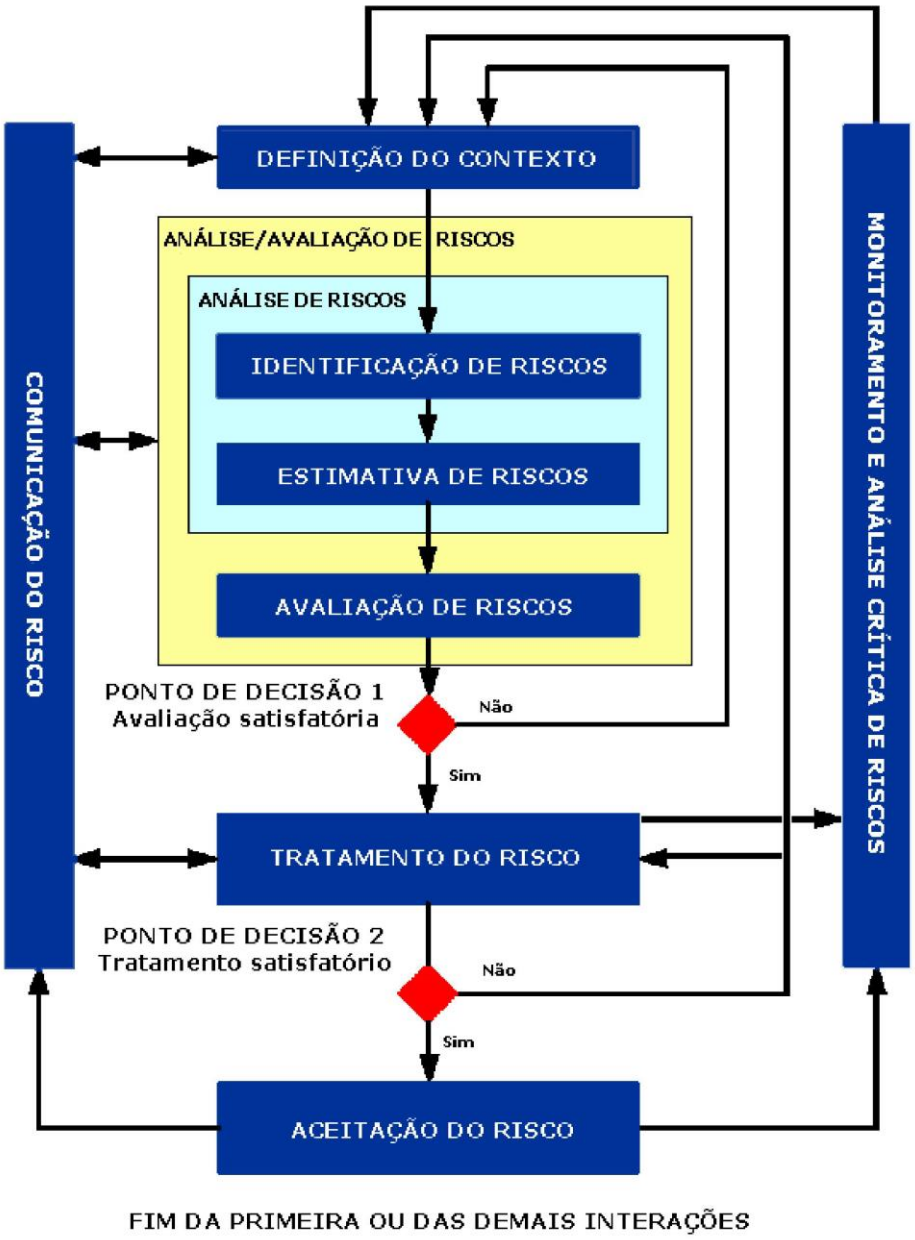

Figura 3 - Etapas e processos da gestão de riscos de SI
Fonte: Norma ABNT ISO/IEC 27005:2008

Após a análise/avaliação do Risco observa-se, na Figura 3 o Ponto de Decisão 1 que possibilita a verificação da avaliação, permitindo classificá-la como satisfatória ou não. Casso a avaliação seja satisfatória, a etapa está concluída, o que permite partir para a próxima etapa que é o Tratamento do Risco, mas, caso seja negativo é necessário repetir a análise/avaliação de Riscos e revisto a Definição do Contexto, quantas vezes forem necessárias, evitando que se

prejudique o tratamento dos riscos, como se pode observar no Ponto de Decisão 2. Mas, caso seja afirmativo é possível partir para a Aceitação do Risco que é a próxima etapa descrita na figura 3. Nesta etapa, se esclarece de forma transparente todos os riscos existentes, dando ciência aos gestores da organização, bem como ao pessoal responsável pela operação do sistema, definindo os recursos necessários para lidar de forma efetiva com este tipo de incidente indesejável e outros eventos não previstos.

No que diz respeito à etapa de Monitoramento e Análise Crítica dos Riscos, as atividades inerentes a esta etapa são constantes, pois os riscos não são estáticos e precisam de monitoramento contínuo. Assim, caso a organização adquira novos ativos, como por exemplo, novos equipamentos e contratação de novos funcionários estes devem ser incluídos no monitoramento

Observa-se, portanto, que as organizações podem e devem tomar providências para limitar as oportunidades de quebra da segurança, como também estabelecer diretivas e procedimentos para minimizar os efeitos da perda ou dano em seu ambiente de TI.

2.5.6 Gestão estratégica da segurança da informação

Ao avaliar os riscos as organizações determinam as necessidades de segurança adequadas, assim como os processos que estão em funcionamento no momento. Como os requisitos de segurança são múltiplos e podem variar de empresa para empresa ou de instituição para instituição, dependendo do seu porte, setor de atuação, leis e regulamentos federais e regionais, entre outros, as organizações podem optar pela política de segurança que melhor se enquadra ao seu segmento corporativo

Sendo assim, após considerar todos os requisitos inerentes à organização o gestor de Segurança da Informação pode definir um processo de segurança apropriado. Com o planejamento adequado, as organizações podem lidar com brechas de segurança de forma proativa.

Para Peltier (2001), a gestão estratégica da segurança deve considerar 8 elementos do sistema de proteção da informação. São eles:

- O sistema de proteção da informação deve estar alinhado com as estratégias e objetivos de negócios da organização;
- A proteção da informação requer comprometimento da alta direção em manter alinhados os objetivos de segurança com os níveis de segurança desejados para o negócio;
- Os investimentos em segurança da informação devem ser compatíveis com o nível de segurança e proteção da informação esperada pela organização, ou melhor, necessário para suportar os negócios;
- As responsabilidades com a segurança e a proteção da informação, devem estar explicitas para todos os funcionários, clientes e fornecedores e as consequências advindas do não cumprimento das políticas, normas e procedimentos devem ser claramente divulgados e conhecidos por todos;
- Os proprietários (responsáveis pela guarda, monitoramento e administração) das informações têm responsabilidades sobre a manutenção da integridade, confidencialidade e disponibilidade, podendo dar permissões de acesso ou retirá-las de acordo com as necessidades do negócio;
- A proteção da informação deve fazer parte de um sistema com análise, revisões e correções permanentes que devem incluir a análise de risco e de impacto no negócio, e a classificação da informação, visando garantir a manutenção do nível esperado de segurança pela organização;
- O sistema de segurança da informação deve ser periodicamente auditado e testado, considerando as disposições ou ações corretivas para desvios ou falhas de funcionamento encontrados, e realimentando assim todo o sistema com a verificação de novas vulnerabilidades que possam ter surgido ao longo de seu funcionamento;
- A segurança da informação é um sistema eficiente de proteção dos ativos, deve ser construída com base na cultura da organização e nas necessidades de proteção identificadas, preservando as devidas regionalidades e propriedades inerentes aos países onde as mesmas existem ou suas filiais estão instaladas;
- A proteção da informação deve ser um meio para organização alcançar seus objetivos e não deve significar um fim em si mesma (Peltier, 2001).

Ainda segundo o autor, a implementação do sistema de proteção da informação deve transpor as fronteiras da implantação de dispositivos de hardware ou software, que protegem o que está armazenado nos bancos de dados e arquivos da empresa, e muitas vezes não oferecem a segurança necessária ou esperada devido a falhas de funcionamento ou de parametrização e instalação (Peltier, 2001).

Peltier (2011) enfatiza, também, que o sistema deve considerar o grau de dependência da organização da utilização da informática como ferramenta de trabalho no seu dia-a-dia, as necessidades de manutenção dos sistemas ativos em caso de desastre e o comprometimento de áreas críticas da organização, com problemas de vazamento de informações, entre outros. Para resolver estes problemas será necessário, e pode-se dizer fundamental a definição da Política de Segurança da Informação, que é o conjunto de diretrizes do sistema de gestão de segurança da informação.

2.5.7 Definição da política de segurança da informação

O desenvolvimento e a implantação de uma política segurança da informação em uma organização é uma importante ferramenta para combater ameaças aos seus ativos. No entanto, trata-se de uma tarefa complexa que exige monitoramento contínuo, revisões e atualizações periódicas, cujos resultados serão perceptíveis a médio e longo prazo. Mas com o crescimento acelerado do uso de tecnologias, com sistemas cada vez mais interligados é fundamental que se invista em segurança.

De acordo com o RFC 2196 (*The Site Security Handbook*), "uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização", ou seja, a política de segurança é um conjunto de diretrizes, normas e orientações de procedimentos que devem ser observados por todos os integrantes e colaboradores de uma organização e, aplicados a todos os sistemas de informação e processos corporativos, visando conscientizar e orientar os funcionários, parceiros, colaboradores e fornecedores para o uso seguro dos ativos da empresa.

Como o bem mais importante que as empresas possuem, atualmente, são as informações gerenciais, uma política de segurança bem elaborada pode minimizar problemas com o aprimoramento constante dos processos de resposta a incidentes, tanto internos quanto

externos. Para tanto, as políticas de segurança devem se adequar a realidade das organizações, ou seja, devem ser objetivas, definindo claramente as áreas de responsabilidade dos usuários, dos gestores de sistemas e redes, bem como dos diretores. Ademais, elas devem se adaptar a alterações que ocorrem na organização.

É importante frisar que as políticas de segurança fornecem parâmetros para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.

Dentro deste contexto, uma das opções que se pode extrair de uma política de segurança preventiva é o gerenciamento de riscos proativo. Mesmo não garantindo imunidade total as organizações, o gerenciamento de riscos de segurança proativo apresenta inúmeras vantagens, pois busca reduzir, preventivamente, a ocorrência de eventos prejudiciais implementando controles capazes de reduzir o risco de exploração de vulnerabilidades, protegendo ativos importantes da organização. Além do mais, este tipo de gerenciamento reduz significativamente o número de incidentes de segurança futuros.

Contudo, convém ressaltar que, a gestão da segurança da informação necessita, da participação de todos os funcionários da organização e por vezes é necessária a participação de fornecedores e clientes que devem ser convocados pela alta direção (diretor, comitê de segurança da informação, comitê de riscos) a quem compete a:

- análise crítica e aprovação da política da segurança da informação e das responsabilidades envolvidas;

- monitoração das principais mudanças na exposição dos ativos das informações às principais ameaças;

- análise crítica e monitoração de incidentes de segurança da informação;

- aprovação das principais iniciativas para aumentar o nível da segurança da informação.

De acordo com o tamanho da organização, pode ser nomeado um representante da alta direção, que ficará incumbido de liderar uma equipe destinada a coordenar a segurança da informação (comitê de riscos).

Este representante da alta diretoria será o responsável pela Gestão do Sistema de Segurança da Informação da organização, com responsabilidade pelo desenvolvimento e implementação da segurança e responsabilidade pelo suporte e à identificação dos controles; ele deve assegurar que o Sistema de Segurança da Informação seja mantido em conformidade com a Normas da família ISO/IEC 27000; ele ficará encarregado de relatar o desempenho e manutenção do Sistema de Segurança à alta direção para sua análise crítica como base para garantia da segurança e continuidade do negócio.

2.5.8 Contexto de mecanismos de segurança

Para alcançar tal objetivo as organizações contam com mecanismos de segurança. Assim, o suporte para as recomendações de segurança pode ser encontrado nos:

- Controles físicos: são barreiras que limitam o contato ou acesso direto a informação ou a infraestrutura (garante a existência da informação) que a suporta. Entre os mecanismos de segurança que apoiam os controles físicos se pode listar os seguintes: portas / trancas / paredes / blindagem /cofres/ câmeras de vídeo/ alarmes/guardas / entre outros;
- Controles lógicos: são barreiras que impedem ou limitam o acesso a informação, que está em ambiente controlado, geralmente eletrônico, e que, de outro modo, ficaria exposta a ação de intrusos e pessoas mal intencionadas que não tem autorização para acessar seu conteúdo, podendo causar graves danos aos ativos da organização. Assim, como os controles físicos, os controles lógicos também dispõem de mecanismos de segurança que o apoiam. Entre eles se pode citar os: mecanismos de criptografia que permitem a transformação reversível da informação de forma a torná-la ininteligível a terceiros, valendo-se de algoritmos determinados e uma chave secreta para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados. Convém lembrar que a operação inversa é a decifração. Tem-se, também a assinatura digital que é um conjunto de dados

criptografados, associados a um documento do qual são função, garantindo a integridade e autenticidade do documento associado, mas não a sua confidencialidade. Existem ainda os mecanismos de garantia da integridade da informação. Usando funções de *Hashing* ou de checagem, consistindo na adição que é a geração de um número identificador de arquivo que é baseado no conteúdo binário do mesmo.

– Mecanismos de controle de acesso: como exemplo se pode citar as palavras-chave, sistemas biométricos, firewalls, cartões inteligentes.
– Mecanismos de certificação: eles atestam a validade de um documento.
– Integridade: trata-se da medida em que um serviço/informação é genuíno, isto é, está protegido contra a personificação por intrusos.
– *Honeypot*: é o nome dado a um *software*, cuja função é detectar ou de impedir a ação de um *cracker*, de um *spammer*, ou de qualquer agente externo estranho ao sistema, enganando-o, fazendo-o pensar que esteja de fato explorando uma vulnerabilidade daquele sistema.
– Protocolos seguros: o uso de protocolos que garantem um grau de segurança e usam alguns dos mecanismos acima citados.

Constata-se, portanto, que se encontram disponíveis no mercado inúmeras ferramentas e sistemas aptos a garantir a segurança da informação, ficando a critério dos gestores a escolha das que melhor atendam as expectativas do seu ambiente corporativo.

3 ESTUDO DE CASO - GESTÃO DA SEGURANÇA

O estudo de caso realizado no Laboratório de TI, subordinado ao Departamento de engenharia Elétrica da UnB foi desenvolvido, por meio de um roteiro de observação, entre março a junho de 2012, onde se buscou explicitar as técnicas e métodos utilizados, bem como a composição da amostra e as características do Laboratório alvo, no que tange ao cenário atual de Segurança da Informação observado.

3.1 CENÁRIO ATUAL

Sabe-se que a segurança da informação pode ser definida como um conjunto de medidas que se constituem basicamente de controles e políticas de segurança, que devem ser implementadas para proteger e defender a informação que está em um ambiente de perigo, risco ou incerteza. Portanto, a adoção das melhores ferramentas tem como principal objetivo a proteção das informações de clientes e empresa, para assegurar que os riscos sejam reduzidos a um nível aceitável evitando-se a revelação ou alteração por pessoas não autorizadas.

Considerando-se esta realidade, o estudo de caso desenvolvido nesta pesquisa, descreve os controles físicos e lógicos do Laboratório e também o comportamento do capital humano alocado neste setor, no que concerne ao Sistema de Gestão da Segurança da Informação existente nesta área. O método adotado foi o dedutivo que é um método lógico que pressupõe que existam verdades gerais já afirmadas e que sirvam de base para se chegar através dele a novos conhecimentos, ou seja, ele parte do geral para o particular.

Como o Sistema de Gestão da Segurança da Informação - SGSI já se encontra implantado buscou-se conhecer seu desempenho, enfatizando aspectos como: os controles físicos e lógicos e a análise/avaliação do o comportamento do capital humano responsável pela condução deste sistema. Assim, a partir de um roteiro, previamente definido (Anexo - A), observou-se a rotina do laboratório por, aproximadamente, quatro meses, com foco específico nos seguintes pontos, a saber:

a) Controles físicos

A segurança da informação pode ser definida como um conjunto de medidas que se constituem basicamente de controles e políticas de segurança, que devem ser implementadas para proteger e defender a informação que está em um ambiente de perigo, risco ou incerteza. Para alcançar tal desiderato o mercado disponibiliza inúmeros mecanismos de segurança para dar suporte às recomendações de Segurança da Informação.

No que tange aos controles físicos, convém reportar que são barreiras que limitam o contato ou acesso direto a informação ou infraestrutura de TI, ou seja, ele garante a existência da informação que a suporta. Entre os mecanismos de segurança que apoiam os controles físicos no âmbito do Laboratório de TI observou-se que ele comporta salas espaçosas com equipamentos modernos que vão desde desktops, notebooks e ferramentas para manutenção do funcionamento deste espaço; o mobiliário e a iluminação são adequados a este ambiente de estudos; as portas são mantidas fechadas e o acesso das pessoas é controlado através de um crachá e senhas de acesso; os armários são trancados para guardar os notebooks e mídias que contém backups, que não estão sendo usados, evitando danos (roubo, furto, depredação) nas instalações físicas e lógicas do local, bem como, a preservação de informações relevantes para o Departamento; existência de sistema de alarme; disponibilização de equipamentos de combate a incêndio (extintores, hidrantes, mangueiras, outros).

Paralelo a isso, observou-se que a Gerência Técnica de Tecnologia da Informação, no SG-11, solicitou a implantação de um sistema de monitoramento por câmeras, mais eficiente, para o ambiente interno e externo, do Laboratório de TI, visando preservar equipamentos e evitar a ação de intrusos que tentam ter acesso a informações relevantes para a instituição.

b) Controles lógicos

Como a informação é um ativo que possui grande valor, ela deve ser adequadamente utilizada e protegida contra ameaças e riscos. Dentro deste contexto, os controles lógicos são barreiras que impedem ou limitam o acesso à informação que está em ambiente controlado, geralmente eletrônico.

No que diz respeito aos mecanismos de segurança que apoiam os controles lógicos, no Laboratório de TI, no SG-11 observa-se que, a política de segurança do Laboratório contempla itens como: sistemas de detecção de intrusos; firewall; antivírus; sistema de backup; criptografia; autenticação e identificação (uso de senha composta por letras, números e caracteres especiais trocadas periodicamente e informações sobre o nome do usuário); concessão de direito de acesso (com regras definidas); registro das autorizações de acesso (rastrear as concessões); proibição do uso de aplicativos não testados; pirataria de software; e detecção e notificação de vulnerabilidades. Cogita-se ainda a implantação de um controle de acesso biométrico, bem como, a elaboração normas de uso de *e-mail* e da *Internet*. Nota-se, contudo, a ausência da Intranet, que poderia facilitar a comunicação e a interação entre os funcionários lotados no mencionado laboratório.

c) Comportamento do capital humano

Conforme abordado, as ameaças à segurança da informação sempre vão existir, porém as vulnerabilidades podem ser tratadas. Um fator preocupante em relação às ameaças está na falta de consciência do capital humano da área de TI.

Em se tratando do Laboratório de Tecnologia de Informação, observou-se que existe uma preocupação por parte dos funcionários lotados no departamento (quatro analistas de sistemas de informação, dois técnicos de informática e um estagiário) com a confidencialidade, integridade e disponibilidade das informações. Por isso, o departamento estabeleceu as diretrizes para a adoção de procedimentos e mecanismos relacionados à segurança da informação, de acordo com a NBR ISO/IEC 27002 – Código de Prática para a Gestão da Segurança da Informação.

Tais diretrizes devem ser cumpridas por todos os que têm direito de acesso para evitar que se explorem vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade das informações, causando possíveis impactos nos controles internos da Gerência Técnica de Tecnologia da Informação.

Sendo assim, os professores, analistas, técnico-administrativos, prestadores de serviços terceirizados, alunos e estagiários devem preservá-la garantindo o acesso somente às pessoas devidamente autorizadas, bem como, manter backups em meios de armazenamentos

seguros, disponibilizados pelos controles físicos e lógicos disponíveis no Laboratório, garantindo que essas informações sejam utilizadas de forma adequada, ou seja, somente para as atividades do Departamento de Engenharia Elétrica ou da instituição, desde que devidamente autorizadas.

Constatou-se, portanto, que no Laboratório de TI, os funcionários se preocupam em controlar o acesso, bem como, em ter *logs* de quem teve acesso. Eles ainda checam permissões e estendem sua preocupação para a segurança das mídias impressas e digitais que contenham dados relevantes para a instituição, evitando que caiam em mãos erradas.

Há ainda uma preocupação maior com as informações que estão em transito na rede visando sua confidencialidade e a integralidade, evitando que elas sejam alteradas ou extraídas por pessoas estranhas ao ambiente institucional e, também pelo público interno que não teve o acesso autorizado. A meta é proteger os dados e as informações contra perdas e danos ou qualquer outro tipo de evento que possa torná-los indisponíveis. Por isso, eles buscam agir preventivamente detectando as brechas de segurança.

Para isso são utilizados diversos mecanismos de segurança disponibilizados para a proteção das informações, como por exemplo, o *firewall,* o antivírus, o *antispyware,* o controle de acesso a *internet* que vem sendo testado no departamento, o *backup* das informações para evitar a indisponibilidade, e as tecnologias de criptografia.

Como os desafios surgem paralelos às inovações trazidas por estas novas tecnologias, a busca pelo conhecimento é incessante. Contudo, é primordial a avaliação dos colaboradores que tem o direito de acesso para checar se o desempenho de suas atividades tem suporte nas melhores práticas preconizadas pelas normas da família ISO/IEC 27000 que são utilizadas na confecção de materiais para consulta diária e na criação de políticas e diretrizes de segurança da informação, posto que elas forneçam suporte para o gerenciamento dos riscos de segurança da informação, descrevendo, o passo a passo, do processo de gestão de riscos.

Percebeu-se ainda, no período de observação, que os funcionários são constantemente conscientizados da importância do repositório de informações institucionais e da importância do não vazamento de informações, tanto no ambiente interno quanto no

ambiente externo e por isso, eles são capacitados e treinados para evitarem este tipo de incidente.

Em outras palavras, a instituição investe em educação continuada do capital humano, que tem acesso a cursos de graduação, pós-graduação, mestrado e doutorado, palestras, *workshops*, publicações especializadas e outros. Além disso, há uma divulgação eficiente das normas de segurança da informação da família ISO/IEC 27000 que contém diretivas para manter e preservar um SGSI eficiente e eficaz e normativos relacionados à segurança da informação aplicáveis à Administração Pública Federal.

Constatou-se que as mencionadas normas são estudadas e debatidas pelos funcionários que sintetizaram alguns pontos importantes transformando-os em um documento (repositório) para consultas emergenciais (Plano de Contingência) na eventualidade de surgirem ameaças que possam tornar indisponíveis as informações institucionais. Além disso, todos os funcionários, e outras partes envolvidas (professores, alunos e estagiários) são convocados a participarem desta cruzada em prol da preservação e proteção das informações disponíveis no repositório do Laboratório. Espera-se com isso, que o nível de conscientização, dos usuários do sistema, se eleve.

Observou-se, no entanto, que independentemente destes cuidados, os funcionários lotados no Laboratório compartilham do mesmo ponto de vista: é possível melhorar os níveis de segurança do Laboratório de TI elegendo um Comitê de Segurança, que apoie o gestor da Gerência Técnica de Tecnologia da Informação na condução dos processos que priorizem a detecção de riscos e o direcionamento dos investimentos nos controles físicos e lógicos que buscam salvaguardar os ativos da área de TI.

Enquanto essas medidas não são implementadas observou-se que existe uma base de conhecimento localizada em um repositório que pode auxiliar o analista no caso de incidentes que envolvem a segurança da informação. Neste repositório, também conhecido internamente como Plano de Contingência, o operador encontra tutoriais, manuais e procedimentos documentados que auxiliam na preservação das informações, pois reduzem as vulnerabilidades.

4 CONCLUSÃO E CONSIDERAÇÕES FINAIS

As ameaças à segurança da informação sempre vão existir, porém as vulnerabilidades podem ser tratadas. Embasado no estudo de caso desenvolvido no âmbito do Laboratório de TI localizado no SG- 11 foi possível avaliar o Sistema de Gestão de Segurança da Informação – SGSI, observando os seus controles físicos e lógicos e a adoção as normas, diretrizes e legislações a que está sujeita, a área de TI, bem como, a conduta do capital humano em relação a cultura de segurança da informação.

Estudos de caso, como o realizado neste trabalho possibilitam a detecção de lacunas no Sistema de Informação das organizações. No caso do Laboratório de TI, do Departamento de Engenharia Elétrica constatou-se que as atividades desenvolvidas estão alinhadas às normas da família ISO 27000. As diretrizes preconizadas por estas normas foram compiladas num repositório (Plano de Contingência) que fica a disposição do capital humano alocado para a área, conforme definido na Política de Segurança da Informação adotada pelo pessoal do Laboratório. O gerenciamento de riscos é proativo com monitoramento contínuo e atualizações periódicas para reduzir e prevenir a ocorrência de eventos prejudiciais aos ativos corporativos.

No que tange às legislações direcionadas à Administração Pública Federal, os normativos também são considerados na Gestão do Sistema de Informação do mencionado laboratório, onde as vulnerabilidades são tratadas de acordo com as disposições contidas nestes normativos, visando garantir a confidencialidade, integridade e disponibilidade das informações. Portanto, o desenvolvimento das atividades, no mencionado Laboratório, também se encontra alinhada com as disposições contidas nas leis e normativos aplicáveis à Administração Pública Federal, todos relacionados à Segurança da Informação, como forma de minimizar problemas e aprimorar os processos de resposta a eventuais incidentes. Mas para agilizar ainda mais o acesso a estes repositórios sugere-se a implantação de uma intranet no âmbito do Laboratório. Sem dúvida ela facilitaria a comunicação entre os funcionários e o gestor do Sistema de Segurança da Informação da área, pois as ocorrências seriam notificadas, também pela *intranet* e o acesso a elas seria mais rápido.

No que se refere aos aspectos físicos, o Laboratório também conta com barreiras que limitam o contato e o acesso direto a informação ou infraestrutura de TI. Considera-se, portanto, que também neste aspecto o Laboratório encontra-se alinhado ao que preconiza a literatura consultada no decorrer do estudo. Contudo, alguns itens relativos à segurança física do laboratório podem melhorar, como por exemplo, o monitoramento por câmeras mais modernas e eficientes que abranjam o ambiente externo e interno desta área para evitar a ação de intrusos. Constata-se, então que em relação aos aspectos físicos, o Laboratório de TI deve investir um pouco mais para ter um alinhamento condizente com o nível das informações ali armazenadas, haja vista que o setor é responsável pelo suporte técnico as demais áreas de TI do Departamento de Engenharia Elétrica.

Em se tratando dos controles lógicos, devido a velocidade com que surgem inovações na área de TI, seja, ela de equipamentos ou até mesmo novas ameaças, não se pode afirmar que os mecanismos de segurança que apoiam os controles lógicos são suficientes, ou melhor estão alinhados com a necessária proteção que o setor requer.

Sendo assim, no período em que foi desenvolvido o estudo de caso, entre março a junho de 2012, a segurança do Laboratório contemplava itens, como por exemplo, sistemas de detecção de intrusos; *firewall*; antivírus; sistema de *backup*; *criptografia*; proibição do uso de aplicativos não testados e pirataria de *software*, entre outros. Contudo, neste mesmo período detectou-se a ausência de controle de acesso biométrico e a falta de normas para o uso do *e-mail* e da *Internet.* Portanto, não se pode afirmar categoricamente que, em relação aos aspectos lógicos o Laboratório de TI esteja completamente alinhado a Gestão de Segurança da Informação.

Considerando-se o cenário atual pode-se dizer que o Laboratório está parcialmente alinhado, no que diz respeito à limitação do acesso a informação que está em ambiente controlado eletronicamente. Neste contexto, propõe-se a implantação do controle biométrico de acesso, bem como a elaboração de normas para o uso do *e-mail* e do acesso *a internet.*

No que se refere à conduta do capital humano, o estudo aponta que os funcionários que atuam no Laboratório de TI estão conscientes do seu papel, ou seja, eles desenvolveram uma cultura de Segurança da Informação, apostando nas diretrizes preconizadas pelas normas

da família ISO 27000, e também nos normativos que versam sobre Segurança da Informação, no âmbito da Administração Pública Federal.

Como o Laboratório de TI conta, ainda, com controles físicos e lógicos, adequados percebe-se que há uma preocupação maior com investimentos em educação continuada. Busca-se a capacitação profissional para lidar com as inovações que a área de TI apresenta quase que diariamente, bem como com as ameaças que surgem com uma velocidade espantosa. Constata-se então que o capital humano lotado no Laboratório se encontra alinhado com os procedimentos e mecanismos relacionados à área de Segurança da Informação e que a implantação da *intranet* facilitaria ainda mais a interação entre eles.

A necessidade de implantação de Sistema de Segurança da Informação é um fato reconhecido pela maioria das organizações contemporâneas, pois uma parada repentina nos sistemas informatizados de uma empresa pode comprometer seus ativos ou seus recursos ocasionando prejuízos financeiros, afetando sua credibilidade perante seus usuários, seus clientes e o mercado. Principalmente se essa parada for ocasionada por algum tipo de ataque bem sucedido que teve por objetivo a captura de informações relevantes.

Estas ameaças, ou melhor, agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades podem ser tratadas pelas organizações com a adoção de um nível adequado de segurança de informações.

Sabe-se que é na conduta do capital humano que a proteção da informação é crítica. Por isso, a tecnologia da informação tornou-se estratégica para as organizações em geral. O tema segurança tem sido priorizado no ambiente corporativo devido às ameaças que podem comprometer os ativos das organizações. É importante proteger dados e recursos contra perdas e danos ou qualquer outro tipo de evento. Por isso, as organizações investem em Sistemas de Segurança, pois buscam garantir à integridade da informação, reduzindo ao máximo os riscos de vazamentos de informações, a integridade dos bancos de dados, as fraudes em arquivos, o roubo de informações, a proteção contra erros humanos e operacionais por falta de treinamento do capital humano, o uso indevido do sistema por pessoas não autorizadas que podem sabotar o sistema, ocasionando paralisações de rede ou serviços, ou

até mesmo ameaças que visam prejudicar as organizações e, também os equipamentos utilizados.

Dentro deste contexto, para atingir o objetivo geral levantado, através do estudo de caso, observou-se o nível de conscientização do capital humano lotado no Laboratório de TI, percebendo que há uma preocupação com a confidencialidade, integridade e disponibilidade das informações emanadas desta área e por isso seguem as recomendações da família ISO/IEC 27000, bem como os normativos dirigidos a Administração Pública que fornecem suporte extra na condução de um SGSI, pois constantemente apresentam novas diretivas para uma segurança mais eficiente, eficaz e efetiva amenizando a exploração de vulnerabilidades do sistema.

A equipe está consciente que não pode garantir segurança plena, apenas com a normatização de processos e procedimentos, por isso, eles se valem dos controles físicos que limitam o contato ou acesso direto a informação ou a infraestrutura que a suporta, mantendo portas fechadas, guardando as mídias em armários trancados e seguros, monitorando a movimentação dentro e fora do laboratório e agindo proativamente.

Além da capacitação do capital humano, das diretivas das normas e dos controles físicos, a equipe não se furta de utilizar os controles lógicos disponibilizados pela instituição, posto que os desafios surgem na mesma proporção em que novas tecnologias são inventadas, sendo assim mecanismos de segurança, como por exemplo, a criptografia, a assinatura digital, funções de *hashing* ou de checagem, firewalls e o uso de protocolos seguros são algumas das barreiras utilizadas por estes profissionais. Mas, a busca por novos conhecimentos continua incessante, haja vista que as políticas de segurança rapidamente se tornam obsoletas diante de invasores cada dia mais ousados. Por isso, novas ideias sempre são bem-vindas, pois a informação é um capital fundamental para as organizações contemporâneas.

A cruzada favorável à preservação da confidencialidade, integridade, disponibilidade, autenticidade e confiabilidade da informação permanece em estado de alerta para evitar as fraudes em arquivos, o roubo de informações, por falta de treinamento ou até mesmo pelo uso indevido do sistema por pessoas não autorizadas que podem sabotá-lo ocasionando paralisações de rede ou serviços, ou até mesmo ameaças que visam prejudicar a instituição e, também os equipamentos utilizados na infraestrutura de TI. Neste sentido, os

riscos e as vulnerabilidades de dados e informações são constantemente checados e classificados conforme sua ordem de prioridade e relevância para que se determine as opções de tratamento, indicadas pela família ISO/IEC 27000 e pelos normativos dirigidos a Administração Pública, que melhor se adéquam a situação vivenciada naquele momento.

Vale ressaltar que a política de segurança adotada é constantemente reavaliada e os riscos e seus fatores são monitorados criticamente visando o aprimoramento dos processos de resposta a incidentes internos e externos como forma de garantir a manutenção do nível de segurança acordado com a instituição. Paralelo a isso se exige o comprometimento dos colaboradores que devem agir de forma proativa, observando as diretrizes, normas e orientações de procedimentos que devem ser aplicados a todos os sistemas de informação e processos corporativos, como forma de reduzir, preventivamente, a ocorrência de eventos prejudiciais, protegendo ativos importantes da organização e reduzindo significativamente o número de incidentes de segurança futuros.

Diante do exposto constata-se que a segurança da informação passou a fazer parte da agenda governamental, posto que as organizações governamentais tem dado grande atenção para este segmento, com o intuito de proteger seus ativos. Vale enfatizar que o acesso a normas de segurança, aliado a uma política de segurança da informação eficaz, que adota as melhores ferramentas e mecanismos de segurança eficientes são capazes de assegurar a redução dos riscos a um nível aceitável.

Conclui-se, portanto, que são efetivas as ações de segurança da informação desenvolvidas, no âmbito do Laboratório, posto que os colaboradores alocados nesta área exerçam controle de acesso aos sistemas críticos da instituição; analisam a segurança física e lógica dos servidores de rede; analisam a segurança contra contaminação por vírus; avaliam periodicamente a configuração do firewall; buscam reavaliar a política de segurança para adequá-la as novas ameaças; valem-se dos mecanismos de criptografia de dados nos e-mails e informações confidenciais da instituição; adotam a política de backup para preservar as informações; cobra do capital humano a exigência de prevenção contra softwares piratas; controlam o acesso dos funcionários à Internet e como plano de contingência o departamento, além dos controles físicos e lógicos, optou por investir na educação continuada dos funcionários, conscientizando-os para tratar e evitar a exploração de vulnerabilidades que

podem causar perdas de confidencialidade, integridade e disponibilidade das informações que podem impactar os controles internos e externos da instituição.

Como os desafios nesta área são constantemente reinventados sugere-se que o pessoal lotado no Laboratório, melhore os níveis de segurança elegendo um Comitê de Segurança da Informação e que procedam auditórias pontuais no sistema, aprovando iniciativas para aumentar a segurança, como por exemplo, a implantação de controle de acesso biométrico, elaboração de normas de uso de e-mail e de uso da Internet, implantação de um sistema de monitoramento por câmeras e conhecimento de novos mecanismos que buscam salvaguardar informações institucionais. Para agilizar todas estas tarefas sugere-se a implantação da *Intranet* para facilitar a comunicação e a interação entre os funcionários do laboratório, agilizando assim os procedimentos de combate à exploração de vulnerabilidades que podem comprometer a confidencialidade, integridade e disponibilidade das informações.

Diante da importância da informação para o ambiente corporativo e da complexidade do assunto sugere-se a elaboração de novos trabalhos que contemplem as inovações sugeridas neste trabalho, como por exemplo, instalação de câmeras de monitoramento, interno e externo, mais modernas; controle biométrico de acesso; a elaboração normas de uso de *e-mail* e da *Internet*; eleição de um Comitê de Segurança e, principalmente, a implantação da *Intranet* que facilitará a comunicação e a interação entre o capital humano lotado no Laboratório para checar a efetividade dessas iniciativas na proteção dos ativos corporativos.

5 BIBLIOGRAFIA

ARAÚJO, A. P. F. Módulo: **Infraestrutura de Tecnologia da Informação** - Curso de especialização em Gestão da Segurança da Informação e Comunicações da UnB, 2010.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **Tecnologia da Informação** – Gestão de Riscos de Segurança da Informação, NBR ISO/IEC 27005. Rio de Janeiro: ABNT, 2008.

_____. **Tecnologia da Informação** – técnicas de segurança - sistemas de gerência da segurança da informação - requisitos, NBR ISO/IEC 27001. Rio de Janeiro: ABNT, 2005

_____. **Tecnologia da Informação** – Técnicas de segurança - Código de prática para a gestão da segurança da informação, NBR ISO/IEC 27002. Rio de Janeiro: ABNT, 2005.

BRASIL, Gabinete de Segurança Institucional da Presidência da República - Comitê Gestor da Segurança da Informação. **Instrução Normativa GSI/PR, nº 1**, de 13 de junho de 2008. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. Disponível em: <http://www.presidencia.gov.br/gsi/cgsi/legislacao.htm> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 02/IN01/DSIC/GSIPR**, de 14 de outubro de 2008. Metodologia de Gestão de Segurança da Informação e Comunicações. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 03/IN01/DSIC/GSIPR**, de 30 de julho de 2009. Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 04/IN01/DSIC/GSIPR**, e seu anexo, de 17 ad agosto de 2009. Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 05/IN01/DSIC/GSIPR**, e seu anexo, de 17 ad agosto de 2009. Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos

órgãos e entidades da Administração Pública Federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 06/IN01/DSIC/GSIPR**, de 23 de novembro de 2009. Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 07/IN01/DSIC/GSIPR**, de 07 de maio de 2010. Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 08/IN01/DSIC/GSIPR**, de 24 de agosto de 2010. Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República – Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 09/IN01/DSIC/GSIPR**, de 22 de novembro de 2010. Estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_9_criptografia.pdf> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República - Departamento de Segurança da Informação e comunicação. **Norma Complementar nº10/IN01/DSIC/GSIPR**, de 10 de fevereiro de 2012. Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República - Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 11/IN01/DSIC/GSIPR**, de 10 de fevereiro de 2012. Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos

órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República - Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 12/IN01/DSIC/GSIPR,** de 10 de fevereiro de 2012. Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República - Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 13/IN01/DSIC/GSIPR**, de 10 de fevereiro de 2012. Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República - Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 14/IN01/DSIC/GSIPR,** de 10 de fevereiro de 2012. Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Gabinete de Segurança Institucional da Presidência da República - Departamento de Segurança da Informação e comunicação. **Norma Complementar nº 15/IN01/DSIC/GSIPR,** de 21 de junho de 2012. Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Disponível em: <http://dsic.planalto.gov.br/legislacaodsic/53> Acesso em: 20 de julho de 2012.

_____, Ministério do Planejamento Orçamento e Gestão – Secretária de Logística e Tecnologia da Informação. **Instrução Normativa nº 04/SLTI/MPOG, de 19 de maio de 2008.** Dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Informação e Informática - SISP do Poder Executivo Federal. Disponível em: http://www.governoeletronico.gov.br/sisp-conteudo/nucleo-de-contratacoes-de-ti/modelo-de-contratacoes-normativos-e-documentos-de-referencia/instrucao-normativa-mp-slti-no04 Acesso em: 21 de agosto de 2012.

_____, Presidência da República – Casa Civil - Subchefia de Assuntos Jurídicos. **Decreto nº 4553,** de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. Disponível

em: <http://www.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm> Acesso em: 20 julho 2012.

_____, Presidência da República – Casa Civil – Subchefia de Assuntos Jurídicos. **Decreto nº 3505,** de 13 de junho de 2000. Institui a Política de Segurança da Informação e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm> Acesso em: 20 julho 2012.

_____, Presidência da República – Casa Civil – Subchefia de Assuntos Jurídicos. **Decreto nº 3.996** de 31 de outubro de 2001. Dispõe sobre a prestação de serviços de certificação digital no âmbito da Administração Pública Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/Quadros/2000.htm> Acesso em: 20 julho 2012.

_____, Tribunal de Contas da União. **Boas Práticas em Segurança da Informação.** 2. ed., Brasília: TCU, 2007.

BUKOWITZ, W. R.; WILLIAMS, R. L. **Manual de gestão do conhecimento:** ferramentas e técnicas que criam valor para a empresa. Porto Alegre: *Bookman*, 2002.

CASTELLS, M. **A Sociedade em Rede.** São Paulo: Paz e Terra, 2007.

CAVALCANTI, M.; GOMES, E.; PEREIRA, A. Os capitais do conhecimento. *In*. **Gestão de empresas na sociedade do conhecimento.** Rio de Janeiro: Campus, 2001.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br . **I Ciberjur**, 2011. São Paulo: OAB. Disponível em: <https://www.google.com.br/search?q=I+Ciberjur&ie=utf-8&oe=utf-8&aq=t&rls=org.mozilla:pt-BR:official&client=firefox-a> Acesso em:17 mai 2012.

CHOO, C. W. **A organização do conhecimento:** Como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: Senac, 2003.

COMITÊ GESTOR DA INTERNET (CGI.Br), **Pesquisa sobre o uso das tecnologias da informação e da comunicação no Brasil 2006.** São Paulo, 2007.

CORREIA, M. **Será que você realmente conhece a família ISO 27000?** Disponível em: <http://marcoacorreia.wordpress.com/2011/03/27/sera-que-voce-realmente-conhece-a-familia-iso-27000/>Acesso em: 12 ago 2012.

CRAWFORD, R. **Na era do capital humano:** o talento, a inteligência e o conhecimento como forças econômicas, seu impacto nas empresas e nas decisões de investimento. São Paulo: Atlas, 1994.

CURY, A. **Organização e Métodos:** uma visão holística. São Paulo: Atlas, 2000.

DAVENPORT, T. H. **Ecologia da informação:** por que só a tecnologia não basta para o sucesso na era da informação. 5. ed. São Paulo: Futura, 2002.

DAVENPORT, T. H.; PRUSAK, L. **O que queremos dizer com conhecimento**?. Rio de Janeiro: Campus, 1998.

DIAS, C., **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

DIAS, E. W. In: CAMPELLO. B. S.; CENDÓN, B. V.; KREMER. J. M. (Org.). **Fontes de informação para pesquisadores e profissionais.** Belo Horizonte: UFMG, 2000.

DIAS, R. Métricas para avaliação de sistemas de informação. **Revista Eletrônica de Sistemas de Informação,** v. 1, n. 1, nov. 2002. Disponível em: <http://www.presidentekennedy.br/resi/edicao1.html> Acesso em: 20 maio 2012.

DRUCKER, P. F. A organização do futuro: como preparar hoje as empresas de amanhã. São Paulo: Futura, 2000.

FERNANDES, Jorge H. C. **Sistemas Complexos**. Universidade de Brasília, Curso de Especialização em Gestão de Segurança da Informação e Comunicações, CEGSIC, Universidade de Brasília, 2008, Apostila.

FERREIRA, A. B. de H. **Novo Dicionário Aurélio Eletrônico Século XXI.** versão 3.0 (1999). WINDOWS, CD-ROM.

FLEURY, M.T.L.; OLIVEIRA JR.M.M (Org.). **Gestão estratégica do conhecimento:** integrando aprendizagem, conhecimento e competências. São Paulo: Atlas, 2001

GARVIN, David A. Construindo a organização que aprende. In **HARVARD BUSINESS REVIEW.** Gestão do conhecimento. 4. ed. Rio de Janeiro: Campus, 2000.

GHOSHAL, S. *A organização individualizada:* as melhores empresas são definidas por propósitos, processos e pessoas. Rio de Janeiro: Campus, 2000.

HOUAISS, A. **Dicionário Houaiss da língua portuguesa.** Rio de Janeiro: Objetiva, 2000

MARCONI, M. de A.; LAKATOS, E. M. **Fundamentos de Metodologia Científica.** São Paulo: Atlas, 2001.

MICROSOFT TECHNET. **Otimização da infraestrutura TechNet:** Jornada de otimização da infraestrutura Microsoft. Disponível em: <http://technet.microsoft.com/pt-br/dd362271.aspx> Acesso em 14. nov 2012.

NÓBREGA, Clemente. **A ciência da gestão.** Rio de Janeiro: Senac Rio, 2004.

PELTIER, T. ***Information Security Policies,*** *Procedures, and Standards – Guideline for effective Information Security Management,* Florida, *Auerbach*, 2001.

ROBBINS, S.P. **Comportamento Organizacional.** 8 ed. Rio de Janeiro: ABDR, 1999

SÊMOLA, M., **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.

SETZER, V. W. Dado, informação, conhecimento e competência. **DataGamaZero.** Rio de Janeiro, 1999.

SOARES, E. C. **Integração da segurança na gestão de TI**: uma proposta de abordagem sistêmica. Dissertação de mestrado UnB, 2011

STAIR, R. H. **Princípios de sistemas de informação:** uma abordagem gerencial. 4. ed. Rio de Janeiro: LTC, 2002.

STEWART, T. A. **Capital intelectual:** a nova vantagem competitiva das empresas. Rio de Janeiro: Campus, 1998.

TAKEUCHI, H; NONAKA, I. **Teoria da criação do conhecimento organizacional.** Rio de Janeiro: Campus, 1997.

TANENBAUM, A. S. Rede de Computadores. Rio de Janeiro: Campus, 2003.

TERRA, J. C. C. **Gestão do conhecimento:** o grande desafio empresarial. 2. ed. rev. e amp. Rio de Janeiro: Elsevier, 2005.

VERGARA, S. C. **Projetos e relatórios de pesquisa em administração**. 4 ed. São Paulo: Atlas, 2003.

6 ANEXO A

ROTEIRO DA OBSERVAÇÃO

Com o objetivo de realizar uma pesquisa, por meio de um estudo de caso, para analisar/avaliar o nível de conscientização do capital humano lotado no Laboratório de TI, da Gerência Técnica de Tecnologia da Informação, localizada no SG-11, subordinada ao Departamento de Engenharia Elétrica na UnB, na condução do Sistema de Gestão da Segurança da Informação - SGSI deste laboratório, adotou-se como instrumento da pesquisa a observação participante, a partir de um roteiro prévio que contempla os controles físicos e lógicos como suporte para a segurança da informação, bem como a conduta dos servidores lotados no mencionado laboratório, inclusive este pesquisador.

A observação contemplou a rotina do Laboratório de TI, no SG-11 e num primeiro momento direcionou-se para os controles físicos, onde foram checados instalações prediais do laboratório, mobiliário, instalação elétrica, alarmes, armários para armazenar backups e demais componentes da estrutura física do laboratório de TI, no SG-11.

Posteriormente, observou-se a disponibilidade de controles lógicos, tais como: firewall; antivírus; sistema de backup; criptografia; autenticação e identificação entre outros itens.

E finalmente, observou-se o comportamento do capital humano em relação ao SGSI implantado neste Laboratório, analisando/avaliando o nível de conscientização em vários aspectos, tais como: conhecimento das normas da família ISO/IEC 27000, conhecimento de normativos relativos à segurança da informação na Administração Pública, Conhecimento da Política de segurança adotada pelo Laboratório de TI, Conhecimento sobre o repositório interno (base de conhecimento) para uso em caso de incidentes de segurança da informação (Plano de Contingência) para reduzir vulnerabilidades; e Conhecimentos sobre a implantação de Comitês de Segurança e de Risco.

7. GLOSSÁRIO

Bridges: dispositivo que liga duas ou mais redes informáticas que usam protocolos distintos ou iguais ou dois segmentos da mesma rede que usam o mesmo protocolo, por exemplo, ethernet ou token ring.

Expertise: Conhecimento que se adquire pelo estudo, experiência e prática; e a capacidade de aplicar o que foi aprendido de forma adequada às solicitações requeridas pela função exercida. É a busca incessante por novas aprendizagens, o autodesenvolvimento e a socialização do conhecimento no meio em que se vive.

Gateway: Responsável por interligar redes que usam protocolos diferentes

Guidelines: Uma instrução ou qualquer outra indicação do procedimento pelo qual determinar um curso de ação.

Hubs: Responsáveis pela comunicação entre diferentes redes de computadores permitindo que computadores distantes se comuniquem.

Internet: Rede Mundial de Computadores

Intranet: é uma rede de computadores privada que assenta sobre a suite de protocolos da Internet, porém, de uso exclusivo de um determinado local, como, por exemplo, a rede de uma empresa, que só pode ser acessada por seus usuários internos.

Microchip: Pastilha feita de material semicondutor, normalmente o silício, sobre a qual são implantados circuitos integrados. Desenvolvido pela norte-americana Intel, 1971, possibilitou a miniaturização e barateamento dos equipamentos eletrônicos.

Plan-Do-Check-Act: Planejar, Fazer, Verificar, Agir

Rack: é um "armário", ou seja, um grande gabinete que foi projetado e padronizado para a montagem modular de equipamentos de informática.

Sevidores Blade: Servidor com computação concentrada e com recursos de níveis empresariais. O servidor fornece uma densidade de memória excepcional e grande flexibilidade de rede para data centers de pequeno e grande porte.

Software: é o programa de computador e toda a documentação e mídia que o acompanha

Storage: servidor de discos para armazenamento de dados em uma rede

Switches: Dispositivos responsáveis por reencaminhar módulos (frames) entre os diversos nós de uma rede.