UNIVERSIDADE FEDERAL DA PARAÍBA

CENTRO DE CIÊNCIAS APLICADAS A EDUCAÇÃO

DEPARTAMENTO DE CIÊNCIAS EXATAS

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

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

Orientador: Prof. Me. Carlos Eduardo Silveira Dias

RIO TINTO– PB

Fevereiro/2013

SÉRGIO CAMPOS DA SILVA

VERIFICAÇÃO DO GRAU DE ADEQUAÇÃO DA SEGURANÇA FÍSICA E DO AMBIENTE DOS LABORATÓRIOS DE INFORMÁTICA DO CCAE CONFORME A NORMA NBR ISO/IEC 27002

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. Me. Carlos Eduardo Silveira Dias.

RIO TINTO– PB

Fevereiro/2013

Ficha catalográfica preparada pela Seção de Catalogação e Classificação da Biblioteca da UFPB

S586v 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.
66f.: il. –

Orientador: Carlos Eduardo Silveira Dias.
Monografia (Graduação) – UFPB/CCAE.

1.Segurança da Informação. 2.Risco. 3.Ameaça. 4.Conformidade. I.Título.

UFPB/BS-CCAE CDU: 004.056(043.2)

SÉRGIO CAMPOS DA SILVA

VERIFICAÇÃO DO GRAU DE ADEQUAÇÃO DA SEGURANÇA FÍSICA E DO AMBIENTE DOS LABORATÓRIOS DE INFORMÁTICA DO CCAE CONFORME A NORMA NBR ISO/IEC 27002

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. Me. Carlos Eduardo Silveira Dias

_____

Orientador: Prof. Me. Rafael Marrocos Magalhães

_____

Orientador: Prof. Dr. Alexandre Scaico

RIO TINTO– PB

Fevereiro/2013

A Deus por permitir este momento, minha família, aos amigos, colegas e professores, minha eterna gratidão por compartilhar comigo seus conhecimentos.

AGRADECIMENTOS

A Deus por estar sempre comigo nos momentos dessa caminhada.

A minha esposa pelo apoio nos momentos de dificuldade, pelos conselhos que me ajudaram nesse trabalho.

A minha mãe pela simplicidade em seus atos de incentivo.

Ao orientador desta monografia, pelo seu exemplo de dinamismo e trabalho que é a maior lição que um professor pode dar a seu aluno, gostaria de agradecê-lo pela paciência e por ter acreditado na minha caminhada.

A todos os amigos, funcionários, professores e colegas que fazem parte do DCE da Universidade Federal da Paraíba que de uma forma ou de outra, contribuíram para a conclusão deste trabalho.

RESUMO

O presente trabalho apresenta o estudo realizado nos laboratórios de informática dos cursos de Bacharelado em Sistemas de Informação e Licenciatura em Ciências da Computação do Centro de Ciências Aplicadas a Educação no Campus IV da UFPB para verificar o grau de adequação da segurança desses laboratórios de acordo com a seção 9 da norma ISO/IEC 27002, que trata especificamente da segurança física e ambiental. Para isso, foi feito o levantamento sobre a situação atual dos laboratórios através de questionários, entrevistas e visitas in loco, que ajudaram a trazer a realidade da segurança oferecida nos laboratórios. Diante do cenário atual da segurança física e do ambiente dos referidos laboratório foi realizada uma comparação com o que recomenda a segurança física e do ambiente descrita no capitulo 9 (nove) da norma NBR 27002. Utilizando-se o modelo de teias para gerenciamento de riscos, foi feito um confrontamento que mostrou o grau de adequação com a norma, sendo este modelo também utilizado para elaborar medidas a serem aplicadas nos laboratórios para reduzir ou evitar os riscos ou a ocorrência de um incidente.

Palavras chave: Segurança da Informação. Risco. Ameaça. Conformidade. Incidente.

ABSTRACT

The present work shows the study done at laboratory of informatics of the courses of Bachelor of Information Systems and Graduation of Computer Science of Applied Science and Education Centre, at University Federal of Paraiba to verify the security compliance of these laboratories according to the section 9 of the NBR 27002, dealing specifically with the physical and environmental security management. To do this, a research was done on the current situation of laboratories, using questionnaires, interviews and site visits to help bring the reality of security offered in laboratories. Given the current scenario, a comparison was performed in the laboratories based on recommendations of the physical and environmental security described in chapter 9 (nine) of NBR 27002. Using the web model to manage risks, a confrontation was made to show the degree of compliance with the NBR 2700. This model is also used to develop and implement a solution to be applied in laboratories in order to reduce or avoid the risks or the occurrence of a security incident.

Keywords: Information Security. Risk. Threat. Compliance. Incident.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

UPS	FONTE DE ENERGIA PERMANENTE
IES	INSTITUIÇÕES DE ENSINO SUPERIOR

SUMÁRIO

1. INTRODUÇÃO

Atualmente com a crescente evolução e disseminação da tecnologia da informação e comunicação nas organizações, seja ela pública ou privada, é grande a atenção dada aos ativos e principalmente a própria informação, que se apresenta armazenada em diversas formas: escrita, impressa ou digital. Para (Campos, 2007), o espaço físico onde informações são processadas e/ou armazenadas precisa ser protegido contra ameaças que poderiam gerar um incidente de segurança da informação. E para evitar tal incidente, precisam-se manter três características da informação: confidencialidade, disponibilidade e integridade.

Apesar da preocupação em proteger a informação, em muitas organizações ainda existe certa dificuldade em entender a importância da segurança em seus diversos níveis (Nakamura, Geus, 2010). Frequentemente o estado atual da informação é ignorado por achar que o que esta implementado é suficiente, que nunca ira ocorrer um incidente ou que jamais alguém ira retirar algum recurso físico. Isto se constitui em um grande risco para organização, visto que mais cedo ou mais tarde poderá ocorrerá um incidente. Por ser um campo recente, pouco se investe: a segurança é vista como uma solução de alto custo e preferem investir em soluções que trazem vantagens aos olhos de todos. Porém a presença da segurança não resulta em melhorias imediatas: é um investimento não perceptível; o papel da segurança é evitar que alguma coisa ocorra: um incidente que traga algum prejuízo. Assim é necessário que numa organização as questões relacionadas à segurança precisem ser discutidas e solucionadas, e esta discussão não deve ser sobre se existe ou não segurança e sim em que nível se encontra. O diferencial que garante a sobrevivência é a ideia de abandonar o principio “se funciona, está bom” e adotar “funcionar com segurança” e que a segurança deva andar junto com o negócio no ambiente organizacional.

Nas Instituições de Ensino Superior (IES) assim como nas empresas, sempre há equipamentos que recebem, transformam e entregam dados e/ou informação. Tais equipamentos são conhecidos como equipamentos processadores de informação e necessitam estar seguros. Essa segurança não envolve apenas estarem localizados em uma área segura, conhecida como perímetro de segurança (CAMPOS, 2007), mas também se faz necessário que sejam supridos por uma fonte de energia segura, confiável e contínua que um sistema de alarmes monitore as áreas não ocupadas, haja uma área de recepção ou qualquer meio para controlar o acesso/entrada física, que os edifícios não deem qualquer indicação de que ali exista ativos (NBR 270002, 2008). Ainda de acordo com a norma NBR 27002 devem-se levar em consideração as ameaças externas e do meio ambiente sendo necessária proteção contra

incêndios, explosões em edificações vizinhas e vazamentos de água em telhado; o pessoal que trabalha nas áreas seguras sejam os únicos a saberem da existência de ativos e sejam supervisionados para evitar atividades mal intencionadas; as áreas seguras quando não utilizadas sejam trancadas e periodicamente verificadas; os equipamentos sejam protegidos contra ameaças físicas e do meio ambiente e haja um plano de manutenção recomendada pelo fornecedor ou fabricante para assegurar a disponibilidade e integridade, além da existência de diretrizes para proteção dos equipamentos quando emprestados para utilização fora das dependências da organização.

As IES possuem características peculiares e estão inseridas em um mercado onde dividem espaço com universidades privadas, ou seja, instituições com fins lucrativos. Assim como estas, os IES necessitam de adequado sistema de controle de riscos para aumentar a segurança de seus ativos (Sedrez, Fernandes, 2011).

Um risco é a possibilidade de ocorrência de um evento adverso para uma determinada situação esperada. As entidades sem fins lucrativos precisam assumir e gerenciar riscos sob forma de garantir sua sustentabilidade e manter projetos beneficentes. Da mesma forma que qualquer entidade, as IES devem identificar os riscos, medi-los, controlando-os e adequando-os aos seus objetivos uma vez que as estruturas podem apresentar semelhanças com as organizacionais, consequentemente os objetivos são parecidos: distribuição de responsabilidades e competências, recursos e tecnologia, produzindo serviços demandados pela sociedade, assumindo riscos e buscando resultados. Isso só é executado de forma ordenada se houver uma adequada gestão de riscos (Sedrez, 2011).

Em Instituições de Ensino além de funcionários há também alunos que frequentam as dependências da instituição e utilizam recursos de informática. Estes usuários devem seguir regras estabelecidas por uma politica de segurança voltada para Instituições de Ensino além de se envolverem e se conscientizarem da importância de cumprir definições estabelecidas na política de segurança da instituição. Esta deve prevenir o acesso não autorizado, danos e interferência as instalações físicas da instituição, as áreas onde há equipamentos precisam ser protegidas por controles de entrada apropriado para assegurar que somente pessoas autorizadas tenham acesso; deve ser considerado uma política de mesa limpa que reduza o risco de perda de dados e informações, além de diretrizes quanto ao uso correto dos equipamentos e salas (Spanceski, 2004).

Para Epaminondas (2009), a alta cúpula executiva deve apoiar desde a implementação, aplicação e divulgação de uma política dentro dos Institutos de Educação Superior (IES).

A politica dos IES deve ainda especificar os procedimentos de como adquirir, configurar, auditar os sistemas computacionais e redes, além de facilitar o gerenciamento destes recursos. Nesta politica deve ainda ser inseridas normas e procedimentos para setores, áreas como de informática, de segurança, de conservação, etc. Considerar também uma lista de Controle de Acessos: que proteja os ativos contra tentativas de invasão, uso do correio eletrônico, redes, acesso às maquinas de laboratórios, dentre outros (EPAMINONDAS, 2009).

Infelizmente há obstáculos para implementação da politica de segurança da informação, como desconfiança por parte dos gestores em não considerar importante e a falta de orçamento.

Mas por meio dela as IES terão controle sobre os recursos, dando sustentabilidade à segurança da informação, fornecendo melhores praticas, minimizando riscos dos ativos e vulnerabilidades. As IES devem também investir em projetos de sensibilização dos funcionários e corpo discente e os altos executivos dêem maior prioridade à segurança da informação ajudando assim na implementação da política (EPAMINONDAS, 2009).

1.1 Motivação e Problema

Como descrito anteriormente, numa organização existem áreas onde há recursos físicos de valor que como qualquer outro bem, é importante ter atenção e proteção nesses ambientes contra ameaças que podem ser de natureza humana e/ou natural.

A necessidade de estabelecer uma politica de segurança é algo recomendado pela NBR ISO/IEC 27002. Segundo a norma, a política de segurança é importante porque a partir dela é que serão elaborados as normas e procedimentos.

Seria importante identificar onde um ou vários riscos existem, além disso, tornar visível para todos os níveis de segurança verificados para os recursos. Para isso a utilização de um método que estabeleça soluções e torne o contexto do ambiente em estudo do conhecimento de todos da organização (desde o usuário até a direção) é de grande interesse, isso porque para se ter um ambiente seguro é essencial a participação de todos.

1.2 Justificativa

A segurança necessária e sua implantação são coisas complexas de serem executadas no ambiente organizacional. Assim, a política de segurança é a base para todas as questões

relacionadas à proteção: pois trata dos aspectos humanos, culturais, tecnológicos e legislação, desempenhando papel importante na organização.

As instituições de ensino superior possuem características peculiares e estão inseridas em um mercado cada vez mais dinâmico onde dividem espaço com instituições particulares e ambos enfrentam riscos a continuidade de seus negócios necessitando de sistemas de controle e gestão de riscos que possam aumentar a segurança da gestão, planejar metas conhecendo melhor os eventos que podem impedir seu cumprimento. Assim os controles previstos na norma NBR ISO/IEC 27002 fornece recomendações para desenvolvimento de práticas para gestão da segurança da informação, aconselhando aos responsáveis implementar, utilizar e manter a segurança da informação. De Acordo com Sedrez e Fernandes (2011), pouco se tem abordado em trabalhos científicos a respeito de gestão de riscos em instituições de ensino superior.

> ...gestão de risco é imprescindível para que as Instituições de Ensino Superior identifiquem os riscos a que estão expostas, medindo-os, controlando-os e adequando-os aos seus objetivos, que sempre devem ser entendidos como uma relação risco-retorno. Da mesma forma que qualquer entidade, as IES possuem objetivos e estruturas organizacionais e distribuem responsabilidades e competências, recursos e tecnologias, produzindo serviços demandados pela sociedade, assumindo riscos e buscando resultados. Para que isso ocorra de forma ordenada, é necessário que tais objetivos, ações e resultados, sejam integrados a uma adequada gestão de risco. (SEDREZ e FERNANDES, 2011).

1.3 Objetivo Geral

Verificar o grau de conformidade da segurança física e ambiental dos laboratórios de informática do DCE com a norma NBR 27002. Através de um estudo que mostre o contexto atual da segurança física e do ambiente dos laboratórios de informática, utilizando um modelo de representação para comparar o nível de segurança atual com o nível proposto pela norma.

1.4 Objetivos específicos

Para que haja uma compreensão da situação da segurança dos laboratórios foi realizado um estudo composto por observação direta, entrevistas com responsáveis pelas áreas e aplicação de questionários com os usuários dos laboratórios que objetivaram:

- Verificar se existiam e eram aplicados controles de segurança.
- Saber se os responsáveis por determinada área conhecia e utilizava/aplicava controles de segurança e qual a visão deles quanto à segurança do ambiente.
- Comparar os níveis de segurança verificado no estudo com os níveis de segurança que estabelece a segurança física e do ambiente estabelecida pela NBR 27002.
- Indicar em que grau de conformidade se apresenta a segurança física e do ambiente dos laboratórios.
- Documento sobre o estado atual e o que deve ser aplicado para chegar à adequação à norma.

1.5 Metodologia

Foram consideradas a aplicação de controles de acesso, regras de segurança no ambiente dos referidos laboratórios, existência de politica de segurança que estabelecesse diretrizes e se todos esses controles seguem alguma norma de segurança.

Para verificar a conformidade com a norma NBR 27002 foi realizada uma pesquisa exploratória, que busca levantar informações acerca da segurança atual dos laboratórios de informática, composta por:

- *Pesquisa Bibliográfica:* necessário para levantar assuntos, estudos relacionados à segurança física e do ambiente, assim como normas e leis que apresentam e recomendam de um modo geral a segurança da informação.
- *Estudo de caso:* caracterizado como uma pesquisa exploratória que tem objetivos de proporcionar familiaridade com o problema (objeto de estudo) (Gil, 2002) e a aprimorar ideias e descobrir intuições. Realizado nos laboratórios de informática com seus responsáveis e em outros setores vinculados como estratégia de pesquisa para verificação da segurança física e do ambiente. Foram utilizadas as seguintes fontes:
  - ✓ *Análise in loco*– realizada no ambiente dos laboratórios: corredores, interior dos laboratórios, no prédio e mediações onde dá acesso aos corredores.

- ✓ Entrevistas individuais – com as pessoas responsáveis por uma área de interesse do presente trabalho e que seja responsável por tomar decisões. Responsáveis direta e indiretamente pela segurança e vigilância dos laboratórios.
- ✓ Aplicação de questionário – com os alunos que utilizam os laboratórios de informática.

2. FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta os conceitos de segurança da informação, política de segurança, normas de gestão de incidentes e Modelo de Teias. A importância de uma política de segurança e da gestão da segurança dos recursos nas Instituições de Ensino Superior e no âmbito federal.

2.1 Segurança da Informação

De acordo com a NBR ISO/IEC 17799, com o grande aumento da interconectividade dos ambientes organizacionais os ativos destas tornam-se dependentes de proteção, isto porque estão expostos a um crescente número de ameaças e vulnerabilidades; assim a informação que pode existir em diversas formas: escrita em papel, armazenada eletronicamente, transmitida, compartilhada ou falada necessita que seja sempre protegida adequadamente e a segurança da informação é o estabelecimento, implementação, monitoração e melhoramento de um conjunto de controles que visam garantir/atender os objetivos de negócio e de segurança da organização.

2.1.1 Importância da Segurança da Informação

Ainda segundo a NBR ISO/IEC 17799 a informação e os ativos, expostos as ameaças cada vez mais comuns, são importantes para o negócio da organização e é essencial que se defina, mantenha e melhore a segurança da informação para assegurar a competitividade, o atendimento aos requisitos. É importante para proteger as infraestrutura críticas tanto do setor privado quanto público, viabilizando os negócios, evitando ou reduzindo riscos relevantes. A segurança da informação pode também apoiar na implantação da gestão da segurança em um ambiente, isso porque para se alcançar o nível desejado é necessário a participação de fornecedores, terceiros, usuários entre outras partes externas (NBR 17799, 2005).

2.2 Política de Segurança

A política de segurança desempenha papel importante porque é a base para todas as questões relacionadas à proteção dos recursos de uma organização e seu estabelecimento é algo recomendado pela ISO/IEC 17799. Trata dos aspectos humanos, culturais e tecnológicos

de uma organização levando em consideração os processos, negócios e a legislação (Nakamura, 2011). Seu desenvolvimento é o primeiro e o principal passo da estratégia de segurança da organização e envolve elaboração e planejamento. É nessa fase onde os aspectos de proteção dos recursos existentes são definidos e assim a política de segurança ganha importância como facilitadora e simplificadora do gerenciamento de todos os recursos.

Politica de segurança da informação também pode ser um conjunto de leis, regras e praticas que gerenciam uma organização, protege e distribui a informação, os recursos e delega responsabilidades e conscientiza a equipe de profissionais (CARUSO, SOARES, 1999).

2.3 Segurança da Informação na Administração Publica Federal

No contexto da administração pública federal a segurança da informação tornou-se um tema que vem sendo debatido, tratado para estabelecer diretrizes que possam servir de modelo para elaboração, implantação, manutenção de uma política de segurança e de controles de segurança nas organizações. O artigo 42 do Decreto 7845 de 14 de novembro de 2012 que regulamenta procedimentos para credenciamento de segurança e tratamento da informação estabelece no capítulo 3, seção VIII que áreas, instalações e materiais que contenham, utilizem ou veiculem informação ou conhecimento que divulgados impliquem em riscos aos interesses da sociedade ou do Estado tenham acesso restrito as pessoas autorizadas pelo órgão ou entidade.

Muitas organizações, sejam elas públicas ou privadas, ainda se mostram despreparadas para lidar com a segurança da informação. Isso decorre do fato dessas empresas possuírem poucos instrumentos de proteção, agravados pelo despreparo gerencial, tornando-as mais vulneráveis às ameaças, com isso os impactos causados pelos eventos negativos tendem a ser mais fortes (LUNARDI; DOLCI, 2006).

Gerenciar os riscos é um dos principais processos da gestão da segurança da informação, pois visa identificar, analisar, avaliar e controlar os riscos inerentes à segurança da informação. Gerenciar os riscos pode ser um processo complexo e oneroso, contribuindo para que as empresas não priorizem esse processo em projetos de segurança da informação (OLIVEIRA et al, 2009).

> O despreparo das organizações para lidar com a segurança da informação as tornam mais vulneráveis às ameaças e os impactos causados

> pelos eventos negativos tendem a serem maiores. Com isso, a implantação da gestão da segurança das informações é fundamental para minimizar os riscos e garantir a continuidade do negócio, maximizando as oportunidades de competitividade. (KOZEN e OUTROS, 2012)

Devido à importância das informações processadas nos órgãos e entidades da Administração Pública Federal, o Decreto 3.505, de 13 de junho de 2000, estabelece que a segurança da informação seja responsável por proteger áreas e instalações de equipamentos que processam informações e documentar eventuais ameaças ao seu desenvolvimento. Então, a partir desse decreto, procurou-se organizar a política nacional de segurança das informações.

> Essa Política de Segurança visa oferecer instrumentos jurídicos, normativos e organizacionais que capacitem órgão e entidades científica, tecnológica e administrativamente a fim de assegurar a confidencialidade, integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.[...]Esta norma aponta à redução de riscos e torna-se necessário um conjunto coordenado de trabalhos no país e a nível de Estado, contribuindo para o uso da TI e diminuição dos riscos advindo da evolução tecnológica, principalmente por empresas e organizações que atuem em áreas consideradas estratégicas e sensíveis ao país. (OSIRO, 2006).

As normas seguem leis e diretrizes específicas, cujo âmbito das organizações, também está inserido o setor público, como autarquias, ministérios, tribunais, universidades, entre outros. Mesmo com toda preocupação com a segurança da informação, é raro achar universidades que se preocupam com aplicação de normas de segurança, apesar de serem organizações que detém ativos importantes e que mereçam a aplicação de normas.

2.4 ABNT NBR ISO/IEC 17799:2005

A ABNT é o fórum nacional de normas cujo conteúdo é de responsabilidade dos comitês brasileiros, dos organismos de normalização setorial e das comissões de estudos especiais temporários e elaboradas pelas comissões de estudos formadas por representantes

dos setores envolvidos: produtores, consumidores e neutros (universidades, laboratórios e outros). A **ABNT NBR ISO/IEC 17799:2005** foi elaborada no comitê brasileiro de computadores e processamento de dados pela comissão de estudo de segurança física em instalações de informática (CE). É equivalente a ISO/IEC 17799:2005. Atualmente existe um novo esquema de numeração, e a partir de 2007 a nova edição da ISO/IEC 17799 passou para ISO/IEC 27002. Outra família de normas: gestão da segurança da informação, gestão de riscos, métricas e medidas e diretrizes para implementação também adotaram este novo esquema de numeração. A norma traz técnicas e controles de segurança e um guia de práticas para gestão da segurança, estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação. Também destaca que é importante a participação de todos os envolvidos na organização para que o sucesso da segurança seja alcançado. Os objetivos definidos nessa norma configuram as melhores práticas quando se fala em gestão da segurança da informação.

2.4.1 Estrutura

Contém 11 seções de controles de segurança da informação que juntas totalizam 39 categorias principais de segurança. São elas:

1. Política de Segurança da Informação – 01
2. Organizando a Segurança da Informação – 02
3. Gestão de Ativos – 02
4. Segurança em Recursos Humanos – 03
5. Segurança Física e do Ambiente – 02
6. Gestão das Operações e Comunicações – 10
7. Controle de Acesso – 07
8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação – 06
9. Gestão de Incidentes de Segurança da Informação – 02
10. Gestão da Continuidade do Negócio – 01
11. Conformidade – 03

Para cada categoria há um objetivo que define o que deve ser alcançado e um ou mais controles que podem ser aplicados para alcançar o objetivo.

Na seção 9 (nove) da NBR ISO/IEC 17799 atualmente NBR ISSO/IEC 27002 são descritas duas grandes categorias que trazem requisitos de segurança para uma organização. Na categoria Áreas seguras cujo objetivo é prevenir o acesso não autorizado, danos e interferências com as instalações e informações da organização, é destacado a proteção Perímetro de segurança física, que consiste em utilizar portões, entrada controlada por cartões e recepção. A norma destaca que a proteção oferecida seja compatível com os riscos identificados. A outra categoria é quanto à segurança de equipamentos com o objetivo de impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização. Em particular esta categoria contem diretrizes consideradas importantes ao contexto deste trabalho que são proteção dos equipamentos, as necessidades quanto ao suprimento de energia, a segurança do cabeamento, a manutenção dos equipamentos e remoção de propriedade.

A ISO/IEC 27002 é aceita mundialmente e sua versão ABNT NBR ISO/IEC 27002 é a tradução brasileira desse padrão que define as melhores praticas para gestão da segurança da informação fornecendo conteúdo básico das diretrizes para usuários e administradores que devem ser parte integrante da política (EPAMINONDAS, 2009).

2.5 Modelo de Teias

A segurança é um processo continuo onde é importante mensurar quantitativamente e qualitativamente todos os aspectos relacionados à proteção dos recursos da organização. Identificar os pontos e definir os níveis de segurança de cada um é um grande desafio devido à complexidade da segurança que envolve aspectos humanos, culturais, sociais, tecnológicos, legislativos de processo e de negócio que devem ser tratados com absoluto cuidado (Nakamura, Geus, 2010). Ainda segundo o autor, o gerenciamento de segurança torna-se difícil porque não se pode gerenciar o que não se conhece. Assim é importante ter uma metodologia que seja capaz de identificar as entidades que influenciam no nível de segurança e de mensurar o nível de segurança dessas entidades, propor soluções e fazer com que todos entendam e visualizem a situação da organização referente à segurança. Essa é a ideia do Modelo de Teias, que traz alguns elementos necessários para procurar contribuir para desenvolver assuntos relacionados ao gerenciamento da complexidade da segurança, procura facilitar a compreensão dos problemas envolvidos. É composto pelos seguintes elementos:

- Figura, que indica a diferença entre a situação real e a desejada.

- Elementos de segurança são os elementos analisados que exercem influência direta no nível de segurança de um determinado recurso.
- Roadmap, medidas de segurança para diminuir a diferença entre os níveis de segurança atual e a desejada.
- Sete fases, que criam a figura.

A seguir a figura 1 e 2, que são a base para o modelo procura torna a segurança mais compreensível para todos os envolvidos.

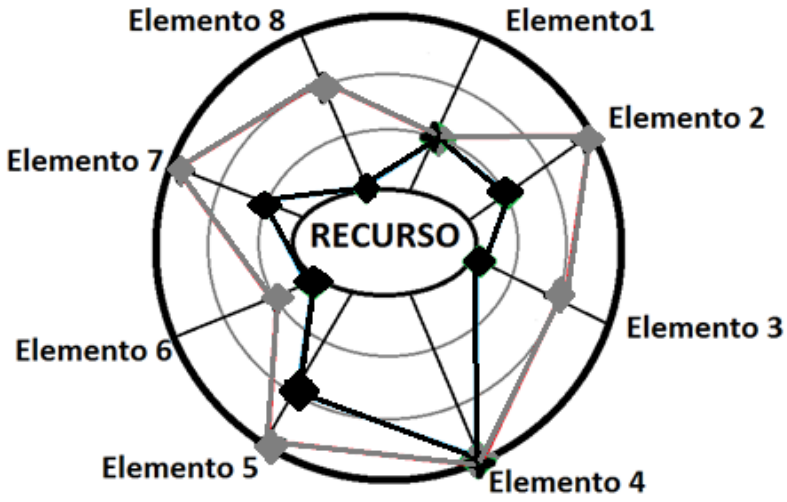

Figura 1: Figura do Modelo de Teias

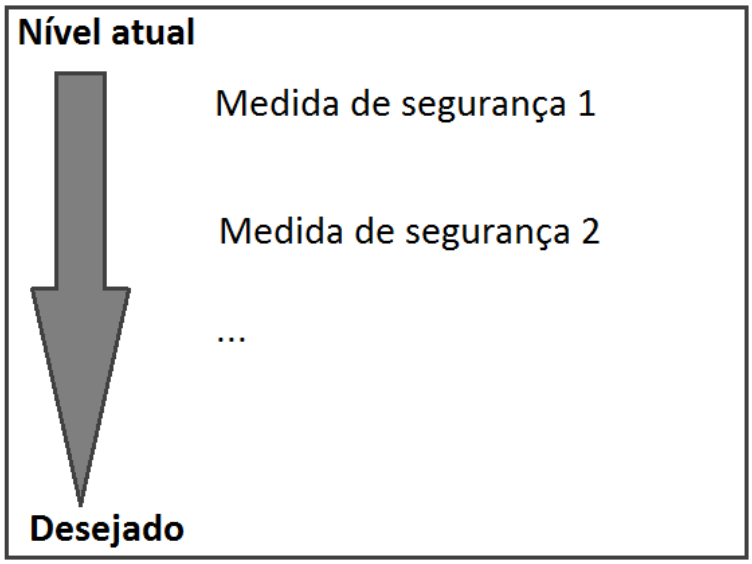

Figura 2: Roadmap de Medidas de Segurança.

A seguir a descrição de todas as fases (tarefas realizadas na criação do modelo) que relaciona quais medidas de segurança devem ser implementadas e em quais recursos.

Fase 1: Definição dos elementos de segurança: *quando dado recurso é analisado e verifica-se influencia direta no nível de segurança.*

Fase 2. Definição dos recursos: *todos ativos da organização que precisem/devem ser analisados. É nessa fase que se pode obter uma visão geral da hierarquia da situação do ambiente da organização quanto à segurança.*

Fase 3. Analise de segurança: *é realizada no recurso, levando-se em conta os elementos de segurança definidos na fase 1*.

Fase 4. Classificação dos recursos: *definir o nível de segurança para cada elemento do recurso.*

Fase 5. Avaliação dos riscos: *esta fase consiste em mensurar os riscos envolvidos com cada recurso.*

Fase 6. Definição do nível de segurança desejado: *define-se o grau de segurança de acordo com a avalição dos riscos combinado com a importância do recurso para a organização.*

Fase 7. Definição das medidas de segurança a serem implementadas: *definir quais medidas serão tomadas para diminuir/eliminar a distancia entre o nível de segurança atual e o desejado.*

2.5.1 Interpretando o modelo de Teias

Classificar um recurso em seguro ou não seguro através da análise de segurança de seus elementos de segurança é difícil (Nakamura, Geus, 2011). Pois se um recurso estiver com a maioria dos seus elementos de segurança com níveis altos e apenas um com nível baixo esse recurso será classificado como desprotegido, pois é neste menor nível que pode ocorrer um incidente. Porém, observando a figura do modelo, dois aspectos sendo considerados pode ajudar na determinação da classificação do recurso: *o nível de segurança atual representado pelo traço preto e o nível de segurança desejado, representado pelo traço de cor verde.*

A análise da figura mostra que temos círculos, estes determinam os degraus, as medidas que se deve tomar para atingir a segurança desejada para o ativo/recurso em análise. Essa quantidade de medidas será determinada pela equipe de TI que deve deter o conhecimento sobre a segurança levando em consideração a experiência, conhecimento de ferramentas, leis

ou normas ou poderá ainda utilizar-se de guias de boas práticas para gestão dos recursos do ambiente.

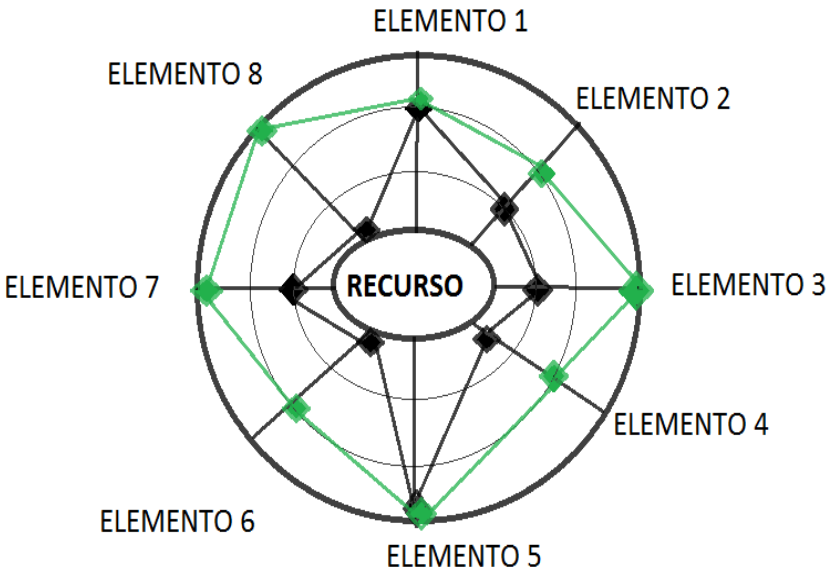

Figura 3: Traço preto representando o nível de segurança atual e de cor verde o desejado.

Determinar os níveis de segurança depende da capacidade e necessidade da organização. Também da experiência do profissional de segurança que determinara se um recurso possui ou não nível adequado de proteção. Deve-se considerar que essas definições dos níveis de segurança mudam à medida que o profissional adquire experiência, ou novas maneiras de ataques surgem. A seguir na figura 4 temos um exemplo de aplicação do Modelo de Teias no recurso/ativo, no caso, um computador foi tomado como exemplo.

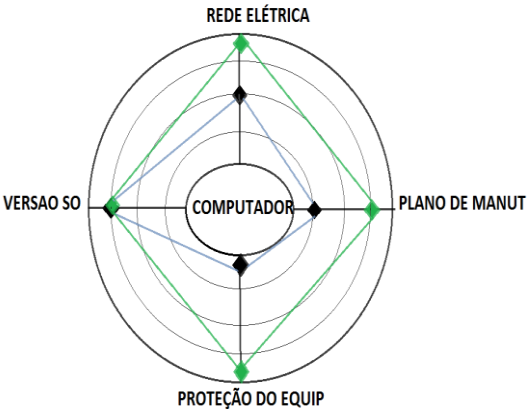

Figura 4a : Aplicação do Modelo de Teias

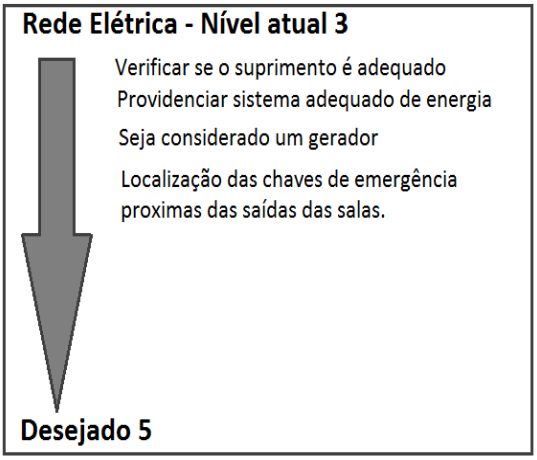

Figura 4b: Roadmap do Modelo

2.5.2 Abstraindo o modelo de Teias

O modelo permite que o nível de segurança da organização seja classificado de acordo com o nível de segurança dos departamentos ou setores, como mostra a figura 5. Já um setor dessa organização tem seu nível de classificação da segurança determinado pelo nível de segurança de cada recurso deste setor, figura 6, enquanto o nível de segurança desse recurso é determinado de acordo com a análise de cada elemento de segurança relacionado, figura 7. Assim todos da organização entendem a situação da segurança do seu departamento, ajudando a torna o gerenciamento mais compreensível.

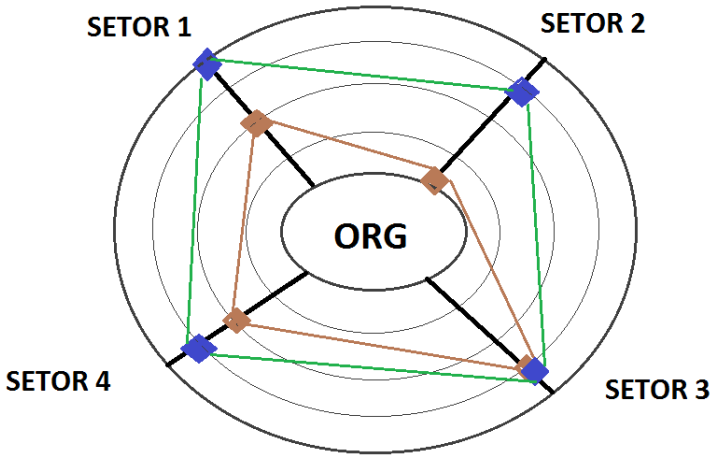

Figura 5: Uma organização tem vários setores.

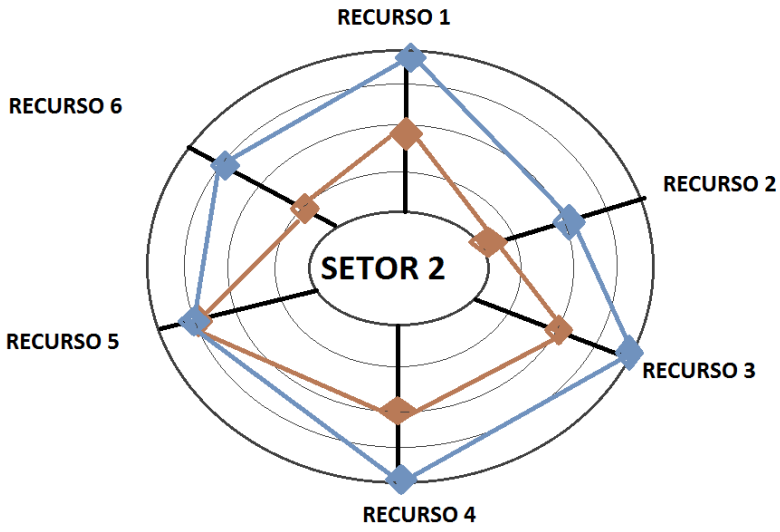

Figura 6: Os diversos recursos de um setor.

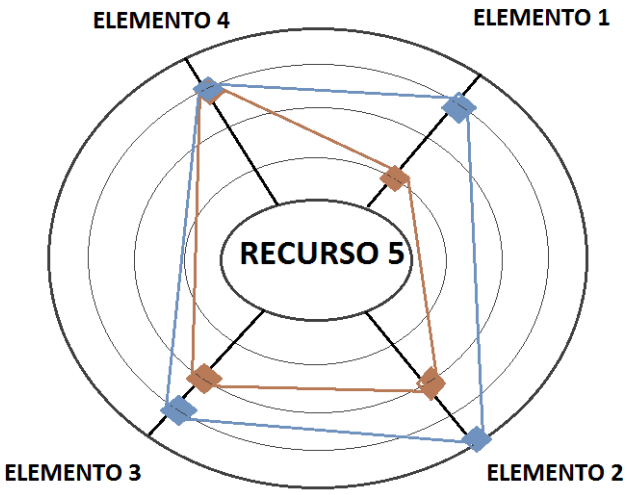

Figura 7: Elementos de segurança do recurso.

3. SEGURANÇA FÍSICA E AMBIENTAL DOS LABORATÓRIOS DE INFORMÁTICA DO DCE/CCAE

Neste capitulo será apresentado a situação dos laboratórios no que se refere à aplicação ou uso de regras ou controles, o grau de segurança verificado nos dois grupos de laboratórios utilizando-se para isso as entrevistas, observação in loco e o resultado dos questionários.

3.1 Os laboratórios do DCE/CCAE

Os laboratórios de informática do campus Rio Tinto atualmente conta com cinco salas equipadas com equipamentos de informática: computadores, estabilizadores e equipamentos de rede, porém apenas três atendem as atividades das disciplinas dos cursos de Sistemas de Informação e Licenciatura em Ciências da Computação além das necessidades de outros alunos. Uma equipe de alunos e professores é responsável por administrar e manter a operação e o funcionamento dos mesmos além do bom uso através de regras de utilização.

As regras de utilização regem os laboratórios e são definidas em cinco resoluções. A primeira trata das regras gerais de utilização dos laboratórios, estabelecendo proibições em relação à instalação de software, de remoção de equipamentos, consumo de alimentos, perturbação da ordem do silêncio, e controle de acesso condicionado à presença de um professor, monitor, dentre outras. Já a segunda resolução trata do uso dos laboratórios pelos alunos, que aborda questões sobre o acesso ao laboratório a partir das contas pessoais dos alunos, sobre reportar quaisquer problemas de hardware. A terceira resolução aborda regras de utilização por professores e monitores, que os mesmos devem comparecer no horário marcado de acordo com a planilha de horários fixada na porta de entrada dos laboratórios, solicitar o fechamento pelos vigilantes e cuidar do ambiente. A quarta resolução trata das condições de solicitação de instalação de software nas maquinas: somente softwares gratuitos são instalados e solicitados por professores. A quinta resolução trata do uso em horário extra expediente: somente solicitações com antecedência de 48 horas, para os professores, basta apenas o nome e o horário, caso seja aluno, será necessário também a identificação do responsável.

Apesar de existirem regras que estabelecem diretrizes para utilização dos laboratórios, não se verificou num primeiro momento a aplicação dessas resoluções. Dessa forma é preciso investigar como essas regras foram definidas.

3.2 Levantamento do nível de segurança dos laboratórios.

Com o objetivo de verificar o quão adequado se encontra a situação da segurança física e do ambiente dos laboratórios de informática dos cursos de Sistemas de Informação e Licenciatura em Ciências da Computação, o estudo teve como base teórica as técnicas de gestão de segurança, mas especificamente a seção 9 (nove) que descreve a segurança física e do ambiente especificados na NBR ISO/IEC 27002. E obtiveram-se os seguintes dados que ajudaram a retratar a segurança através das metodologias abaixo:

3.2.1 Análise in loco

Realizada no período entre novembro e dezembro de 2012, observou-se o ambiente físico dos laboratórios quando estavam sendo utilizados e quando não estavam sendo utilizados.

O ambiente dos laboratórios é atualmente livre, seja durante utilização (uso em aulas, pesquisas) ou quando estão fechados sem utilização. O fluxo de qualquer pessoa é permitido no prédio que os acomoda e também nos corredores dos andares superiores onde se localizam. No prédio, onde estão localizados os laboratórios na parte superior, existe uma escada que dá acesso ao andar superior e que não se verifica nenhum obstáculo que possa controlar o acesso de pessoas a este andar. O vigilante responsável pela segurança está presente em boa parte de seu tempo de trabalho no térreo e visitando outros prédios. Ocorre que neste intervalo esta escada que dá acesso ao corredor dos laboratórios fica sem supervisão, além do acesso livre aos corredores onde ficam as portas dos laboratórios e de funcionários que realizam a limpeza em todo prédio. Nos corredores verificam-se a presença de extintores de incêndio.

Já o interior dos laboratórios pode-se dividir em dois grupos: os mais antigos em número de 2 (dois) são os primeiros laboratórios que vieram a funcionar no novo prédio e apresenta estruturação de cabeamento de rede e de energia exposta, apenas fixadas por presilhas ou enroladas/presas as bancadas, alguns soltos, desconectados das máquinas. Também verificou-se que muitos periféricos encontram-se desconectados dos computadores e gabinetes, estabilizadores e monitores problemáticos encontram-se posicionados junto à paredes ou mesmo sob as bancadas, muitas vezes até confundindo o usuário com os equipamentos em bom estado. Outra realidade verificada foi o livre acesso ao dispositivo de rede onde os cabos de rede das máquinas estão conectados. Nesses laboratórios, para que o usuário possa fazer uso dos computadores é necessário que ele esteja acompanhado de um responsável (professor, monitor) ou portando um documento liberado e assinado pela direção.

Nos 3 (três) laboratórios mais novos uma realidade um pouco diferente é constatada, a começar pela presença física de um funcionário da UFPB que permanece no interior do laboratório durante todo o período em este se encontra em funcionamento. Nesses laboratórios o acesso de usuários é livre, bastando apenas o mesmo se identificar e ter direito de utilizar os computadores. A porta que dá acesso ao interior dos laboratórios fica aberta durante todo período de funcionamento, uma vez que não existe sistema de ar-condicionado. Há supervisão aos usuários pelo funcionário, pois o mesmo ocupa uma posição que tem visão dos equipamentos. Nos corredores verifica-se a presença de extintores. Nesses laboratórios as máquinas utilizam travas evitando qualquer intenção de roubo de peças dos gabinetes. Quanto ao cabeamento, apresenta uma grande melhoria onde os cabos de rede são segregados dos cabos de energia e embutidos por tubulações e a rede mostra-se mais organizada, onde um armário localizado na parede ao lado da posição onde fica o funcionário concentra os equipamentos de rede, porém não há marcações nos cabos que facilitariam o manuseio. Também não há periféricos ou equipamentos defeituosos espalhados pela bancada, porém existem caixas com equipamentos empilhados em um canto da sala. De acordo com a tabela 2, podem-se verificar os ambientes visualizados.

Questões Observadas	**Laboratórios**	**Ativa/ Existe**	**Parcial**	**Nenhuma**
Presença do vigilante nos corredores.	Antigos			X
	Novos			X
Controle de acesso ao corredor dos laboratórios.	Antigos			X
	Novos			X
Proteção na área dos laboratórios: portas trancadas quando não ocupados	Antigos	X		
	Novos	X		
Equipamentos de combate a incêndios.	Antigos	X		
	Novos	X		
Cabeamento (proteção contra danos, segregados da rede elétrica, uso de marcações).	Antigos			X
	Novos		X	
Cumprimento de normas quanto ao consumo de alimentos.	Antigos		X	
	Novos		X	

Tabela 1: resultados da análise in loco realizada no ambiente dos laboratórios.

Dessa análise *in loco*, constatou-se que, no ambiente externo, percebe-se a presença de seguranças que vigiam o prédio, porém ocupam com maior frequência o térreo, somente quando é solicitado para abrir algum laboratório é que o vigilante se desloca para o andar onde ficam os laboratórios. Já no acesso aos laboratórios não há nenhum obstáculo, pois qualquer pessoa tem acesso aos corredores através da escada. Nos corredores é possível

encontrar extintores de incêndio; e quando não estão sendo usadas, as portas dos laboratórios ficam trancadas. Quanto ao cabeamento de rede externo que entra nas salas dos laboratórios, verificou-se que se apresenta de maneira exposta, visível. No ambiente interno foi possível averiguar que, durante uso qualquer pessoa podia abrir a porta, muitas vezes atrapalhando a aula. Alguns avisos diziam que era proibido consumo de alimentos, bebida no local, mas algumas observações mostraram embalagens de bombons e chicletes deixados sobre a bancada no laboratório novo enquanto no antigo nenhum vestígio verificado. O cabeamento interno dos laboratórios antigos é exposto e segui junto aos cabos de energia por traz dos gabinetes dos computadores. Muitos estavam soltos e o acesso aos equipamentos de rede onde os cabos estão conectados é exposto, podendo qualquer pessoa ter acesso aos equipamentos. Já os novos laboratórios, os cabos de rede são segregados da fiação elétrica e instalados em tubulações próprias, porém não se observa utilização de marcações e o equipamento de rede está protegido, numa caixa apropriada, contra acesso.

A análise in loco demonstrou que necessita melhorias quanto ao controle de acesso aos corredores e verificação por parte dos seguranças, maior rigidez na aplicação de regras quanto a comer e beber no ambiente dos laboratórios além de melhorias na estrutura do cabeamento de rede.

3.2.2 Entrevistas

O ambiente dos laboratórios: prédio e corredores são de acesso livre, isso é justificado também devido ao próprio ramo de atividade onde estão inseridos os laboratórios: numa organização onde o ensino, aprendizagem dos usuários é em primeiro lugar e dar acesso à informação e ao conhecimento é muito importante, pois nos laboratórios é possível realizar pesquisas através da internet, além de executar atividades através do uso de softwares instalados nas máquinas. Este livre acesso ao prédio e aos corredores é confirmado com a declaração do vigilante que, perguntado sobre a permissão de tráfego de pessoas nos corredores dos laboratórios:

> “... não é proibido andar, subir para o andar superior dos laboratórios.”

A segurança oferecida ao ambiente dos laboratórios que ficam localizados em um dos novos prédios do campus se resume a presença de vigilantes que fazem a segurança 24 horas todos os dias. Essa proteção é complementada com outras ações: verificação de portas e janelas quando se encerra o expediente daquele funcionário da segurança, proibição de abertura dos laboratórios para usuários sem identificação e garantia da guarda de todas as

chaves das portas dos laboratórios. Porém, quando estão sendo utilizados, os vigilantes não garantem nenhuma proteção aos laboratórios. Essas afirmações são confirmadas com o chefe dos vigilantes que perguntado sobre como é atualmente feita a segurança oferecida aos laboratórios:

> "... a segurança é totalmente voltada para a instituição, não podemos reagir a qualquer ação de alunos: se o mesmo persistir em entrar, não abriremos, somente com documento carimbado e assinado pela coordenação de curso. Todas as chaves ficam sob nossa responsabilidade e somente quando solicitado é que abrimos o laboratório. Têm direito ao acesso aqueles alunos monitores, funcionários que trabalham como responsáveis pelo funcionamento dos laboratórios e também alunos acompanhados de monitores ou professores. É responsabilidade pelo laboratório aquele que solicitou a abertura do mesmo, nós garantimos a segurança das chaves. Sempre que vai haver troca de vigilante, aquele que esta deixando o plantão confere portas e janelas registrando no livro de ocorrências e essa é a única verificação feita antes de outro vigilante assumir."

O sistema de utilidades, ou seja, suprimento de energia dos laboratórios é recente assim como todas as construções e instalações do campus que ainda vem sendo construído. O prédio que acomoda os laboratórios foram um dos primeiros a ser construído, todo o projeto arquitetônico, elétrico e de rede encontram-se na prefeitura universitária no campus I. Como o serviço que os laboratórios oferecem aos usuários dependem do fornecimento e suprimento dessas utilidades, atualmente não se verifica a presença de uma unidade que garanta a continuidade das atividades acadêmicas desenvolvidas nesses ambientes, caso haja queda no fornecimento de energia através da rede pública, nem em todas as máquinas, nem no prédio. Pode-se constatar com as afirmações do engenheiro responsável pela manutenção do campus de Rio Tinto e pelo analista de TI que compõe a equipe de suporte respectivamente, quando perguntados sobre como era o fornecimento de energia nos laboratórios, o sistema de refrigeração, se existe gerador que garantisse o fornecimento de energia aos computadores, existência de para-raios e de múltiplas linhas de entrada:

> "Nenhuma construção aqui possui para-raios, nem geradores e só temos um único transformador que garante o fornecimento do campus todo, apenas uma linha de conexão entre nossa rede e a rede elétrica existe. Os ar-condicionados foram

solicitados levando em consideração o tamanho das salas dos laboratórios e muitos até vieram acima da capacidade solicitada."

"... pelo que sei, desconheço uso de gerador em qualquer campus da UFPB. Não existem para-raios aqui e não temos como garantir nobreak para todas as maquinas dos laboratórios, pois os que existiam foram perdendo capacidade de suas baterias e queimando. O transformador presente aqui no campus é trifásico e possui um sistema que caso haja falha numa linha elétrica do campus, ele garante o fornecimento em outras duas."

Inicialmente apenas dois laboratórios funcionavam quando do término da construção do prédio, outros três são mais recentes e apresentam melhorias em relação aos antigos. Estas melhorias são principalmente quanto à segurança do cabeamento estruturado interno, apresentando organização, proteção e segregação entre rede e elétrico; outra melhora é no equipamento de rede que apresenta proteção quanto ao acesso indevido. Essa informação é confirmada com as respostas dos dois técnicos em TI que são responsáveis pelo funcionamento dos laboratórios quando perguntados sobre a segurança do cabeamento:

"O cabeamento dos laboratórios antigos não possui uma organização adequada: estão sem marcações, alguns ficam soltos após utilização em computadores portáteis e os equipamentos de rede ficam próximos e na mesma bancada dos computadores. Já os novos laboratórios apresentam melhorias como utilização de tubulações que protegem os cabos de rede e separam da rede elétrica, os equipamentos de rede estão posicionados em caixas apropriadas com fechadura evitando que alguém tenha contato."

O controle de acesso no ambiente dos laboratórios é resumido ao fechamento dos laboratórios e à presença de um responsável que possui o livre acesso. Pode-se verificar na afirmação de um dos técnicos de TI quando perguntado quais os controles utilizados contra o acesso não autorizado:

"A utilização dos laboratórios é somente para alunos dos cursos de Sistemas de Informação e Licenciatura em Ciências da Computação, além dos outros cursos. Não existe nenhuma proteção desde o térreo até o interior dos laboratórios que garanta que somente alunos tenham acesso. Qualquer pessoa pode chegar e entrar no caso dos novos laboratórios porque não temos como, a cada pessoa que entrar, perguntar se é

> aluno; como os mais antigos são abertos geralmente por um professor que ministra aula, ao fim das atividades o laboratório é fechado."

O suporte dado aos computadores dos laboratórios é dado a princípio pelos técnicos que revezam os horários manhã e tarde, ou seja, qualquer problema verificado por um usuário inicialmente é ele quem irá verificar. Caso o problema não seja sanado, a equipe de manutenção receberá um chamado solicitando o reparo do equipamento. Além desses procedimentos, existem também outras alternativas, isso porque muitas das máquinas ainda estão na garantia e portanto o suporte é dado pelo fabricante, como podemos constatar com a resposta do analista de TI que perguntado como funciona a manutenção dos equipamentos:

> "Inicialmente os técnicos verificam o problema lá no próprio local onde está o computador e caso não resolva, é registrado um chamado no sistema que temos para nos auxiliar nas requisições e então iremos pegar o equipamento, caso esteja na garantia, matemos contato com o fabricante que vem até nós."

Sobre tal procedimento descrito na fala do analista: de realização do reparo no próprio laboratório, foi perguntado se esta atividade é supervisionada:

> "...sim, sempre vai alguém com a pessoa que vem prestar o serviço."

A equipe de suporte segue um plano de manutenção elaborado pelos próprios membros que, na medida do possível, mantém os equipamentos funcionando e aqueles equipamentos sem solução são encaminhados para o campus I da UFPB, onde lá eles darão destino. As operações são registradas no sistema de suporte. Pode-se constatar que muitos dos computadores não possuem equipamentos que garanta o fornecimento de energia, isso pôde ser verificado na resposta do analista quando perguntado sobre o planejamento de manutenção:

> "Temos um plano de manutenção que é próprio e foi elaborado levando em consideração as recomendações do fabricante; todo período é feito um levantamento das ocorrências e modificamos esse plano. Nós registramos tudo em um sistema online que temos. Atualmente realiza-se uma manutenção corretiva que na maioria das vezes busca-se garantir disponibilidade do equipamento. Também não temos como

garantir nobreak para todos os computadores dos laboratórios, ao longo do tempo as baterias tiveram problemas e fomos substituindo por estabilizadores.”

Realizadas nos meses de novembro e dezembro de 2012 e janeiro de 2013 com os responsáveis pela segurança e vigilância do ambiente dos laboratórios (prédio e corredores), além dos funcionários responsáveis pelo funcionamento dos equipamentos nos laboratórios e empréstimo dos mesmos.

A entrevista com os funcionários responsáveis pelo funcionamento e segurança dos equipamentos teve como base o questionário apresentado no Apêndice.

Os resultados das respostas das entrevistas podem ser vistos na tabela 2.

Questões Observadas	**Laboratórios**	**Existe/ Sim**	**Parcial**	**Nenhuma**	**Não opinar**
Participação dos responsáveis em planejar, melhorar os ativos dos laboratórios.	Funcionário1			X	
	Funcionario2			X	
Proteção oferecida contra incêndios	Funcionario1		X		
	Funcionario2		X		
Existência de controle de acesso físico	Funcionario1			X	
	Funcionario2			X	
Utilização de suprimento de energia que garanta continuidade das atividades(gerador, UPS)	Fuincionari1			X	
	Funcionario2			X	
O suprimento de energia inclui múltiplas linhas de energia?	Fuincionari1				X
	Funcionario2				X
	Funcionario2				
Existência e cumprimento de politica de mesa limpa	Funcionario1		X		
	Funcionario2		X		
Cabeamento recebe proteção contra danos e possuem marcações.	Funcionario1		X		
	Funcionario2			X	
O cabeamento é protegido de trajetos de áreas publicas?	Funcionario1			X	
	Funcionario2			X	
O cabeamento de rede é segregado da rede elétrica?	Funcionario1	X			
	Funcionario2	X			
A manutenção segue recomendações do fornecer e das especificações?	Funcionario1			X	
	Funcionario2			X	
A manutenção é realizada somente por pessoal autorizado?	Funcionario1	X			
	Funcionario2	X			
É mantido registro das manutenções?	Funcionario1	X			
	Funcionario2	X			

Tabela 2: Resultado da entrevista com funcionários dos laboratórios.

As respostas mostram que o envolvimento dos responsáveis no planejamento, manutenção e melhoria dos laboratórios não existe, o que contraria com o que estabelece a

norma; quanto à proteção contra incêndios dentro dos laboratórios é necessário existência de maior numero de equipamentos de combate a incêndios. Nenhum controle de acesso físico é aplicado, necessitando de regras. Deve-se ser considerado um suprimento de energia que garanta a continuidade das atividades. E regras quanto a comer, beber e fumar no ambiente necessitam ser aplicadas com maior rigor. Sobre o cabeamento (caminhos da fiação, proteção contra danos, marcação) obteve-se que pouco melhorou dos antigos para os novos laboratórios. Observa-se também que não há um plano de manutenção para os equipamentos estabelecido como recomenda fabricante e especificações.

Já a entrevista realizada com um funcionário e seu chefe responsáveis pela vigilância, obteve-se os resultados mostrados na tabela 3.

Questões Observadas	**Sim**	**Parcial**	**Não**	**Não opinar**
O laboratório pode ser utilizado por qualquer pessoa?			X	
Utiliza-se algum controle de acesso?	X			
Quando estão fechados, os laboratórios são frequentemente verificados?			X	
É permitido o trânsito de pessoas nos corredores.	X			

Tabela 3: Resultado da entrevista com vigilante.

Os resultados mostram que deve haver uma inspeção maior nos corredores e salas e nos acessos aos laboratórios.

A entrevista com o funcionário responsável pela garantia de empréstimo dos equipamentos teve como foco a subseção 9.2.7 intitulada Remoção de propriedade da norma NBR 27002. Abaixo a tabela 4 com as respostas obtidas.

Questões Observadas	**Sim**	**Parcial**	**Não**	**Não opinar**
É necessária autorização prévia para realização empréstimo?	X			
É registrado dados: nome, data e hora?	X			
Somente pessoas autorizadas realizam empréstimos?	X			

Tabela 4: Resultado da entrevista com funcionário responsável pelo empréstimo.

Nessa entrevista verificou-se que os equipamentos necessitam de autorização prévia para empréstimo, que somente pessoas autorizadas podem solicitar e todas as ações são registradas.

3.2.3 Aplicação de questionários

Ocorreram no mês de novembro de 2012 e entre janeiro e fevereiro de 2013 com objetivo de conhecer a visão que os usuários têm da segurança existente no ambiente dos laboratórios. O questionário foi aplicado a uma quantidade de 60 usuários dos laboratórios dentre alunos dos cursos de Sistemas de Informação e Licenciatura em Ciências da Computação e também professores e funcionários responsáveis pelo funcionamento dos laboratórios. Contém 14 (quatorze) perguntas que abordaram aplicação de controles de segurança descritos nas sessões do capitulo 9 (nove) da norma NBR 27002, a saber:

- Planejamento de melhorias.
- Segurança em salas e instalações.
- Perímetro de segurança física.
- Trabalho em áreas seguras.
- Proteção contra ameaças externas e do meio ambiente.
- Proteção de equipamentos.
- Segurança do cabeamento.
- Remoção de propriedade.

A seguir são apresentados os gráficos de cada questão abordada com os resultados.

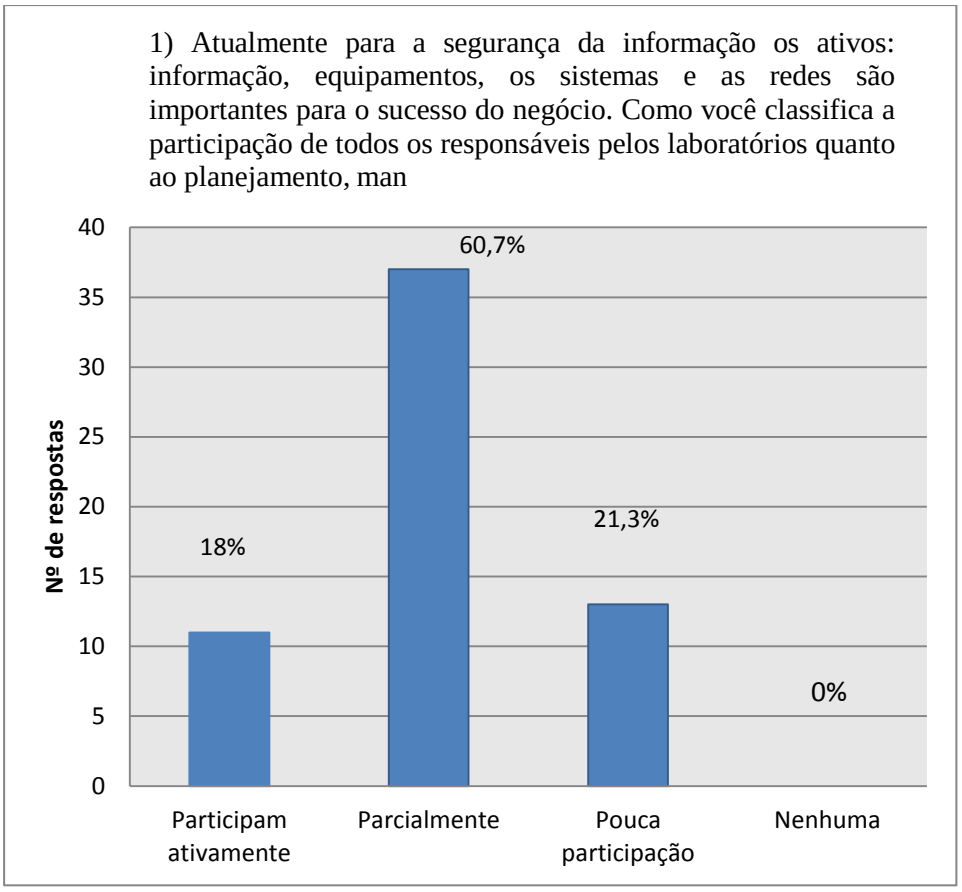

Figura 8: Envolvimento dos responsáveis na segurança dos recursos.

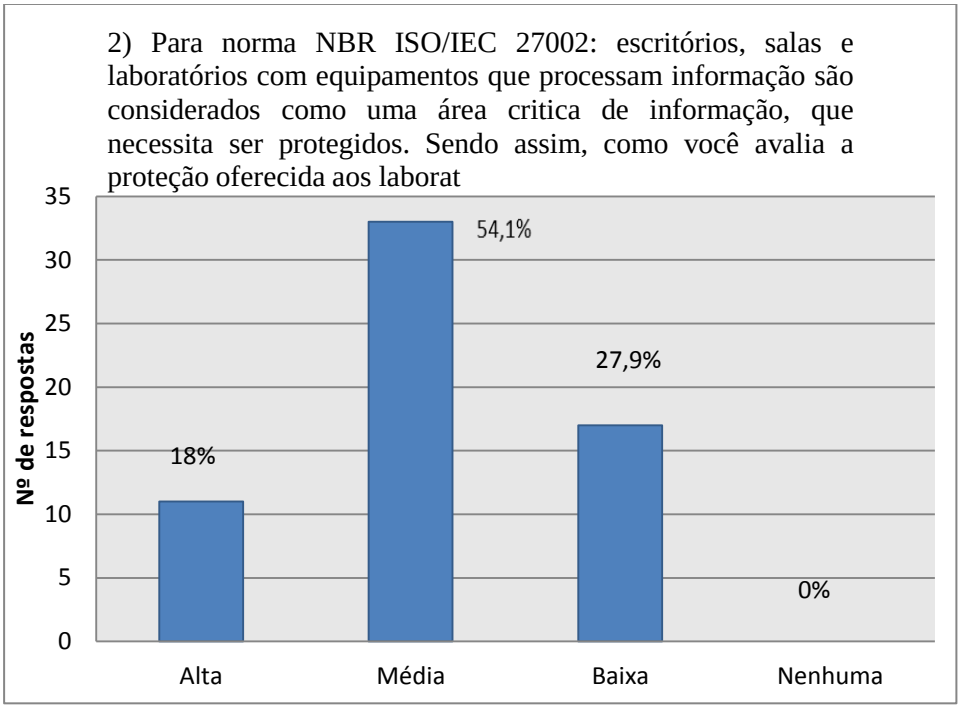

Figura 9: segurança nas áreas críticas.

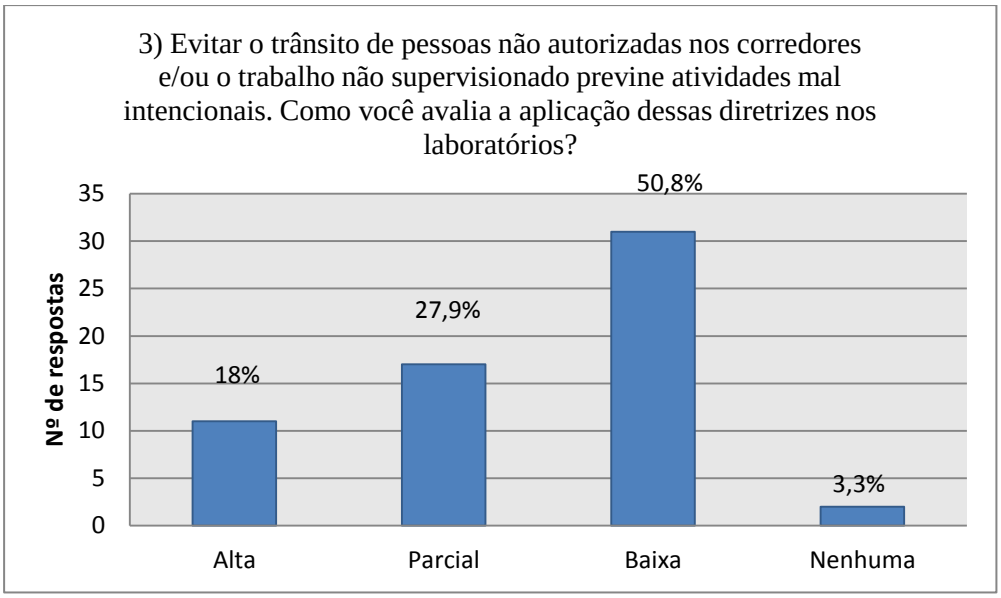

Figura 10: Controle de acesso

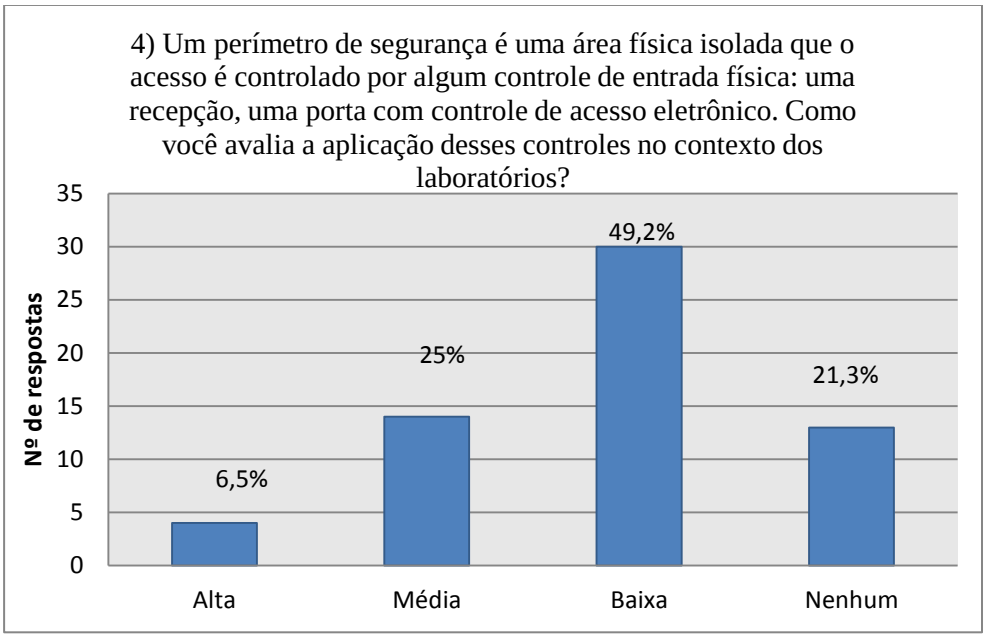

Figura 11: Controle de acesso físico.

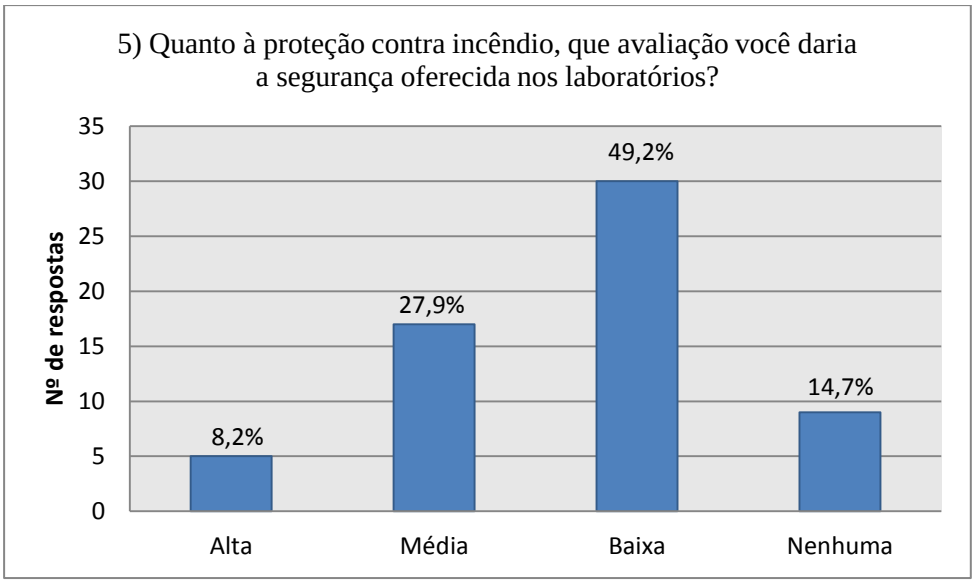

Figura 12: Segurança contra ameaças do meio ambiente

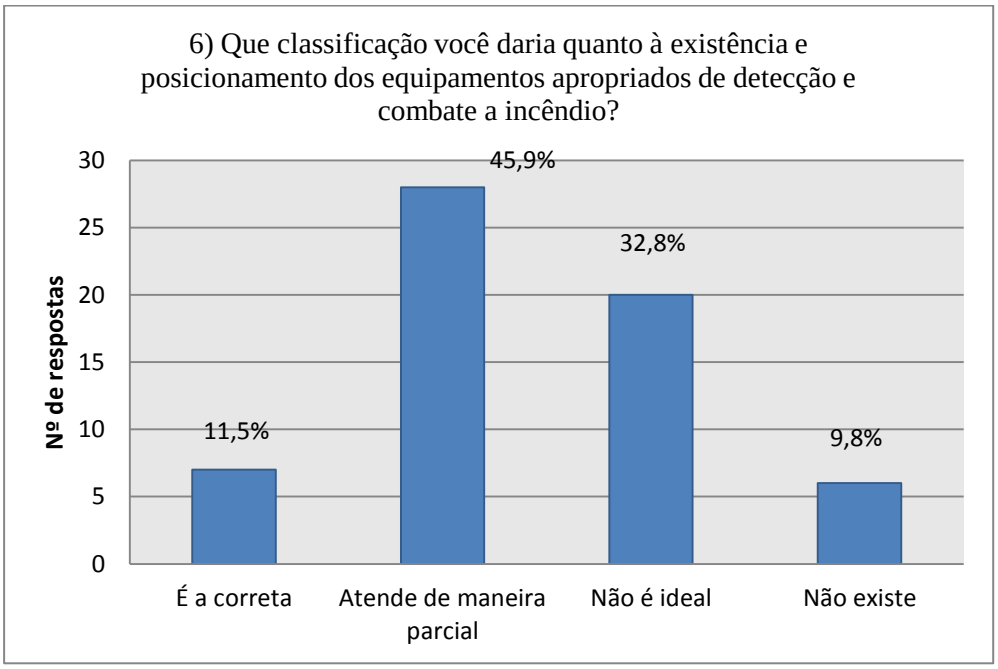

Figura 13: Proteção contra ameaças externas e do meio ambiente.

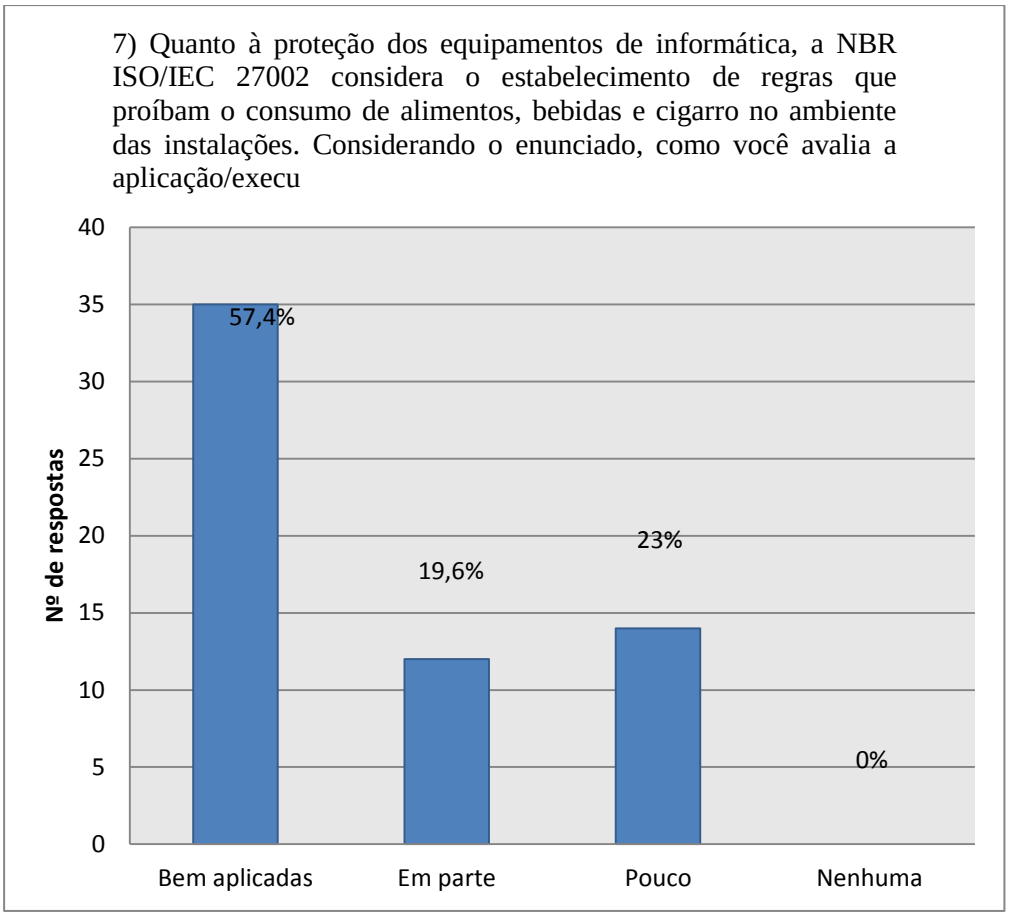

Figura 14: Proteção do equipamento.

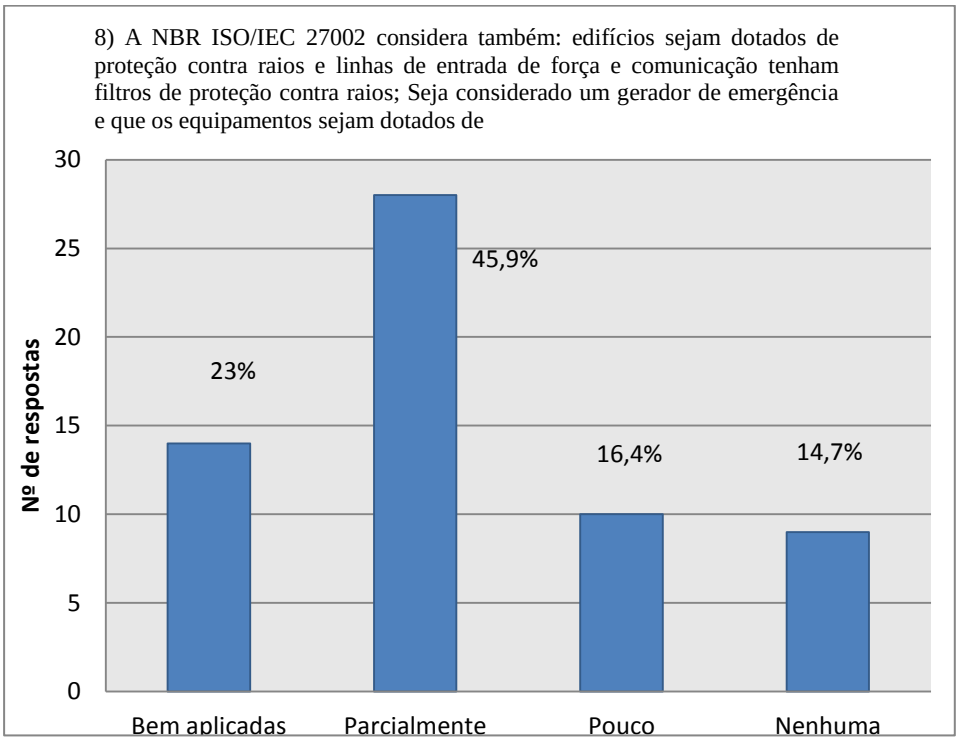

Figura 15: Utilidades e proteção dos equipamentos.

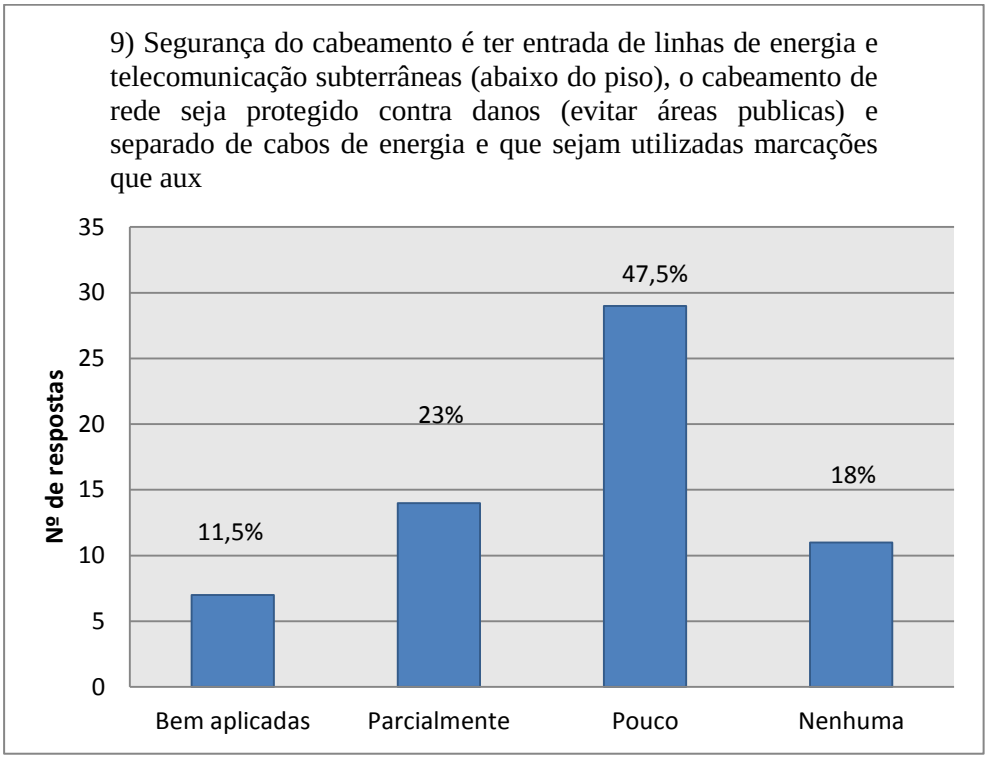

Figura 16:Segurança do cabeamento.

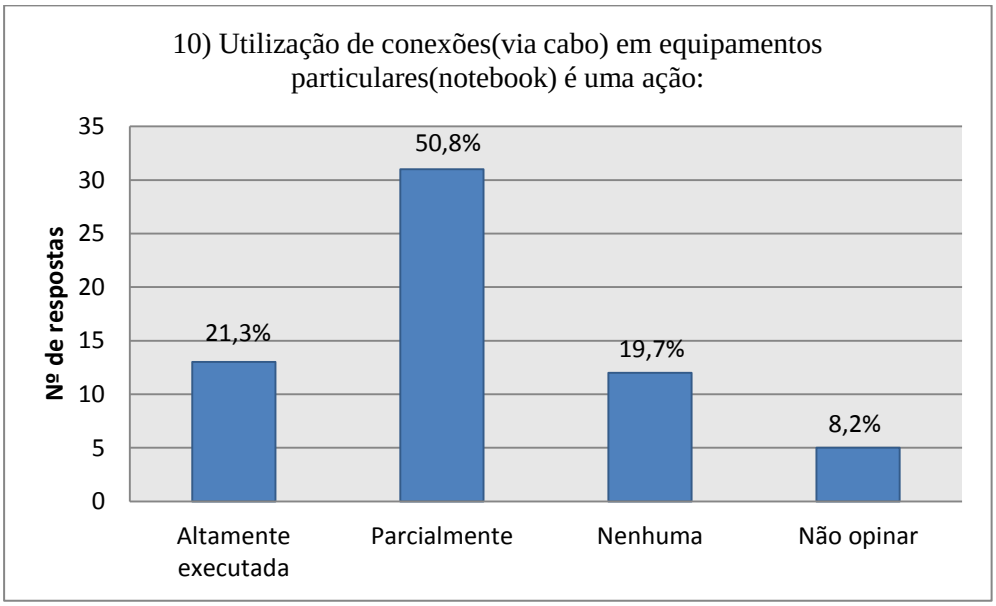

Figura 17: Segurança do cabeamento.

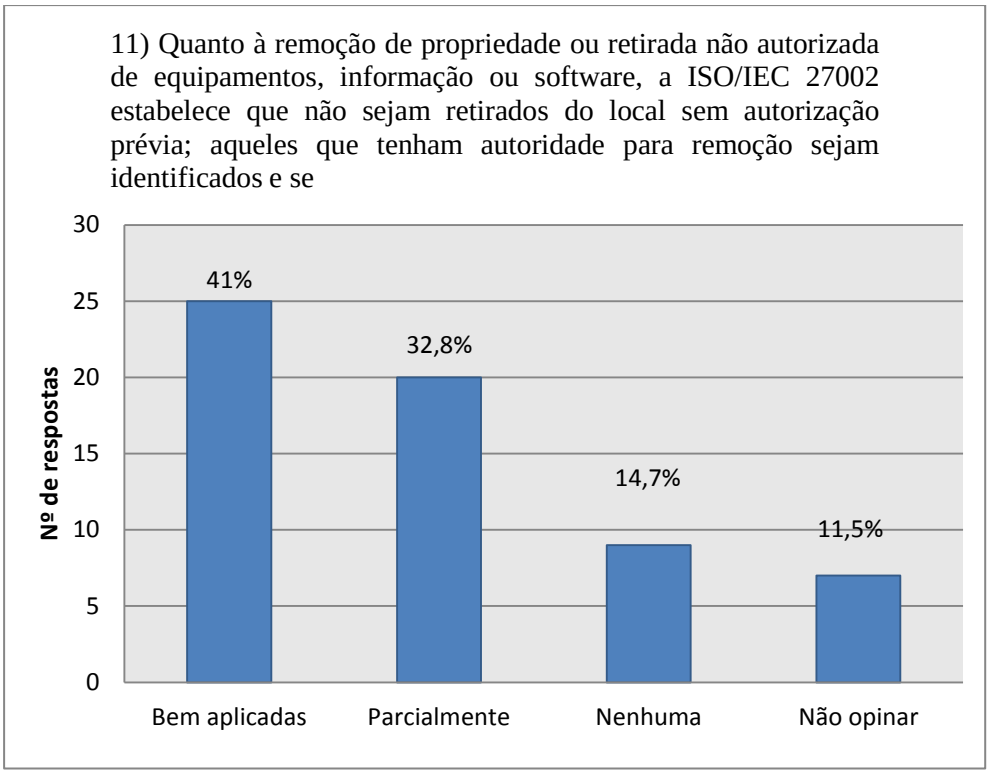

Figura 18: Empréstimo de equipamento.

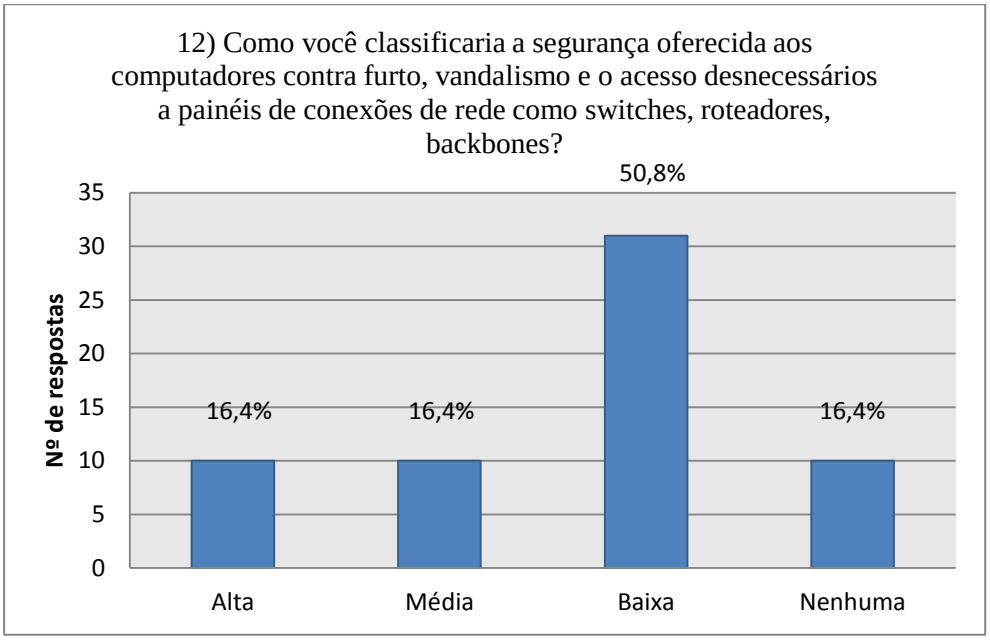

Figura 19: Segurança do equipamento

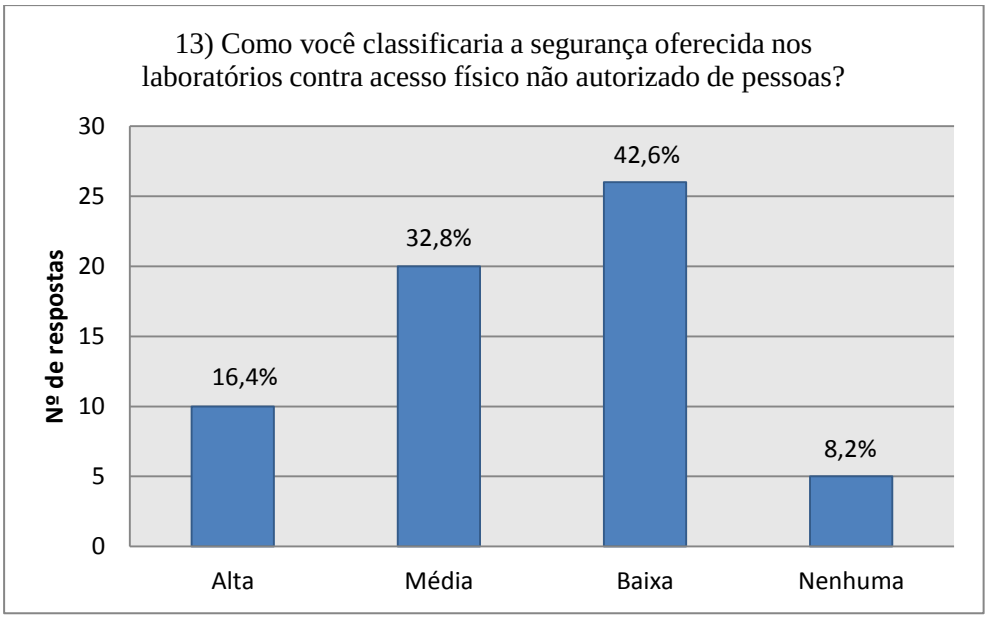

Figura 20: Controles de entrada física.

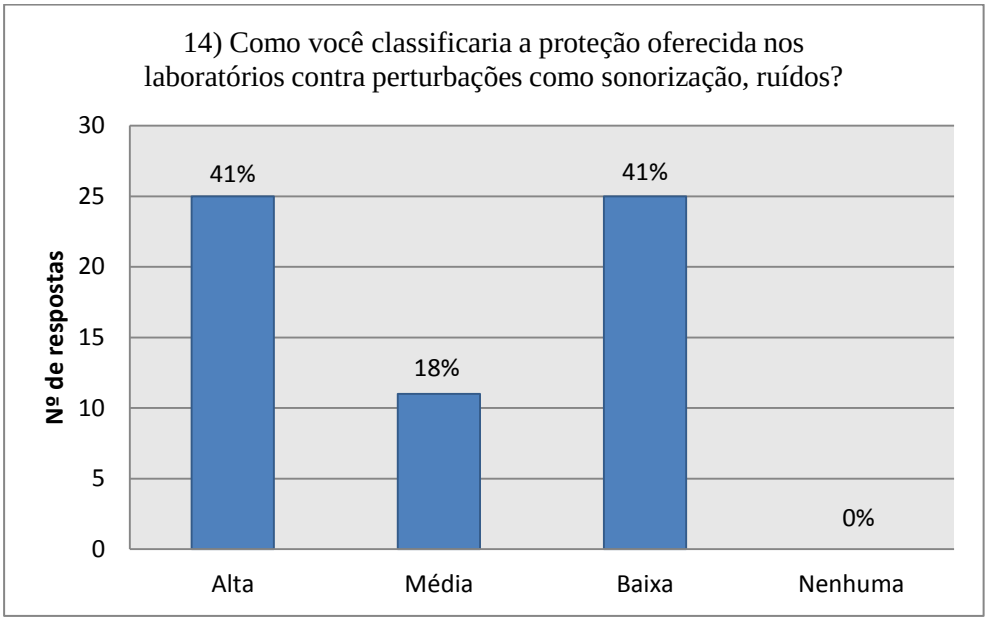

Figura 21: Proteção contra ameaças externas e do meio ambiente.

Os resultados mostraram que 60,7% dos usuários acreditam que os responsáveis pelos laboratórios envolvem-se de forma parcial na busca por melhoria aos ativos dos laboratórios. Outros 50,8% consideram como baixo a aplicação de controles que evitem o acesso físico não autorizado em corredores e salas dos laboratórios e outros 42,6% dos usuários considera baixa a segurança nos laboratórios contra o acesso físico não autorizado. Em relação ao ambiente dos laboratórios, houve um empate, 41% considera que os laboratórios são livre de perturbações externas, ruídos; outros 49,2 % consideram a proteção contra incêndio baixa e

45,9% classifica como parcial a existência e posicionamento de equipamentos apropriado de combate a incêndio. Já a segurança dos equipamentos é caracterizada da seguinte maneira: 57,4% consideram bem aplicadas as regras que proíbem consumo de alimento e bebidas no ambiente dos laboratórios, considera também de maneira parcial a proteção contra raios, presença de suprimento de energia que garanta continuidade das atividades. E no geral, 54,1% dos usuários classificam a proteção oferecida aos laboratórios como intermediária.

3.3 Considerações sobre a segurança dos laboratórios

Na seção 3.2 foram apresentados dados coletados através de *análise in loco*, questionários e entrevistas. Analisando os resultados, vemos que os laboratórios em estudo seguem regulamentos ou normas instituídos no âmbito interno da organização, neste caso o CCAE da UFPB. Como já apresentado no capítulo 1, normas para segurança da informação existem, sendo um guia para padronização das boas práticas de segurança, neste caso nos laboratórios do CCAE.

Portanto, é imperativo confrontar as normas de segurança atualmente implementadas nos laboratórios com as normas estabelecidas pela NBR ISO/IEC 27002, conseguindo como resultado qual o grau de adequação das normas atuais em vigor com a padronização pela norma NBR ISO/IEC 27002, obtendo assim adequação dos laboratórios as boas práticas de segurança da informação estabelecidas. A verificação com a norma e seus resultados são apresentados no capítulo 4.

4. GRAU DE ADEQUAÇÃO DA SEGURANÇA FÍSICA E AMBIENTAL

Este capítulo aborda o resultado do estudo caracterizado e realizado no capítulo anterior descritos nas seções 3.1 e 3.2 e também traz um estudo sobre a segurança física e do ambiente descrito na seção 9 (nove), subseções 9.1.1, 9.1.2, 9.1.4, 9.1.5, 9.2.1, 9.2.3, 9.2.4 e 9.2.7 da norma NBR ISO/IEC 27002 e realizará uma comparação entre ambos os estudos mostrando o grau de adequação da segurança dos laboratórios em relação à norma.

4.1 Estudo sobre a segurança física e do ambiente conforme a NBR ISO/IEC 27002

A segurança física e do ambiente estabelecida na norma NBR ISO/IEC 27002 trata da segurança de áreas onde há equipamentos de valor para organização. O capitulo está dividido em duas seções: Áreas de Segurança e Segurança dos Equipamentos, onde são estabelecidos controles de combate e prevenção contra acesso físico não autorizado, manutenção dessas áreas, fiscalização, proteção contra ameaças externas e ambientais e segurança dos equipamentos.

Áreas de Segurança é o espaço físico que precisa ser protegido contra as ameaças que poderiam gerar um incidente de segurança da informação. Esse espaço considerado como área crítica tem importância e valor para organização, e necessita de proteção física: difícil acesso para o publico, portas e janelas devem permanecer trancados, equipamentos de detecção de intrusos devem ser instalados, seja considerado equipamentos de combate a incêndios e desastres naturais. Essas áreas com acesso público deve ser controlado através da definição de um perímetro de segurança que aumenta o nível de segurança.

Os equipamentos que processam dados devem estar seguros, garantidos, tais como computadores, impressoras, projetores, etc. Essa segurança envolve uma fonte ideal de energia, proteção contra ameaça física (furto, vandalismo), contra ameaças externas e do meio ambiente (incêndio, água, vibração). Todo equipamento deve ser protegido por um perímetro de segurança que na maioria das vezes envolve toda uma área. Porém uma área pode ser considerada segura apenas em função do ativo nela existente. Neste caso talvez a aplicação ou isolamento do ativo poderia diminuir a necessidade de segurança para toda área. Deve ser considerada uma política de proibição de consumo de alimentos nos interiores de salas e que todo cabeamento permaneça seguro com proteção contra danos. Já a manutenção dos equipamentos necessita ser planejada e realizada de maneira rápida e correta, garantindo as condições de uso.

Para este trabalho foram selecionados desta norma os seguintes tópicos:

- Perímetro de segurança física (subseção 9.1.1).
- Proteção contra ameaças externas e do meio ambiente (subseção 9.1.4).
- Trabalho em Áreas seguras (subseção 9.1.5).
- Proteção dos equipamentos (subseção 9.2.1).
- Utilidades (subseção 9.2.2).
- Segurança do cabeamento (subseção 9.2.3).
- Manutenção dos equipamentos (subseção 9.2.4).
- Remoção de propriedade (subseção 9.2.7).

Juntos, esses tópicos formam duas categorias de segurança que estabelece a Segurança Física e Ambiental da NBR 27002, estabelecendo controles, medidas e diretrizes de segurança. A seguir serão apresentadas cada uma e seus objetivos.

4.1.1 Áreas seguras

O objetivo é prevenir o acesso físico não autorizado, danos ou interferências às instalações de uma organização. Nessa categoria estão inclusos Perímetro de segurança física, Proteção contra ameaças externas e do meio ambiente e Trabalho em Áreas seguras. A norma NBR ISO/IEC 27002 estabelece que um perímetro de segurança seja uma área física isolada que o acesso é controlado pelos seguintes controles de entrada física:

1. Porta com mecanismo de controle de acesso através de cartão ou uma área de recepção ou balcão com recepcionistas.
2. Uso de proteção como portas e janelas trancadas.
3. Sistemas adequados de detecção como alarmes.

O objetivo do perímetro de segurança é dificultar o acesso aos ativos através de uma dessas barreiras física. As áreas de segurança também podem ser implantados controles de acesso através de senhas que além da segurança, garante registro de todos os acessos que podem ser utilizados por eventuais auditorias. Deve-se levar em conta na definição do perímetro, a importância dos ativos para definir os investimentos em controles, além da sintonia dos colaboradores com uma cultura de segurança da informação. Esta cultura deve ser divulgada em toda empresa.

A Proteção contra ameaças externas e do meio ambiente é a aplicação de diretrizes, controles ou proteção contra ameaças físicas. São eles:

1. Providências e posicionamentos correto de equipamentos apropriados de combate a incêndios.
2. Proteção contra perturbações: barulho de som, ruídos.

O Trabalho em Áreas seguras é definido na norma como planejamento e aplicação de proteções físicas e diretrizes para o trabalho nessas áreas:

1. Áreas seguras não ocupadas estejam trancadas e sejam periodicamente verificadas.
2. Seja evitado o trabalho não supervisionado para prevenir e evitar atividades mal intencionais.

4.1.2 Segurança de equipamentos

O objetivo dessa categoria é impedir perdas, danos ou furtos de ativos e estabelece os seguintes controles: Proteção dos equipamentos que é a adoção de medidas para minimizar o risco de ameaças físicas: furto, vandalismo, incêndio, água; estabelece que sejam adotadas as seguintes diretrizes:

1. Regras quanto a comer, beber e fumar no ambiente.
2. Que todos os prédios sejam dotados de para-raios, que haja gerador de emergência e o suprimento de energia garanta o funcionamento dos equipamentos e continuidade das atividades.
3. Controles para minimizar os riscos de ameaças físicas como furto, vandalismo.
4. O sistema de refrigeração seja adequado às necessidades do ambiente.

Também inclui Segurança do cabeamento que estabelece:

1. Proteção contra danos.
2. Que as linhas sejam subterrâneas, evitando áreas públicas.
3. A rede elétrica seja segregada da rede de computadores.
4. Os cabos devem utilizar marcações que auxiliem no manuseio.

Quanto à Manutenção dos equipamentos, são consideradas as seguintes diretrizes:

1. Que seja realizada manutenção correta garantindo disponibilidade e integridade dos equipamentos de informática.

2. Que a manutenção preventiva obedeça aos prazos estabelecidos pelo fabricante ou fornecedor e de acordo com as especificações do equipamento.
3. Que a manutenção seja realizada por pessoal autorizado ou caso não, sempre realizado na supervisão de um responsável.

A Remoção de propriedade estabelece:

1. Que somente pessoal autorizado e identificado possa retirar equipamentos.
2. Que não sejam retirados sem autorização prévia.
3. E sejam registrados os horários de retirada e devolução.

Os tópicos listados serão abordados e utilizados como medidas a serem aplicadas no modelo de teias como elemento para a verificação do grau de adequação dos laboratórios com a norma. Para cada laboratório, será aplicado um modelo de teias (ver figura 1). Ao final da análise dos laboratórios através do modelo de teias, espera-se como resultado o grau de adequação dos laboratórios em estudo com a segurança física e do ambiente descrita na NBR 27002.

4.2 Considerações acerca da Segurança Física e do Ambiente dos Laboratórios

A pesquisa realizada mostrou que os laboratórios de informática do CCAE apresentam normas internas de utilização que estabelece regras que buscam a segurança no ambiente dos laboratórios, descrevendo procedimentos e conduta dos usuários, além de penalidades. Também demostrou a segurança oferecida aos laboratórios através da visão dos usuários e funcionários da instituição. Percebe-se que muitos dos controles estabelecidos nas normas dos laboratórios não são cumpridos, outros em parte e alguns o são.

A seguir serão apresentados os elementos de segurança estabelecidos pela segurança física e do ambiente da norma NBR ISO/IEC 27002 e a segurança verificada dos resultados da pesquisa realizada nos laboratórios.

- **Perímetro de segurança física.**

  Foi observado através das respostas dos questionários que é baixa a aplicação de controles de proteção contra o acesso físico não autorizado no ambiente dos laboratórios. Não se verifica a presença de nenhum

obstáculo que possa restringir somente ao pessoal autorizado. Porém, há barreiras físicas que impedem o acesso nos laboratórios quando não estão ocupados como portas e janelas trancadas.

- **Proteção contra ameaças externas e do meio ambiente.**

  Aqui foram encontradas proteções físicas contra as ameaças à segurança das instalações dos laboratórios. Como mostra a análise in loco, nos corredores existem equipamentos de combate a incêndios, porém as entrevistas e os questionários mostraram que os usuários consideram baixa e parcial a proteção oferecida aos laboratórios e a existência e posicionamento desses equipamentos, respectivamente. Também é adequada a proteção contra perturbações externas.

- **Trabalho em áreas seguras.**

  A segurança dos laboratórios quando não estão sendo utilizados resume-se ao trancamento das portas e a verificação de todas elas pelos vigilantes. A limpeza dos laboratórios sempre acontece antes de iniciarem atividades com a supervisão do fiscal de limpeza.

- **Instalação e proteção do equipamento.**

  Conforme respostas na entrevista ao engenheiro e analista de suporte, atualmente o prédio que acomoda os laboratórios não possuem para-raios nem um gerador ou suprimento de energia que garanta a continuidade dos serviços oferecidos pelos laboratórios. As diretrizes quanto a comer e beber nos laboratórios são cumpridas. Os locais onde estão os gabinetes dos computadores não apresentam proteção contra risco de ameaças físicas como furto, vandalismo. O sistema de ar-condicionado é adequado para as salas dos laboratórios, porém estão ausentes nos novos laboratórios.

- **Segurança do cabeamento.**

  Verifica-se melhoria no cabeamento dos laboratórios mais novos enquanto nos outros é sem proteção. O cabeamento nos laboratórios antigos não apresenta segurança contra interceptação ou danos, expostos e não apresentam marcações, os equipamentos de rede ficam expostos. Os novos laboratórios apresentam utilização de tubulações para proteger os cabos e o equipamento de rede fica protegido contra acesso.

- **Manutenção dos equipamentos.**

  A manutenção dos equipamentos de informática dos laboratórios é realizada pela equipe de suporte dos laboratórios, seguindo um plano que considera as recomendações do fabricante. As ocorrências e operações são registradas em um sistema. Os procedimentos realizados por terceiros são realizados na presença de um técnico ou analista da equipe.

- **Remoção de propriedade.**

  A pesquisa demonstrou que as regras de empréstimo de equipamentos são bem aplicadas: somente os empréstimos agendados são concedidos, há registro de dados do solicitante.

Todas as diretrizes existentes nas resoluções de utilização dos laboratórios que estabelecem regras que devem ser atentadas pelos usuários dos laboratórios necessitam de maior divulgação, concordância com outras regras de normas de segurança para que haja prevenção contra incidentes. Isso exige conhecimento dos aspectos envolvidos na proteção e no bom funcionamento do ambiente.

4.3 Avalição de conformidade dos controles de segurança dos laboratórios com a Segurança Física e do Ambiente descrito na NBR ISO/IEC 27002.

Serão utilizados os resultados do estudo realizado nos laboratórios em níveis quantitativos de controles de segurança utilizados/verificados ou aplicados no ambiente, os controles da segurança física e do ambiente e o modelo de teias que utilizará o nível de segurança verificado nos laboratórios e a segurança estabelecida pela norma para comparar e estabelecer a conformidade com os requisitos. A seguir serão apresentados duas instancias do Modelo de Teias aplicado aos laboratórios antigos, figura 23, e aos laboratórios novos, figura 24.

4.3.1 Modelo de Teias aplicado aos laboratórios

Através dessa metodologia será apresentada a segurança atual e quais medidas aplicar para alcançar o nível ideal de segurança, utilizando para isso as análises dos resultados das entrevistas, questionários e o estudo sobre a segurança física e do ambiente realizado na seção 4.1 e 4.2. Como já foi mencionado no capítulo 2 seção 2.5, o Modelo de Teias é composto por

uma figura, Roadmap (elementos de segurança) e pelas sete fases. A seguir são mostradas as fases de elaboração do modelo para os laboratórios.

Fase 1. Os elementos de segurança definidos que influenciam na segurança dos laboratórios foram os tópicos de segurança apresentados na norma e estão descritos na seção 4.1.

Fase 2. Definiu-se os laboratórios por serem ambientes com recursos, ativos de valor para organização.

Fase 3. Análise de segurança.

Fase 4. Classificação dos recursos envolveu a análise dos questionários, entrevistas; coletando-se os controles aplicados aos laboratórios.

Fase 5. Avalição dos riscos.

Fase 6. Definição do nível de segurança desejado levou em consideração os riscos e a importância dos laboratórios para as atividades acadêmicas da organização.

Fase 7. Definição das medidas de segurança a serem implementadas são as diretrizes, controles de segurança da norma NBR 27002 que devem ser aplicados para atingir a segurança desejada.

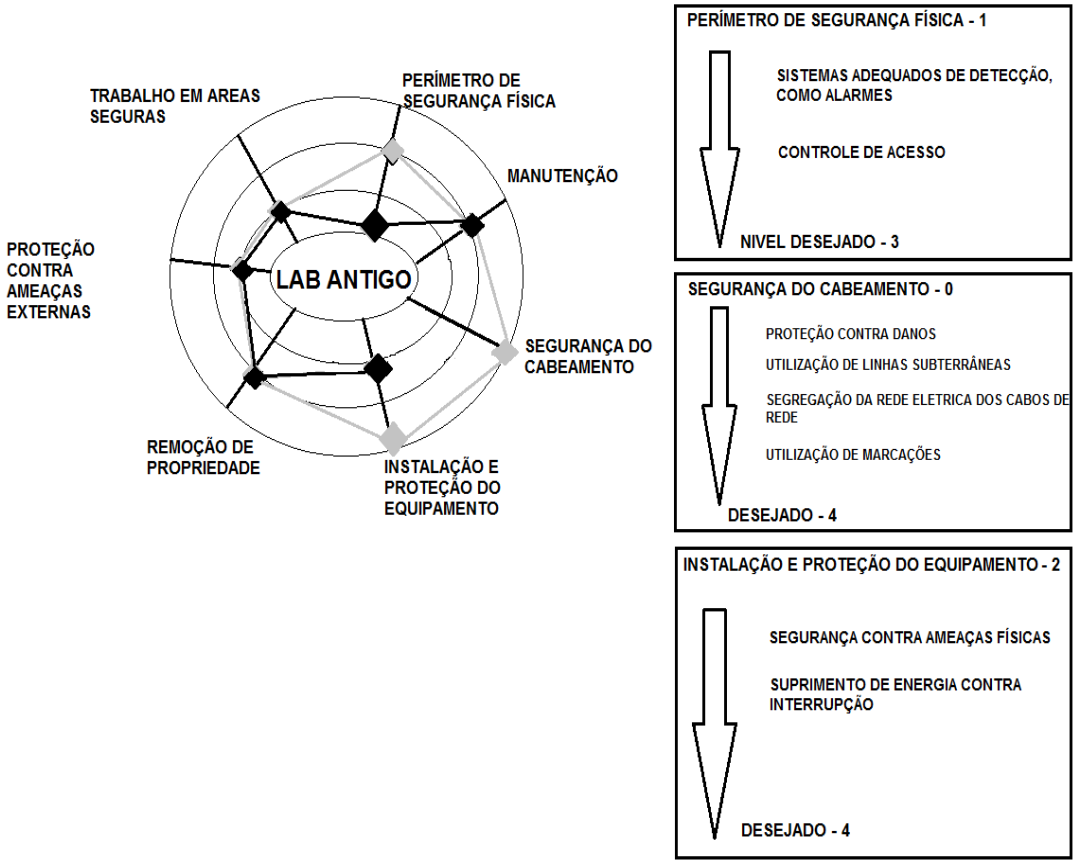

Figura 21: Modelo de Teias aplicado aos laboratórios antigos.

Analisando a figura 23, percebe-se que a segurança nos elementos manutenção, trabalho realizado em áreas seguras, proteção contra ameaças externas e remoção de propriedade estão de acordo com o que estabelece a Segurança Física e Ambiental da NBR 27002: nesses elementos de segurança o traço e o ponto preto que representa o nível atual de segurança com a presença das diretrizes estabelecida pela norma coincidem com o traço e o ponto em cinza, não necessitando de medidas. Já os elementos perímetro de segurança física, cabeamento e instalação e proteção do equipamento não tem o mesmo nível de segurança que estabelece a norma, necessitando implementar as medidas de segurança contidas no Roadmap (retângulos onde estão descritas medidas de segurança a serem aplicadas naquele elemento). Como se tem um total de três elementos de segurança em discordância com os parâmetros estabelecidos pela Segurança Física e Ambiental, os três Roadmap trazem cada um, o nível de segurança atual que, aplicando-se as medidas de segurança descritas em seu interior e definidas de acordo com que estabelece a norma, chega-se ao atendimento dos controles de segurança da NBR 27002. O perímetro de segurança física precisa avançar nos controles sistemas de detecção, alarmes e controle de acesso (uma recepção com recepcionista, acesso através de controle eletrônico ou cartão) atingiria as recomendações da norma. A segurança do

cabeamento necessita avançar implementando proteção contra danos, que as linhas sejam subterrâneas, utilização de marcações e segregação entre cabos de rede e elétrico. E por fim o elemento instalação e proteção do equipamento que apresenta dois controles, para alcançar um total de quatro preciso implementar segurança contra ameaça física e seja considerado um suprimento de energia que suporte as interrupções.

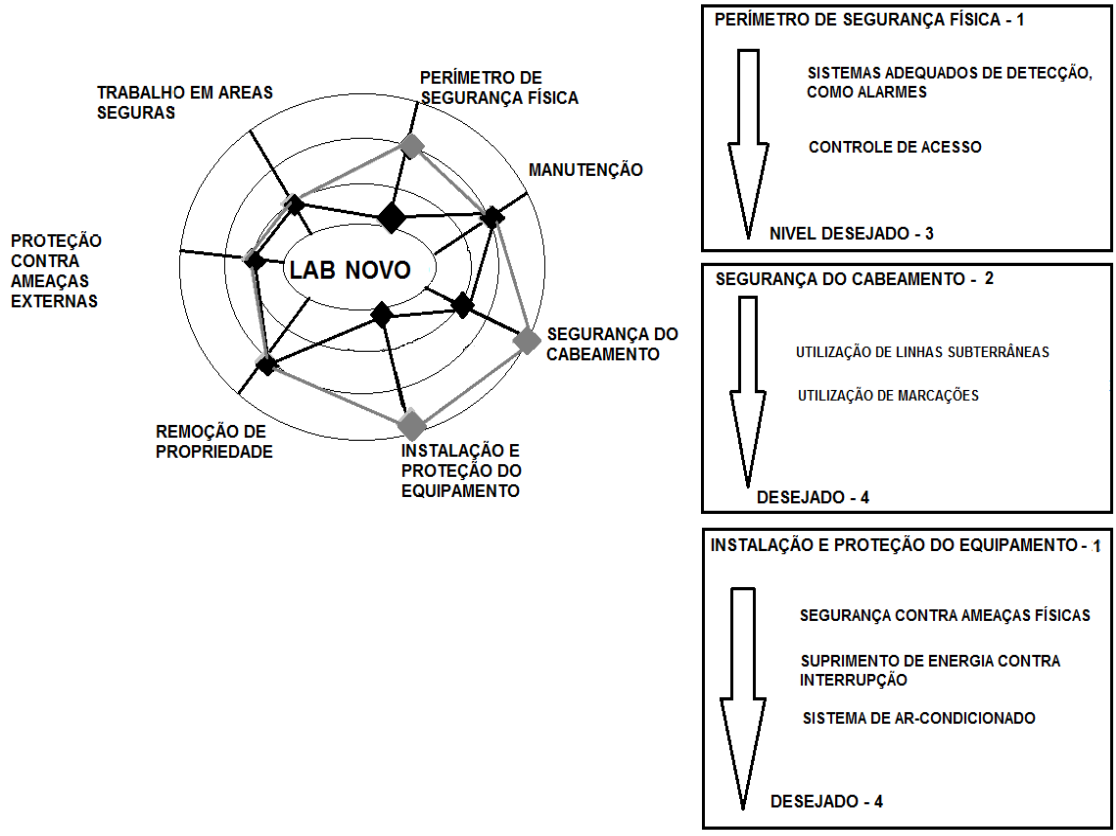

Figura 22: Modelo de Teias aplicado aos laboratórios novos

Para os novos laboratórios percebe-se que os elementos de segurança: trabalho em áreas seguras, manutenção, remoção de propriedade e proteção do equipamento apresentam conformidade de existência de controles de segurança com a Segurança Física e Ambiental, pois os pontos e os traços em preto que representam a segurança atual estão no mesmo nível do ponto e traço em cinza que representa o nível desejado estabelecido pela Segurança Física e Ambiental, não necessitando de implementar nenhuma medida. Porém os níveis de segurança atuais representado pelo traço preto dos elementos: perímetro de segurança física, segurança do cabeamento e instalação e proteção do equipamento não coincidem com o traço cinza. Dai necessitam de implementar as medidas de segurança contidas no Roadmap para chegar ao nível de segurança desejado. No caso do perímetro de segurança física, implementando os controles sistemas de detecção e controle de acesso (uma recepção com

recepcionista, acesso através de controle eletrônico ou cartão) atingiria as recomendações da norma. A segurança do cabeamento necessita-se de utilização de marcações e que as linhas sejam subterrâneas. As instalações e proteções dos equipamentos precisam avançar em três medidas: seguranças contra ameaças físicas (roubo, vandalismo), suprimento de energia contra interrupção e haver um sistema de refrigeração adequado.

4.4 Plano de Ação

A utilização do modelo possibilita visualizar a existência de dois grupos de laboratórios com algumas diferenças no nível de segurança atual estabelecido pelos resultados dos questionários, entrevistas e análises in loco, e a partir dos elementos de segurança definidos com base no estudo realizado sobre a segurança física e do ambiente é definido as medidas que aplicadas aos laboratórios obtém-se os controles ideais para segurança.

A implementação dos controles de segurança levantados através do modelo de teias é uma tarefa complexa, que envolve planejamento de curto, médio e longo prazo. Para isso, faz-se necessário a definição de um plano de ação que contemple as etapas para se chegar à solução total ou parcial dos riscos de segurança dos laboratórios.

4.4.1 Ações e iniciativas

Nos laboratórios antigos os elementos de segurança que necessitam de aplicar medidas de segurança são:

- Perímetro de segurança física
- Segurança do cabeamento
- Instalação e proteção dos equipamentos.

De acordo com o modelo da figura 23 o Perímetro de segurança física precisa implementar as seguintes ações para alcançar o nível recomendado:

a) Sistema de detecção. Haver maior participação dos responsáveis na análise do ambiente para estabelecer os níveis de necessidades de salas e corredores dos laboratórios, os requisitos e planejar a aquisição dos equipamentos adequados.

b) Controle de Acesso: restrição do acesso através da utilizado de sistemas de acesso ao interior dos laboratórios que utilize cartão ou leitura biométrica nas portas. Esse sistema deve atender aos usuários, professores e funcionários dos laboratórios. Ou também deveria ser considerada uma área de recepção com vigilante que garantisse o acesso somente as pessoas autorizadas.

As ações necessárias para melhoria da segurança do cabeamento envolve aplicar:

a) Proteção contra danos: convém que haja melhoramento no cabeamento estruturado, utilização de canduítes e evitem trajetos em áreas publicas.
b) Utilização de proteção para linhas: essa alteração no cabeamento deve atender as linhas que devem passar e permanecer embutidas em canaletas.
c) Utilização de marcações: que todos os cabos sejam identificados utilizando numerações para ajudar no manuseio.
d) Segregação entre rede elétrica e cabos de rede: convém que os cabos de rede sejam separados dos cabos elétricos para evitar interferências.

A instalação e proteção dos equipamentos necessitam das seguintes ações:

a) Segurança contra ameaças físicas: convém adotar controles que minimizem os riscos de ameaças físicas (roubo, vandalismo). Maior envolvimento dos funcionários e seguranças para que monitorem qualquer atividade mal intencional.
b) Suprimento de energia contra interrupção: necessário um projeto elétrico sobre o dimensionamento do uso de energia nos laboratórios para dar entrada na compra de um gerador. Ou por exemplo, compra de nobreaks para todas as máquinas.

Nos novos laboratórios os recursos de segurança que também necessitam de ações são:

- Perímetro de segurança física.
- Segurança do cabeamento.
- Instalação e proteção do equipamento.

A figura 24 mostra que o perímetro de segurança física desses laboratórios necessitam das mesmas ações dos laboratórios antigos.

A segurança do cabeamento precisa implementar as seguintes ações:

a) Utilização de linhas subterrâneas:
b) Utilização de marcações:

A instalação e proteção dos equipamentos desses laboratórios precisam melhorar implementando além das ações definidas nos laboratórios antigos, as seguintes ações:

a) Sistema de ar-condicionado: convém que seja considerado um sistema de refrigeração para o interior desses laboratórios, seguindo recomendações e especificações técnicas. Que seja levado em consideração para aquisição dos aparelhos normas de saúde, a capacidade supra a necessidade da área.

5. CONCLUSÃO

Este trabalho apresentou uma análise dos laboratórios do DCE, a partir de entrevistas, questionários e observação in loco, de maneira que se analisou a segurança física e ambiental atualmente implantada neste ambiente. O resultado das entrevistas, questionários são apresentados no capítulo 3, onde é possível perceber o nível de segurança dos laboratórios através da aplicação de regras e controles no ambiente; a partir desses dados, trabalhou-se em uma verificação e adequação dessas normas às atualmente instaladas. Esta verificação e adequação foram realizadas através do modelo de teias, que foi descrita no capitulo 4 e constatou-se que para os laboratório antigos a segurança necessita de aplicação de regras e controles de proteção para a estrutura do cabeamento, regras de controle de acesso para usuários e utilização de sistemas de detecção, que seja considerado proteção aos equipamentos contra perdas.

Já nos laboratórios novos a melhoria é verificada no cabeamento, porém ainda precisa implementar medidas para que se torne seguro e padronizado. Por outro lado verificou-se que não há um sistema de refrigeração para o ambiente, agravando os riscos de ameaças externas ao ambiente como poeira, fumaça ou até um eventual incidente causado pelo funcionário em esquecer de trancar janelas.

Além desse estudo e dos resultados obtidos para verificar a adequação da segurança dos laboratórios com a segurança física e do ambiente estabelecida pela NBR 27002, pôde-se também verificar que a participação dos responsáveis pelos laboratórios em busca de planejamento e melhorias é baixa e que de acordo com a própria NBR, a segurança só poderá ser alcançada se além de meios técnicos, tiver a colaboração de todos os funcionários e envolvidos no negócio.

5.1 Limitações e trabalhos futuros

Na elaboração do presente trabalho as fontes de pesquisas mostravam conteúdo abrangente, mas nem sempre atendia o objetivo da pesquisa. Na maioria das vezes somente trabalhos acadêmicos continha algum conteúdo útil sempre havendo necessidade de sempre recorrer às referencias ou citações. Uma dificuldade que merece destaque foi encontrar leis, normas, livros ou trabalhos acadêmicos que descrevesse sobre política de segurança da informação nas IES.

Nas vistas in loco todas as observações foram possíveis e sem nenhum empecilho. O acesso aos laboratórios e as áreas analisadas não teve nenhum obstáculo.

Quanto aos questionários, obteve-se uma quantidade considerável, mas nem todos responderam e muitos opinavam sobre o tipo de questão abordado que não era ideal, fugia do conhecimento do participante.

As entrevistas foram realizadas com responsáveis por determinadas áreas e sempre demonstrava boa vontade, disposição e indicavam até outros participantes.

Um estudo do cenário das universidades públicas que mostre a maneira como a gestão da segurança dos recursos de informação é praticada ajuda entender tanto o contexto como na busca por melhorias para as regras internas, também tornando cada vez mais madura a ideia de segurança através da definição de uma politica.

REFERÊNCIAS BIBLIOGRÁFICAS

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

AGOSTINHO, D. A. **Leis de Segurança da Informação.** Santa Catarina. Disponível em: < http://www.inf.ufsc.br/~bosco/ensino/ine5630/material-seg-redes/artigo-Leis-de-Seguranca.pdf > Acesso em: 13 jan. 2013.

BEAL, A. Segurança da Informação: princípios e melhores práticas para proteção de ativos de informação nas organizações . São Paulo. Editora Atlas. 2005.

CACIATO, L. E. **Gerenciamento da Segurança de Informação em Redes de Computadores e a Aplicação da Norma ISO/IEC 17799:2001**. Campinas, 2004 24p. Monografia (Especialista em Análise de Sistemas). Pontifícia Universidade Católica de Campinas – PUC

CAMPOS, A. **Sistemas de Segurança da Informação**. 2. ed. Florianópolis : Visual Books, 2007.

EPAMINONDAS, J. M. Políticas de segurança da informação aplicada à instituição de educação superior. **Anuário de produção acadêmica docente**. Vol III, Nº 4, p. 183-194, mar. 2009. Faculdade de Negócios e Tecnologias da Informação. FACNET. BRASILIA, DF.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4. ed. São Paulo: Atlas, 2002.

GOMES, B. B. **Estudo de caso sobre o impacto da implementação da Norma NBR ISO/IEC 27002 em micro e pequenas empresas.** Caraguatatuba – SP. 2010.

Gualberto, Éder Souza. Um estudo de caso sobre a gestão da segurança da informação em uma organização pública / Éder Souza Gualberto. Brasília: UnB, 2010.

KOZEN, M. P.; FONTOURA, L. M.; NUNES, R. C. **Gestão de riscos de segurança da informação baseada na Norma ISO/IEC 27005 usando padrões de segurança.** IV Simpósio de Excelência em Gestão e Tecnologia. Resende-RJ. Out, 2012. Disponível em: < http://www.aedb.br/seget/artigos12/57616827.pdf > Acesso em: 13 jan. 2013.

OSIRO, A. K. (2006). Estudo de Segurança da Informação com enfoque nas Normas ABNT NBR ISO/IEC 17799:2005 e NBR ISO/IEC 27001:2006, para aplicação no Senado Federal. Monografia de Especialização, Publicação agosto/2006, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 114p.

MÓDULO. **10ª Pesquisa Nacional de Segurança da Informação.** Disponível em: < http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf > Acesso em: 13 jan. 2013.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes Em Ambientes Cooperativos.** São Paulo: Editora Futura, 2007.

NBR/ISO/IEC 17799. *Tecnologia da Informação: Código de prática para a gestão da segurança da informação.* Rio de Janeiro. Associação Brasileira de Normas Técnicas, 2005.

NBR/ISO/IEC 27002. *Tecnologia da Informação: Código de prática para a gestão da segurança da informação.* Rio de Janeiro. Associação Brasileira de Normas Técnicas, 2005.

OHTOSHI, P. H. **Análise comparativa de metodologias de gestão e de análise de riscos sob a ótica da norma NBR-ISO/IEC 27005**. Brasília, 2008. 99p. Monografia (Especialização em Ciência da Computação: Gestão da Segurança da Informação e Comunicações). Universidade de Brasília – UnB.

PSI – Política de Segurança da Informação Documento de Diretrizes e Normas Administrativas.Disponívelem:< http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf> Acesso em: 13 Jan. 2013.

SEDREZ, C. S.; FERNANDES, F. C. **Gestão de riscos nas universidades e centros universitários do estado de Santa Catarina.** Revista Gestão Universitária na América Latina - GUAL, ISSN 1983-4535, Florianópolis, Santa Catarina. p.70-93. Edição especial 2011.

APÊNDICE

Levantamento de informações acerca da situação atual dos Laboratórios.

Questionário para levantar informações sobre a situação dos laboratórios de informática do CCAE como fonte de dados para utilização em estudo de caso. Pediria a todos os alunos que colaborassem com essa pesquisa, principalmente usuários dos laboratórios, pois é de suma importância para meu trabalho de conclusão do curso.

1) Atualmente para a segurança da informação os ativos: informação, equipamentos, os sistemas e as redes são importantes para o sucesso do negócio. Como você classifica a participação de todos os responsáveis pelos laboratórios quanto ao planejamento, manutenção e melhoramento de tais ativos ?

- Participam ativamente
- Parcialmente
- Nenhuma
- Não opinar

2) Para norma NBR ISO/IEC 27002: escritórios, salas e laboratórios com equipamentos que processam informação são considerados como uma área critica de informação, que necessita ser protegidos. Sendo assim, como você avalia a proteção oferecida aos laboratórios?

- Bem protegido
- Precisa Melhorar
- Nenhuma
- Não opinar

3) Um perímetro de segurança é uma área física isolada que o acesso é controlado por algum controle de entrada física: uma recepção, uma porta com controle de acesso eletrônico, o uso de crachá ou mesmo identificação visual, evidenciando a presença de pessoas não autorizadas. Como você avalia a aplicação desses controles citados no contexto dos laboratórios?

- Bem aplicado
- Pouco se aplica.
- Nenhum

- Não opinar

4) Evitar o trânsito de pessoas não autorizadas nos corredores e/ou o trabalho não supervisionado previne atividades mal intencionais. Como você avalia a aplicação dessas diretrizes nos laboratórios?

- Bem aplicado
- Pouco se aplica.
- Nenhum
- Não opinar

5) Quanto à proteção contra incêndio, que avaliação você daria a segurança oferecida nos laboratórios?

- Bem aplicada.
- Pouco se aplica.
- Nenhum
- Não opinar

6) Qual sua avaliação quanto à existência e posicionamento dos equipamentos apropriados de detecção e combate a incêndio?

- Medida aplicada.
- Pouco se aplica.
- Nenhum
- Não opinar

7) Quanto à proteção dos equipamentos de informática, a NBR ISO/IEC 27002 considera o estabelecimento de regras quanto a comer, beber e fumar no ambiente das instalações. Considerando o enunciado, como você avalia a aplicação dessas diretrizes aos computadores e equipamentos do laboratório?

- Medida bem aplicada.
- Pouco se aplica.

- Nenhum
- Não opinar

8) A NBR ISO/IEC 27002 considera também: edifícios sejam dotados de proteção contra raios e linhas de entrada de força e comunicação tenham filtros de proteção contra raios; Seja considerado um gerador de emergência e que os equipamentos sejam dotados de suprimentos de energia que suportem as paradas e desligamento. Como você avalia a aplicação dessas diretrizes aos computadores e equipamentos do laboratório?

- Medida bem aplicada.
- Pouco se aplica.
- Nenhum
- Não opinar

9) Segurança do cabeamento é ter entrada de linhas de energia e telecomunicação subterrâneas (abaixo do piso), o cabeamento de rede seja protegido contra danos (evitar áreas publicas) e separado de cabos de energia e que sejam utilizadas marcações que auxilie no manuseio dos cabos. Qual sua avaliação quanto à aplicação dessas medidas nos laboratórios?

- Medidas bem aplicadas.
- Em parte. Pouco se aplicam.
- Nenhuma
- Não opinar

10) Utilização de conexões(via cabo) em equipamentos particulares(notebook) e acesso a painéis de conexões como switch são medidas:

- Realizadas.
- Em parte. Pouco.
- Nenhuma
- Não opinar

11) Quanto à remoção de propriedade ou retirada não autorizada de equipamentos, informação ou software, a ISO/IEC 27002 estabelece que não sejam retirados do local sem

autorização prévia; aqueles que tenham autoridade para remoção sejam identificados e seja feito um registro da retirada e devolução do ativo para posterior inspeção. Essas diretrizes:

- São bem aplicadas.
- Em parte. Pouco se aplicam.
- Nenhuma
- Não opinar

12) Como você classificaria a segurança oferecida aos computadores contra furto, vandalismo e o acesso desnecessários a painéis de conexões de rede como switches, roteadores, backbones:

- Alta
- Média
- Baixa
- Nenhuma

13) Como você classificaria a segurança oferecida nos laboratórios contra acesso físico não autorizado de pessoas?

- Alta
- Média
- Baixa
- Nenhuma

14) Como você classificaria a proteção oferecida nos laboratórios contra perturbações como sonorização, ruídos?

- Alta
- Média
- Baixa
- Nenhuma