UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS APLICADAS A EDUCAÇÃO

DEPARTAMENTO DE CIÊNCIAS EXATAS

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA CONTRIBUIÇÃO PARA O CAMPUS IV

Autor: Marcus Vinicius Freire Pontes

Orientador: Prof. Dr. Hermann Hrdlicka

RIO TINTO - PB

2014

MARCUS VINICIUS FREIRE PONTES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA CONTRIBUIÇÃO PARA O CAMPUS IV

Monografia apresentada para obtenção do título de Bacharel à banca examinadora no Curso de Bacharelado em Sistemas de Informação do Centro de Ciências Aplicadas e Educação (CCAE), Campus IV da Universidade Federal da Paraíba.

Orientador: Prof. Dr. Hermann Hrdlicka.

RIO TINTO - PB
2014

P813p Pontes, Marcus Vinicius Freire.

Política de segurança da informação: uma contribuição para o Campus IV. / Marcus Vinicius Freire Pontes. – Rio Tinto: [s.n.], 2014.

89 f.: il. –

Orientador: Prof. Dr. Hermann Hrdlicka.
Monografia (Graduação) – UFPB/CCAE.

1. Segurança da informação. 2. Política de segurança. 3. Informação.

UFPB/BS-CCAE CDU: 004.56(043.2)

MARCUS VINICIUS FREIRE PONTES

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO: UMA CONTRIBUIÇÃO PARA O CAMPUS IV

Trabalho de Conclusão de Curso submetido ao Curso de Bacharelado em Sistemas de Informação da Universidade Federal da Paraíba, Campus IV, como parte dos requisitos necessários para obtenção do grau de BACHAREL EM SISTEMAS DE INFORMAÇÃO.

Assinatura do autor:_____

APROVADO POR:

_____

Orientador: Prof. Dr. Hermann Hrdlicka
Universidade Federal da Paraíba – Campus IV

_____

Prof. Dra. Adriana Clericuzi
Universidade Federal da Paraíba – Campus IV

_____

Prof. Dra. Juliana de Albuquerque Gonçalves Saraiva
Universidade Federal da Paraíba – Campus IV

RIO TINTO – PB
2014

Dedico este trabalho à memória de Nilton Correia Sales, meu tio, pessoa que admirei e amei, que sempre acreditou em mim, o único exemplo de pai que tive em minha vida.

AGRADECIMENTOS

Quero agradecer primeiramente a minha família, em especial, minha mãe Edileuza Pontes e minha segunda mãe Lucia Pontes Sales que sempre acreditaram em mim.

Agradeço a minha namorada Gabriela Toscano, por estar sempre ao meu lado, por todo o carinho e compreensão, principalmente nos momentos de dificuldade ao longo dos anos.

Ao orientador deste trabalho, Hermann Hrdlicka, por ter acreditado em mim, pela paciência e atenção dedicada, pelo seu exemplo de dinamismo e trabalho, que é a maior lição que um professor pode dar a seu aluno.

A todos os colegas e amigos que fiz ao longo de minha graduação, alguns desses, amigos para todos os momentos, amigos que com certeza levarei para o resto da vida.

Quero agradecer a todos os professores que eu tive nesses anos de graduação.

Agradeço aos amigos e amigas que sempre estiveram comigo, me apoiando, me ajudando quando necessário, e sempre torcendo por mim.

Agradeço também a todos que participaram, de uma forma ou de outra, desses anos de graduação.

RESUMO

Esta monografia discute a importância da política de segurança da informação como um meio para garantir a segurança das informações organizacionais. O objetivo desse trabalho é contribuir em uma Política de Segurança da Informação (PSI) para uma instituição de ensino situada em Rio Tinto e Mamanguape, Estado da Paraíba, especificamente na Universidade Federal da Paraíba – Campus IV. Atualmente existem algumas metodologias e práticas sugeridas pelo conhecimento de Gerência da Segurança da Informação, como as sugeridas pela Organização para a Cooperação e Desenvolvimento Económico (OCDE); uma revisão de literatura acerca do tema e das práticas estabelecidas foi realizada a fim de entender fatores cruciais para o sucesso e as maiores dificuldades que as organizações encontram para criar barreiras e proteger-se de ataques e ameaças, virtuais ou não. Como uma pesquisa exploratória, foi usada a metodologia de estudo de caso, mas com flexibilidade suficiente para entender a complexidade do tema envolvendo o objeto de estudo. Além disso, foi feita uma comparação entre os padrões ISO/IEC 27002:2005, como parâmetro, com duas PSIs de instituições distintas disponíveis online, para entender o que é importante ou não, e como escrever uma PSI. Uma contribuição para departamento de segurança da UFPB foi desenvolvida como parte do trabalho de pesquisa final.

Palavras chave: Informação; Segurança da Informação; Política de Segurança; Política de segurança da Informação.

ABSTRACT

This monograph discusses the importance of information security policy as a means to ensure organization's information security. The objective of this paper is to contribute to an Information Security Policy (IFP) towards an educational institution situated in Rio Tinto and Mamanguape, state of Paraiba, specifically Paraiba Federal University - Campus IV. Currently there are some methodologies and best practices suggested by Information Security and Knowledge Management being adopted, such as the ones created by the Economic Development and Cooperation Organization (OCDE); a review on the literature regarding the theme, as well as the inherent practices established by it was conducted to understand critical factors for success and the main difficulties that organizations face to create barriers and protect themselves from attacks and threats, whether virtual or not. As an exploratory research, a case study methodology was used, but with enough flexibility to understand the complexity involved with the object of study. Furthermore, a comparison was made between ISO / IEC 27002:2005 standards (as parameters) and two educational institutions' IFP available on the internet to understand what is important and what is not, and how to write an IFP. A contribution to the UFPB's security department was developed as a part of this final research work.

Keywords: Information; Information Security; Security Policy; Security Police Information.

LISTA DE FIGURAS

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
BS	*British Standard* – Padrões Britânicos
BSi	*British Standard Institute* – Instituição Britânica de Padrões
CCAE	Centro de Ciências Aplicadas e Educação
CID	Confidencialidade, Integridade e Disponibilidade
CMMI	*Capability Maturity Model - Integration* – Modelo de Maturidade em Capacitação - Integração
COBIT	*Control Objectives for Information and relface faated Technology* – Objetivo de Controle para Tecnologia da Informação e Áreas Relacionadas
DCE	Departamento de Ciências Exatas
DCS	Departamento de Ciências Sociais
DCSA	Departamento de Ciências Sociais Aplicadas
DDESIGN	Departamento de Design
DED	Departamento de Educação
DEMA	Departamento de Engenharia e Meio Ambiente
DHG	Departamento de Hotelaria e Gastronomia
DL	Departamento de Letras
DOS	*Denial of Service* – Ataque de Negação de Serviço
IBGE	Instituto Brasileiro de Geografia e Estatística
IEC	*International Electrotechnical Commission* – Comissão Eletrotécnica Internacional
IPHAN	Instituto do Patrimônio Histórico e Artístico Nacional

ISO *International Organization for Standardization* – Organização Internacional para Padronização

ITIL *Information Technology Infrastructure Library* – Biblioteca de Infraestrutura de TI

LCC Licenciatura em Ciências da Computação

MOODLE *Modular Object-Oriented Dynamic Learning Environment* – Ambiente Modular de Aprendizagem Dinâmica Orientada a Objetos

NBR Norma Brasileira

NIST *National Institute of Standards and Technology* – Instituto Nacional de Padrões e Tecnologia

OCDE Organização para a Cooperação e Desenvolvimento Económico

PDCA *Plan-Do-Check-Act* – Planejar-Executar-Verificar-Agir

PSI Política de Segurança da Informação

SABSA *Sherwood Applied Business Security Architecture* – Arquitetura de Segurança Aplicada a Negócios Sherwood

SENAC Serviço Nacional de Aprendizagem Comercial

SERPRO Serviço Federal de Processamento de Dados

SGSI Sistema de Gestão de Segurança da Informação

SI Sistemas de Informação

SoA *Statement of Applicability* – Declaração de Aplicabilidade

SOCIESC Sociedade Educacional de Santa Catarina

SPAM *Sending and Posting Advertisement in Mass* – Enviar e Postar Publicidade em Massa

TIC Tecnologia da Informação e Comunicação

UFPB Universidade Federal da Paraíba

SUMÁRIO

1 INTRODUÇÃO

Muito embora a importância da informação tenha sido o pilar principal na ascensão e queda de impérios e civilizações, num mundo globalizado a informação precisa estar disponível para decisões presentes e do futuro, tornando-se um ativo imprescindível e de uso corrente no dia a dia das organizações. O valor que a ela se dá representa a diferença entre se estar ser bem sucedido ou não. Por esse motivo, cada vez mais administrar a informação é vital em seus diferentes níveis estratégico, táticos ou operacionais. Portanto, a informação envolve riquezas (tangíveis ou não), e, por isso, os sistemas que a produzem e a mantém precisam estar seguros para se evitar que ela não caia em mãos erradas – a segurança da informação é uma das responsabilidades do profissional de sistemas de informação.

> Quando se pensa em segurança da informação, a primeira ideia que nos vem à mente é a proteção das informações, não importando onde estas informações estejam armazenadas. Um computador ou sistema computacional é considerado seguro se houver uma garantia de que é capaz de atuar exatamente como o esperado. Porém a segurança não é apenas isto. A expectativa de todo usuário é que as informações armazenadas hoje em seu computador, lá permaneçam, mesmo depois de algumas semanas, sem que pessoas não autorizadas tenham tido qualquer acesso a seu conteúdo. (DIAS, 2000, p.42)

De acordo com Dias (2000), a segurança da informação tem como prioridade proteger as informações contra diversos tipos de ameaças e garantir os princípios básicos de segurança, que seriam: confidencialidade, integridade e disponibilidade da informação. Para obter a segurança da informação deve-se criar e implantar práticas, procedimentos e políticas que devem ser seguidas a fim de minimizar os riscos e melhorar o controle e a segurança das informações, a fim de evitar que, de algum modo, informações acabem sendo extraviadas (ou roubadas) e possam acabar causando algum prejuízo à organização proprietária (DIAS, 2000).

De fato, uma pesquisa realizada pelo IBGE sobre o uso das tecnologias de informação e comunicação nas empresas brasileiras apurou que 40,5% das empresas, com 10 ou mais pessoas ocupadas que utilizaram a Internet, relataram ter problemas com ataques à Internet e apenas 21,1% declararam ter uma política de segurança definida (IBGE, 2012).

A importância da segurança da informação muitas vezes só é compreendida após a organização já ter passado por algum incidente que acabou causando algum tipo de prejuízo à organização. Segundo uma pesquisa realizada pelo ESET se “identificou que 73% das corporações consultadas foram vítimas de algum incidente relacionado à segurança da informação nos últimos meses, o que sugere falhas nas políticas e ferramentas voltadas a

combater esse tipo de problema.” (ESET, 2013). Para entender a gravidade dessa situação, precisamos entender o que é uma política organizacional, que para Abreu representa “... padrões de conduta para garantir o sucesso do negócio” (ABREU, 2001), ou como sendo um guia para a tomada de decisões.

Em uma organização, é ideal que uma Política de Segurança da Informação (PSI) seja criada previamente, antes que ocorra algum tipo de incidente com a segurança, ou, caso já tenha ocorrido, para evitar que o mesmo torne a se repetir, ou ainda, como elemento fundamental para que melhorias contínuas preservem, cada vez mais, os ativos informacionais das organizações. A PSI de uma organização consiste em um conjunto de normas, procedimentos, ferramentas e deveres que cada pessoa deve ter dentro da organização a fim de garantir que os recursos da organização e a informação estarão sendo usadas de maneira adequada, reduzindo assim riscos e ameaças à organização; é provavelmente um dos documentos mais importantes dentro de uma organização, pois dele se pode obter maior controle e segurança das informações.

> Atualmente, a PSI é adotada em grande parte das organizações em todo o mundo, inclusive no Brasil. Mesmo aquelas empresas que ainda não tem uma política efetiva, reconhecem a necessidade de elaborar e implementar uma. (CAMPOS, 2007, p. 131)

Tendo em vista a importância das PSIs para as organizações, as perguntas que orientaram este trabalho foram: O que é e por que é importante uma PSI para a gestão de TIC e como se elabora uma PSI, em especial, que possa ser aplicada no campus IV.

1.1 Objetivos

1.1.1 Objetivos Gerais

Compreender a importância de uma Política de Segurança da Informação (PSI) para as organizações, entendendo como esta pode ajudar a melhorá-las, levantando no referencial teórico alguns fatores-chave de sucesso para que, através deles, seja possível elaborar como contribuição uma proposta de PSI para o Campus IV da UFPB.

1.1.2 Objetivos Específicos

São objetivos específicos deste trabalho:

1. Fazer revisão bibliográfica com vistas a apresentar conceitos, modelos e verificar quais são os fatores-chave para se elaborar uma PSI que seja eficaz;
2. A partir da revisão da bibliografia, construir uma lista de verificação com os principais fatores-chave apontados pela literatura, para permitir a comparação de duas ou mais políticas de segurança disponíveis na internet para fins de verificação de aderência ou não ao modelo proposto;

1.2 Justificativa

Na área de segurança de informação o crescimento exponencial na quantidade de informações que lidamos diariamente e o aumento considerável na proporção de espionagem, roubo e vendas de informações sigilosas direcionam para a eficaz gestão da informação, imprescindível tanto para o sucesso organizacional quanto o profissional. Uma boa gestão desse tema se inicia com o estabelecimento de políticas específicas de segurança, inclusive visando à governança corporativa eficaz.

A proposta de elaborar uma política de segurança da informação voltada para o Campus IV da UFPB (e suas características) é inovadora, pois se observou que não existe tal documento, embora ocorra um processo de estabelecimento de uma na sede da UFPB. As vulnerabilidades no Campus IV são tratadas quase que exclusivamente de forma pontual – daí, também, a relevância deste trabalho.

Este trabalho se desenvolveu através das diferentes práticas e conceitos que foram adquiridos ao longo dos anos no curso de S.I., em diferentes disciplinas como Administração I e II, Metodologia do Trabalho Cientifico, Gestão da Informação, Auditoria e Segurança de sistemas, Redes, Gerencia de Redes, Gerencia de Projeto, Gestão da qualidade de software, Interface com o usuário e Engenharia de software. Daí sua importância de formação para o profissional.

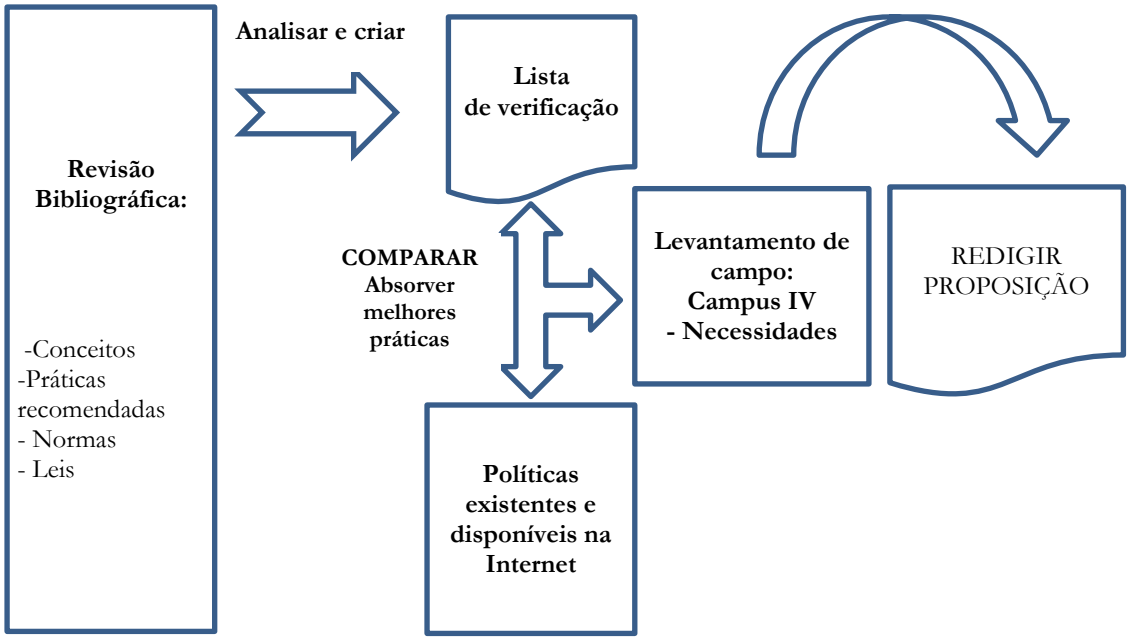
Em complemento, às contribuições do levantamento no referencial teórico sugerem pronta aplicação para a disciplina de auditoria e segurança de sistemas.

E por fim, e não menos importante, para realização pessoal, pois tenho particular interesse profissional nessa área.

1.3 Metodologia

A pesquisa desse trabalho se caracteriza como uma Pesquisa Exploratória Propositiva fundamentada em livros, artigos científicos e outros documentos disponíveis na internet para ser aplicada a um caso específico - o Campus IV da UFPB. Seu desenho é o seguinte:

Figura 1 – Desenho da pesquisa.



Fonte: Elaborada pelo autor.

De acordo com Marconi e Lakatos (2007), entende-se por pesquisa bibliográfica o levantamento de livros, relatórios de pesquisa, monografias, documentos e artigos científicos relacionados com um tema a ser estudado e disponíveis no meio público. Ao realizar a pesquisa, o pesquisador precisa levantar os dados a respeito do assunto a ser estudado e analisá-los considerando as contribuições e suas compreensões para o tema em questão, bem como apontar as controvérsias existentes entre os autores. De acordo com Malhotra (2001), a pesquisa exploratória proporciona a formação de ideias para o entendimento do conjunto do problema. Os estudos exploratórios são frequentemente usados para gerar modelos, hipóteses e identificar variáveis que devem ser incluídas na pesquisa.

A pesquisa exploratória foi realizada através de levantamento bibliográfico nos seguintes assuntos: A) gestão de segurança da informação; B) política de segurança da informação; C) boas práticas em segurança da informação; D) normas de segurança da informação em entidades públicas; e E) metodologia e implantação de política de segurança da informação. Pois esses são os assuntos principais abordados na família da ISO 27000.

Com esses fundamentos, foram selecionados procedimentos comuns para a elaboração de um modelo, sob a forma de lista de verificação, contendo os fatores-chave para o sucesso e que norteará a elaboração da proposta da política de segurança da informação e comunicações, objetivo desta pesquisa.

A proposta alinha-se principalmente nos seguintes normativos apontados abaixo, e nas melhores praticas de segurança citadas em diferentes fontes do referencial teórico:

- NBR ISO/IEC 27002:2005 - Técnicas de segurança – Código de prática para gestão da segurança da informação.
- Decreto nº. 3505 de 2000, que institui a Política de segurança da informação nos órgãos da Administração Pública Federal.
- IN nº. 0001 de 2008 do GSI que disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta.

A fase do estudo de caso abrangeu algumas recomendações propostas por Yin, porém o estudo limitou-se mais a compreender as necessidades percebidas na pesquisa de campo.

A análise do material levantado, bem como a pesquisa de campo efetuada no Campus IV, foi indispensável para o entendimento e caracterização de elementos importantes para o desenvolvimento dos tópicos abordados pela contribuição proposta.

Para comparar duas políticas disponíveis na internet, foi utilizada uma lista de verificação com base na ISO/IEC 27002:2005 abrangendo todas as 11 seções da norma; num primeiro momento verificou-se se as duas políticas estão em conformidade com todos os 133 elementos de controles que ali estão presentes. A esses controles adotados classificou-se cada uma das diretrizes das políticas comparadas, seguindo-se a codificação abaixo:

a) S – está em conformidade com a norma;
b) N – não está em conformidade com a norma;
c) N/A – não se aplica à PSI.

Em seguida, após análise, se constatou quais das duas políticas estariam em melhor conformidade com a norma, por dois motivos: i) aferir pontos importantes que não foram previstos nas políticas comparadas; e ii) servir de guia para o desenvolvimento da contribuição pretendida.

Para o estudo de caso foi realizado um levantamento através de um questionário que continha perguntas abertas e fechadas e foi respondido pelo principal responsável pela gestão da tecnologia da informação no campus IV. Esse questionário se apresentou em quatro partes: A) na primeira foi onde constavam informações da instituição; B) a segunda foi constituída de informações sobre orçamentos, investimentos, existência de políticas, dentre outros fatores da

instituição sobre segurança; C) na terceira ele possui informações sobre falhas de segurança; e D) na quarta e última parte, onde estão as perguntas e comentários adicionais. Através desse questionário foi possível fazer uma análise sobre os problemas, dificuldades e ameaças do campus IV.

A razão pela escolha do campus IV da Universidade Federal da Paraíba (UFPB) envolveu os seguintes aspectos: A) conveniência do pesquisador, pois reside em outra cidade; e, B) viabilidade, haja vista do contato mais próximo do principal gestor de TIC do Campus IV – Rio Tinto.

1.4 Organização do Trabalho

Este trabalho está organizado em cinco capítulos, que são expostos da seguinte forma:

O Capítulo 1 apresenta a definição do problema e as dificuldades que ele pode gerar, os objetivos gerais e específicos, a justificativa, a metodologia, as questões da pesquisa e o desenho da pesquisa.

O Capítulo 2 apresenta o referencial teórico do trabalho, onde se tem o levantamento de informações a respeito do tema abordado, demonstrando modelos para segurança da informação e fazendo uma explanação sobre os melhores métodos e boas práticas para a elaboração e implantação de uma PSI.

O Capítulo 3 apresentada uma comparação de duas PSIs disponíveis na internet, também mostra a organização, seu histórico e características da instituição, a segurança da informação na instituição, as principais ameaças e falhas na segurança, os principais ativos e o que deve ser protegido.

O Capítulo 4 apresenta alguns elementos substanciais da proposta de política de segurança da informação, sendo que a contribuição proposta encontra-se no Apêndice II neste trabalho.

O Capítulo 5 apresenta às considerações finais do trabalho, incluindo os objetivos atingidos, as principais dificuldades de pesquisa encontradas, as limitações e recomendações para trabalhos futuros sobre o assunto e a conclusão do trabalho.

2 REFERENCIAL TEÓRICO

Este capítulo faz uma leitura sobre os conceitos envolvidos com segurança da informação, define o que é política, sistemas de informação e outros elementos de TIC, para subsidiar um modelo de fatores importantes que devem se apresentar em uma política de segurança de informação. Será dada especial ênfase na importância da classificação da informação e o mapeamento de duas vulnerabilidades

2.1 Informação e Segurança da Informação

2.1.1 A Informação

Segundo uma plêiade de autores, a informação é um conjunto de dados que, quando processados, ganham significado e são úteis nos processos decisórios, dentre outras aplicações. Uma informação só é uma informação quando, a partir dos dados, se gera conhecimento, aqui entendido como um conjunto de informações que tenha valor para uma organização, um grupo ou indivíduo.

Diversas são as formas de como se apresenta uma informação: pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas, segundo a ABNT (ABNT NBR ISO/IEC 27002:2005, 2005).

A informação como ativo[1] possui seu valor intrínseco. De fato, "... a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida." (ABNT NBR ISO/IEC 27002:2005, 2005). Sua vitalidade reside nas possibilidades de melhor gerenciamento de recursos, seu controle e monitoramento, uma melhor percepção do ambiente competitivo das organizações, ou em visões de empreendedores individuais.

E por ser um ativo, está sujeito a ameaças e vulnerabilidades, além da desatualização ou perda de valor conforme os anos passam. A bibliografia ressalta o conceito de ciclo de vida da informação como elemento importante para uma boa gestão informacional, porém o conceito não será apresentado neste trabalho.

[1] Nesse trabalho definimos ativo como um conjunto de bens e ou direitos de propriedade, valorizados por indivíduos e organizações.

2.1.2 Segurança da Informação

O conceito de segurança da informação atualmente está padronizado na referida norma ISO/IEC 27002:2005, "A segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio." (ABNT NBR ISO/IEC 27002:2005, 2005), a segurança da informação tem como foco a proteção das informações que existem em uma determinada organização ou pessoa, isto quer dizer que ela deve ser protegida da maneira adequada, independente de como a informação se mostre.

Segundo Oliveira (2001), são as pessoas que tem o papel principal no processo de prover a segurança da informação, pois, independentemente das ferramentas que sejam utilizadas, a segurança da informação começa e termina com pessoas:

> Nenhuma área da informática é tão apreciada como a segurança da informação, todo processo de segurança inicia e tem seu termino em um ser humano. Segurança não é uma questão técnica, mas uma questão gerencial e humana. Não adianta adquirir uma série de dispositivos de hardware e software sem treinar e conscientizar o nível gerencial da empresa e todos os seus funcionários. (OLIVEIRA, 2001, p.43)

Entende-se então, no tocante à salvaguarda do sistema informacional, que: i) para que a informação seja protegida adequadamente, a melhor forma seria criar um conjunto de medidas de controle que se adequam à organização; ii) essas medidas precisam ser estabelecidas, implementadas, monitoradas e analisadas criteriosamente para assim poderem ir se adequando melhor ao quadro atual da organização; iii) pessoas relacionadas à organização também precisam ter o comprometimento de seguir essas medidas da maneira correta, pois por si só essas mesmas medidas não trazem benefício ou salvaguardam ativos.

Ao se pensar em segurança da informação, alguns fundamentos devem ser respeitados, com destaque a tríade Confidencialidade, Integridade e Disponibilidade (CID), cujos conceitos envolvidos estão bastante difundidos na bibliografia sobre o assunto e estão apresentados na Figura 2.

Figura 2 – Pilares básicos da segurança da informação.

Fonte: DODT, 2011.

Esses conceitos são explicados segundo a NBR ISO/IEC 27002:2005:

- A **confidencialidade** é o que garante que a informação só será acessada por pessoas autorizadas a terem acesso, ou seja, aquelas pessoas que foram previamente autorizadas pelo proprietário da informação.
- A **integridade** é a garantia da exatidão da informação e dos métodos de processamento, ou seja, ela garante que a informação mantenha todas as características originais estabelecidas pelo proprietário.
- A **disponibilidade** garante que os usuários que tenham autorização sempre tenham acesso à informação e aos ativos correspondentes quando necessário.

Fica esclarecido que outros modelos conceituais foram encontrados na literatura, porém o trabalho foi estabelecido segundo a norma referida.

2.2 Classificação da Informação

É um passo importante no estabelecimento de uma PSI classificar as informações presentes na organização segundo a lógica de importância estratégica. Devem-se classificar as informações porque cada informação possui um grau de importância (ou valor) diferente para a organização e as pessoas envolvidas, por isso requer um nível de proteção diferente em diferentes níveis hierárquicos: quanto mais decisiva ou estratégica é a informação para a

organização tanto mais será maior sua importância para os negócios. Por exemplo, enquanto um relatório sobre a queda na produção de uma empresa pode não significar nada para um simples empregado, para um alto executivo mostra que alguma coisa está errada, e essa informação deve ser preservada para que futuramente ele possa fazer uma melhor análise. Portanto, a informação deve ser classificada a todo tempo em qualquer ambiente de armazenamento.

Segundo a descrição do item 7.2 da ABNT NBR ISO/IEC 27002:2005, que fala sobre classificação da informação:

> Recomenda-se que a informação seja classificada para indicar as necessidades, prioridades e nível esperado de proteção da mesma. A informação possui vários níveis de sensibilidade e criticidade. Alguns itens podem necessitar um nível adicional de proteção ou tratamento especial. A classificação da informação deve ser usada para definir um conjunto apropriado de níveis de proteção e determinar a necessidade de medidas especiais de tratamento. (ABNT NBR ISO/IEC 17799:2005, 2005)

Para se classificar uma informação deve-se antes de tudo estabelecer algumas regras: i) toda informação deve ter um proprietário; e ii) verificar a importância daquela informação perante a organização, de modo que informações que são de vital importância para organização não acabem sendo classificadas erroneamente, ou extraviadas, e acabem causando algum dano a mesma. Para Freitas e Araújo (2008), podem ser criados diferentes fatores classificatórios:

> Antes de se iniciar o processo de classificação, é necessário conhecer o processo de negócio da organização, compreender as atividades realizadas e, a partir disso, iniciar as respectivas classificações. As informações podem ser classificadas em informações públicas, quando não necessitam de sigilo algum; informações internas, quando o acesso externo às informações deve ser negado; e informações confidencias, as informações devem ser confidencias dentro da empresa e protegidas contra tentativas de acesso externo. (FREITAS E ARAUJO, 2008)

Uma boa prática de classificação da informação seria aquele que se divide em quatro níveis, a saber (FREITAS E ARAUJO, 2008):

- **Secreta** – Informações consideradas secretas são aquelas essenciais para as atividades da empresa; sua integridade deve preservada, e por isso o acesso a elas deve ser restrito a um número reduzido de pessoas. O acesso externo ou interno a essas informações por pessoas não autorizadas pode ser prejudicial à organização.

- **Confidencial** – As informações consideradas confidenciais devem ficar restritas aos limites da empresa, sua divulgação ou perda pode levar a empresa à danos financeiros, ou perdas na fatia do mercado perante o concorrente. O usuário só deve acessar essas informações com estrita necessidade.
- **Interna** – As informações consideradas internas são aquelas que nem sempre são de domínio da empresa, seu acesso deve ser evitado embora as consequências do seu uso não venham a causar grandes danos a empresa, mesmo assim podem causar prejuízos indiretos não desejáveis.
- **Pública** – Informações consideradas públicas são aquelas que podem ser divulgadas, ou seja, que podem vir a publico sem maiores consequências à empresa, já que não são de vital importância.

2.3 Vulnerabilidades: Ameaças, Ataques e Riscos

A NBR ISO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade é uma fraqueza, falha ou deficiência que pode ser acidentalmente utilizada ou intencionalmente explorada por possíveis ameaças, ou seja, é um ponto onde poderá acontecer um ataque. Campos diz que "vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação" (CAMPOS, 2007).

> A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos, configurações, etc. Condição causada muitas vezes pela ausência ou ineficiência das medidas de proteção utilizadas de salvaguardar os bens da empresa. (MOREIRA, 2001, p. 22)

Moreira (2001) também afirmava que as vulnerabilidades podem ter diversas causas para surgirem, sendo elas melhor entendidas como uma relação N para N, ou seja, cada ambiente pode apresentar diversas vulnerabilidades e cada vulnerabilidade pode estar em diversos ambientes.

As vulnerabilidades podem ocorrer de vários aspectos como: falta de proteção contra incêndios, desastres naturais, falta de treinamento dos funcionários, falta de uma política de segurança e etc. Saber identificar uma vulnerabilidade é de essencial importância, quando se identifica uma vulnerabilidade é possível eliminá-la e se precaver contra a mesma, a

identificação também é importante pois só assim é possível avaliar se as medidas de segurança adotadas estão sendo eficientes para evitar um ponto de vulnerabilidade.

2.3.1 Identificação de Ameaças

Segundo Ferreira e Araújo (2008) ameaça é a possibilidade de um invasor ou evento inesperado explorar uma vulnerabilidade, com embasamento nisso se pode dizer que se não existir vulnerabilidade que possa ser explorada, uma ameaça não representa risco. As potencias ameaças devem ser identificadas e formalizadas, pois podem causar danos aos sistemas informatizados, as ameaças mais comuns são relacionadas à falhas humanas ou ambientais.

Identificar uma ameaça é saber a motivação que pode levar a um possível ataque: esse ataque pode vir desde um funcionário insatisfeito ou desonesto, ou de uma organização concorrente/rival; e a motivação varia de acordo com a fonte. Ao juntar esses aspectos, se torna possível fazer uma avaliação sobre as ameaças e respectivos métodos mitigadores que podem ser utilizados.

A Figura 3 apresenta as diferentes fontes de ameaças mais comuns, as principais motivações e os métodos de ataque.

Figura 3 – Fontes de ameaças.

FONTES DE AMEAÇA	MOTIVAÇÃO	MÉTODOS
Hacker, cracker	• Desafio • Ego • Rebeldia	• *Hacking* • Engenharia social • Invasão de sistemas • Acesso não autorizado aos sistemas
Criminoso de computador	• Destruição da informação • Divulgação e alteração não autorizada das informações • Retorno financeiro	• Crime por computador (espionagem) • Atos fraudulentos (interceptação de informações) • Suborno • Invasão de sistemas
Terrorista	• Chantagem • Destruição • Vingança • Exploração	• Bombas/terrorismo • Guerra de informação • Ataque aos sistemas (ex.: ataques DOS)
Espionagem industrial (companhias, países, etc.)	• Vantagem competitiva • Espionagem	• Exploração econômica • Roubo de informações • Engenharia social • Invasão de sistemas • Acesso as informações classificadas
Funcionários da própria organização (aqueles que não recebem treinamento adequado, negligentes, desonestos ou demitidos)	• Curiosidade • Ego • Inteligência • Retorno financeiro • Vingança • Erros não intencionais	• Abuso dos recursos de TI • Roubo e fraude • Inclusão de dados falsos • Interceptação • Inclusão de códigos maliciosos (ex.: vírus, cavalos de tróia) • Venda de informações • Falhas nos sistemas • Acesso não autorizado aos sistemas

Fonte: FERREIRA E ARAÚJO, 2008, p. 172.

2.3.2 Tipos de Ataque

Quando se fala sobre segurança da informação não há como não citar alguns tipos de ataque. Esses ataques podem ser complexos e sofisticados ou simples e bem elaborados. Um ataque a uma rede ou computador normalmente pode ser feita de diversas maneiras, porém se pode simplificar especificando em dois métodos:

2.3.2.1 Ataque direto

O ataque direto normalmente tem como característica o contado pessoal, são planejados antecipadamente e minuciosamente, normalmente acontecem através de telefone ou fax. Nesse tipo de ataque é bem comum a utilização de engenharia social, que seria uma prática de ataque que o invasor se aproxima da vitima que normalmente tem acesso ao sistema alvo (que o invasor pretende atacar) para, através de influência e manipulação, conseguir os dados que deseja; esse tipo de ataque é uma forma de "entrar" na organização sem que seja preciso brutalidade ou vulnerabilidade aparente do sistema, ou seja, explora as falhas de segurança das próprias pessoas da organização (DELLA VALLE-ULBRICH, 2009).

2.3.2.2 Ataque indireto

O ataque indireto normalmente utiliza ferramentas de invasão como cavalos de troia, falsos e-mails, pesquisa de dados, sites falsos e o famoso *phishing scam* (pesca de dados) para obter informações, sendo que a internet é ainda a forma mais fácil de conseguí-las. Normalmente as vitimas que os *hackers* ou *crackers* atacam são apenas o portador da informação, as informações tem real importância em uma escala maior, pois fazem parte de alguma organização (ou governo) e essas organizações são o foco principal do ataque (DELLA VALLE-ULBRICH, 2009).

2.3.3 Gestão de Riscos

Um risco significa a possibilidade de perigo incerto, mas previsível, que ameaça dano à pessoa ou à coisa, ou a ambos (Dicionário Michaelis); no caso a informação é entendida como ativo – uma coisa.

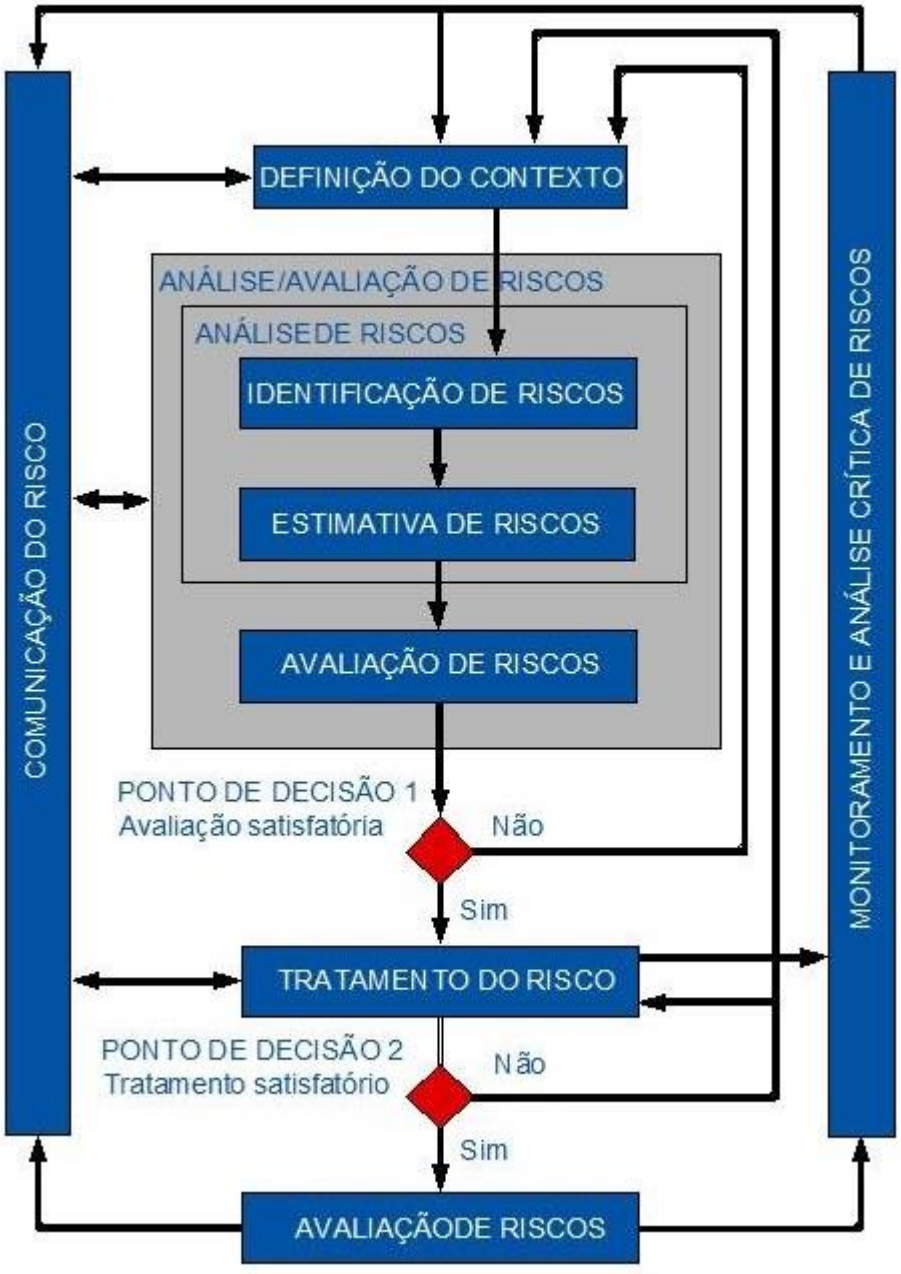
Segundo a NBR ISO/IEC 27005:2008 que fala sobre gestão de riscos de segurança da informação, um risco de segurança da informação é a chance de uma determinada ameaça explorar a vulnerabilidade de um ativo ou de um grupo de ativos. A norma fornece e descreve um processo geral para a correta gestão de riscos de segurança da informação em uma organização.

O processo de gestão de riscos tem início com a definição do contexto, logo depois é feito uma análise/avalição de risco onde os mesmos são identificados, estimados e avaliados com base nos critérios definidos no momento do estabelecimento do contexto. No fim dessa fase se chega ao primeiro ponto de decisão onde se avalia se a decisão foi ou não satisfatória, caso não seja o processo é repetido. Caso a avaliação seja satisfatória se passa para próxima fase que é a do tratamento do risco. Essa fase é onde os riscos podem ser reduzidos,

encerrados, transferidos ou evitados. Caso o tratamento não seja satisfatório se faz outra analise de riscos.

Na Figura 4 se pode ver uma visão geral do processo de gestão de riscos de segurança da informação.

Figura 4 – Processo de gestão de riscos de segurança da informação.



Fonte: ABNT NBR ISO/IEC 27005:2008, 2008, p. 5.

O processo passa por uma análise ambiental, para verificar possíveis ameaças e vulnerabilidades, a identificação e estimativa dos riscos associados, e o resultado da

avaliação. A seguir, um processo de tratamento dos riscos é realizado, seguido de nova avaliação ou monitoramento, entendendo-se a comunicação como parte importante do processo.

2.4 Modelos de Segurança da Informação

No levantamento do referencial teórico constatou-se a existência de diferentes modelos (ou *frameworks*) que tratam sobre segurança da informação, dentre eles a americana NIST, SABSA e a família ISO 27000. Outros, como COBIT, ITIL e CMMI possuem alinhamento com as práticas preconizadas na ISO 27002. A NBR ISO/IEC 27002:2005 juntamente com a NBR ISO/IEC 27001:2006 são mundialmente reconhecidas por suas metodologias e melhores praticas em governança para o ambiente de tecnologia; são amplamente utilizadas e podem ser referenciadas como pilares na questão de modelos de segurança da informação (SOOMRO, 2012).

2.4.1 NBR ISO/IEC 27002 e NBR ISO/IEC 27001

A NBR ISO/IEC 27002:2005 teve como base a norma BS 7799 que foi criada pelo BSi (*British Standard Institute*), a norma BS 7799 quando foi criada era considerada o mais completo padrão para gerenciamento da segurança da informação existente, já que ela proporcionava a possibilidade de criar um sistema de gestão de segurança bastante eficaz.

A BS 7799 em dezembro de 2000 se tornou ISO/IEC 17799 a norma oficial da ISO (*International Organization for Standardization*) e no ano seguinte foi adotada no Brasil pela ABNT (Associação Brasileira de Normas Técnicas) sendo chamada de NBR ISO/IEC 17799 que teve uma nova versão publicada em 2005, totalmente revisada e com novos capítulos. A ISO então criou a serie 27000 com intuito de reunir várias normas a respeito de segurança da informação, em 2006 foi publicada a norma NBR ISO/IEC 27001:2006 que era a antiga BS7799-2:2002 revisada melhorada, em 2007 a norma NBR ISO/IEC 17799 foi rebatizada de NBR ISO/27002.

A NBR ISO/IEC 27002:2005 tem como objetivo “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.” (ABNT NBR ISO/IEC 27002:2005, 2005). As orientações descritas nesta norma são amplamente aceitas para a gestão de segurança da informação, ou seja, esta norma é um conjunto de recomendações gerais para melhores práticas da gestão da segurança de informação e procedimentos para a segurança da informação.

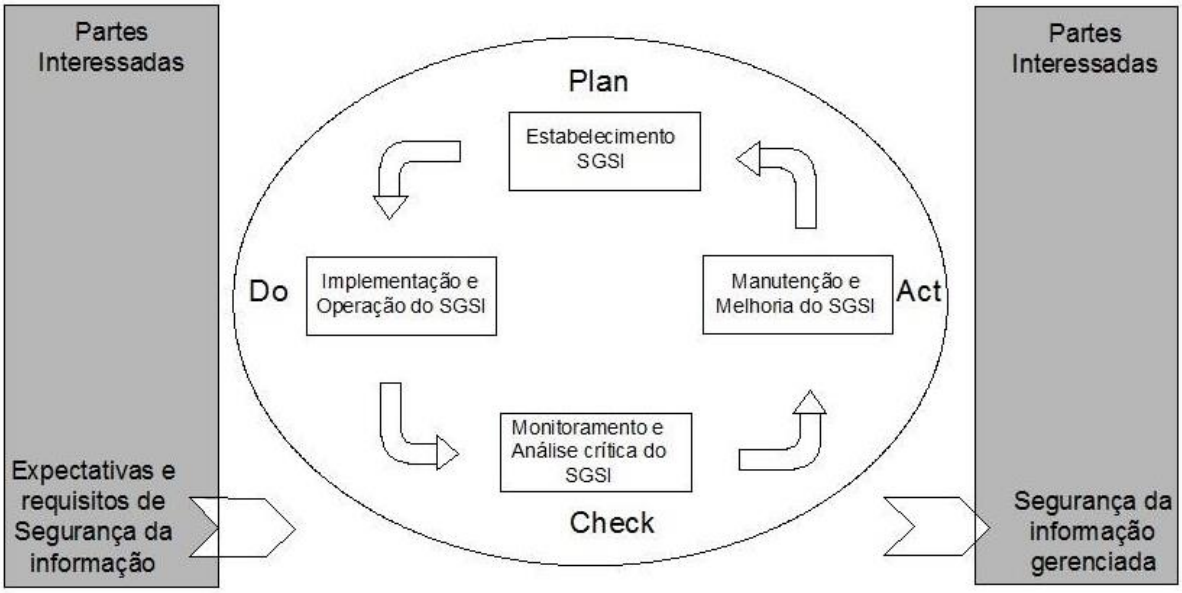
A NBR ISO/IEC 27001:2006 "foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)." (ABNT NBR ISO/IEC 27001:2006, 2006). Esta norma pode ser utilizada juntamente com a NBR ISO/IEC 27002:2005. Adotar um SGSI em uma organização é uma escolha estratégica, pois sua implementação e especificações vão de acordo com a estrutura e as necessidades que organização apresente. A norma também estabelece critérios para a certificação; para que uma organização possa solicitar a certificação, tem que estar em conformidade com todos os requisitos estabelecidos pela mesma.

2.4.1.1 Sistema de gestão de segurança da informação (SGSI)

Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de procedimentos, políticas, diretrizes e outras determinações relacionadas à segurança da informação ou à gestão da informação, que determinam como são reduzidos os risco para a segurança da informação (NBR ISO/IEC 27001:2006, 2006).

Como em todos os processos de gestão, um SGSI deve permanecer eficaz e eficiente mesmo em longo prazo (efetivo), ele deve se adaptar às mudanças na organização interna e ao ambiente externo. Para isto NBR ISO/IEC 27001 estabeleceu um processo com algumas etapas para a implementação de um SGSI e incorporou o PDCA (*Plan-Do-Check-Act* – Planejar-Executar-Verificar-Agir) que é um modelo oriundo da ISO 9001 que trata da Gestão da Qualidade e é empregado para garantir uma efetiva gestão da organização.

Figura 5 – Modelo do PDCA aplicado aos processos de SGSI.



Fonte: NBR ISO/IEC 27001:2006, 2006.

Como se pode observar na Figura 5, o SGSI se caracteriza por um ciclo de ações que se repete continuamente de forma a incorporar alterações no ambiente e outras melhorias, além de estipular auditorias necessárias e uma política composta por diretrizes eficazes. As etapas do processo de implementação de um SGSI abrangem:

I. Definir o escopo e os limites do SGSI de acordo com as características do negócio.
II. Definir uma política do SGSI de acordo com as características do negócio.
III. Definir a abordagem de analise/avaliação de riscos da organização.
IV. Identificar riscos.
V. Analisar e avaliar os riscos.
VI. Identificar e avaliar as opções para o tratamento de riscos.
VII. Selecionar os objetivos de controles para o tratamento de riscos.
VIII. Obter aprovação da direção dos riscos residuais propostos.
IX. Obter aprovação da direção para implementar e operar o SGSI.
X. Preparar uma SoA (*Statement of Applicability* – Declaração de aplicabilidade).

Conforme a Figura 6, se pode observar as diferentes atividades exigidas em cada fase do estabelecimento de um SGSI.

Figura 6 – Ciclo PDCA.

Fase I – Plan	Fase II – Do	Fase III – Check	Fase IV – Act
• **Estruturação do SGSI** • **Plano Diretor de Segurança** • **Diagnóstico de Segurança** • **Avaliação, Tratamento dos Riscos e Seleção dos Controles de Segurança** • **Declaração de Aplicabilidade (Statement of Applicability)**	• **Comitê de Segurança da Informação** • **Política de Segurança** • **Classificação da Informação** • **Plano de Continuidade dos Negócios e de TI** • **Treinamento e Conscientização** • **Implementação dos Controles Especificados na Declaração de Aplicabilidade**	• **Monitoração dos Controles de Segurança** • **Gestão de Incidentes** • **Revisão do Nível de Risco Residual** • **Auditoria Interna de SGSI**	• **Implementação de Melhorias** • **Ações Corretivas e Preventivas** • **Comunicação das Ações e Resultados para Alta Administração e Partes Interessadas** • **Assegurar que as Melhorias foram Implementadas e Atenderam as Expectativas**

Fonte: FERREIRA E ARAÚJO, 2008, p. 55.

2.5 Política de segurança

A política de segurança tem um papel extremamente importante dentro de uma organização: ela é a base de tudo que tem relação com a proteção da informação e de seus ativos, busca prevenir problemas e evita que problemas passados tornem a acontecer. É composta por:

- Um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações e ativos da organização recebem a proteção adequada.
- Atribuir responsabilidades a colaboradores internos e externos em relação à segurança dos recursos com os quais trabalham, pois qualquer coisa que venha a descumprir a política de segurança é considerada um incidente de segurança.
- Definir procedimentos a serem adotados para cada caso de violação, de acordo com sua severidade. As penalidades às quais estão sujeitos aqueles que não cumprem a política vão desde uma simples advertência verbal ou escrita, até uma ação judicial.

Segundo Wadlow (2000) uma política de segurança deve: i) descrever o que está sendo protegido e por que; ii) definir sobre o que precisa ser protegido em primeiro lugar e com qual custo; iii) estabelecer um acordo explícito com varias partes da organização em relação ao valor da segurança; iv) fornecer autoridade ao departamento de segurança para dizer "não" e sustentar esse "não" quando necessário; e v) impedir que o departamento de segurança tenha um desempenho fútil dentro da organização.

A elaboração de uma política de segurança é uma tarefa complexa e difícil, pois ela deve atender a vários aspectos e requer um conhecimento abrangente sobre o tema, organização, cultura, pessoas e tecnologias, e como implementá-la. Além disso, é necessário ter visão sobre a magnitude dos riscos envolvidos para que assim se possa combatê-los; sabe-se que uma corrente é tão forte quanto seu elo mais fraco, então somente com a comunicação e o compartilhamento das responsabilidades pela segurança nos diferentes níveis da organização se pode criar um ambiente proativo para perceber e tratar possíveis incidentes.

Uma política de segurança deve ser definida de acordo com os objetivos de negócios da organização. Segundo Ferreira e Araújo (2008), uma boa política de segurança deve ser:

- Simples;
- Compreensível (escrita de maneira clara e concisa);
- Homologada e assinada pela alta administração;
- Estruturada de forma a permitir a sua implantação por fases;
- Alinhada com as estratégias de negócios da organização, padrões e procedimentos já existentes;
- Orientadas aos riscos (qualquer medida de proteção das informações deve direcionar para os riscos da organização);
- Flexível (moldáveis aos novos requerimentos de tecnologia e negócio);
- Protetora dos ativos de informação, priorizando os de maior valor e de maior importância;
- Positiva, e não apenas concentrada em ações proibitivas ou punitivas.

Uma política de segurança para ser bem sucedida deve ser patrocinada e aprovada pela alta administração da organização, publicada, comunicada interna e externamente, de forma expressa e acessível para cada um dos diferentes públicos, e revista periodicamente. De outra forma, a implementação deve envolver toda a organização: todos os usuários devem conhecer, formalizar esse conhecimento e respeitar a política desenvolvida.

2.5.1 Políticas, Diretrizes, Normas e Procedimentos

A distinção entre políticas, diretrizes, normas e procedimentos é necessária uma vez que elas fazem parte de um conjunto de regras formais que servem como ferramenta para a avaliação e execução dos processos organizacionais e auditorias periódicas.

Uma política de segurança é um conjunto de diretrizes, normas e procedimentos designados respectivamente aos níveis estratégico, tático e operacional, com o objetivo de estabelecer, padronizar e normatizar a segurança tanto no escopo humano como no tecnológico da organização. São regras gerais e básicas que orientam a tomada de decisão na organização. Elas devem refletir o pensamento da organização quanto às suas diferentes funções; uma política limita o que se pode ou não fazer, ou aonde se quer chegar e para que.

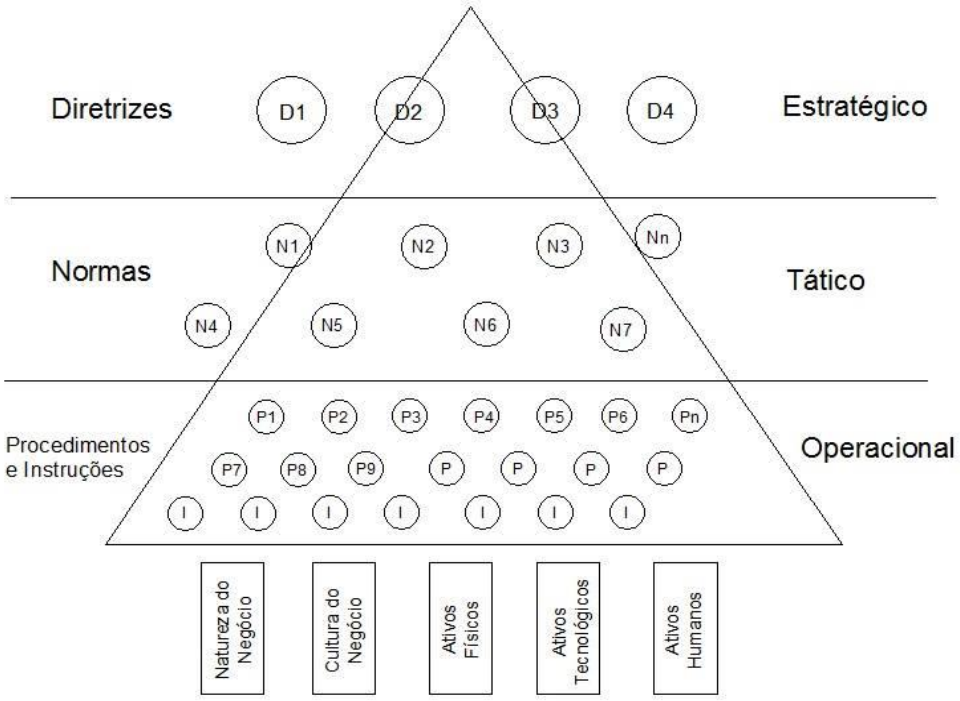
Uma política de segurança deve ser capaz de preparar a organização com instrumentos jurídicos, normativos e processuais, esses instrumentos devem envolver estruturas (pilares) administrativas, físicas e tecnológicas.

As diretrizes, por sua vez, possuem o papel estratégico e estabelecem objetivos e ações a cumprir; uma política é composta por diretrizes. Em complemento, as normas são os requisitos a serem observados no desempenho do trabalho, ou seja, como é para ser feito ao nível tático na organização.

Os procedimentos, por sua vez, são os atos a serem realizados ao nível operacional, entendendo como as ações que serão implementadas, descrição em detalhes de como atingir o resultado, ou seja, o que é para ser feito em termos de atividades e tarefas. Cabe notar que as normas definem os objetivos a serem alcançados com o uso dos procedimentos adotados, bem como tratam das medidas de qualidade na execução desses procedimentos.

A Figura 7 oferece a visão dos diferentes níveis afetados por uma política (mais abrangente), por suas diretrizes, normas e procedimentos, respectivamente (Abreu, 2001).

Figura 7 – Diagrama do conceito dos componentes da política e seus pilares.



Fonte: FERREIRA E ARAÚJO, 2008, p. 86.

Uma política de segurança deve ser capaz de preparar a organização com instrumentos jurídicos, normativos e processuais, esses instrumentos devem envolver estruturas (pilares) administrativas, físicas e tecnológicas. Segundo Abreu (2001) uma política de segurança pode ser dividida em três tipos de níveis: Nível estratégico, nível tático e nível operacional, como mostra a Figura 7.

- **Nível estratégico:** Algumas situações exigem decisões não programadas que podem afetar substancialmente uma organização. Novos desafios, oportunidades ou ameaças que podem impactar na sobrevivência da organização exigem ponderação e cuidado, e são conduzidas tendo como fundamento os valores da organização: uma decisão errada pode mudar completamente o rumo da organização. Assim são as políticas de segurança de informação.
- **Nível tático:** Nesse nível, a palavra é padronização: software, correio eletrônico, equipamentos, entre outras coisas, devem ser padronizados, pois assim todos os pontos da organização terão o mesmo nível de segurança e não haverá nenhuma vulnerabilidade aparente.

- **Nível operacional:** O essencial no nível operacional é o detalhamento, pois assim se garante a perfeição no atendimento e na continuidade dos negócios independente do fator humano. Se existe um padrão formalizado então esse padrão deve ser seguindo; na política de segurança a parte operacional vem para padronizar detalhes de configurações do ambiente. Pode-se criar um único padrão que sirva para toda organização, ou criar vários padrões para varias localidades da organização, isso vai de acordo com a necessidade que a organização apresenta; o essencial é saber que o padrão é importante.

2.5.2 Tipos de Política

De acordo com Ferreira (2003), existem três tipos de políticas: regulatórias, consultivas e informativas.

2.5.2.1 Regulatória

A essência de uma política regulatória é definida como se fosse uma série de especificações legais. Descreve, com grande riqueza de detalhes, o que deve ser feito, quem deve fazer e fornecer algum tipo de parecer, relatando a importância de tal. Desta forma, Ferreira (2003) afirma que políticas regulatórias são implementadas devido às necessidades legais que são impostas à organização.

2.5.2.2 Consultiva

A política consultiva apenas sugere quais ações ou métodos devem ser utilizados para a realização de uma tarefa; não são obrigatórios, porém são bastante recomendados. A característica principal é esclarecer aos usuários as atividades cotidianas da organização.

2.5.2.3 Informativa

Uma política informativa possui caráter apenas informativo, nenhuma ação é desejada e não existem riscos, caso não seja cumprida. A política informativa não é tão exigente quanto as demais, porém, também pode conter uma série de observações importantes, bem como advertências severas.

2.5.3 Política de Segurança da Informação

Uma política de segurança da informação (PSI) é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da organização, ou seja, uma política de segurança atribui direitos e responsabilidades às pessoas que lidam com os recursos tecnológicos de uma organização e com as informações neles armazenados (FERREIRA e ARAÚJO, 2008).

Para tanto, uma PSI deve definir um conjunto de normas, métodos e procedimentos utilizados para manutenção da segurança da informação, devendo ser formalizada e divulgada a todos os usuários que utilizam os ativos de informação da organização, e deve manifestar os anseios dos proprietários ou acionistas da organização.

Em complemento, uma PSI não é um documento definitivo, inalterável ou inquestionável, pelo contrário, requer constante atualização e participação de gerentes, usuários e equipe de TI, seu desenvolvimento deve ser feito de forma que possa ser sugerida novas alterações na configuração de equipamentos, na escolha da tecnologia, na definição de responsabilidades e na elaboração de melhores políticas com o perfil da organização e dos seus negócios (Ferreira e Araújo 2008).

O propósito de uma PSI é garantir que os recursos de informática e a informação estarão sendo usados de maneira adequada, elaborando critérios apropriados para o manuseio, armazenamento, transporte e descarte das informações, além de informar às pessoas que estão envolvidas na organização quais são suas obrigações para a proteção da tecnologia e do acesso à informação; deve especificar os mecanismos através dos quais estes requisitos podem ser conseguidos, e oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que assim os mesmos sejam adequados aos requisitos propostos. Com isso o uso de um conjunto de ferramentas de segurança sem que exista uma PSI orientadora seria ineficiente e sem sentido.

2.5.3.1 Processo de Desenvolvimento de uma PSI

Segundo Ferreira e Araújo (2008), o processo de desenvolvimento e implantação de uma política de segurança da informação pode ser dividido em quatro fases.

I. Levantamento de informações
    a. Onde se obtém padrões, normas e procedimentos de segurança já existentes para analise.

b. É onde se tem o entendimento das necessidades e uso dos recursos da tecnologia da informação (sistemas, equipamentos e dados) nos processos de negocio.
c. É onde se obtém a informação sobre os ambientes de negócios:
    - Processos de negócios;
    - Tendências de mercado;
    - Controles e áreas de risco.
d. É onde se obtém a informação sobre o ambiente tecnológico:
    - *Workflow* entre ambientes;
    - Redes de aplicações;
    - Plataformas computacionais.

II. Desenvolvimento de conteúdo da política e normas de segurança
a. É onde se faz o gerenciamento da política de segurança:
    - Definição da segurança da informação;
    - Objetivo do gerenciamento;
    - Fatores críticos de sucesso;
    - Gerenciamento da versão e manutenção da política;
    - Referência outras políticas, padrões e procedimentos.
b. É onde se atribui as regras de responsabilidade:
    - Comitê de segurança da informação;
    - Proprietário das informações;
    - Área de segurança da informação;
    - Usuários de informação;
    - Recursos humanos;
    - Auditoria interna.
c. É onde se diz os critérios para classificação das informações:
    - Introdução;
    - Classificação da informação;
    - Níveis de classificação;
    - Reclassificação;
    - Armazenamento e descarte;
    - Armazenamento e saídas.
d. É onde se define os procedimentos de segurança de informações:

- Classificação e tratamento da informação;
- Notificação e gerenciamento de incidentes de segurança da informação;
- Processo disciplinar;
- Aquisição e uso de hardware e software;
- Proteção contra software malicioso;
- Segurança e tratamento de mídias;
- Uso de internet;
- Uso do correio eletrônico;
- Utilização dos recursos de TI;
- *Backup*;
- Manutenção de teste e equipamentos;
- Coleta e registro de falhas;
- Gerenciamento e controle da rede;
- Monitoração de uso e acesso aos sistemas;
- Uso de controles de criptografia e gerenciamento de chaves;
- Controle de acesso físico ás áreas sensíveis;
- Segurança física;
- Supervisão de visitantes e prestadores de serviço;

III. Elaboração dos procedimentos de segurança da informação
   a. É onde são realizadas pesquisas sobre as melhores práticas em segurança da informação.
   b. Onde se desenvolve procedimentos e padrões, para discussão com a Alta Administração, de acordo com as melhores práticas de mercado e com as necessidades e metas da organização.
   c. É onde se formaliza os procedimentos para integra-los ás políticas corporativas.

IV. Revisão, aprovação e implantação das políticas, normas e procedimentos de segurança da informação.
   a. É onde se faz a revisão e aprovação das políticas, normas e procedimentos de segurança da informação.

b. É onde se faz uma efetiva implantação das políticas , normas e procedimentos de segurança da informação por meio das seguintes iniciativas:
    - Atuação junto á área que tem a responsabilidade de comunicação na organização, no dever de orientar para preparação de material de divulgação e de consulta, ou semelhante;
    - Divulgar as responsabilidades dos colaboradores, enfatizando a importância das políticas, normas e procedimentos de segurança da informação;
    - Realizar palestras eficazes que terão como publico alvo os presidentes, gerentes e diretores da organização, palestras que serão referentes às políticas normas e procedimentos de segurança da informação desenvolvidos;
    - Realizar palestras referentes às políticas, normas e procedimentos de segurança da informação, tendo como público-alvo outros colaboradores da organização.

O autor também sugere que se crie um cronograma para acompanhar o desenvolvimento da política de forma mais eficaz.

2.5.3.2 Fatores comuns que caracterizam boas PSI

De acordo com Ferreira e Araújo (2008) todas as políticas bem elaboradas geralmente possuem os mesmos conceitos, os aspectos que contem uma boa política de segurança são:

- Especificação da política

Esta parte é considerada a parte mais importante do documento. Uma política deve ser breve, utilizar palavras simples evitando jargões técnicos e formalizar o que é aguardado dos funcionários da organização. Deve proporcionar informações suficientes para quem estiver lendo saber se os procedimentos descritos na política são aplicáveis a ele ou não. Deve descrever sua finalidade específica, ou seja, se é orientada a pessoas, departamentos, equipamentos, etc.

- Declaração da Alta administração

Um dos itens mais importantes. É uma declaração do comprometimento da direção, consequentemente, demonstra aos colaboradores que a alta administração e seus executivos estão de acordo com a política apresentada no documento bem como demonstra seu apoio às metas e princípios da segurança da informação.

- Autores/patrocinadores da política

Os nomes dos profissionais ou equipes que desenvolveram a política devem estar especificados no documento para em caso de dúvidas ou sugestões de mudanças.

- Referências a outras políticas, normas e procedimentos.

Em inúmeras organizações é comum que as políticas de segurança em vigor façam referência a outros regulamentos internos já existentes ou em desenvolvimento.

- Procedimentos para requisição de exceção à política

É de grande importante preparar e divulgar a política, mas também é essencial ter um processo para requisição de exceção a ela. É importante descrever apenas os procedimentos de solicitações, não descrever sob quais condições as exceções serão concedidas.

- Procedimentos para mudanças da política

Diversas organizações não atualizam suas políticas, com isso é necessário ter um procedimento para atualização dela. Há situações que podem requerer somente revisões técnicas, mas outras necessitarão de justificativas detalhadas para solicitar mudanças nas políticas, por isso atualmente as políticas devem especificar responsabilidades, em nível hierárquico ou especialização técnica, para seu controle e atualização,

- Punição para aqueles que violarem a política

A alta administração deve demonstrar que poderão ocorrer punições severas aos servidores da organização caso haja um desrespeito ou violação a política.

- Data de publicação, validade e revisão da política.

A política e seus documentos complementares devem possuir assinatura do principal executivo aprovando-a, a data da última atualização e do início de sua vigência. Essas informações ajudam a controlar suas revisões e atualizações.

2.5.3.3 Pontos críticos para o sucesso de uma PSI

Para que uma PSI seja bem sucedida ela deve ser:

- Clara – Deve ser escrita em uma linguagem formal que seja acessível para todos;
- Concisa – Uma PSI não pode ter informações desnecessárias e redundantes;
- Adequada – A PSI deve ser apropriada para a realidade da organização;
- Atualizada periodicamente – Caso ocorra mudança nos negócios, novas ameaças ou até mesmo falhas encontradas posteriormente.

> Convém que a PSI seja analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia. (ABNT NBR ISO/IEC 27002:2005, 2005)

Ferreira e Araújo (2008) também mencionam alguns itens de extrema importância para o sucesso de uma política de segurança são:

- Formalização dos processos e instruções de trabalho;
- Utilização de tecnologias capazes de prover segurança;
- Atribuição formal das responsabilidades e das respectivas penalidades;
- Classificação das informações;
- Treinamento e conscientização constantes.

2.6 Conclusão do Capítulo

Este capítulo mostrou o estudo sobre informação e segurança da informação; também abordou as formas que uma informação pode ser classificada e as vulnerabilidades e ameaças a qual toda organização está exposta. Foram abordados também modelos e melhores práticas de segurança da informação e cuidados ao se elaborar e implantar uma PSI dentro de uma organização.

O próximo capítulo apresenta os resultados da pesquisa comparativa realizada entre as PSIs de duas instituições distintas. Também apresenta o estudo de caso realizado segundo o escopo deste trabalho.

3 RESULTADOS DA PESQUISA

Este capítulo aborda os resultados obtidos a partir do levantamento do referencial teórico e as praticas recomendadas pela NBR 27002 e o estudo de caso proposto, qual seja o Campus IV da Ufpb Litoral Norte, sediado no município de Rio Tinto (PB).

De início será apresentada uma comparação entre duas PSIs de instituições distintas, e a seguir será apresentado o objeto de estudo mencionado.

3.1 O Padrão NBR 27002 em Análise: A Comparação de Duas PSI

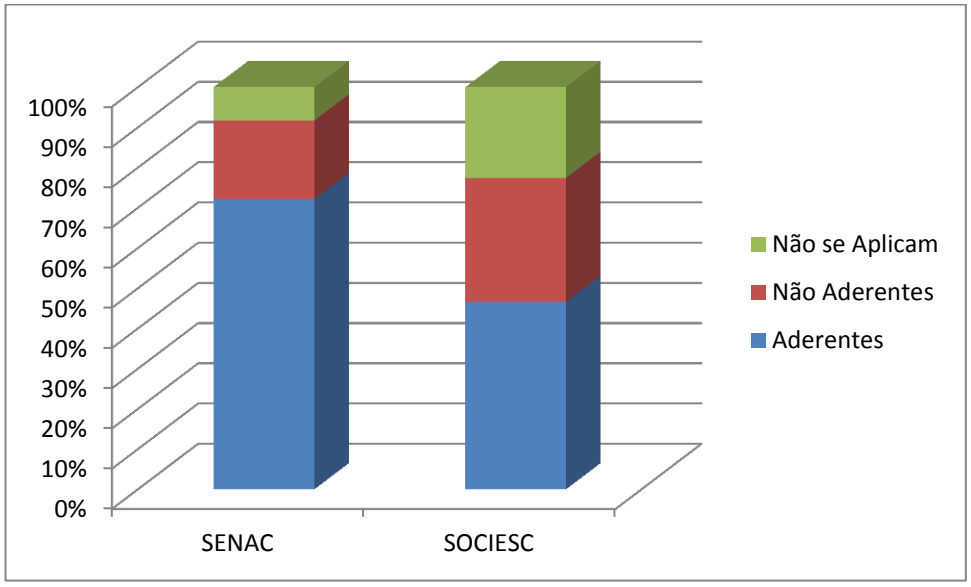
Para aprender mais sobre o assunto foi realizada uma comparação entre duas políticas de segurança disponíveis na internet. O intuito foi verificar qual das duas está em melhor conformidade com os itens contidos na norma ABNT NBR ISO/IEC 27002:2005, e para tanto, foi criada uma lista contendo as 11 seções da norma, a saber: I) Política de segurança; II) organizando a segurança da informação; III) gestão de ativos; IV) segurança em recursos humanos; V) segurança física e do ambiente; VI) gerenciamento das operações e comunicações; VII) controle de acesso; VIII) Aquisição, desenvolvimento e manutenção de sistemas de informação; IX) Gestão de incidentes de segurança da informação; X) Gestão da continuidade do negócio; XI) conformidade.

Os critérios pensados para pontuar o alinhamento dos fatores de controle foram os seguintes, sendo que a cada critério associado (ou não) se somava 1 ao total acumulado a cada critério respectivo; os resultados são apresentados no Apêndice I:

a) S – está em conformidade com a norma;
b) N – não está em conformidade com a norma;
c) N/A – não se aplica à PSI.

A primeira PSI adotada na comparação foi na proposta de política de segurança da informação para instituições de ensino SOCIESC, desenvolvido por Francini Reitz Spanceski (SPANCESKI, 2004). A segunda PSI em comparação escolhida foi à política de segurança da informação do SENAC São Paulo (SENAC). Os resultados estão apresentados na Figura 8.

Figura 8 – Demonstrativo comparativo entre duas políticas.



Fonte: Elaborada pelo autor.

Após se verificar o alinhamento (ou não) dos 133 itens constantes da NBR ISO/IEC 27002:2005 entre ambas às políticas, se observou que a política do SENAC apresenta 96 controladores aderentes à norma; 26 que não aderentes e 11 controladores não se aplicavam à política respectiva. Por sua vez, o levantamento e comparação realizado no caso da SOCIESC apresentou 62 controladores aderentes à norma; 41 não aderentes e 30 não se aplicavam à política. Isso mostra que há diferentes graus de maturidade[2] com relação às políticas de segurança entre organizações distintas: a política do SENAC parece estar melhor preparada para reações ou pro ações defensivas de segurança, em comparação à política da SOCIESC.

3.2 Estudo de Caso

A pesquisa foi realizada no Campus IV da Universidade Federal da Paraíba, que fica situado no litoral norte, mais especificamente na cidade de Mamanguape e Rio Tinto. Nesse local, não existe um normativo geral vinculado à segurança da informação, e, portanto, as vulnerabilidades são tratadas praticamente de forma pontual – daí a relevância deste trabalho.

[2] Maturidade representa, neste estudo, o grau de alinhamento com os controladores (aspectos) propostos pela norma ABNT 27002. Quanto mais alinhado, maior o nível de maturidade.

3.2.1 A Organização: Histórico e Características

O Campus IV faz parte da Universidade Federal da Paraíba (UFPB), ex-Universidade da Paraíba, criada pela Lei Estadual nº. 1.366, de 02 de dezembro de 1955, e federalizada pela Lei nº. 3.835 de 13 de dezembro de 1960 é uma instituição autárquica, de regime especial, de ensino pesquisa e extensão, vinculada ao Ministério de Educação, com sede e foro na cidade de João Pessoa e atuação no Estado da Paraíba.

A implantação do Centro de Ciências Aplicadas e Educação – Campus IV, nos Municípios de Rio Tinto e Mamanguape, ocorreu em Outubro de 2006 com o início de implantação de sete cursos: Ecologia, Ciências Contábeis, Secretariado Executivo, Ciências da Computação (LCC), Hotelaria, Matemática e Pedagogia. Em Maio de 2007 iniciam as atividades dos três Cursos restantes no planejamento inicial do Projeto de Implantação: Sistemas de Informação (SI), Antropologia e Design.

O campus IV é composto por 60 funcionários, cerca de 3400 discentes e 157 docentes divididos em 8 departamentos: Departamento de Ciências Exatas (DCE), Departamento de Ciências Sociais (DCS), Departamento de Ciências Sociais Aplicadas (DCSA), Departamento de Design (DDesign), Departamento de Educação (DED), Departamento de Engenharia e Meio Ambiente (DEMA), Departamento de Hotelaria e Gastronomia (DHG) e Departamento de Letras (DL). O mesmo conta com 28 laboratórios, distribuídos da seguinte maneira: 8 para Ecologia; 3 para Design; 1 para Ciências Contábeis; 1 para Antropologia; 1 para Matemática; 1 para Hotelaria; 5 para SI e LCC; 1 para Secretariado Executivo; 1 para Pedagogia; 1 para Letras e 5 laboratórios de informática aberto a todos os cursos.

3.2.2 Segurança da Informação do Campus IV

Conforme entrevista com o principal responsável pela segurança da informação do Campus IV, em 2015 se espera um maior número de problemas relacionados com segurança da informação, porem existem algumas medidas de segurança em uso, como:

- Assinatura digital;
- Autorização certificadora;
- Capacitação e treinamento;
- Certificação digital;
- Controle de conteúdo;

- Criptografia;
- *Firewall;*
- Monitoração de log;
- Prevenção contra pirataria;
- Procedimentos formalizados;
- Segurança em acesso remoto;
- Segurança em internet;
- Sistemas de *backup*;
- Termo de responsabilidade;
- Câmeras de segurança.

Outras medidas como melhor capacitação da equipe técnica, controle de conteúdo, implementação de firewall e câmeras de segurança foram implantas em 2014. Não obstante, os principais obstáculos para a implementação das melhorias é a falta de apoio especializado e a falta de ferramentas (equipamento adequado).

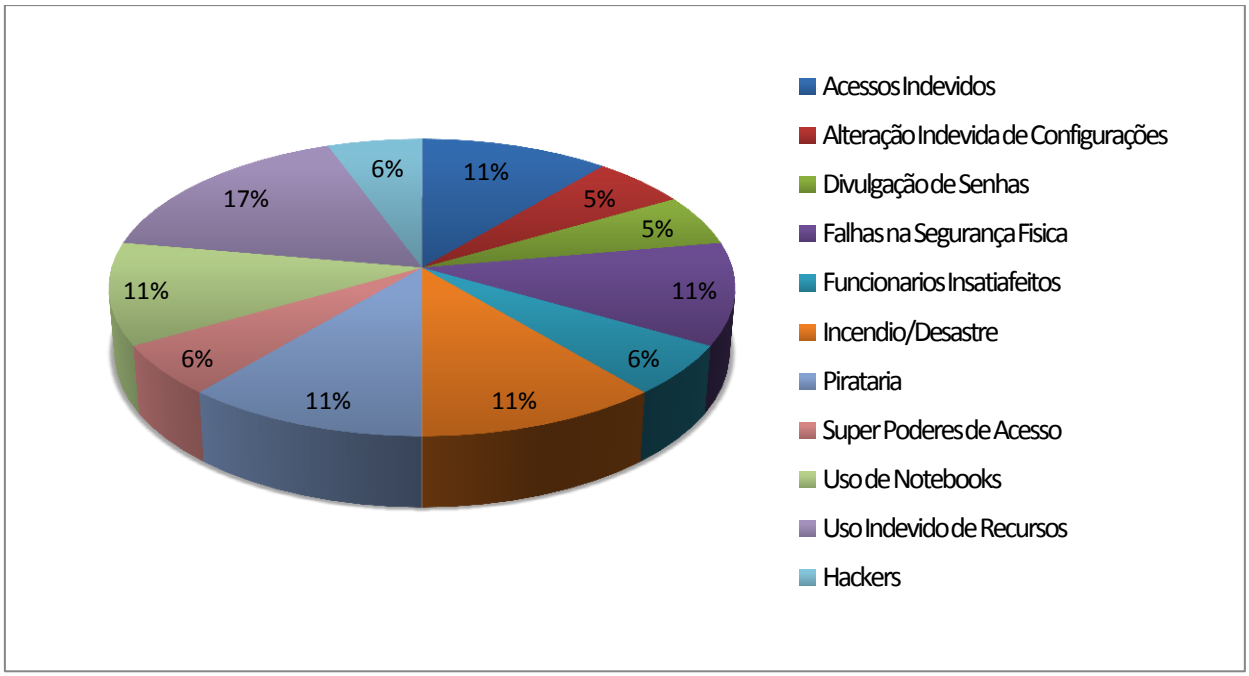
A internet no campus IV tem seu uso liberado para todos os níveis de usuários (funcionários, docentes e discentes) sem limitações; a mesma é usada para diversas aplicações, como por exemplo: biblioteca, consultas a banco de dados, divulgação de documentos e informativos, funções administrativas, *HelpDesk* e etc. O uso corporativo da internet é através da rede da organização; normalmente é utilizada para uso do correio eletrônico, acesso a páginas da organização na *web*, compras via internet, internet *banking* e utilização do SERPRO.

Apesar de aparentemente existirem regras tácitas que estabelecem diretrizes sobre a segurança da informação do campus IV, não se verificou sua aplicabilidade tendo como princípios os normativos que fundamentam este trabalho.

3.2.3 Principais Ameaças e Falhas de Segurança

Segundo o levantamento feito, foi constatado que as principais ameaças à segurança da informação no Campus IV partiram tanto do âmbito interno quanto externo, como mostra a Figura 9.

Figura 9 – Principais ameaças à segurança da informação.



Fonte: Elaborada pelo autor.

O Campus IV sofreu alguns ataques nos últimos seis meses, grande parte das vezes os responsáveis foram *hackers*; porém, também houve falhas internas. Não existe nenhum tipo de plano de continuidade no caso de falhas de segurança: a única providência adotada é a de correção dos problemas.

3.2.4 Principais ativos da organização

Através da pesquisa feita e do questionário aplicado ao principal responsável pela segurança da informação do campus IV, notou-se que os principais ativos da organização seriam todo aquele equipamento ligado à rede, ou seja, equipamentos como computadores, switch, roteadores, impressoras e etc. Esses itens que fazem parte da infraestrutura física da organização precisam tanto da proteção contra ameaças virtuais (*hackers*, vírus), quanto da proteção contra ameaças físicas (furtos, vandalismo), como também de proteção para ameaças externas e do meio ambiente (incêndio, água).

3.3 Conclusão do Capítulo

Este capítulo realizou como exercício prático, uma análise comparativa entre duas políticas de segurança disponíveis na internet; essas políticas tiveram como parâmetro a NBR ISO/IEC 27002:2005 - Técnicas de segurança – Código de prática para gestão da segurança

da informação. Em complemento e como estudo de caso, o capítulo abordou um pouco sobre o Campus IV - Rio Tinto, sua história e características principais; evidenciando a necessidade por uma PSI.

No próximo capítulo, serão expostos alguns princípios que serão demandados pela PSI no Campus IV; todavia, é no Apêndice II que se encontra a contribuição completa com as diretrizes fundamentadas com o padrão NBR 27002.

4 PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Para a elaboração desta política de segurança, foram utilizados alguns princípios citados no referencial teórico, a NBR ISO/IEC 27002:2005, informações a respeito do campus IV e instituição geral da qual ele faz parte, além das melhores praticas observadas em políticas disponíveis na internet.

No Apêndice II se apresenta, como contribuição, a política de segurança da informação para o campus IV da UFPB contendo regras que devem ser seguidas e conhecidas por todos que fazem parte da instituição. A razão de ser incluída no Apêndice II foi para que o leitor não desviasse dos pontos fundamentais que uma PSI precisa ter – o exercício desenvolvido inclui, de forma detalhada, no texto contributivo mencionado.

Dessa forma, algumas condições são consideradas primordiais em qualquer política, estão presentes na contribuição e devem ser aplicadas a todos os usuários dos recursos de TI da organização, essas condições são:

I. Uso de Computadores e Internet

- O acesso à internet deve ser especificamente limitado às atividades de suporte direto de negócios oficiais da organização.
- Além do acesso para suporte de tarefas especificamente relacionadas ao trabalho, a internet na organização pode ser usada para educação e pesquisa.
- Se algum usuário tiver dúvidas sobre o que é aceito ou não, ele deve consultar o seu responsável.

II. Uso inapropriado de Computadores e Internet

- A Internet não deve ser utilizada para fins ilegais ou ilícitos. Um exemplo disto constitui o compartilhamento de conteúdo violento, ameaças, fraudes, pornografias, matérias de conteúdo obsceno ou ilícitos.
- O e-mail da organização e os serviços de mensagem devem ser utilizados somente para negócios que se referem a mesma. Esses serviços não devem ser utilizados para ameaçar, intimidar ou perturbar pessoas.
- A Internet não deve ser utilizada para acesso privado, diversão ou qualquer outra atividade não relacionada à organização no horário de expediente.
- A Internet não deve ser utilizada para fins comerciais ou políticos.

- Funcionários não devem usar a rede da empresa para ganho através de venda de acesso à *login*. O acesso à Internet da Companhia não deve ser utilizado para lucro de pessoas não autorizadas.
- Usuários não devem tentar burlar ou subverter medidas de seguranças realizadas pela rede da organização ou por qualquer outro sistema conectado à internet da mesma.
- Funcionários não devem usar a internet para interceptar informações exceto se autorizadas para fins de administração da rede.
- Usuários da organização não devem fazer uso de cópias ilegais de matérias privados, salvar ou transmitir tais matérias.

III. Segurança no uso de Computadores e Internet

- Usuários que identificarem qualquer atividade suspeita devem contatar imediatamente o Departamento de Segurança de TI.
- Usuários não devem dar suas senhas a outras pessoas ou usuários, nem usar o sistema fazendo uso da senha outrem.
- Todo e qualquer uso de TI está sujeito à monitorização pela Segurança de TI.
- O acesso aos recursos da rede da organização deve ser revogado se qualquer usuário for identificado como risco de segurança ou demostrar histórico de problemas com segurança.

IV. Uso da Internet e E-mail

- Todos os funcionários da organização devem prezar para que a comunicação por e-mail ou mensagem seja feita de forma profissional. O uso de linguagem vulgar ou obscena estão proibidos.
- Usuários não devem prover informações pessoais por e-mail ou mensagem sem aprovação prévia da diretoria.
- Os usuários devem se certificar que estão enviando e-mails especificamente para seu público-alvo. E-mails e mensagens para grandes grupos, com lista de distribuição e arquivos grandes devem ser evitados.
- A privacidade dos e-mails não pode ser resguardada. Devido à isso, por medidas de segurança, mensagens transmitidas pelo e-mail da organização ou por sistemas pertencem à mesma, estão sujeitos a inspeção.

V. Penalidades

- Qualquer usuário que violar uma política ou qualquer lei local, estadual ou federal usando a rede da organização, estará sujeito a perda de acesso à rede e a qualquer outra punição considerada apropriada, podendo incluir demissão ou processo criminal ou civil.

VI. Termo de Compromisso

- Todos os envolvidos da organização devem assinar o termo de compromisso concordando com a política de segurança e seus itens relacionados. Devem entender também que qualquer violação dessa política é considerado anti-ético e constitui uma ação criminosa. Se vier a cometer qualquer violação, o acesso pode ser negado e ações disciplinares ou ações legais apropriadas serão tomadas.

4.1 O Padrão NBR 27002 em Análise: Conformidade da Proposta

Para demonstrar a conformidade da política proposta em relação aos 133 itens da NBR ISO/IEC 27002:2005, os critérios pensados para pontuar o alinhamento dos fatores de controle foram os seguintes:

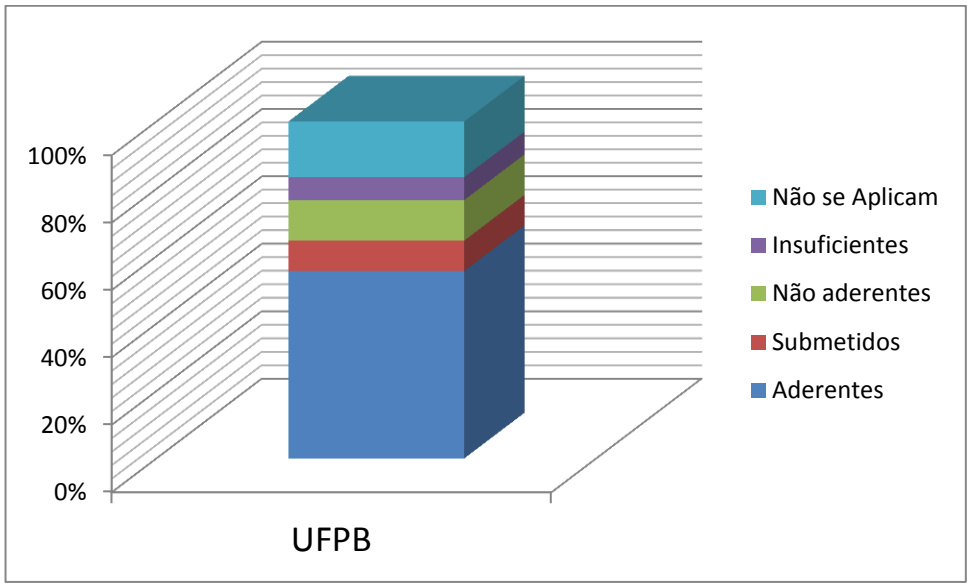
a) S – está em conformidade com a norma;
b) S1 – está submetido a uma instancia superior;
c) N – não está em conformidade com a norma;
d) N1 – insuficiência de informações;
e) N/A – não se aplica à PSI.

No Apêndice I é apresentado os resultados em relação aos itens da política que estão em aderência com a norma.

O pontuador S1 refere-se ao item se fazer presente nas Leis, normas e regulamentos da Universidade Federal da Paraíba (ex.: Estatuto da UFPB), ou em alguma outra instancia superior.

No pontuador N1, as informações disponíveis e/ou levantadas na instituição foram insuficientes para a elaboração ou melhoria de um ou mais tópicos/itens na política. Por isso, esses itens acabaram não ficando em conformidade com a norma.

Figura 10 – Demonstração da conformidade da política proposta com a ISO/IEC 27002.



Fonte: Elaborada pelo autor.

A Figura 10 apresenta, através de gráfico, o alinhamento pretendido; na política proposta, dos 133 itens pontuados, 74 são aderentes a ISO; 16 não são; 22 não se aplicam a PSI; 12 estão submetidos a uma instancia superior; e em 9 tiveram insuficiência de informação.

Apesar de algumas limitações e dificuldades na sua elaboração, a política proposta atente à boa parte dos requisitos de segurança da informação do campus IV, em sua maior parte, em conformidade com a NBR ISO/IEC 27002:2005.

4.2 Conclusão do Capítulo

Este capítulo expôs os subsídios fundamentais para uma proposta de política de segurança da informação para o campus IV da UFPB, visando à criação de regras a serem seguidas por todos os envolvidos da instituição.

A contribuição elaborada buscou a simplicidade, sendo, ao mesmo tempo, efetiva o suficiente para abranger boa parte das necessidades de segurança da informação da instituição, mostrando o papel de todos e especificando os papeis designados para funcionários e alunos.

5 CONSIDERAÇOES FINAIS

Este trabalhou fundamentou-se na importância da segurança da informação para qualquer organização, seja ela de pequeno, médio ou grande porte. Ativos organizacionais devem ser protegidos adequadamente, e por isso uma política de segurança da informação é tão importante.

O principal objetivo deste trabalho foi apresentar uma proposta de política de segurança da informação voltada para o campus IV da UFPB que se encontra no Apêndice II.

Foi realizada revisão bibliográfica apresentando conceitos e alguns modelos de políticas existentes; também foram considerados os fatores-chave para se elaborar uma PSI que seja eficaz. Optou-se pela família NBR 27000 para direcionar o trabalho como modelo, por estar sedimentado na literatura, ser uma norma internacional de uso recorrente por organizações.

Em sequência, se construiu uma lista de verificação com os principais elementos de controle sugeridos pela NBR 27002, para permitir a comparação de duas ou mais políticas de segurança disponíveis na internet para fins de verificação de aderência ou não ao modelo proposto. Na comparação, sobressaiu-se o SENAC como mais aderente e aparente nível de maturidade em segurança da informação.

A mesma comparação utilizando a lista de verificação com os principais elementos de controle sugeridos pela NBR 27002 foi realizada com a política de segurança da informação proposta neste trabalho, porém, foram utilizados alguns critérios a mais para pontuar a lista. Na comparação, a proposta apresentada como contribuição para o campus IV se mostrou bastante aderente aos elementos da NBR 27002, deixando evidente a sua prestabilidade.

Quanto às limitações do trabalho, estas dizem respeito, entre outras:

- Ao método adotado – estudo de caso, que embora permita aprofundar o conhecimento e estimular a compreensão sobre um determinado assunto, a sua flexibilidade conceitual permitiu a exposição de somente algumas características do objeto, devido à dificuldade de obtenção de dados relativos aos ativos informacionais tangíveis e intangíveis respectivos.
- À técnica de coleta de dados através de entrevista pessoal suportada por roteiro de perguntas apresentou restrições decorrentes pela disposição e desprendimento dos entrevistados em responder às questões com sinceridade, haja vista o assunto abordado ser delicado.

- À própria natureza do estudo – exploratório, que limitou o estudo a apreender conceitos e práticas adotadas.

Recomenda-se, para novos estudos, o aprofundamento no levantamento de ativos informacionais no Campus IV, bem como comparar a novel PSI em fase de aprovação na UFPB segundo o nível de maturidade com relação aos normativos da família ISO 27000.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Dimitri. “Melhores Práticas para Classificar as Informações”. Módulo e-Security Magazine. São Paulo, agosto 2001. Disponível em: <http://www.modulo.com.br>. Acessado em 10 de dezembro de 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27005: Tecnologia da informação — técnicas de segurança — gestão de riscos de segurança da informação. Rio de Janeiro, mar. 2008.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISSO/IEC 27002:2005 tecnologia da informação - técnicas de segurança - código de pratica para gestão da informação. Rio de janeiro: 2005, Disponível em: <http://search.4shared.com/postDownload/M0vePGU6/ISO-IEC_27002-2005.html>. Acessado em 02 de fevereiro de 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos: ABNT NBR ISO/IEC 27001:2006. 1a. ed. Rio de Janeiro, 2006.

BRASIL. DECRETO No 3.505 DE 13 DE JUNHO DE 2000: Institui a Política de segurança da informação nos Órgãos da Administração Pública Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acessado em 02 de fevereiro de 2014.

CAMPOS, A. SISTEMAS DE SEGURANÇA DA INFORMAÇÃO. 2 ed. Florianopolis: Visual Books, 2007.

CERVO, A. L. (2007). Metodologia Científica. (6 ed.). São Paulo: Pearson Prentice Hall.

CORRÊA, N C C.O uso indevido da Engenharia Social na Informática. 2006. 61 f. Monografia (Graduação em Sistemas de Informação) – Centro Universitário do Maranhão – UniCEUMA, São Luís, 2006.

DANTAS, M. SEGURANÇA DA INFORMAÇÃO: UMA ABORDAGEM FOCADA EM GESTÃO DE RISCOS. 1 ed. Olinda: Livro rápido, 2011.

DELLA VALLE, James; ULBRICH, Henrique César. Universidade Hacker. 6. ed. São Paulo: Digerati Books, 2009.

DIAS, S. Q. (2000)., (p. 42). Dicionário do Aurélio Online - Versão Beta. (2014). Disponível em Dicionário do Aurélio: <http://www.dicionariodoaurelio.com/Política.html>. Acesso em 15 de maio de 2014.

DODT, Claudio. Transformando sua política de segurança da informação em um ativo estratégico. GRC – Governança, riscos e conformidade. Disponível em: <http://claudiododt.com/category/seguranca-da-informacao/política-de-seguranca-da informacao/>. Acesso em 20 de fevereiro de 2014.

ESET. Pesquisa a respeito de Segurança da informação, 2013. Disponível em: <http://www.eset.com.br>. Acesso em: 03 março de 2014.

FERREIRA, Fernando Nicolau Freitas. Segurança da Informação. Rio de Janeiro: Ciência Moderna, 2003.

FERREIRA, Milton. O que vem ser segurança da informação. Disponível em: <http://www.apinfo.com/artigo81.htm16>. Acesso em 20 de fevereiro de 2014.

FONTES, E. Políticas e Normas para a segurança da informação. Rio de Janeiro, Brasport, 2012.

FREITAS,F;ARAUJO, M. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO: Guia pratico para elaboração e implementação. 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008.

FURTADO, E M. ABNT NBR ISO/IEC 27002:2005: um norte para a gestão de segurança da informação na Organização: Auditoria de sistemas e de segurança. 2011. 88 f.; Ilustrado; 25 cm. Monografia (especialização) – Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2011.

GHAYATRI, J., & PRIYA, E. M. (2013). Software Quality Models: a comparative study. International Journal of Advanced Research in Computer Science and Electronics Engineering (IJARCSEE, 2013).

GOMES, E. G. (2009). Gestão por Resultados e eficiência na Administração Pública:. FGV/EAESP, Pós graduação em Administração Pública e Governo, São Paulo.

HRDLICKA, H. (2011). A Internacionalização das empresas brasileiras. S.Paulo: Editora Atlas.

IBGC. (2009). Código das Melhores Práticas de Governança Corporativa. In: I. B. Corporativa. S.Paulo: IBGC.

IBGE. (2012). Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil: TIC Domicílios e TIC Empresas 2011. São Paulo: Comitê Gestor da Internet no Brasil.

INSTRUÇÃO NORMATIVA GSI Nº 01, 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.planalto.gov.br/ccivil_03/decreto/D3505.htm>. Acessado em 02 de fevereiro de 2014.

IPHAN. Política de Segurança da Informação do IPHAN. Ministério da Cultura. Instituto do Patrimônio Histórico e Artístico, 2013. Disponível em: <http://www.iphan.gov.br>. Acesso em 20 de julho 2014.

IPCC. (2006). IPCC Good Practice Guidance and Uncertainty Management in National Greenhouse Gas Inventories. In: IPCC, IPCC Good Practice Guidance and Uncertainty Management in National Greenhouse Gas Inventories.

JÂNIO, Fábio. Segurança da informação (Classificação da informação). Disponível em: <http://fabiojanio.com/?p=400>. Acesso em 20 de fevereiro de 2014.

LUCKY, E. O.-I., & OLESUN, A. I. (July de 2012). Determinants of business success: trust or business policy? (I. R. Journal, Ed.) Journal of Arts, Science & Commerce, 3, pp. 37-42.

MALHOTRA, N. Pesquisa de Marketing: uma orientação aplicada. 3 ed. Porto Alegre: Bookman, 2001.

MARCONI, M. A. & LAKATOS, E. M. Fundamentos de Metodologia Científica. 6.ed. São Paulo: Atlas, 2007.

MODULO SECURITY 9 a. Pesquisa Nacional de Segurança da Informação, 2003. Disponível em: <http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf>. Acessado em 20 de fevereiro de 2014.

MONTEIRO, I. L. C.O. Proposta de uma guia para elaboração de políticas de segurança da informação e comunicações em órgãos da administração pública federal. 2009. 67f. Monografia (especialização) - Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2009.

MOREIRA, Nilton Stringasci. Segurança Mínima. Rio de Janeiro: Axcel Books, 2001.

NASCIMENTO NETO, E. F., & REIS, L. C. (2013). Risk IT based on COBIT: Uma visão sistêmica para a auditoria de TI. Disponível em CNASI - Congresso de segurança da Informação, Auditoria e Governança TIC: <http://www.cnasi.com.br/risk-it-based-on-cobit-uma-visao-sistemica-para-a-auditoria-de-ti>. Acesso em 15 de maio de 2014.

OLIVEIRA, Wilson José de. Segurança da Informação. Florianópolis:Visual Books, Maio, 2001.

PMES NO BRASIL ADMITEM ATAQUES À SEGURANÇA DA INFORMAÇÃO E ABRAÇAM O SOFTWARE LIVRE. UOL (2012). Disponível em: <http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32642&sid=16>. Acesso em 20 de fevereiro de 2014.

RIBEIRO NETO, G. L. (1999). Os impactos da tecnologia de informação nas organizações: uma visão política. Revista Um, 5, 95-101.

ROGERS, D. (2003). Política. In: C. COOPER, & C. ARGYRIS, Dicionário enciclopédico de Administração (L. M. ESTEVES, , & C. A. RIMOLI,, Trads., p. 1455). São Paulo, S.Paulo: Editora Atlas.

SEGURANÇA DA INFORMAÇÃO. Disponível em: <http://www.itforum365.com.br/>. Acesso em 20 de fevereiro de 2014.

SENAC. PSI - Política de Segurança da Informação. Documento de Diretrizes e Normas Administrativas. Senac, Fls: 3 / 24. Versão: 1.0. Disponível em:

<http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf>. Acesso em 15 de maio 2014.

SILVA, SÉRGIO CAMPOS DA. Verificação do grau de adequação da segurança física e do ambiente dos laboratórios de informática do CCAE conforme a Norma NBR ISO/IEC 27002/ Sérgio Campos da Silva. – Rio Tinto: [s.n.], 2013.

SOOMRO, T.R. and M. HESSON, 2012. Supporting best practices and standards for information technology infrastructure library. J. Comput. Sci., 8: 272-276.

SPANCESKI, F. R. Política de Segurança da informação – Desenvolvimento de um modelo voltado para instituições de ensino. 2004. 102 f. Trabalho de conclusão de curso (Bacharelado) - Instituto Superior Tupy, Joinville, 2004.

STEINER, G. A., & MINER, J. B. (1981). Política e Estrategia Administrativa. São Paulo: Editora Interciência Ltda. - EPUSP.

TADEU, L.S. Políticas de Segurança da Informação: Recomendações para Redução de Riscos e Vulnerabilidades Humanas. 2006. 73 f. Monografia (licenciatura) - Instituto de Ciências Exatas, Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2006.

TEIXEIRA, A. (2004). O Uso das Novas Tecnologias de Informação e Comunicação (TIC) e a Transparência na Gestão Pública Municipal no Ceará. Fundação Konrad Adenauer. Fortaleza: Fundação Konrad Adenauer.

VERN, R., & DUBEY, K. S. (2013). Survey on Evaluation of the Quality of Software System by Using Fuzzy Logic Approach. (G. J. (USA), Ed.) Global Journal of Computer Science and Technology, Software & Data Engineering, 13(1), pp. 14-22.

VINHAS, L. P., MANSO, F. V., & DA SILVA, M. C. (2012). As tecnologias da informação e comunicação como ferramentas de modernização da gestão do Rio de Janeiro. V Congresso CONSAD de Administração Pública, (p. 31). Brasília.

WADLOW, Tomas A. Segurança de Redes : Projeto e gerenciamento de redes seguras. Rio de Janeiro : Campus, 2000. Tradução: Fábio Freitas da Silva

WAGNER, S. (2006). A Literature Survey of the Quality Economics of Defect-Detection Techniques. ISESE 2006 - International Symposium on Empirical Software Engineering (pp. 194-203). Rio de Janeiro: ACM Digital Library.

WIES, R. (1994). Policy definition and classification: aspects, criteria and examples. IFIP/IEEE International Workshop on distributed systems: Operations & Management. Toulouse - França: IEEE.

WIES, R. (1994). Policy Definition and Classification: Aspects, Criteria, and Examples. IFIP/IEEE International Workshop on Distributed Systems: Operations & Management (pp. 1-12). Toulose: University of Munich, Department of Computer Science.

YIN, Robert K. Estudo de caso – planejamento e métodos. (2Ed.). Porto Alegre: Bookman. 2001.

APÊNDICE I – LISTA DE CONTROLES - ISO/IEC 27002:2005

CONTROLES	CONFORMIDADES		
	SOCIESC	SENAC	UFPB
1. Política de segurança			
1.1. Política de segurança da informação			
1.1.1. Documento da política de segurança da informação	**S**	**S**	**S**
1.1.2. Análise crítica da política de segurança da informação	**S**	**S**	**S**
2. Organizando a segurança da informação			
2.1. Infraestrutura da segurança da informação			
2.1.1. Comprometimento da direção com a segurança da informação	**N**	**S**	**S1**
2.1.2. Coordenação da segurança da informação	**S**	**S**	**S**
2.1.3. Atribuição de responsabilidade para a segurança da informação	**S**	**S**	**S**
2.1.4. Processo de autorização para os recursos de processamento da informação	**S**	**N**	**S**
2.1.5. Acordos de confidencialidade	**S**	**S**	**S**
2.1.6. Contato com autoridades	**N/A**	**N**	**N**
2.1.7. Contato com grupos especiais	**N/A**	**N**	**N/A**
2.1.8. Análise critica independente de segurança da informação	**S**	**S**	**S**
2.2. Partes externas			
2.2.1. Identificação dos riscos relacionados com partes externas	**S**	**S**	**S**
2.2.2. Identificando a segurança da informação quando tratando os clientes	**N/A**	**S**	**N/A**
2.2.3. Identificando segurança da informação nos acordos com terceiros	**N/A**	**N**	**N1**
3. Gestão de ativos			
3.1. Responsabilidade pelos ativos			
3.1.1. Inventário dos ativos	**S**	**S**	**S**
3.1.2. Proprietário dos ativos	**N**	**S**	**N**
3.1.3. Uso aceitável dos ativos	**N**	**S**	**S**
3.2. Classificação da informação			
3.2.1. Recomendações para classificação	**S**	**S**	**S**
3.2.2. Rótulos e tratamento da informação	**S**	**S**	**S**
4. Segurança em recursos humanos			
4.1. Antes da contratação			
4.1.1. Papéis e responsabilidades	**N/A**	**S**	**S1**
4.1.2. Seleção	**N/A**	**N**	**S1**
4.1.3. Termos e condições de contratação	**N/A**	**S**	**S1**
4.2. Durante a contratação			
4.2.1. Responsabilidades da direção	**S**	**S**	**S**
4.2.2. Conscientização, educação e treinamento em segurança da informação	**S**	**S**	**S**
4.2.3. Processo disciplinar	**N**	**S**	**S1**
4.3. Encerramento ou mudança da contratação			
4.3.1. Encerramento de atividades	**N**	**S**	**N**
4.3.2. Devolução de ativos	**N/A**	**N**	**N/A**
4.3.3. Retirada de direitos de acesso	**S**	**S**	**S**
5. Segurança física e do ambiente			
5.1. Áreas seguras			
5.1.1. Perímetro de segurança física	**S**	**S**	**S**
5.1.2. Controles de entrada física	**S**	**S**	**S**

5.1.3. Segurança em escritórios, salas e instalações	**S**	**S**	**S**
5.1.4. Proteção contra ameaças externas e do meio ambiente	**N**	**S**	**S**
5.1.5. Trabalho em áreas seguras	**S**	**S**	**S**
5.1.6. Acesso do público, áreas de entrega e de carregamento	**N/A**	**N/A**	**N/A**
5.2. Segurança de equipamentos			
5.2.1. Instalação e proteção do equipamento	**S**	**S**	**S**
5.2.2. Utilidades	**S**	**S**	**S**
5.2.3. Segurança do cabeamento	**N**	**N**	**N**
5.2.4. Manutenção dos equipamentos	**S**	**S**	**S**
5.2.5. Segurança de equipamentos fora das dependências da organização	**N**	**S**	**N**
5.2.6. Reutilização e alimentação segura de equipamentos	**N**	**S**	**N1**
5.2.7. Remoção de propriedade	**S**	**S**	**S**
6. Gerenciamento das operações e comunicações			
6.1. Procedimentos e responsabilidades operacionais			
6.1.1. Documentação dos procedimentos de operação	**N**	**S**	**N**
6.1.2. Gestão de mudanças	**N**	**S**	**S**
6.1.3. Segregação de funções	**N/A**	**S**	**N/A**
6.1.4. Separação dos recursos de desenvolvimento, teste e de produção	**N/A**	**N**	**N/A**
6.2. Gerenciamento de serviços terceirizados			
6.2.1. Entrega de serviços	**N/A**	**N/A**	**N/A**
6.2.2. Monitoramento e análise crítica de serviços terceirizados	**N/A**	**N/A**	**N/A**
6.2.3. Gerenciamento de mudanças para serviços terceirizados	**N/A**	**N/A**	**N/A**
6.3. Planejamento e aceitação dos sistemas			
6.3.1. Gestão de capacidade	**N**	**N**	**N**
6.3.2. Aceitação de sistemas	**N**	**N**	**N**
6.4. Proteção contra códigos maliciosos e códigos móveis			
6.4.1. Controle contra códigos maliciosos	**S**	**S**	**S**
6.4.2. Controle contra códigos móveis	**N/A**	**N/A**	**N/A**
6.5. Cópias de segurança			
6.5.1. Cópias de segurança das informações	**S**	**S**	**S**
6.6. Gerenciamento da segurança em redes			
6.6.1. Controles de redes	**S**	**S**	**S**
6.6.2. Segurança dos serviços de rede	**S**	**S**	**S**
6.7. Manuseio de mídias			
6.7.1. Gerenciamento de mídias removíveis	**S**	**S**	**S**
6.7.2. Descarte de mídias	**N**	**S**	**N1**
6.7.3. Procedimentos para tratamento de informações	**S**	**S**	**S**
6.7.4. Segurança da documentação dos sistemas	**S**	**S**	**S**
6.8. Troca de informações			
6.8.1. Política e procedimentos para troca de informações	**N**	**S**	**S**
6.8.2. Acordos para troca de informações	**N**	**S**	**S1**
6.8.3. Mídias em trânsito	**S**	**S**	**S**
6.8.4. Mensagens eletrônicas	**S**	**S**	**S**
6.8.5. Sistema de informações do negócio	**S**	**S**	**S**
6.9. Serviços de comercio eletrônico			
6.9.1. Comercio eletrônico	**N**	**S**	**N**
6.9.2. Transações on-line	**S**	**S**	**S**
6.9.3. Informações publicamente disponíveis	**S**	**S**	**S**

6.10. Monitoramento			
6.10.1. Registros de auditoria	**N**	**S**	**S**
6.10.2. Monitoramento de uso do sistema	**S**	**S**	**S**
6.10.3. Proteção das informações dos registros (logs)	**S**	**S**	**S**
6.10.4. Registros (log) de administrador e operador	**S**	**S**	**S**
6.10.5. Registros (logs) de falhas	**S**	**S**	**S**
6.10.6. Sincronização dos relógios	**N**	**S**	**S1**
7. Controle de acesso			
7.1. Requisitos de negócio para controle de acesso			
7.1.1. Política de controle de acesso	**S**	**S**	**S**
7.2. Gerenciamento de acesso do usuário			
7.2.1. Registro de usuário	**S**	**S**	**S**
7.2.2. Gerenciamento de privilégios	**S**	**S**	**S**
7.2.3. Gerenciamento de senha do usuário	**S**	**S**	**S**
7.2.4. Análise crítica dos direitos de acesso de usuário	**S**	**S**	**S**
7.3. Responsabilidades dos usuários			
7.3.1. Uso de senhas	**S**	**S**	**S**
7.3.2. Equipamento de usuário sem monitoração	**N**	**S**	**S**
7.3.3. Política de mesa limpa e tela limpa	**S**	**N**	**S**
7.4. Controle de acesso à rede			
7.4.1. Política de uso dos serviços de rede	**N**	**N**	**N**
7.4.2. Autenticação para conexão externa do usuário	**N**	**N**	**N1**
7.4.3. Identificação dos equipamentos em rede	**S**	**S**	**S**
7.4.4. Proteção e configuração de portas de diagnostico remota	**S**	**N**	**S**
7.4.5. Segregação de redes	**N**	**S**	**N1**
7.4.6. Controle de conexão de rede	**N**	**S**	**S**
7.4.7. Controle de roteamento de redes	**N/A**	**N**	**N1**
7.5. Controle de acesso ao sistema operacional			
7.5.1. Procedimentos seguros de entrada no sistema (log-on)	**N/A**	**N/A**	**S**
7.5.2. Identificação e autenticação de usuário	**S**	**S**	**S**
7.5.3. Sistema de gerenciamento de senha	**S**	**S**	**S**
7.5.4. Uso de utilitários de sistema	**S**	**S**	**S**
7.5.5. Desconexão de terminal por inatividade	**S**	**N**	**N/A**
7.5.6. Limitação de horário de conexão	**S**	**N**	**N/A**
7.6. Controle de acesso à aplicação e à informação			
7.6.1. Restrição de acesso à informação	**S**	**S**	**S**
7.6.2. Isolamento de sistemas sensíveis	**N**	**N/A**	**S**
7.7. Computação móvel e trabalho remoto			
7.7.1. Computação e comunicação móvel	**N**	**S**	**N**
7.7.2. Trabalho remoto	**N**	**N/A**	**N1**
8. Aquisição, desenvolvimento e manutenção de sistemas de informação			
8.1. Requisitos de segurança de sistemas de informação			
8.1.1. Análise e especificação dos requisitos de segurança	**S**	**S**	**S**
Processamento correto de aplicações			
8.1.2. Validação dos dados de entrada	**N**	**N**	**N**
8.1.3. Controle de processamento interno	**S**	**S**	**S**
8.1.4. Integridade de mensagens	**S**	**N**	**S**
8.1.5. Validação de dados de saída	**N**	**N**	**N**

8.2. Controles criptográficos			
8.2.1. Política para o uso de controles criptográficos	**N**	**N**	**N1**
8.2.2. Gerenciamento de chaves	**N**	**N**	**S**
8.3. Segurança dos arquivos do sistema			
8.3.1. Controle de software operacional	**N/A**	**S**	**S**
8.3.2. Proteção dos dados para teste de sistema	**N/A**	**N/A**	**N/A**
8.3.3. Controle de acesso ao código fonte de programa	**N/A**	**N/A**	**N/A**
8.4. Segurança em processos de desenvolvimento e de suporte			
8.4.1. Procedimentos para controle de mudanças	**N**	**S**	**S1**
8.4.2. Análise crítica técnica das aplicações após mudanças no S.O.	**N/A**	**S**	**N/A**
8.4.3. Restrições sobre mudanças em pacotes de software	**N**	**N**	**N**
8.4.4. Vazamento de informações	**S**	**S**	**S**
8.4.5. Desenvolvimento terceirizado de software	**N**	**N/A**	**N/A**
8.5. Gestão de vulnerabilidade			
8.5.1. Controle de vulnerabilidades técnicas	**N**	**N**	**N**
9. Gestão de incidentes de segurança da informação			
9.1. Notificação de fragilidades e eventos de segurança da informação			
9.1.1. Notificação de eventos de segurança da informação	**N**	**S**	**S**
9.1.2. Notificando fragilidades de segurança da informação	**N**	**S**	**S**
9.2. Gestão de incidentes de segurança da informação e melhoria			
9.2.1. Responsabilidades e procedimentos	**S**	**S**	**S**
9.2.2. Aprendendo com os incidentes de segurança da informação	**N**	**S**	**S**
9.2.3. Coleta de evidências	**N**	**S**	**N**
10. Gestão da continuidade do negócio			
10.1. Aspectos da gestão da continuidade do negócio			
10.1.1. Incluindo S.I. no processo de gestão de continuidade de negócio	**N/A**	**S**	**N/A**
10.1.2. Continuidade de negócio e análise/avaliação de risco	**N/A**	**S**	**N/A**
10.1.3. Desenvolvimento e implementação de planos de continuidade relativos à S.I.	**N/A**	**S**	**N/A**
10.1.4. Estrutura do plano de continuidade do negócio	**N/A**	**S**	**N/A**
10.1.5. Testes, manutenção e reavaliação dos planos de continuidade do negócio	**N/A**	**S**	**N/A**
11. Conformidade			
11.1. Conformidade com requisitos legais			
11.1.1. Identificação da legislação vigente	**N/A**	**S**	**S1**
11.1.2. Direitos de propriedade intelectual	**N/A**	**N**	**S1**
11.1.3. Proteção dos registros organizacionais	**N**	**S**	**S1**
11.1.4. Proteção de dados e privacidade da informação pessoal	**S**	**S**	**S**
11.1.5. Prevenção de mau uso de recursos de processamento da informação	**S**	**S**	**S**
11.1.6. Regulamentação de controles de criptografia	**N**	**N**	**N1**
11.2. Conformidade com normas e políticas de S.I. conf. Técnicas			
11.2.1. Conformidade com as políticas e normas de segurança da informação	**S**	**S**	**S**
11.2.2. Verificação da conformidade técnica	**S**	**S**	**S**
11.3. Considerações quanto à auditoria de sistemas de informação			
11.3.1. Controles de auditoria de sistemas de informação	**N/A**	**S**	**N/A**
11.3.2. Proteção de ferramentas de auditoria de Sistemas de Informação	**N/A**	**S**	**S1**

Fonte: Elaborada pelo autor.

APÊNDICE II – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Uma contribuição para o Campus IV

INTRODUÇÃO

Uma política de segurança voltada para o campus IV estabelece regras que deverão ser seguidas por todos os usuários que utilizam recursos de tecnologia de informação, de modo a compartilhar sua importância e conscientizar acerca da necessidade de se zelar pelos ativos informacionais da instituição.

Entende-se por usuários os funcionários (servidores e docentes), os alunos (discentes), e outras pessoas ou organizações externas que possam interagir com os sistemas informacionais do Campus IV.

Para a elaboração desta política de segurança, foram utilizadas além das melhores praticas de segurança citadas no referencial teórico, algumas informações como:

- A NBR ISO/IEC 27002:2005 - Técnicas de segurança – Código de prática para gestão da segurança da informação.
- O decreto nº. 3505 de 2000, que Institui a Política de Segurança da Informação nos Órgãos da Administração Pública Federal.
- A IN nº. 0001 de 2008 do GSI que disciplina a gestão de segurança da informação e comunicações na administração pública federal, direta e indireta.
- Informações sobre a segurança da informação do campus IV da UFPB.
- Consulta em políticas de segurança de outras organizações:
    - Política de Segurança da informação – Desenvolvimento de um modelo voltado para instituições de ensino SOCIESC;
    - Política de Segurança da Informação do SENAC – Documento de Diretrizes e Normas Administrativas;
    - Política de Segurança da Informação do IPHAN.

Esta política de segurança mostrará itens como estrutura de informática, estrutura física, penalidades e outros. A estrutura de informática possui tópicos como utilização da rede, identificação, correio eletrônico, uso e acesso a internet, servidor central, uso de computadores, controle de conta de usuário, uso de projetores e impressoras. A estrutura

física aborda controle de acesso, segurança ambiental, utilização dos laboratórios e política da mesa limpa e tela limpa. Em cada um desses tópicos serão criadas regras gerais, que podem ser aplicadas a todos; caso necessário, serão criadas regras especificas para funcionários e alunos.

1 Objetivos

Além de preservar as informações quanto à sua integridade, confidencialidade, disponibilidade e autenticidade; são objetivos desta política de segurança da informação:

- Garantir que os recursos de informática e a informação estarão sendo usados da maneira adequada.
- Estabelecer diretrizes que permitam a disponibilidade e utilização dos recursos de informática, da informação, serviços de rede, internet e telecomunicações.
- Designar, definir ou alterar papéis e responsabilidades de todos os responsáveis pela Segurança da Informação.
- Apoiar a implantação de iniciativas relativas à Segurança da Informação.
- Possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.
- Fornecer a todos a quem a política se direciona, informações suficientes para saber se os procedimentos descritos na política são aplicáveis a eles ou não, utilizando linguagem simples e de fácil entendimento.
- Assegurar que todos devem estar conscientes da importância dos procedimentos de segurança desta política, se necessário, devem receber instruções de como fazer uso correto das informações que nela estão descritas.
- Estabelecer que caso os procedimentos e normas contidos nesta política sejam violados, os infratores estarão passíveis de punições declaradas nesta política.

2 Estrutura de Informática

Na estrutura de informação serão abordados os seguintes tópicos:

- Utilização de Rede
- Identificação
- Correio Eletrônico
- Uso e Acesso a Internet
- Servidor Central
- Uso de Computadores

- Controle de Conta de Usuário
- Uso de Projetores e Impressoras

2.1 Utilização da Rede

Este tópico define normas de utilização da rede, que engloba: *login*, manutenção de arquivos no servidor e tentativas não autorizadas de acesso. Estes itens estarão sendo abordados para todos os usuários do sistema e da rede de computadores do campus IV.

2.1.1 Regras Gerais

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

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

C. O usuário que estiver utilizando a rede, ao se ausentar do seu local de trabalho, deverá fechar todos os programas em uso, evitando, desta maneira, o acesso por pessoas não autorizadas, se possível efetuar o *logout/logoff* da rede ou bloqueio do computador através de senha.

D. Qualquer material de natureza pornográfica, preconceituosa e racista não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede.

E. Qualquer tipo de software/aplicativo (jogos e outros tais) que não estejam previamente instalados ou não condizem com a organização não pode ser gravados ou instalados no computador local e/ou em qualquer outro diretório da rede;

F. Não é permitido criar e/ou remover arquivos que venham a comprometer o desempenho e funcionamento dos sistemas ou da rede.

G. É proibida a instalação ou remoção de softwares/aplicações na rede que não forem devidamente acompanhadas pelo departamento de T.I; é necessário autorização por escrito do responsável da área solicitante.

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

I. Quanto à utilização de equipamentos de informática particulares, computadores, tablets, impressoras, projetores entre outros, o campus IV não fornecerá acessórios, software ou suporte técnico para itens pessoais (que não pertencem a organização), incluindo assistência para recuperar perda de dados decorrentes de falha humana, ou pelo mau funcionamento do equipamento ou do software. Esses itens são de total responsabilidade dos seus donos e usuários.

J. O acesso a sistemas, como sistemas acadêmicos (ex.: MOODLE) ou sistemas do governo (ex.: SERPRO), deve ser controlado pela identificação do usuário e pelas senhas designadas para usuários autorizados; as senhas compartilhadas devem ser excepcionais e autorizadas pela equipe de T.I.

2.1.2 Regras para Funcionários

A. É obrigatório armazenar os arquivos inerentes à organização no banco de dados do servidor para garantir a cópia de segurança dos mesmos.

B. Quanto à utilização de equipamentos de informática particulares para uso da rede, o funcionário deverá comunicar ao responsável do seu departamento.

C. Quanto a um funcionário transferido entre departamentos, o responsável pela transferência deve certificar-se de que todos os direitos de acesso aos sistemas e outros controles de segurança que serão necessários na sua nova função sejam informados a equipe de TI para qualquer modificação necessária.

D. Quanto à demissão de um funcionário, o responsável pelo mesmo deve informar a equipe de T.I para providenciar a desvinculação e desativação dos acessos do usuário à qualquer recurso da rede. Em caso de conta de uso comum a membros do departamento, deve-se haver a troca de senha para evitar o acesso as informações.

2.1.3 Regras para Alunos

A. Quanto à utilização de equipamentos de informática particulares para acesso a rede, o aluno deverá assumir total responsabilidade pelo mesmo, estando sujeito às punições necessárias no caso de violação da política.

B. O acesso administrativo a rede (que pertence a funcionários) só deverá ser fornecido a alunos em caso de necessidade e mediante a autorização do responsável do departamento ou área.

2.2 Identificação

A identificação é necessária como forma de autenticação do usuário. Esse controle é utilizado pela grande maioria dos sistemas de autenticação através de identificador (ex.: *login*) e senha única e intrasferível.

2.2.1 Regras Gerais

A. Convém que dispositivos de identificação e senhas protejam a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o campus IV.

B. Senhas são um meio comum de validação da identidade do usuário para obtenção de acesso a um sistema de informação ou serviço. Convém que a concessão de senhas seja controlada, levando em consideração que as senhas temporárias devem ser alteradas no prazo de até 48 horas e não devem ser repassadas para terceiros.

C. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

D. As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como por exemplo: próprio nome, nome de familiares, data de nascimento, nome do animal de estimação, endereço, placa de veículo, telefone residencial ou celular, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

E. Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o administrador da rede, sendo que, o administrador da rede e o usuário devem ser notificados sobre estas tentativas.

F. As responsabilidades do administrador do sistema incluem o cuidado na

criação e alteração das identificações e senhas dos usuários, além da necessidade de manter atualizados os dados dos mesmos.

G. O acesso à rede corporativa (administrativa) deve dar-se de forma a permitir a rastreabilidade e a identificação do usuário.

H. As responsabilidades do usuário incluem, principalmente, os cuidados para a manutenção da segurança dos recursos, tais como sigilo da senha e o monitoramento de sua conta, evitando sua utilização indevida. As senhas são sigilosas, individuais e intransferíveis, não podendo ser divulgadas em nenhuma hipótese.

I. Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu *login*/senha.

J. Tudo que for executado com a identificação de um usuário da rede ou do sistema, será de inteira responsabilidade do usuário, por isso, é preciso tomar cuidado em manter sua senha e/ou outra forma de identificação secreta.

K. Todo e qualquer dispositivo de identificação pessoal, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

2.3 Correio Eletrônico

O objetivo deste tópico é informar as normas de utilização do correio eletrônico (e-mail), que engloba desde o envio, recebimento e gerenciamento das contas.

Todos os usuários de e-mail devem tomar ciência que a Internet opera em domínio publico que foge do controle do departamento de T.I do campus IV. As mensagens podem estar sujeitas a demora e serviços potencialmente não confiáveis. Por isso é importante lembrar que grande parte das pragas eletrônicas atuais chegam por e-mail, por isso, é importante que algumas regras sejam obedecidas pelo usuário.

2.3.1 Regras Gerais

A. O correio eletrônico é uma ferramenta disponível e obrigatória para todos os usuários do campus IV, independentemente de seu vínculo com a instituição.

B. O e-mail deve ser utilizado de forma consciente, evitando qualquer tipo de perturbação a outras pessoas, seja através frequência de envios ou tamanho das mensagens.

C. O envio de e-mail deve ser efetuado somente para pessoas que você tenha realmente a intenção de interagir, enviar e-mails aleatórios para outras pessoas da rede, ou para os grupos, não serão tolerados.

D. É proibido o envio de grande quantidade de mensagens de e-mail (*SPAM)* que seja prejudicial ou gere reclamações de outros usuários. Isso inclui qualquer tipo de mala direta, como, por exemplo, publicidade, comercial ou não, anúncios e informativos, ou propaganda política.

E. É proibido o envio de e-mail que contenha ameaças eletrônicas, como: *spam, mail bombing*[3], vírus de computador e outras.

F. É proibido o envio de e-mail que tenha conteúdo considerado impróprio, obsceno ou ilegal.

G. É proibido reenviar ou de qualquer forma propagar, mensagens em cadeia independentemente da vontade do destinatário de receber tais mensagens;

H. Caso o departamento de T.I do campus IV julgue necessário, haverá bloqueios de e-mail com arquivos anexos que comprometa o uso de banda ou perturbem o bom andamento dos trabalhos; e- mail para destinatários ou domínios que comprometa o uso de banda ou perturbe o bom andamento dos trabalhos.

I. É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários.

J. É obrigatória a manutenção da caixa de e-mail, evitando acúmulo de e-mails e arquivos inúteis.

K. Deve-se evitar executar ou abrir arquivos anexados enviados por emitentes desconhecidos ou suspeitos.

L. Não se deve abrir arquivos anexados com as extensões contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança; se não tiver certeza absoluta que solicitou este e-mail, ou que o remetendo é de confiança.

M. Devesse ter cautela de todos os e-mails com assuntos estranhos (coisas fora do comum, como por exemplo: "você ganhou na mega-sena").

N. Deve-se evitar anexos muito grandes.

[3] *Mail bombing* é como é chama o terrorismo eletrônico que envolve contínuos ataques à caixa de correio de alguém, ou de alguma organização, com grandes e inúteis arquivos.

2.3.2 Regras para Funcionários

A. Não devem ser enviadas mensagens de correio eletrônico cujo conteúdo seja confidencial ou restrito ao campus IV, ou seja, que não possa tornar-se público.

B. Deve-se evitar utilizar o e-mail do campus IV para fins pessoais.

C. É obrigatória a utilização de assinatura nos e- mails, seguindo padrão a ser estabelecido pelo campus IV.

2.4 Uso e Acesso a Internet

Esse tópico visa definir as normas de utilização e acesso à Internet, que engloba desde a navegação à sites, downloads e etc.

A Internet é uma ferramenta tanto de trabalho como de outras coisas, que deve ser usada pelos funcionários e alunos do campus IV; não é permitido o seu uso para fins recreativos durante o horário de trabalho ou de aula.

2.4.1 Regras Gerais

A. Todas as regras sobre uso de Internet visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional. Embora a conexão direta e permanente da rede da instituição com a internet ofereça um grande potencial de benefícios, a proteção dos ativos de informação do campus IV deverá sempre ser privilegiada.

B. Qualquer informação que seja acessada, transmitida, recebida ou produzida na *internet* está sujeita à divulgação e auditoria. Portanto, o campus IV, reserva-se ao direito de monitorar e registrar os acessos à rede mundial de computadores.

C. Somente navegação de sites é permitida. Casos específicos que exijam outros tipos de serviços (ex.: download de arquivos) deverão ser solicitados diretamente à equipe de T.I com autorização do supervisor do usuário que deseja este acesso.

D. É proibida a divulgação de informações confidenciais do campus IV na internet por qualquer meio possível, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou na forma da lei.

E. Caso o departamento de T.I do campus IV julgue necessário, haverá bloqueio de arquivos e domínios que comprometam o uso de banda ou perturbem o bom andamento dos trabalhos.

F. Não será permitido software de comunicação instantânea não homologados/autorizados pela equipe de T.I.

G. Não será permitido o acesso a softwares *peer-to-peer* (Kazaa, BitTorrent e afins), serviços de streaming (rádios on-line, canais de *broadcast* e afins). Porém, os serviços de comunicação instantânea (chats instantâneos, ICQ e afins) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso venham causar algum dano à rede, ou perturbar o bom andamento dos trabalhos.

H. O acesso à sites com conteúdo pornográfico, jogos, bate-papo, apostas, é bloqueado e as tentativas de acesso serão monitoradas.

2.4.2 Regras para Funcionários

A. Os funcionários poderão utilizar a Internet para atividades não relacionadas com ao trabalho durante o horário de almoço, ou fora do expediente, desde que dentro das regras de uso definidas nesta política.

B. Os funcionários com acesso à Internet podem baixar somente programas ligados diretamente às atividades da empresa e devem providenciar o que for necessário para regularizar a licença e o registro desses programas, evitando assim a propagação da pirataria.

C. Funcionários com acesso à Internet não podem disponibilizar, sob nenhuma hipótese, softwares licenciado para o campus IV ou de dados de propriedade do campus IV ou de seus funcionários e alunos, sem expressa autorização do responsável pelo software ou pelos dados.

D. Haverá geração de relatório sobre os sites acessados pelo usuário; se necessário, esse relatório poderá ser usado para prestação de contas do usuário dos acessos.

2.5 Servidor Central

O servidor central do campus IV é identificado em uma rede maior (da UFPB) e é responsável por receber e distribuir toda a banda do campus IV. Tudo que for executado na no diretório do servidor é de responsabilidade do usuário que deve pertencer ou está acompanhado da equipe de T.I.

2.5.1 Regras Gerais

A. Todo acesso ao servidor central deverá ser feito por meio de forte autenticação, registrando usuário, data e hora mediante software próprio.

B. Deverá ser executada semanalmente uma auditoria dos acessos ao servidor central do campus IV, por meio de relatório do sistema de registro.

C. O acesso ao servidor central por visitantes ou terceiros somente poderá ser realizado com acompanhamento de uma pessoa autorizada, normalmente um membro do departamento de TI.

D. Não é permitida a utilização de nenhum tipo de software/hardware no servidor sem autorização da equipe de T.I.

E. Não é permitido adicionar, modificar ou excluir nada no servidor sem autorização da equipe de TI.

2.6 Uso de Computadores

No uso dos computadores do campus IV, algumas normas devem ser atendidas. Os computadores da instituição possibilitam acesso tanto para funcionários quando para alunos, por esse motivo, ambos precisam seguir algumas regras para o manuseio correto das maquinas.

2.6.1 Regras Gerais

A. Os equipamentos (computadores) disponíveis são de propriedade do campus IV, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelo fabricante.

B. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico determinado pela instituição.

C. Todos os computadores de uso individual deverão exigir identificação (*login* e senha) para restringir o acesso de usuários não autorizados.

D. Os usuários devem informar ao departamento de TI qualquer identificação de dispositivo estranho conectado ao seu computador.

E. É proibida a abertura ou o manuseio e/ou reparo de qualquer tipo em computadores, seja isto em departamentos ou laboratórios de informática, isso só poderá ser realizado por um técnico indicado pela instituição.

F. Deverão ser protegidos por senha (bloqueados), todos os computadores pessoais (de uso particular de um funcionário), quando não estiverem sendo utilizados.

G. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos usuários, datas e horários de acesso.

H. No uso do computador é proibido tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

I. Ao utilizar o computador é proibido burlar quaisquer sistemas de segurança.

J. Ao utilizar o computador é proibido acessar informações confidenciais sem explícita autorização do proprietário.

K. Ao utilizar o computador é proibido vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (*sniffers*[4]).

L. Ao utilizar o computador é proibido interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

M. Ao utilizar o computador é proibido usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

N. Ao utilizar o computador é proibido hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

O. Ao utilizar o computador é proibido utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

P. Arquivos pessoais e/ou não pertinentes ao campus IV (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os computadores.

2.7 Controle de Conta de Usuário

Este tópico visa definir normas e procedimentos para uso das contas de usuário de "Aluno" e "Administrador" que os laboratórios e outras partes (biblioteca, salas de projetos) possuem em suas máquinas.

[4] É o procedimento realizado por uma ferramenta conhecida como Sniffer. Esta ferramenta, constituída de um software ou hardware, é capaz de interceptar e registrar o tráfego de dados em uma rede de computadores.

2.7.1 Regras Gerais

A. Todo computador de uso comum (que todos ligados a instituição podem ter acesso) deve ter em seu sistema duas contas de usuária: Aluno e Administrador.

B. Não é permitido a ninguém, fora o departamento de T.I ou quem tenha recebido provia autorização, que modifique, exclua ou adicione contas de usuário às maquinas da instituição.

C. A manutenção e/ou qualquer tipo de alteração nas contas só poderão ser feitas pelos membros do departamento de T.I, ou por pessoas que receberam autorização.

2.7.2 Regras para Funcionários

A. Funcionários que tenham acesso a conta de usuário "Administrador" terão tal privilegio mediante assumir a responsabilidade de usá-las apenas em prol das atividades relacionadas ao campus IV.

B. Não é permitida a instalação e/ou modificação de qualquer software/aplicativo na conta de usuário "Administrador" sem antes consultar a equipe de T.I da instituição.

2.7.3 Regras para Alunos

A. Não é permitido salvar qualquer conteúdo adicional (que não foi definido pela equipe de T.I) nas máquinas, sempre que a máquina for desligada o conteúdo da conta de usuário "Aluno" será deletado, portanto o aluno que desejar salvar informações no período em que estiver usando a máquina deve providenciar salvar os arquivos em algum dispositivo portátil de armazenamento ou serviço de armazenamento e partilha de arquivos ("computação em nuvem").

B. Alunos só podem ter acesso à conta de usuário "Administrador" perante autorização da equipe de T.I, ou em casos especiais (algum projeto/trabalho/estagio que necessite desse acesso).

2.8 Uso de Projetores e Impressoras

Esse tópico tem como objetivo definir as normas de utilização de projetores e impressoras disponíveis nos departamentos do campus IV. Só funcionários tem permissão de utilizar esses itens; alunos apenas podem utilizar sobe circunstâncias especiais (defesa de TCC, impressão de documentos referentes à projetos e afins) e/ou com autorização do

responsável do departamento.

2.8.1 Regras Gerais

A. Os equipamentos (projetores e impressoras) disponíveis são de propriedade do campus IV, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelo fabricante.

B. É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico determinado pela instituição.

C. Se o projetor não funcionar ou apresentar alguma variação na imagem e/ou sua luz estiver mais fraca, pare de utiliza-lo, procure outro equipamento e comunique a equipe técnica responsável.

D. Ao mandar imprimir, verifique na impressora se o que foi solicitado já foi impresso.

E. Se a impressão deu errado e o papel pode ser reaproveitado na sua próxima tentativa, recoloque-o na bandeja de impressão. Se o papel servir para rascunho, reaproveite. Se o papel não servir para mais nada, jogue no lixo.

F. Se a impressora emitir alguma folha em branco, recoloque-a na bandeja.

G. Se você notar que o papel de alguma das impressoras está no final, faça a gentileza de reabastece-lá. Isso evita que você e outras pessoas tenham seus pedidos de impressão prejudicados e evita acúmulo de trabalhos na fila de impressão.

3 Estrutura Física

Este item pode ser compreendido por um aspecto: a segurança física. A segurança física da informação é tão importante quanto a segurança logica, já que é a base para proteção de qualquer investimento feito na instituição. Qualquer acesso às dependências do campus IV, desde áreas de trabalho restritas, até áreas de uso comum (todos tem acesso) precisão estar seguras.

Na estrutura física, serão abordados os seguintes tópicos:

- Controle de Acesso
- Segurança Ambiental

- Utilização dos Laboratórios
- Mesa Limpa e Tela Limpa

3.1 Controle de Acesso

Algumas áreas merecem maior atenção que outras quando se trata de controle de acesso. Áreas como os departamentos contém informações ou equipamentos que devem ser protegidos, para essas áreas é necessário um sistemas de segurança que garanta a proteção adequada da mesma. Quanto maior for a sensibilidade do local, maiores serão os investimentos em recursos de segurança.

3.1.1 Regras Gerais

A. Convém que áreas sejam protegidas por sistemas de segurança apropriado, para assegurar que pessoas sem autorização não as acessem.

B. Apenas pessoas autorizadas podem acessar as instalações que são consideradas de alto risco (que possuem informações ou equipamentos vitais para instituição) no campus IV.

C. Convém que instalações consideradas de alto risco devam contemplar procedimentos de acesso físico (senhas, chaves codificadas e afins).

D. Áreas consideradas de alto risco devem possuir sistemas de monitoração por circuito fechado (câmeras, sensores de movimento e afins), para que equipes de segurança possam realizar monitoramento e executar ações em casos de ocorrência de acesso não autorizado.

E. Departamentos que tratem com informações confidenciais de alunos, como por exemplo, documentação, informações financeiras, acadêmicas o acesso deve ser permitido somente para pessoas autorizadas.

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

3.2 Segurança Ambiental

A segurança do ambiente é de indispensável importância para proteção dos ativos do campus IV. Quanto maior a importância dos ativos, maior será o investimento feito no embiente em que ele se encontra.

3.2.1 Regras Gerais

A. A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

B. A rede elétrica deve ser sempre estabilizada e dimensionada por profissionais especializados.

C. Convém que a manutenção da rede elétrica deva ser feita semestralmente, considerando a segurança contra incêndio.

D. Para cada ativo considerado critico em particular os de processamento e armazenamento de dados, deve-se haver fornecimento de energia alternativo, independentes das concessionarias de energia elétrica.

E. Deve-se ter um gerador de energia para, em especial, ser usado em situações de contingencia e/ou eventuais emergências.

F. Convém a avaliação da capacidade mínima requerida para utilização de equipamentos de ar-condicionado em um ambiente.

G. Todo ambiente do campus IV deve ter itens de segurança contra incêndio (extintores e afins).

H. Em ambientes fechados, é necessário ter sistemas de detecção de fumaça e temperatura.

I. Convém que locais que possuam equipamos críticos (de grande valor e importância), possuam portas corta-fogo.

J. Todo campus IV deve ter alarme de incêndio localizado em locais estratégicos.

K. Servidores devem ser agrupados em locais que não façam uso de material combustível, e devem possuir identificação para facilitar sua localização e/ou manutenção em caso de emergência.

3.3 Utilização dos Laboratórios

Para a utilização dos laboratórios de informática, algumas regras devem ser cumpridas para que assim se possa preservar o ambiente e os equipamentos que ali estão. Evitando assim qualquer tipo de dano aos laboratórios do campus IV.

3.3.1 Regras Gerais

A. O acesso a laboratórios de informática deve ser controlado, somente sendo permito o uso dos mesmos com um funcionário responsável. Em casos especiais (monitores, alunos de projeto), um aluno poderá ficar como responsável.

B. É de responsabilidade do funcionário responsável que utilizou o laboratório zelar pela ordem das instalações, sendo necessário qualquer tipo de manutenção a equipe de T.I deve ser informado.

C. No momento em que entrar no laboratório o funcionário responsável deve verificar se todos os computadores estão funcionando corretamente, após a utilização esta verificação deve ser repetida. Qualquer problema a equipe de T.I deve ser informada.

D. Os laboratórios devem ser trancados em segurança quando deixados sem supervisão, não sendo permitida a utilização de laboratórios sem supervisão.

E. Nenhum equipamento pode ser conectado aos sistemas ou rede sem aprovação prévia e, se necessário, sob supervisão.

F. Não é permitida a retirada de equipamentos dos laboratórios, sendo eles, periféricos (mouse, teclado) ou não.

G. Não é permitida a retirada dos cabos de rede, energia ou que forneçam qualquer espécie de conexão aos computadores. O usuário deve utilizar tomados que não estejam ocupadas e cabos de rede que estejam disponíveis.

H. Alimentos, bebidas, fumo e o uso de aparelhos móveis e celulares nos laboratórios, são de total responsabilidade do proprietário; o campus IV não tem obrigação de dar qualquer tipo de assistência em caso de problemas e/ou dificuldades.

I. As chaves de acesso aos laboratórios devem ficas guardadas em locais controlados, que não seja permitida a entrada de pessoas não autorizadas, evitando que possam ter acesso às chaves.

J. Somente os vigilantes podem ficar com a chave dos laboratórios enquanto os mesmos não estiverem em uso, qualquer outro professor ou funcionário, ao terminar seu uso, deve entregar as chaves para o vigilante.

K. Os departamentos e coordenações deveram ter copias das chaves de seus respectivos laboratórios guardadas.

L. Se a utilização do laboratório não for previamente marcada no horário desejado, cabe a coordenação do curso/departamento liberar ou não seu uso; a utilização

de laboratórios deverá ser feita somente mediante a reserva, garantindo assim que exista um registro de utilização dos laboratórios.

M. O campus IV se reserva ao direito de tomar as medidas cabíveis caso seja comprovado por meio de seu monitoramento (câmeras e afins) o uso irregular dos equipamentos do laboratório.

3.4 Mesa Limpa e Tela Limpa

A política de mesa limpa deve ser considerada para todos os departamentos e seguida por todos os funcionários do campus IV, de forma a garantir que papéis e mídias removíveis não fiquem expostas ao acesso não autorizado.

A política de tela limpa deve ser considerada para todos os departamentos e seguida por todos os funcionários, de forma a garantir que as informações manipuladas por sistemas aplicativos, planilhas Excel, documentos Word etc., não fiquem expostas, permitindo o seu acesso a pessoas não autorizadas.

3.4.1 Regras Gerais

A. Papéis ou mídias de computador não devem ser deixados sobre as mesas; quando não estiverem sendo usados devem ser guardados de maneira adequada, em preferência em gavetas ou armários trancados.

B. As salas devem ser mantidas limpas, sem caixa ou qualquer outro material sobre o chão de modo a facilitar o deslocamento dos funcionários.

C. Sempre que o computador não estiver em uso, não se deve deixar nenhum arquivo aberto, de modo que as informações possam ser visualizadas por outras pessoas que estiverem no local.

D. Agendas, livros ou qualquer outro material que possa conter informações sobre a empresa ou informações particulares devem sempre ser guardadas em locais fechados, evitando o acesso de outras pessoas que não as responsáveis pela informação.

E. Chaves de gavetas, armários, de portas de acesso às salas e laboratórios devem ser guardadas em lugar adequado, e não deixadas sobre a mesa ou guardadas com funcionários não autorizados.

4 Termo de Compromisso

O termo de compromisso é utilizado para que funcionários e alunos no geral se comprometam formalmente em seguir a política de segurança, tomando ciência das punições impostas ao seu não cumprimento.

No termo de compromisso são reforçados os principais pontos da política de segurança e, deve ser assinado por todos os funcionários no ato da contratação e alunos no ato da matrícula, na instituição. Sua renovação deve ser feita sempre que necessário.

5 Verificação da Utilização da Política

Para garantir que as regras mencionadas acima estão sendo cumpridas, o Campus IV se reserva no direito de:

- Utilizar softwares e sistemas que monitorem e gravem todos os usos de Internet através da rede da instituição.
- Inspecionar qualquer arquivo armazenado na rede esteja eles no disco local dos computadores ou em áreas restritas da rede.

6 Penalidades

Quando a política é violada, em primeiro lugar se deve determinar a razão dessa violação, ou seja, se a violação foi por negligencia, acidente, erro, desconhecimento da política ou foi uma violação de má fé (proposital).

Nos termos da Política de Segurança, o campus IV procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento dos trabalhos da instituição ou por em risco algum ativo da mesma.

É recomendado o treinamento dos usuários em segurança da informação, com o intuito de divulgar e conscientizar os funcionários e alunos sobre a política de segurança a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos funcionário e do programa de integração de novos alunos (ao início de cada ano letivo). Os treinamentos de reciclagem devem ser previstos quando necessários.

6.1 Regras Gerais

Algumas infrações são puníveis pelos termos da lei, como por exemplo:

A. Encaminhar por meio eletrônico mensagem para várias pessoas contendo algum boato. (Difamação – Artigo 139 do Código Penal)

B. Enviar uma mensagem para terceiros com informações consideradas sigilosas pela a instituição. (Divulgação de segredo – Artigo 153 do Código Penal)

C. Enviar um vírus que comprometa o equipamento ou conteúdo do campus IV. (Dano – Artigo 163 do Código Penal)

D. Enviar mensagem de correio eletrônico com remetente falso (SPAM). (Falsa identidade – Artigo 307 do Código Penal)

E. Entrar em rede corporativa e alterar informações lá existentes sem autorização. (Adulterar dados em sistema de informações – Artigo 313-B do Código Penal)

F. Ver ou enviar fotos de crianças e menores de 18 anos nus, através da internet. (Pedofilia – Artigo 247 da Lei 8.069/90 "Estatuto da Criança e do Adolescente")

G. Uso de mecanismos (software ou ferramentas diversas) para coleta de informações sem autorização do proprietário. (Interceptação de comunicação de informática – Artigo 10 da Li 9.296/96)

H. Usar cópia de software sem ter licença para tanto. (Crimes contra Software "Pirataria" – Artigo 12 da Lei 9.609/98)

Para maiores informações, consultar a legislação brasileira.

6.1 Regras para Funcionários

A. Caso seja necessário advertir o funcionário, será informado o departamento de Recursos Humanos para interagir e manter-se informado da situação.

B. O não cumprimento, pelo funcionário, das normas estabelecidas neste documento seja isolada ou cumulativamente, poderá causar de acordo com a infração cometida, as seguintes punições: Comunicação de descumprimento, Advertência ou suspensão e demissão por justa causa.

1. **Comunicação de descumprimento:** Será encaminhado ao funcionário, por e-mail, comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. Cópia desse comunicado permanecerá arquivada junto ao Departamento de Recursos Humanos na respectiva pasta do funcionário.

2. **Advertência ou suspensão:** A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade.
3. **Demissão por justa causa:** Esta punição só poderá ser aplicada estando em acordo com as Leis, normas e regulamentos da Universidade Federal da Paraíba.

Para maiores informações, consultar o estatuto da Universidade Federal da Paraíba.

6.1 Regras para Alunos

A. Caso seja necessário advertir um aluno, será informado ao departamento do qual o mesmo faz parte, para mantê-lo informado da situação.

B. O não cumprimento pelo aluno das normas estabelecidas neste documento, seja isolada ou cumulativamente, poderá causar, de acordo com a infração cometida, as seguintes punições: comunicação de descumprimento, advertência ou suspensão e expulsão.

1. **Comunicação de descumprimento:** Será encaminhado ao aluno, através de e-mail, o comunicado informando o descumprimento da norma, com a indicação precisa da violação praticada. A cópia desse comunicado permanecerá arquivada na respectiva pasta do aluno.
2. **Advertência ou suspensão:** A pena de advertência ou suspensão será aplicada, por escrito, somente nos casos de natureza grave ou na hipótese de reincidência na prática de infrações de menor gravidade. Antes da aplicação desta punição será realizado um conselho disciplinar, que será formado conforme regimento interno da instituição.
3. **Expulsão:** Esta punição só poderá ser aplicada estando em acordo com as Leis, normas e regulamentos da Universidade Federal da Paraíba.

Para maiores informações, consultar o estatuto da Universidade Federal da Paraíba.

ANEXO – ROTEIRO DE PERGUNTAS

PARTE 1: INFORMAÇÕES DA INSTITUIÇÃO

1 . Nome da instituição: _____

2 . Cidade Onde se Localiza: _____

3 . Ano de criação: ____/____/____

4 . Número de Funcionários (servidores/empregados)

( ) até 19
( ) de 20 a 99
( ) de 100 a 499
( ) de 500 a 999
( ) mais de 1000

5 . O departamento de segurança da instituição é:

( ) Próprio da Empresa
( ) Terceirizado
( ) Não Existe

6 . No caso de ser próprio, o número de funcionários do departamento

( ) Até 5
( ) De 6 a 10
( ) De 11 a 20
( ) Mais de 20

PARTE 2: INFORMAÇÕES SOBRE A CONSCIÊNCIA DA INSTITUIÇÃO SOBRE SEGURANÇA

7 . O orçamento destinado à área de segurança em 2014 é/foi: (em milhares de Reais)

( ) Proporcional aos Lucros
( ) Até 50
( ) De 51 a 100
( ) De 101 a 250
( ) De 251 a 500
( ) De 501 a 1000
( ) Acima de 1000
( ) Informação Não Disponível

8 . Investimentos na área de segurança em 2014 é:

( ) Análise de Riscos
( ) Autoridade Certificadora
( ) Biometria
( ) Capacitação da Equipe Técnica
( ) Certificado Digital
( ) Contratação de Empresas Especializadas
( ) Controle de Conteúdo
( ) Criptografia
( ) Implementação de Firewall
( ) Política de Segurança
( ) Sala Cofre/Contra Incêndio
( ) Segurança em Acesso Remoto
( ) Segurança em Internet
( ) Sistemas de Detecção de Intrusos
( ) Sistemas de Gestão de Segurança Centralizada
( ) Smartcard
( ) Software de Controle de Acesso
( ) Testes de Invasão
( ) Câmeras de segurança
( ) Virtual Private Network (VPN)
( ) Outros:

9 . Principais obstáculos para implementação de segurança:

( ) Consciência dos Funcionários
( ) Falta de Apoio Especializado
( ) Ferramentas
( ) Gerência/Diretoria
( ) Orçamento
( ) Recursos Humanos
( ) Outros:

10 . Expectativas quanto aos problemas de segurança para 2015:

( ) Aumentarão
( ) Diminuirão
( ) Permanecerão os Mesmos

11 . Política de segurança:

( ) Existe e está atualizada
( ) Existe, mas está desatualizada
( ) Não existe

12 . Se existe uma política de segurança, quais os principais tópicos abordados nela:

( ) Acesso Remoto
( ) Análise de Riscos
( ) Cadastro de Usuários
( ) Classificação de Informações
( ) Conceitos Gerais
( ) Cultura de Segurança
( ) Recuperação no caso de Contingências
( ) Segurança Física
( ) Uso da Internet
( ) Uso da Intranet
( ) Uso de Notebooks
( ) Uso de Senhas
( ) Uso de Software
( ) Vírus
( ) Outros:

PARTE 3: INFORMAÇÕES SOBRE FALHAS DE SEGURANÇA

13 . Principais Ameaças:

Peso: 0 á 3

0 = Sem ameaça

3 = Muito ameaçado

( ) Acessos Indevidos
( ) Acessos Remotos Indevidos
( ) Alteração Indevida
( ) Alteração Indevida de Configurações
( ) Divulgação de Senhas
( ) Divulgação Indevida
( ) Falhas na Segurança Física
( ) Fraudes, Erros e Acidentes
( ) Fraudes em E-mails
( ) Funcionários Insatisfeitos
( ) Hackers
( ) Incêndio/Desastre
( ) Lixo Informático
( ) Pirataria
( ) Roubo de Senhas
( ) Roubo/Furto
( ) Sabotagens
( ) Super Poderes de Acesso
( ) Uso de Notebooks
( ) Uso Indevido de Recursos
( ) Vazamento de Informações
( ) Vírus
( ) Outras:

14 . Prováveis pontos de invasão:

( ) Acesso Remoto
( ) Internet
( ) Invasão Física
( ) Sistemas Internos
( ) Engenharia Social
( ) Outros:

15 . Ataques

( ) Já Sofreu Algum
( ) Nunca Sofreu
( ) Não Sabe se Sofreu

16 . Se já sofreu algum tipo de ataque, qual o último registro:

( ) Menos de 1 Mês
( ) De 1 a 6 Meses
( ) De 7 a 12 Meses
( ) De 1 a 2 Anos
( ) Mais de 2 Anos

17 . Responsáveis por problemas de segurança registrados:

( ) Internos
( ) Externos

18 . Responsáveis por problemas de segurança registrados:

( ) Causa Desconhecida
( ) Vírus
( ) Cavalo de tróia
( ) Funcionários
( ) Hackers
( ) Prestadores de Serviços
( ) Outros:

19 . Providências adotadas no caso de alguma falha de segurança:

( ) Apenas a Correção dos Problemas
( ) Nenhuma Providência
( ) Providências Internas
( ) Providências Legais

20 . Plano de continuidade em caso de falhas de segurança:

( ) Existe
( ) Não Existe

21 . Medidas de segurança já implementadas:

( ) Análise Ataques Real Time
( ) Análise de Riscos
( ) Assinatura Digital
( ) Autoridade Certificadora
( ) Biométrica
( ) Capacitação e Treinamento
( ) Certificação Digital
( ) Classificação das Informações
( ) Cofre Anti-Incêndio
( ) Contratação de Empresas Especializadas
( ) Controle de Conteúdo
( ) Criptografia
( ) Firewall
( ) Monitoração de Log
( ) Palestras para Usuários
( ) Plano de Continuidade de Negócios
( ) Política de Segurança
( ) Prevenção contra Cavalos-de-Tróia
( ) Prevenção contra Pirataria
( ) Prevenção contra Vírus
( ) Procedimentos Formalizados
( ) Proxy Server
( ) Scanner de Redes
( ) Segurança em Acesso Remoto
( ) Segurança em Internet
( ) Segurança na Sala dos Servidores
( ) Sistemas de Backup
( ) Sistemas de Detecção de Intrusos
( ) Sistemas de Gestão de Segurança Centralizada
( ) Smartcard
( ) Software de Auditoria
( ) Software de Controle de Acesso
( ) Software de Segurança de Estação
( ) Termo de Responsabilidade
( ) Testes de Invasão
( ) Câmeras de segurança
( ) Virtual Private Network (VPN)

22 . Uso de aplicações:

( ) Extranet
( ) Intranet
( ) Internet

23 . Uso corporativo da Internet:

( ) Acesso através da rede da empresa
( ) Acesso via modem na empresa
( ) Acesso via modem na residência
( ) A empresa possui página na Web
( ) É permitido comprar via Internet
( ) Não é permitido usar na empresa
( ) Permite acesso externo de terceiros (Extranet)
( ) Usa apenas correio eletrônico
( ) Utiliza VPN
( ) Utiliza Internet Banking
( ) Outras:

24 . A instituição utiliza a Internet para transações eletrônicas:

( ) Sim
( ) Não

25 . Principais aplicações efetuadas na Intranet:

( ) Biblioteca
( ) Certificação Digital
( ) Consultas a Cadastro/Banco de Dados
( ) Corporativos com Manuais e Procedimentos
( ) Diagnóstico Remoto
( ) Divulgação de Documentos e Informativos
( ) Funções Administrativas
( ) HelpDesk
( ) Projetos
( ) Relatórios Internos
( ) RH
( ) Segurança Patrimonial
( ) Sistema de Gestão Empresarial
( ) Sistema de Informações e Controles
( ) Outras:

26 . A instituição permite o uso de Internet:

( ) Não permite
( ) Para todos (alunos/funcionários)
( ) Para todos funcionários
( ) Para todos alunos
( ) Somente para funcionários autorizados
( ) Somente para alunos autorizados

27. A instituição limita os acessos a Internet:

( ) Sim
( ) Não

Se sim, quem tem autorização para usar livremente a internet:

( ) Todos (alunos/funcionários)
( ) Todos funcionários
( ) Todos alunos
( ) Somente funcionários autorizados
( ) Somente alunos autorizados

28. Soluções para proteção de documentos na Internet:

( ) Criptografia Integrada a Aplicações
( ) Criptografia Integrada a Serviços de Rede
( ) Produtos Específicos
( ) SSL - Secure Sockets Layer
( ) Tecnologia Proprietária
( ) VPN - Virtual Private Network
( ) Outras:

PARTE 4: PERGUNTAS E COMENTÁRIOS ADICIONONAIS

29. Quais os principais ativos da instituição:

Qual o nível de ameaça desses ativos:

Peso: 0 á 3

0 = Sem ameaça

3 = Muito ameaçado

30. Comentários Adicionais:

Respondido por: _____

Entrevistado por: _____