UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
DEPARTAMENTO DE COMPUTAÇÃO E SISTEMAS DE INFORMAÇÃO

Fernanda Lara Ferreira Rocha

ESTUDOS DE METODOLOGIAS PARA A AVALIAÇÃO E AUDITORIA DA SEGURANÇA DA INFORMAÇÃO E DAS TECNOLOGIAS DO ICEA

João Monlevade
2017

FERNANDA LARA FERREIRA ROCHA

ESTUDOS DE METODOLOGIAS PARA A AVALIAÇÃO DA SEGURANÇA DA INFORMAÇÃO E DAS TECNOLOGIAS DO ICEA

Monografia apresentada ao curso Sistemas de Informação do Instituto de Ciências Exatas e Aplicadas, da Universidade Federal de Ouro Preto, como requisito parcial para aprovação na Disciplina “Trabalho de Conclusão de Curso II”.

Orientador: Dr. Fernando Bernardes de Oliveira

Coorientador: Plínio Roque de Almeida Pessoa

João Monlevade

2017

Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Colegiado do Curso de Sistemas de Informação
Campus João Monlevade

ATA DE DEFESA

Aos 31 dias do mês de março de 2017, às 13 horas, na sala C304 do Instituto de Ciências Exatas e Aplicadas, foi realizada a defesa de Monografia pela aluna **Fernanda Lara Ferreira Rocha,** sendo a Comissão Examinadora constituída por: Prof. Dr. Fernando Bernardes de Oliveira, Bel. Plínio Roque de Almeida Pessoa, Prof. Msc. Theo Silva Lins e Prof. Dr. Euler Horta Marinho.

A candidata apresentou a monografia intitulada: *"Estudo de metodologias para a avaliação e auditoria da segurança de informação e das tecnologias do ICEA"*. A comissão examinadora deliberou, por unanimidade, pela aprovação do candidato, com nota 9,5 (nove e meio), concedendo-lhe o prazo de 15 dias para incorporação das alterações sugeridas ao texto final.

Na forma regulamentar, foi lavrada a presente ata que é assinada pelos membros da Comissão Examinadora e pelo graduando.

João Monlevade, 31 de março de 2017.

Fernando Bernardes de Oliveira.
Prof. Dr. Fernando Bernardes de Olivera
Professor Orientador/Presidente

Plínio Roque de Almeida Pessoa
Bel. Plínio Roque de Almeida Pessoa
Coorientador

Theo Silva Lins
Prof. Msc. Theo Silva Lins
Professor Convidado

Euler H. M.
Prof. Dr. Euler Horta Marinho
Professor Convidado

Fernanda Lara Ferreira Rocha
Fernanda Lara Ferreira Rocha
Graduanda

Universidade Federal de Ouro Preto
Instituto de Ciências Exatas e Aplicadas
Colegiado do Curso de Sistemas de Informação
Campus João Monlevade

Folha de Aprovação

Curso de Sistemas de Informação

FOLHA DE APROVAÇÃO DA BANCA EXAMINADORA

ESTUDO DE METODOLOGIAS PARA A AVALIAÇÃO E AUDITORIA DA SEGURANÇA DE INFORMAÇÃO E DAS TECNOLOGIAS DO ICEA

Fernanda Lara Ferreira Rocha

Monografia apresentada ao Instituto de Ciências Exatas e Aplicadas da Universidade Federal de Ouro Preto como requisito parcial da disciplina CSI499 – Trabalho de Conclusão de Curso II do curso de Bacharelado em Sistemas de Informação e aprovada pela Banca Examinadora abaixo assinada:

Prof. Dr. Fernando Bernardes de Oliveira
DECSI – UFOP

Bel. Plínio Roque de Almeida Pessoa
NTI/ICEA

Profª. Prof. Msc. Theo Silva Lins
DECSI – UFOP

Prof. Dr. Euler Horta Marinho
DECSI – UFOP

João Monlevade, 31 de março de 2017.

Rua Trinta e seis, 115 – Bairro Loanda – CEP 35931-008 – João Monlevade – MG – Brasil
Página: http://www.icea.ufop.br – **E-mail:** cosi@decea.ufop.br – **Telefone: (31) 3852-8709**

UNIVERSIDADE FEDERAL DE OURO PRETO
INSTITUTO DE CIÊNCIAS EXATAS E APLICADAS
COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

TERMO DE RESPONSABILIDADE

Eu, Fernanda Lara Ferreira Rocha,
declaro que o texto do trabalho de conclusão de curso intitulado "Estudos de metodologias para a avaliação e auditoria da Segurança da informação e dos tecnologias do ICEA" é de minha inteira responsabilidade e que não há utilização de texto, material fotográfico, código fonte de programa ou qualquer outro material pertencente a terceiros sem as devidas referências ou consentimento dos respectivos autores.

João Monlevade, 03 de abril de 2017

Fernanda Lara Ferreira Rocha
Assinatura do aluno

DEDICATÓRIA

Dedico esta monografia a minha mãe, Maria do Carmo (in memoriam) que nos deixou em 2003 e desde então esteve sempre presente no meu coração. Amo você incondicionalmente!

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter me guiado, me abençoado e me dado força para chegar até aqui.

A minha mãe, Maria do Carmo (*in memoriam*), minha irmã, Lúrian, meus tios, maternos e ao meu tio Teco e família, aos meus avôs, Nazita e Púri (*in memoriam*) pelo carinho, amor e por me incentivarem a buscar o que eu quero sempre. Vocês sempre estiveram presentes e me deram forças para continuar e sei que nunca estive sozinha. Amo vocês incondicionalmente!

Ao meu namorado, Michel, pelo amor, companheirismo, incentivo, força, perseverança e pela paciência durante todos esses anos.

Aos amigos do Centro de Extensão ICEA, por sempre se fazerem presentes, me apoiando e incentivando diariamente. Obrigada por acreditarem no meu potencial!

Aos meus amigos pelo apoio, companheirismo e pelos momentos compartilhados. Agradeço em especial à minha amiga Thaís e às minhas primas Simone, Mariana e Luciana, por todo carinho e por aguentarem minhas reclamações ao logo desses anos.

Aos meus amigos Bárbara, Danielle, Eduardo, Lanna e Manoel, obrigada por fazerem parte dos melhores momentos da minha vida, pelos incentivos, pelo carinho e por sempre estarem presentes durante todos esses anos de faculdade. Que sejam eternos!

Ao meu orientador Fernando pela paciência, incentivo, pelos ensinamentos transmitidos e por me guiar durante todo esse processo, seu apoio foi fundamental.

Ao meu coorientador Plínio pelo aprendizado que você me proporcionou e pela paciência a longo desse período.

A todos que de alguma forma contribuíram direta ou indiretamente para a conclusão deste trabalho, o meu muito obrigada!!

Que os vossos esforços desafiem as impossibilidades, lembrai-vos de que as grandes coisas do homem foram conquistadas do que parecia impossível." **(Charles Chaplin)**

RESUMO

As questões referentes à Segurança da Informação e de ativos tecnológicos são preocupações constantes das organizações. A segurança deve garantir que a confidencialidade, a integridade e a disponibilidade estejam de fato resguardadas. Entretanto, definir e aplicar metodologias práticas para a Segurança da Informação não são tarefas fáceis, pois envolvem um conhecimento amplo da organização, além de modificar hábitos e ações individuais. Do mesmo modo, a Segurança da Informação no Instituto de Ciências Exatas e Aplicadas (ICEA) também é fundamental. Assim o objetivo deste trabalho é levantar os principais pontos de vulnerabilidades e identificar as melhorias pertinentes que devem ser propostas, afim de sanar os problemas identificados. Além disso, propor métodos eficazes e eficientes, de modo a garantir a segurança dos recursos tecnológicos e de informações presentes. O estudo justifica-se pela necessidade de atender as recomendações propostas pelas leis voltadas à segurança da informação, e para garantir a proteção dos recursos tecnológicos e de informação presentes no campus. De tal modo, foram coletados dados acerca do instituto por meio de elaboração de questionários, entrevistas com os técnicos de informática e avaliações por meio de observação exploratória, que posteriormente foram documentação. A partir dos dados coletados, foram analisados os principais pontos de vulnerabilidades que comprometeriam de maneira direta e indireta a continuidade dos serviços prestados pelo instituto. Com base nos resultados obtidos, foi então proposta a estruturação de uma Política de Segurança da Informação no contexto ICEA, e por consequência optou-se pela realização de uma auditoria como modo de prover os melhores recursos de proteção. Notou-se que o ICEA já adota algumas práticas para garantir a segurança no campus, todavia, não são por si só suficientes, essas devem ser reavaliadas e reestruturadas constantemente, considerando que a tecnologia está em constante mudança.

Palavras-chave: Segurança da Informação. Recursos Tecnológicos. Auditoria, Instituto, Política de Segurança da Informação, Informação.

ABSTRACT

Issues related to Information Security and technological assets are constant concern of organizations. The security must ensure confidentiality, integrity and availability are effectively safeguarded. However, defining and applying practical methodologies for Information Security are not easy tasks because they involve a large knowledge of the organization, besides changing individual habits and actions. Likewise, Information Security at the “Instituto de Ciências Exatas e Aplicadas” (ICEA) is also crucial. Therefore, the aim of this project is to identify the main points of vulnerability and the pertinent improvements that have to be proposed, in order to solve the identified problems. Beyond that, it will propose effective and efficient methods to guarantee the security of the present technological resources and information. The study is justified by the need to meet the recommendations proposed by laws focused in Information Security and to ensure the protection of the technological and information resources present on campus. In this way, data about the institute were collected through questionnaires, interviews with computer technicians, and evaluations through exploratory observation, which were documented later. Based on the collected data, the main vulnerability points that would directly and indirectly compromise the continuity of the services by the institute were analyzed. Based on the results obtained it was proposed the structuring of an Information Security Policy in the context of ICEA and consequently an audit was chosen as a way to provide the best protection resources. It was noticed that ICEA already adopts some practices to guarantee security on campus, but still they are not sufficient by themselves, these should be constantly re-evaluated and restructured considering that technology is always changing.

Keywords: Information Security, Technological Resources, Audit, Institute, Information Security Policy, Information.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS

ABNT	_	Associação Brasileira de Normas Técnicas
BSI	–	Britsh Standard International
COBIT	–	Control Objectives for Information and Related Technology
DECEA	–	Departamento de Ciências Exatas e Aplicadas
DECSI	–	Departamento de Computação e Sistemas
DEELT	–	Departamento de Engenharia Elétrica
DEENP	–	Departamento de Engenharia de Produção
ICEA	–	Instituto de Ciências Exatas e Aplicadas
IEC	–	International Electrotechnical Commission
ISO	_	International Organization for Standardizati.on
ITIL	–	Information Tecnology Infrastructure Library
NTI	–	Núcleo de Tecnologia da Informação
PSI	–	Política de Segurança da Informação
SLA	_	Service Level Agreements
TI	–	Tecnologia da Informação
UFOP	–	Universidade Federal de Ouro Preto.

SUMÁRIO

1 INTRODUÇÃO

Segurança da informação é uma abordagem fundamental para as organizações, indiferente do segmento que ela atue, sejam elas públicas ou privadas. A constante necessidade de proteger e garantir a correta adequação dos ativos gerados é algo de extrema significância e necessidade para a qualidade do serviço final prestado. Todavia, nem sempre são implementadas as corretas práticas para tal, visto que projetos utilizados para essa finalidade são muitas das vezes caros, complexos demais, além de demandarem muito tempo.

Conforme Harold e Krause (2008) a expressão segurança da informação é amplamente utilizada no ambiente corporativo e envolve uma série de possibilidades, muitas delas, associadas à Tecnologia da Informação (TI): controle de acesso a recursos (dispositivos ou documentos), segurança em comunicação, gestão de riscos, políticas de informação, sistemas de segurança, diretrizes legais, segurança física, criptografia, arquivista, dentre outros. Por mais investimentos que as organizações façam na implantação de recursos tecnológicos com a finalidade de garantir a segurança em seu ambiente, falhas sempre ocorrem. De modo geral, essas falhas podem acontecer pela não adequação de um determinado recurso ao contexto ou pela não capacitação do fator humano que fará de um recurso (COLWILL, 2009).

No contexto do Instituto de Ciências Exatas e Aplicadas (ICEA), a preocupação com a Segurança da Informação também é algo constante. Existe a necessidade estratégica de criar mecanismos de proteção das informações e dos recursos tecnológicos, considerando que acessos indevidos a mecanismos e recursos tecnológicos tais como a ruptura de acesso à rede, ou até mesmo a indisponibilidade devido à falta de orientações e ou correta aplicabilidade de proteções. Desse modo, é importante conscientizar os usuários e mantenedores presentes e futuros para a importância em garantir a segurança dentro ambiente, como modo de afirmar por consequência a continuidade do funcionamento desses recursos. Além disso, guia-los no correto uso dos ativos tecnológicos acerca do ambiente institucional, bem como a garantia dos recursos fundamentais da segurança: confidencialidade disponibilidade e integridade.

Este trabalho tem como finalidade apresentar problemas cotidianos enfrentados pelo Instituto, acarretados pelo crescente aumento das tecnologias, e a importância da aplicação imediata de uma Política de Segurança da Informação e dos ativos presentes no ICEA. Isso é fundamental para que os recursos do ICEA atendam aos quesitos primordiais da segurança da informação: integridade, confidencialidade e disponibilidade.

1.1 Problema

Atualmente, o ICEA possui aproximadamente 1545 pessoas que, de modo direto ou indireto, fazem acesso aos recursos tecnológicos. Esse grupo é composto por alunos, professores, técnicos administrativos, funcionários anistiados e trabalhadores terceirizados. O volume relativamente grande de pessoas que acessam a tecnologia no ICEA e a não conscientização do seu uso correto podem tornar o ambiente institucional um local com maior vulnerabilidade a práticas maliciosas. Com isso requer um controle mais efetivo sob os ativos tecnológicos do instituto.

O ICEA possui em seu ambiente um departamento responsável pela gestão das tecnologias presentes no instituto este, é denominado como Núcleo de Tecnologia da Informação (NTI/ICEA). O departamento que tem por finalidade desenvolver e gerenciar os recursos da Tecnologia da Informação, é um setor essencial para a correta adequação dos serviços tecnológicos presentes no ICEA. O NTI/ICEA é responsável por toda infraestrutura tecnológica do ICEA, garantindo que ela esteja disponível de maneira adequada para todo o instituto. Ele gerencia os domínios referentes a infraestrutura de redes e soluções de sistemas multimídias. As principais tarefas do departamento são: manter a segurança no acesso à Rede Nacional de Pesquisa (RPN), controlar o acesso à rede interna (rede *wi-fi* e rede cabeada) e administrar os recursos de informática, com a intenção de prover o máximo de disponibilidade dos serviços do instituto.

Um ponto importante a ser destacado é que o NTI/ICEA responde diretamente à diretoria do ICEA. Ele não possui vínculo hierárquico direto com o departamento de informática em Ouro Preto (NTI/Ouro Preto). Porém, o NTI/ICEA depende de alguns serviços do NTI/Ouro Preto como, por exemplo, a criação de *e-mails* e a hospedagem do site institucional. As atribuições do NTI/Ouro Preto são descritas a seguir:

> "*É um setor ligado diretamente à Reitoria e tem como finalidade principais gerir e disponibilizar recursos de Tecnologia da Informação e telefonia. O NTI/Ouro Preto contribui para racionalizar os processos de tomada de decisão, por disponibilizar as informações e potencializar a comunicação entre os agentes, por meio do uso de redes de computadores e serviços. "* (NTI/OURO PRETO, 2016)

Uma consideração importante a ser feita é que tanto o NTI/ICEA quanto o NTI/Ouro Preto não possuem um Política de Segurança da Informação (PSI) em vigência. O que pode contribuir para o aparecimento de vulnerabilidades e por consequência, tornar o ambiente propício à praticas maliciosas. Um exemplo disso seria o incorreto uso dos ativos por parte de alunos, professores e técnicos administrativos, além, daqueles advindos de

meios externos, acarretando a indisponibilidade do serviço prestado. A PSI permite estabelecer as regras e as Normas de condutas referentes ao correto uso dos ativos tecnológicos por todas as pessoas envolvidas. Além disso, a construção dessa política permite identificar as principais vulnerabilidades, propondo melhorias a serem aplicadas, bem como utilizar mecanismos para que revisões e auditórias dos processos sejam realizadas.

Considerando os pontos identificados acerca da Segurança da Informação do ICEA, a seguir serão apresentados os objetivos gerais e específicos deste trabalho.

1.2 Objetivos

O objetivo geral deste trabalho é estudar metodologias e realizar propostas para a avaliação e a auditoria da segurança da informação e das tecnologias no ICEA, utilizando como referência documentos especializados ao contexto. Versões personalizadas desses documentos foram elaboradas, de maneira a identificar as necessidades e as características do ICEA. Deste modo, o escopo do projeto engloba o levantamento de documentos de boas práticas, a elaboração de uma Política de Segurança da Informação adequada ao contexto e características do ICEA e a elaboração de documentos relacionados ao processo de avaliação e auditoria de quesitos de segurança da informação e da infraestrutura tecnológica do instituto.

Como resultado, espera-se que esses documentos auxiliem na identificação de pontos de falhas, por conseguinte a elaboração das propostas de melhoria e de garantia de boas práticas de uso dos recursos tecnológicos presentes.

1.2.1 Objetivos específicos

Este trabalho possui os seguintes objetivos específicos:

1. Revisar a literatura sobre os documentos de boas práticas sobre segurança e auditoria, Normas e Política de Segurança da Informação.
2. Propor um documento sobre as Normas e Políticas de Segurança para o instituto juntamente com os responsáveis pela tecnologia da informação do ICEA.
3. Definir uma metodologia para a avaliação e a auditória das principais tecnologias do ICEA.

4. Analisar e discutir os resultados com os responsáveis e com toda comunidade acadêmica, caso se aplique.

1.3 Justificativa

O Instituto de Ciências Exatas e Aplicadas da Universidade Federal de Ouro Preto, como outras organizações, está em constante busca pela garantia da confidencialidade, disponibilidade e integridade de suas tecnologias e informações vigentes. Atualmente os processos de segurança adotados no instituto contam com recursos que em sua maioria não garantem a inexistência de vulnerabilidades, ou seja, estão num nível de segurança que necessita ser constantemente avaliados. Como um instituto de ensino superior, o ICEA deve ter seus procedimentos baseados em uma Política de Segurança da Informação bem estabelecida, bem como, normas de segurança consolidadas e voltadas para os principais pontos de insegurança que o ambiente como um todo apresenta.

Deste modo, este trabalho justifica-se, pela necessidade constante de avaliar de modo geral o nível de segurança presente no instituto, de maneira a constatar os principais pontos de vulnerabilidades, seguindo para tal, orientações das principais normas de segurança adotadas de maneira a garantir que as tecnologias presentes e suas informações estejam protegidas e prontamente disponíveis de maneira integra e segura a todos os usuários da mesma.

1.4 Estrutura do Trabalho

O restante deste trabalho é organizado como segue. O Capítulo 2 contém o referencial teórico utilizado para o desenvolvimento do projeto final. Aqui são englobados os conceitos, o uso da informação em uma organização, classificação da informação, níveis de segurança da informação, o uso de ativos tecnológicos, a importância das principais Normas de segurança da informação, informações sobre o ITIL e por informações sobre o COBIT. Todos esses conceitos foram de extrema significância para obter os resultados esperados. Já o Capítulo 3 é apresentado de modo geral o ICEA, local escolhido para a realização deste trabalho. Por sua vez, o capítulo 4 possui todos os detalhes referentes a definição de uma Política de Segurança da Informação no ICEA, nele é possível acompanhar todos os passos seguidos para a elaboração da mesma. Seguindo, o capítulo 5 possui todas as informações referentes a aplicação de uma auditoria tecnológica que foi proposta e então realizada dentro das dependências do instituto. Por fim, o capítulo 6 será apresentado as considerações finais acerca do trabalho apresentado.

2 CONCEITOS GERAIS E REVISÃO DA LITERATURA

Este capítulo está estruturado conforme descrito a seguir. A Seção 2.1 descreve qual a importância de do uso da informação dentro de um ambiente organizacional e sua classificação, a seção 2.2 descreve as Normas de segurança utilizadas como referências para a elaboração dos documentos de Política de Segurança da Informação e para a realização da auditoria, a seção 2.3 apresenta o *framework* ITIL, a seção 2.4 apresenta o guia de boas práticas COBIT e os processos de maturidade apresentados, a seção 2.5 descreve o conceito de uma Política de Segurança da Informação e sua importância para a garantia da segurança e por fim a seção 2.6 apresenta o conceito de uma auditoria interna voltada para a tecnologia.

2.1 O Uso da Informação em um Ambiente Organizacional

Segundo ISO/IEC:27002 (2013), a informação é um ativo crucial para o andamento do negócio e de grande importância dentro de qualquer organização, independentemente do ramo que ela atue. Isto é, para o correto desenvolvimento de seus processos tanto internos quanto externos, dependem que sejam constantemente protegidas de vulnerabilidades que possam por consequência comprometer a continuidade dos serviços prestados.

Sêmola (2003) define a informação como o ativo de maior criticidade para uma organização, uma vez que, ela é quem permite a continuidade operacional progressiva do negócio e sua interrupção acarreta danos significativos ao ambiente em que ela está inserida. Com isso, necessita ser resguardada e protegida de vulnerabilidades existentes que são transmitidas de maneira lógica ou física.

O modo no qual uma informação está disponibilizada dependerá do contexto ao qual ela se aplica, podendo ser apresentada segundo a norma (NBR ISO/IEC:27002, 2005) como uma escrita em papel, armazenada eletronicamente, transmitida via *email*, retransmitida por meio de uma conversa informal entre funcionários e diversos outros tipos de meios ao qual poderá ser empregada.

O tratamento dado a uma informação dependerá da sua importância dentro do ambiente no qual está envolvida, e pode levar a diferentes modos de manipulação em suas etapas de criação, transporte e descarte com o intuito de minimizar os danos que serão gerados caso ocorra de maneira não planejada e segura. A preocupação em como gerenciar a informação é feita devido ao crescente aumento da tecnologia e o que tornou

eminente observar os riscos e as vulnerabilidades as quais estão expostas, o que pode levar a perda de sua legitimidade.

O termo informação, contudo, se difere de um outro bastante utilizado no meio tecnológico, que é o dado, e é importante considera-los como partes isoladas de um processo. Segundo Stair e Reynolds (2002), dados consistem em fatos que ainda não foram trabalhados e que possuem pouco valor ou nenhum valor, isso é, sem um significado útil, como por exemplo, um número de uma casa, nomes sem descrições, além de diversos outros tipos. Observa-se pelo Quadro 1 que o conceito dado pode ser representado por diferentes tipos.

Quadro 1 - Representação dos Diferentes tipos de dados

Dados	**Representados por**
Dados Alfanuméricos	Números, letras e outros caracteres
Dados de Imagem	Imagens Gráficas ou Fotos
Dados de Áudio	Som, ruídos ou tons
Dados de Vídeo	Imagens em movimento ou fotos

Fonte: Stair e Reynolds (2002, p.4)

O modo como a informação será manipulada dentro de uma organização dependerá da maneira como os dados estão relacionados, o que pode gerar alterações à medida que novas informações são geradas. Os dados sofrem transformações ao longo da manipulação da informação a partir de um processo logicamente definido, seguindo tarefas preestabelecidas de modo a alcançar um objetivo final.

O processo pelo qual o dado percorre até criar uma informação com algum tipo de significado requer um conhecimento. O conceito de conhecimento segundo Laudon e Laudon (2014) é definido como uma experiência previa sobre algo, uma sabedoria sobre um conjunto de informações para a realização de uma tarefa, isso implica na escolha e na rejeição de fatos para que uma modelagem da informação possa ser feita. Portanto, uma base de conhecimento pode ser criada, sendo essa descrita como um conjunto de dados relevantes que agrega algum valor quando relacionados corretamente.

2.1.1 Classificando uma informação

Segundo Freitas e Araújo (2008), existem aspectos importantes, os quais devem ser considerados para realizar a classificação da informação. A informação deve ser

considerada de acordo com seu tipo específico e então ser classificada de acordo com seu conteúdo.

A (NBR ISO/IEC:27002, 2005) recomenda que a classificação da informação obedeça a critérios que estão relacionados com o valor, a criticidade, os requisitos legais, e a sensibilidade que a mesma apresente para a organização. Ao mesmo passo a norma em questão recomenda-se que o proprietário do ativo defina a melhor maneira para classifica-los e responsabilize-se por sua constante avaliação.

Existem quatro tipos de aspectos importantes que devem ser considerados quando deseja-se classificar uma informação, sendo eles a confidencialidade, a disponibilidade, a integridade e o valor que a mesma possui para a organização.

A classificação da informação é de suma importância pois, é por meio dela que os recursos são corretamente direcionados para a proteção dos ativos provenientes desse meio atendendo todas as necessidades de modo eficaz e eficiente. A necessidade de resguardar uma informação é crucial para o correto desenvolvimento das atividades, todavia, saber qual o nível em que cada informação conhecida está inserida é um ponto fundamental para que essa classificação seja feita da melhor maneira possível.

As organizações necessitam de sistemas e maneiras de categorizações para classificar as informações, sendo que algumas necessitam de tratamentos diferenciados devido ao seu alto risco para o negócio, e com isso o nível de segurança se torna diversificado. Observa-se pelo Quadro 2 que apesar de não ter uma maneira padronizada para a classificação da informação, Kovacich (1998) sugere que ela seja enquadrada em três categorias diferentes.

Quadro 2 - Categorização quanto ao nível de segurança de uma informação.

Categoria	**Tipo de informação presente**
Informações pessoais	Dados individuais de empregados, clientes e outras pessoas
Informações de segurança nacional	Informações que precisam ser protegidas para garantir a segurança da sociedade e do Estado
Informações de negócio	Informações utilizadas pelas organizações para desempenhar suas tarefas de negócio

Fonte: Adaptado Kovacich (1998)

Nessa atividade de categorizar a informação é determinado o tipo de controle que cada uma deve conter. Para tal é preciso saber qual o nível em que cada informação deverá estar inserida, isso facilitará o seu controle e seu correto manuseio. Informações que

são manipuladas por pessoas que não possuem autorização para tal pode acarretar em situações errôneas para as organizações.

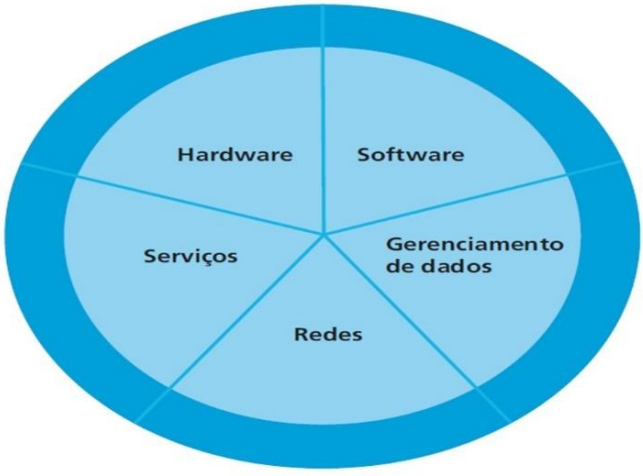
2.1.1.1 Uso dos ativos tecnológicos dentro das organizações

A informação é tida como um ativo de principal importância para as organizações. Para tal, é necessário que seja tratada e adequada de maneira que o nível de proteção aplicada, esteja de acordo com o valor que ela ocupa dentro do ambiente organizacional.

Dantas (2011) define que ativos em geral corresponde um conjunto de bens e direitos de uma entidade, contudo, esse conceito tem se expandido e refere-se a tudo aquilo que agrega valor para as organizações.

A infraestrutura tecnológica de TI, ativo importante dentro das organizações é composta por cinco principais elementos: software, hardware, tecnologias que envolvam gestão de dados, tecnologias de redes e telecomunicações e por fim os serviços de tecnologia (LAUDON e LAUDON, 2014). Observa-se que a Figura 1 representa os principais elementos que compõe a infraestrutura tecnológica de TI.

Figura 1 - Elementos que compõem a infraestrutura de TI nas organizações



Fonte: Laudon e Laudon (2014, p.147)

2.1.1.2 Estabelecendo níveis de segurança da informação

A Norma (NBR ISO/IEC:27002, 2005) apresenta que o objetivo da classificação da informação é assegurar que os ativos da informação recebam um nível

correto e adequado de proteção de acordo com a significância e a importância que ela apresenta para a organização. O processo de classificar uma informação assegura que critérios de legibilidade e transparência sejam estabelecido e que somente pessoas autorizadas tenham acesso.

A informação deve ser classificada de acordo com o risco que ela pode alavancar caso não seja tratada de maneira correta. É importante saber sua aplicabilidade e qual deve ser o nível de proteção, dado que nem todas as informações possuem o mesmo valor/importância para a organização. Algumas podem ser mais relevantes que outras.

Reis et al. (2008, p. 6) sugerem que o nivelamento siga a seguinte ordem:

- **Irrestrita**: é a informação também conhecida como irrelevante ao negócio e que pode ser acessada por qualquer usuário dentro da organização sem causar danos ao negócio;
- **Interna**: é a informação interna de uma organização, cujo conteúdo deve ser disponibilizado de preferência para pessoas da organização. O acesso por parte de pessoas externas deve ser evitado sempre que possível. Todavia, não causará danos sérios caso seja disponibilizada.
- **Confidencial**: é a informação também conhecida como classificada. É uma informação sigilosa cujo acesso deve ser feito apenas por usuários autorizados. O acesso por pessoas externas pode causar danos financeiros e ou a imagem do negócio. A incorreta divulgação deste tipo de informação, pode gerar vantagens por parte de concorrentes e uma possível perda de clientes.
- **Secreta**: é a informação interna. Deve ser acessada apenas por um grupo limitado dentro na organização. A integridade do conteúdo desse tipo de informação deve ser preservada. Considerada de grande valor para o negócio, não podendo ser acessada em nenhuma hipótese por pessoas externas ou por aquelas que não estão autorizadas.

O nivelamento da classificação de uma informação fornece subsídios para a gestão de ativos e, por consequência indicadores que contribuíram para o controle e para a elaboração das diretrizes que irá compor a Política de Segurança da Informação. Além do mais, essa atividade de classificar o inventário permite realizar um *checkup* da organização, identificando todos os processos e necessidades de informação. É uma etapa crucial para a elaboração de uma Política de Segurança da Informação que será abordada no Capítulo 4.

2.1.1.3. Características da Informação Valiosa

As informações de cunho valioso, por possuir conteúdo de grande importância para as organizações, apresentam características próprias que as diferem de outros tipos de informações vistas anteriormente. O Quadro 3 apresenta essas características de acordo com as definições de (STAIR e REYNOLDS, 2002).

Quadro 3 - Principais características da informação valiosa em um ambiente organizacional.

Característica	**Definição**
Precisa	É a informação que não contém erros.
Completa	É considerada completa, pois possui todos os fatos relevantes para compor sua estrutura.
Econômica	Contém apenas o essencial, ou seja, é o tipo de informação mais econômica possível para ser viabilizada.
Flexível	Pode ser articulada para diversificados propósitos, atende a mais de um assunto.
Confiável	É a informação que pode ser considerada sem contraindicações, advêm de fontes confiáveis.
Relevante	Considerada crucial para o tomador de decisões.
Simples	Descrita sem muita complexidade, adequada ao contexto e de fácil entendimento.
Pontual	Informação disponível sempre quando necessária.
Verificável	Pode ser verificável a qualquer momento, isso é, assegurar que a mesma está correta.
Acessível	Deve ser acessível com facilidades por pessoas autorizadas de forma fácil e objetiva.
Segura	Acessada apenas por um grupo seleto de pessoas.

Fonte: Adaptado Stair e Reynolds (2002)

A importância que a informação valiosa tem para a organização está no fato de possuir conteúdo que tem impacto direto sobre o negócio caso manuseada de maneira incorreta. Deve-se assegurar que todo tratamento necessário para garantir os quesitos fundamentais da Segurança da Informação seja resguardado ao tratar deste tipo de informação. Uma vez que dados relevantes quando relacionados, agregam valores para as informações.

2.1.2 Importância da segurança da informação

Garantir a segurança das informações é fundamental para o correto andamento do negócio. Independentemente do modo como uma informação é manuseada, transmitida, armazenada e até descartada, é necessário que todo um procedimento para garantir sua proteção e controle de acesso seja bem descrito.

As organizações possuem ativos físicos, como salas, arquivos, cofres, dentre outros. Ativos tecnológicos como *notebooks*, e*mails,* sistemas e servidores. Além dos ativos humanos, como secretárias, parceiros, funcionários que devem ser constantemente monitorados e resguardados para garantir a perfeita sincronização do negócio. Estes ativos estão sujeitos a diferentes tipos de vulnerabilidades que de modo direto ou indireto podem colocar em risco a informação.

Para tal, é necessário assegurar a aplicabilidade do gerenciamento da segurança para que se possa garantir a legibilidade e aplicação dos quesitos fundamentais da Segurança da Informação (LOUREIRO, 2008).

2.1.2.1 Riscos

Os riscos podem ser descritos como qualquer tipo de evento ou ação que possa causar uma espécie de incapacidade de empresas atingirem seus objetivos propostos. É um evento inesperado, informações pertinentes a constantes riscos e devem ser protegidas por consequência (STEFANINI, 2016).

2.1.2.2 Ameaças

As ameaças são eventos ou atitudes não desejadas que podem desabilitar, danificar ou até mesmos destruir por completo um recurso. A maioria das vezes são causadas de modo acidental ou mesmo proposital e afeta de maneira direta ou indireta um ativo da informação. Os agentes de ameaças podem ser os vírus, *worm*, *trojan, Keylogger, Bot,* dentre outros (LAUREANO, 2005).

2.1.2.3 Vulnerabilidades

As vulnerabilidades podem ser consideradas pontos fracos nos quais os ativos estão suscetíveis a ataques internos. Com isso permitem o constante aparecimento de ameaças que boqueiam a continuidade do negócio.

Segundo Costa (2010), os principais ataques relacionados a exploração da vulnerabilidade de tecnologia são:

- **Ataques ativos:** São aqueles que interferem diretamente no negócio, colocando-o em risco eminente. Apresentam como resultado, alteração do conteúdo, e produção de informações errôneas.
- **Ataques passivos:** São aqueles que não interferem diretamente, além de não alterarem as informações produzidas.

2.1.3 Ciclo de vida da informação

O ciclo de vida da informação é formado basicamente por quatro etapas as quais podem ser observadas na Figura 2.

Figura 2 – Ciclo de Vida de uma informação

Marcondes (2015) sugere que as etapas do ciclo de vida da informação podem ser identificadas do seguinte modo:

- **Manuseio**: momento no qual a informação é criada para determinado fim, ela pode ser apresentada em papéis, digitadas, usadas como senhas de acesso ou até mesmo criadas durante uma fala. É essencial o correto manuseio de uma informação.
- **Armazenamento**: maneira na qual uma informação é guardada depois de manuseadas, esse armazenamento pode ser feito em banco de dados, arquivos físicos, arquivos lógicos, ou até mesmo dentro de uma mesa de escritório. Todavia é importante que seu armazenamento seja feito de maneira segura.
- **Transporte**: momento no qual a informação é transportada, seja ao encaminhar um *email*, ao falar ao telefone uma informação ou encaminhar algo via correio.
- **Descarte**: momento no qual a informação em uso perde sua utilidade é então deverá ser desprezada por não possuir mais nenhum tipo de

utilidade para o uso. Essa é etapa é considerada crucial, pois o incorreto descarte pode causar danos catastróficos para as organizações.

Por ser considerado um bem de grande importância organizações, as informações devem ser tratadas com cuidado, desde a sua criação o momento em que é feito o seu descarte, isso porque, se feito de maneira indevida pode colocar em risco o negócio de uma organização. Para tal, é preciso criar mecanismos que assegurem que as informações descartadas não sejam acessadas por pessoas que não possuem autorização.

2.2 Normas de Segurança da Informação

Como parte do referencial teórico foram feitos estudos em torno de algumas normas que envolvem Segurança da Informação. As normas surgiram com o intuito de assegurar a Segurança da Informação quando manuseadas em equipamentos tecnológicos, visto que é necessário proteger e resguardar uma informação da maneira correta quando manuseadas por diferentes tipos de pessoas.

É notório que diferentes tipos de normas atendam a diferentes tipos de recurso, porém, todas possuem objetivos em comum, assegurar a proteção e a legibilidade de seus ativos. Segundo Cardoso e Oliveira (2012), observa-se que o foco principal foco de uma Norma acerca do tema é assegurar a garantia dos quesitos fundamentais da segurança da informação e da tecnologia definidos como:

- **Confidencialidade**: responsável por garantir que as informações e ou recursos tecnológicos serão acessados somente por pessoas autorizadas. Quando uma informação ou recurso tecnológico é acessado por pessoas não autorizadas, seja por meio intencional, ou não, ocorre a quebra de confidencialidade. A ausência da confidencialidade em um ambiente organizacional pode gerar danos, na maioria das vezes, irreparáveis para uma empresa. Exemplo: Em se tratando de uma instituição de ensino, o acesso de um aluno ao sistema de lançamento de notas destinado apenas ao uso de docentes da instituição.

- **Disponibilidade**: responsável por garantir que as informações e ou recursos tecnológicos estejam disponíveis para todos os usuários que dela necessitarem para a realização de algum objetivo em prol da organização. Quando ocorre a indisponibilidade do serviço para o acesso,

seja por questões de não operabilidade de servidores, ou mesmo por indisponibilidade de outros recursos tecnológicos, considera-se que houve um incidente de segurança causado pela falta de disponibilidade, mesmo aquelas causadas de maneira involuntária, ou não intencionais. Isso logo implica na quebra de um dos quesitos fundamentais da segurança.

- **Integridade**: responsável por garantir que as informações e ou recursos tecnológicos mantenham sua exatidão, além de garantir que sua proteção será mantida, mesmo que ocorra mudanças intencionais, indevidas ou acidentais.

Segundo a empresa (PILZ, 2016), ”*Normas são acordos entre diferentes associações de interesses (fabricantes, consumidores, órgãos de inspeção, autoridades de proteção do trabalho e governos). Elas descrevem a situação da tecnologia no momento da elaboração”.* Empresas constantemente estão investindo em segurança mediante a obrigação que elas possuem em cumprir regras e Normas, impostas pelas regulamentações (CAUBIT 2006).

2.2.1 Norma NBR ISO/IEC 27002:2013

A norma NBR IEC/27002:2013 é a versão mais recente norma NBR IEC/27002, que teve sua origem na norma Britânica BSI-7799 a qual foi criada pelo Órgão de Padrão Britânico no ano de 1993, por sua vez, baseou-se em um código de boas práticas de Segurança da Informação usados pelo governo do Reino Unido. Com o crescente aumento na preocupação em garantir a Segurança da Informação foi republicado pelo *British Satandard International* (BSI) o código e em 1995 foi criada a então Norma BS-7799. Com a grande visibilidade na qual a Segurança da Informação ganhou, a norma BS-7799 foi atualizada e reestruturada de modo que atendesse as novas exigências impostas, além do mais, esta norma foi subdividida em duas partes: BS-7799-1 (Código de Prática) e BS-7799-2 (Requisitos para certificação).

Como próximo passo tomado, a norma BS-7799-1 foi então publicada pela *International Organization for Standardization* (ISO)*,* como a norma ISO 17799 e no ano de 2004 depois de uma revisão foi novamente publicada como a norma ISO/IEC 17799:2005. Já a norma BS-7799-2 quando transformada em ISO, passou a adotar a nomenclatura da

nova família para ISO/IEC 27001:2005. De modo a padronizar todas as normas que trata o quesito Segurança da Informação a ISO em 2013 divulgou a nova versão da norma 27002, no mesmo instante a ABNT – Associação de Normas Técnicas publicou a versão em português (ABNT-27002:2013, p.xi).

A norma NBR IEC/27002:2013 Tecnologia da Informação – Técnicas de Segurança – Código de Práticas para a Segurança da Informação tem a seguinte finalidade estabelecer ``*diretrizes e princípios gerais nos quais organizações irão iniciar, implantar, manter e melhorar a gestão de Segurança da Informação em seu ambiente corporativo*'' (NBR ISO/IEC 27002:2013). Esta Norma é composta por um conjunto de controles que tem como objetivo resguardar as informações presentes em seu ambiente. Além de indicar fatores críticos de sucesso para a implantação de uma Norma de segurança adequando-a corretamente ao contextos e objetivos das áreas de negócio. Um outro fator que se destaca nessa Norma é o comprometimento de todos os níveis gerenciais da organização, além de descrever que o "*processo de Segurança da Informação deve ser feito de uma maneira conjunta com outros processos de gestão de negócio*" (FONTES 2014, p.1521).

2.2.2 Norma NBR ISO/IEC 27001

A norma NBR ISO/IEC 27001 é uma outra norma que orienta a segurança sugerindo um Sistema de Gestão de Segurança da Informação (SGSI) dentro da organização, diferente da NBR/IEC 27002:2013 que apresenta um guia de melhores práticas no que tange à Segurança da Informação (ABNT 2006). Como apresentado anteriormente esta norma é parte integrante da então norma BS-7799, com a subdivisão passou a ser chamada de BS-7799-2, todavia quando foi transformada em ISO, a norma foi renomeada para ISO/IEC 27001, que tem por finalidade promover a adoção de uma abordagem de processo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar o SGSI da maneira correta.

2.3 ITIL

Organizações frequentemente tem enfrentado problemas relacionados ao incorreto uso da tecnologia devido a isso, na maioria das vezes isso tem causado impacto negativo aos diversos envolvidos no negócio e até mesmo a própria organização, prejudicando diretamente em suas atividades rotineiras. Estabelecer um plano no qual eventos negativos que possa acontecer sejam previamente definidos, padronizados e estruturados e fator fundamental para saber como agir mediante a situações que coloque a

organização e seu negócio em risco. Estrategistas devem constantemente investir em treinamentos e técnicas que os auxiliem nas melhores tomadas de decisões.

Smith (2010) define o *Information Technology Infrastructure Library* (ITIL) como um *framework* que possui um conjunto de boas práticas e diretrizes, no qual é definida uma abordagem integrada com processos de gerenciamento de serviços de TI, podendo ser aplicada em qualquer ambiente que envolva a tecnologia dentro de uma organização.

Mendes e Moreira (2008) definem que o ITIL descreve uma metodologia na qual a intensão é gerenciar todos os serviços de TI de maneira sistemática. Possui foco em satisfazer os requisitos tecnológicos de modo econômico, além de focar no cliente, possui o intuito de padronizar a comunicação entre todas as partes envolvidas.

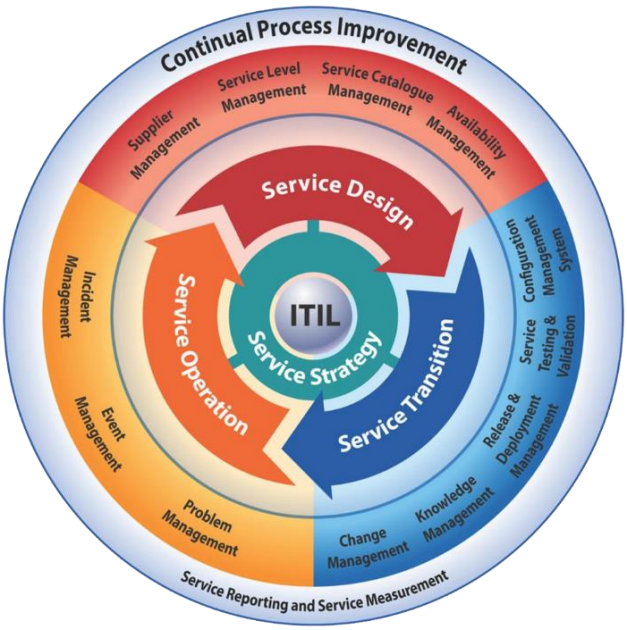
O modelo ITIL busca assegurar que a Segurança da Informação esteja implantada nos 3 níveis, o estratégico, o tático e operacional (Ribeiro 2012). Por meio deste modelo, é possível empregar a Segurança da Informação a partir de:

- **Políticas**: nestes são descritos todos os objetivos gerais e específicos que uma organização pretende atingir;
- **Processos**: são caminhos que devem ser seguidos com o intuito de alcançar o que foi definido na política;
- **Procedimentos**: descreve quem, quando e como devem ser feitos os passos a fim de atingir os objetivos.
- **Instruções de trabalho**: é descrito o passo-a-passo de como executar ações específicas.

Na Gestão da Segurança, o ITIL possui processos específicos para lidar com a Segurança da Informação, para tal utiliza das *Service Level Agreements* (SLA's), que é um acordo formal no qual é descrito o nível de serviço, além do nível de segurança que a área de TI deve prover para os clientes. Uma SLA deve prover todas as informações necessárias sobre Segurança da Informação feitas em uma organização (INFOSEC COUNCIL, 2005).

O ITIL divide suas funções e processos em cinco fases do ciclo de vida que pode ser visto na Figura 3, sendo que cada fase possui seus objetivos e especificações próprias.

Figura 3 - Ciclo de vida do ITIL



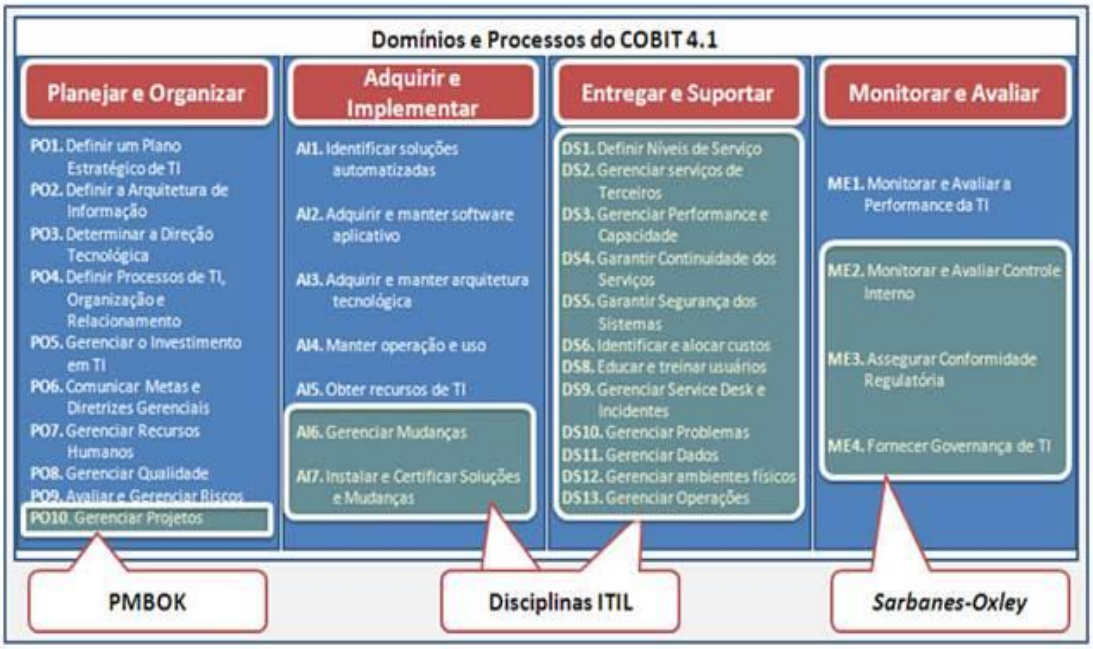
Fonte: DESPNET (2015)

2.4 COBIT

O *Control Objectives for Information and Related Technology* (COBIT) é um guia de boas práticas no qual `` *ferramentas de gestão da área de TI e de alinhamento estratégico que ajuda a entender e a gerenciar os riscos e benefícios associados à TI, juntamente aos objetivos da organização* ´´ (LOUREIRO et al. 2012). A estrutura do COBIT abrange critérios da Informação relacionadas aos quesitos de segurança (integridade, disponibilidade e confidencialidade), tornando-o uma ferramenta que auxilia nas melhores tomadas de decisões dentro do ambiente organizacional.

O principal objetivo do COBIT é o alinhamento entre os objetivos do negócio e os objetivos propostos pela TI em uma organização, de modo a atender todas as necessidades impostas pelo negócio de uma maneira bem eficiente. Deste modo, serão realizados investimentos em TI conforme a necessidade que o negócio apresenta e entrega algum valor de volta a organização mantendo um balanço entre os benefícios adquiridos e os níveis de riscos de uso dos seus recursos. Observa-se pela Figura 4 que o COBIT engloba 34 processos agrupados em quatro domínios: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, por fim a Monitoração.

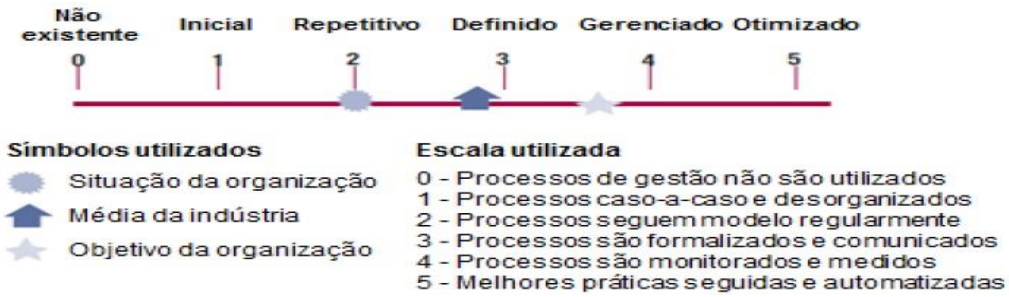
Figura 4 - Domínios e Processos do COBIT



Fonte: ITGI (2007)

Observando-se o COBIT é possível avaliar o nível de Segurança da Informação dentro de um ambiente organizacional. Para tal é feita a definição de um escopo, logo que definido é feito sua avaliação e por consequência a análise dos resultados obtidos. Segundo Rigon e Westphall (2011), o conjunto de indicadores obtidos por meio de consenso de experts, garantem que serviços sejam entregues de maneira otimizada. Um modelo de escala de maturidade usada na medição, pode ser vista na Figura 5.

Figura 5 - Representação gráfica do modelo de maturidade utilizado pelo guia de boas



Fonte: ITGI (2007)

O Quadro 4 apresenta a definição de cada nível de maturidade apresentado pela figura anterior.

Quadro 4 - Escala que compõem o nível de maturidade

Nível de Maturidade	**Definição**
0- Inexistente	Não existe nenhum reconhecimento por parte da empresa que algum tipo de risco se apresenta de maneira eminente.
1- Inicial	Existe a evidência por parte das empresas que algum tipo de risco e o reconhecimento que o mesmo deve ser tratado. Todavia, não existe um processo previamente padronizado, seguindo um procedimento individual e casual.
2- Repetitivo	São tipos de processos definidos dentro das empresas a partir de um conhecimento já adquirido em atividades similares feitas anteriormente. Não possuem qualquer tipo de treinamento e está sempre sujeito a erros.
3- Definido	São tipos de procedimentos aplicados dentro das empresas de modo que são devidamente documentados. Formalizados e comunicados. Existe a obrigatoriedade de seguir um padrão.
4- Gerenciado	A gerência monitora e mensura conformidade em todas as etapas do procedimento, tomando ações sempre que erros acontecem. Processos estão sempre em melhorias devido ao uso constante de ferramentas automatizadas.
5- Otimizado	Os processos foram refinados ao nível da aplicação de melhores práticas. Com isso, a TI é utilizada de maneira integrada para a automatização do fluxo de trabalho.

Fonte: Adaptado ITGI (2007)

A correta implantação dos recursos que irão garantir a Segurança da Informação em uma organização, depende da avaliação do ambiente e, por consequência, a aplicabilidade dos quesitos que irão suprir as necessidades dos pontos importantes apresentados nos resultados avaliados. Com isso, os processos que compõem a estrutura do COBIT podem ser utilizados para a elaboração de uma auditoria de TI.

2.5 Política de Segurança da Informação

Oliveira (2013) apresenta a informação como o elemento base para que a correta evolução aconteça, isto é, representado como elemento fundamental para o sincronismo de todos os processos organizacionais, por consequência é considerada um ativo de grande valor para o negócio. Por isso, é essencial que meios para garantir sua segurança sejam aplicados ao negócio como meio de protegê-la de eventuais riscos.

A Política de Segurança da Informação (PSI), é um documento responsável por orientar e estabelecer diretrizes, normas e procedimentos a serem seguidos, de modo a garantir a segurança dos ativos de informação e tecnológicos, além de responsabilizar os usuários para sua prevenção. Devendo ser cumprida por todas as áreas corporativas da instituição (SENAC, 2013).

Spanceski (2004) apresenta a importância em criar uma PSI com foco em instituições de ensino, por se tratar de um ambiente diferente daqueles vistos em organizações coorporativas. Sendo assim, as informações que irão compor este documento deverão conter normativas e diretrizes próprias que serão seguidas por todos os usuários dos recursos institucionais, de modo a conscientizá-los pela importância em garantir a segurança da informação e dos recursos tecnológicos da instituição.

A PSI tem por objetivo prover diretrizes e normas de acordo com os requisitos do negócio e com regulamentações vigentes, afim de guiar os usuários para o correto uso das informações e dos ativos tecnológicos de cada organização (NBR IEC/17799:2005). Ela descreve como os recursos de TI de uma organização deverão ser manuseados a fim de evitar a ocorrência de incidentes, o que pode levar a uma indisponibilidade do serviço prestado. Deve-se ressaltar que o comprometimento da direção é fundamental para sua aplicação, bem como, pela sua manutenção.

A elaboração de uma PSI deverá ser redigida por um comitê de segurança da informação, constituído de profissionais de diversificados departamentos da organização em questão, tais quais, informática, diretoria, jurídico, e demais departamentos. Esse comitê será responsável por estruturar, organizar, estabelecer procedimentos de segurança que atendam todas as expectativas da organização quando relacionado ao quesito segurança e sua implementação (FREITAS e ARAUJO, 2008). Ao final, esse mesmo comitê deverá ser responsável pela divulgação e conscientização dos usuários finais.

De um modo geral, os passos seguidos desde o planejamento até a implantação de uma PSI podem ser observados na Figura 6. É importante que a organização apresente um colaborador que ficará responsável por monitorar a política, além de atentar-se a

possíveis incoerências que venham surgir com o passar do tempo, é importante a observação de possíveis vulnerabilidades e mudanças nos processos e na infraestrutura.

Figura 6 - **Passos para a implantação de uma PSI**

Fonte: Adaptado Macêdo (2013)

Desse modo, segundo Macêdo (2013) os passos para a criação de uma PSI podem ser definidos como:

- **Planejamento**: é preciso fazer um planejamento prévio, considerando informações como: quem se responsabilizará pela sua estruturação, o que deverá ser protegido, como será protegido, melhores práticas a serem estabelecidas, além de conhecer o perfil da organização. De um modo geral, o planejamento deverá identificar todas informações importantes para a criação de uma PSI, considerando que um planejamento consolidado, apresentará justificativas plausíveis mediante a direção para a sua implantação.

- **Elaboração de normas, diretrizes e procedimentos**: considerada uma etapa crucial para a estruturação da PSI, uma vez que, nesta fase serão elaboradas as normas, diretrizes e procedimentos para acesso aos recursos. É fundamental que estejam detalhados de modo que os futuros usuários, não tenham dúvidas quanto ao seu uso, aqui deverão ser criadas normas de acessos aos recursos de rede, recursos lógicos, bloqueios de sites, etc.

- **Estruturação do documento**: tendo em mãos o planejamento da PSI, bem como as normas que deverão compor o documento, é necessário então estruturar o documento. Para tal, organiza-se o documento de modo a amparar todos os objetivos propostos na fase de preparação da PSI.

- **Aprovação do documento por parte da diretoria e do comitê de segurança**: uma vez estruturada e documentada a PSI o próximo passo a ser seguido deverá ser feito pela direção e do comitê gestor da segurança. Ficará

a cargo de ambos a validação e posterior implantação da PSI dentro do ambiente organizacional.

- **Implantação e treinamento da política elaborada**: considerada a fase mais importante do processo de elaboração de uma PSI. Nessa etapa é importante conscientizar os futuros usuários sobre a importância em seguir a PSI criada. Desse modo, deverão ser realizados treinamentos, palestras e conscientizações, com a finalidade de adaptá-los à nova cultura organizacional que será implantada.

2.6 Auditoria

Segundo Mello (2005), a auditoria pode ser definida como o processo pelo qual é verificado se a completude das atividades, processos, operações, sistemas e responsabilidades gerenciais estão em conformidade com os objetivos e políticas institucionais. Ou seja, avalia se os orçamentos, regras, normas e padrões estão de acordo com as exigências estabelecidas.

Uma auditoria tecnológica apresenta indicativos pelos quais é possível verificar qual a situação atual da organização e quais são as principais melhorias que deverão ser realizadas acerca do ambiente em análise, bem como, a identificação de oportunidades que produzirá conhecimentos relevantes sobre principais necessidades. Além, de identificar oportunidades de competitividade mediante a seus concorrentes (RIBEIRO, 2011).

Arundel, Corvers e Hocke (2000) apresentam que as informações geradas durante um processo de auditória tecnológica serão utilizadas para avaliar como anda a performance e práticas estratégicas das empresas, em prol da garantia da aplicabilidade da segurança. Isso permitirá identificar os principais pontos de vulnerabilidades detectados pela análise, bem como, a identificação das tecnologias que deverão ser adquiridas para apoiar na garantia da qualidade do serviço prestado.

Uma auditoria tecnológica auxilia na identificação de alguns pontos, tais quais:

- Servir como fonte de informações estratégicas.
- Identificar possíveis problemas provenientes de vulnerabilidades.
- Orientar a possíveis mudanças do mercado global, tecnologias e processos.
- Construir uma base de conhecimento sobre os recursos tecnológicos e informacionais presentes.
- Contribuir para o desenvolvimento cultural e tecnológico da organização.

- Obter a perspectiva do negócio, bem como, de sua situação mediante aos seus concorrentes.
- Identificar pontos de falhas dentro das organizações.

A finalidade de uma auditoria de segurança é avaliar a completude da gestão de segurança da informação, o controle dos ativos tecnológicos e os riscos acerca do ambiente organizacional. Com isso, aborda-se aspectos de confidencialidade, disponibilidade e integridade dos recursos físicos e lógicos presentes (LENTO, 2011).

2.7 Considerações Finais

Este capítulo apresentou o referencial teórico necessário para o entendimento do trabalho proposto. Nele foi explanada a importância da informação dentro de uma organização, bem como a definição de conceitos de segurança da informação. Posteriormente foram apresentadas as normas NBR IEC/27002:2013 e a NBR IEC/27001, essenciais para a garantia da segurança em um ambiente coorporativo. Uma breve definição sobre o *framework* ITIL e do guia de boas práticas COBIT foram realizadas, além de uma breve introdução sobre a Política de Segurança da Informação e qual a importância da realização de uma auditoria dentro de um ambiente institucional. A seguir, no Capítulo 3, será apresentado o Instituto de Ciências Exatas e Aplicadas, local escolhido para a realização do trabalho proposto.

3 A UNIVERSIDADE FEDERAL DE OURO PRETO – CAMPUS ICEA

O campus ICEA foi criado em 22 de setembro de 2002, numa parceria entre a Universidade Federal de Ouro Preto e a Prefeitura Municipal de João Monlevade. No início de sua criação apenas dois cursos de graduação eram ofertados, sendo eles, Engenharia de Produção e Sistemas de Informação. Atualmente, o campus conta com mais dois cursos de graduação: Engenharia Elétrica e Engenharia de Computação.

O instituto conta com uma infraestrutura compostas por 8 blocos. Divididos entre blocos educacionais (A, B, C, D, E, H e I), bloco administrativo (G) e o bloco destinado ao almoxarifado (F). No Quadro 5 estão subdivididos os setores por blocos, que compõem o ambiente institucional.

Quadro 5 – Distribuição dos setores que compõem o ambiente institucional.

Bloco	**Setores**
Bloco A	• Laboratório de Engenharia e Desenvolvimento de Sistemas (LEDS). • Empresas júniores: Ascender Treinamentos e Projetos Elétricos, Inova Consultoria Jr e Visão Tecnologia de Sistemas Jr. • Sala do NTI. • Salas de aula. • Laboratório de Inteligência Computacional (LAIC).
Bloco B	• Salas de monitoria. • Sala de reunião. • Salas de aula
Bloco C	• Laboratórios de computadores de uso geral e laboratórios de computadores destinado a ensino. • Laboratório destinado a pesquisas. • Núcleo de Assuntos Comunitários Estudantis (NACE). • Salas de Aula.
Bloco D	• Cantina.

	• Incubadora de Empreendimentos Sociais e Solidários (INCOP). • Salas de aula.
Bloco E	• Restaurante universitário. • Salas de aula. • Xerox.
Bloco F	• Garagem. • Almoxarifado. • Sala de Manutenção. • Copa.
Bloco G	• Colegiados de todos os cursos de graduação. • Seção de Ensino. • Recepção. • Centro de Extensão. • Secretárias: Departamento de Engenharia de Produção (DEENP), Departamento de Ciências Exatas e Aplicadas (DECEA), Departamento de Computação e Sistemas de Informação (DECSI) e o Departamento de Engenharia Elétrica). • Sala da diretoria e da vice diretoria. • Salas dos Professores. • Biblioteca.
Bloco H	• Laboratório do *LocoBots*. • Laboratório de química. • Laboratório de física. • Laboratório de IHC/Ergonomia. • Laboratório de circuitos elétricos. • Laboratório de controle e automação. • Laboratório de processamento de sinais (Telecomunicações) / Radiofrequência. • Laboratórios Digital.

	• Laboratório de sistemas industriais.
Bloco I	• Laboratório do *Imobiles*. • Salas para prática de esportes.

Fonte: Elaborado pela autora

A seguir, na Tabela 1 serão apresentadas a quantidade de pessoas que compõem o ambiente institucional até março de 2017. Estes estão divididos entre alunos, docentes, técnicos administrativos, terceirizados e anistiados.

Tabela 1 - Quantidade de pessoas que compõem o ambiente institucional

Descrição	**Número Aproximado**
Docentes	92
Alunos	1368
Técnicos Administrativos	24
Terceirizados	35
Anistiados	26

Fonte: Elaborada pela autora

O ICEA, por contar com uma infraestrutura física e tecnológica consolidada e com um considerável número de pessoas que fazem acessos a esses recursos tecnológicos, viu-se a necessidade de elaborar mecanismos de proteção. Desse modo, foi proposta a elaboração de uma PSI para que os recursos pudessem ser acessados da maneira correta, restringindo por consequência a exposição dos recursos à práticas maliciosas e acesso por parte de pessoas não autorizadas, além da realização de uma auditória tecnológica. Ambos com o intuito de garantir a segurança no contexto ICEA.

3.1 Considerações Finais

Este capítulo apresentou o ICEA, local definido para a elaboração do trabalho proposto, por meio de avaliações e aplicações de métodos que garantam a segurança dos recursos tecnológicos e de informações presentes.

A seguir, no Capítulo 4, será abordada a PSI proposta para o ICEA, de modo a guiar os usuários dos recursos tecnológicos e de informação presentes para seu correto uso.

4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NO ICEA

A PSI, conforme visto, é um documento cuja finalidade é estabelecer e orientar usuários por meio de diretrizes, normativas e procedimentos para o correto uso dos ativos de informação e tecnológicos presentes em um ambiente institucional. Além, de responsabilizá-los pela garantia da segurança.

O objetivo da PSI a ser proposta é minimizar a ocorrência de ameaças que colocam em risco a eficácia e a eficiência dos serviços prestados pelo ICEA. As ameaças presentes envolvem a interrupção dos serviços de rede, a indisponibilidade de informações cruciais para o negócio, a quebra de integridade e confidencialidade dos recursos tecnológicos e constantes exposições ao risco de maneira eminente.

Considerando-se o crescente avanço de novas tecnologias e como consequência desse feito, o surgimento de novos tipos de ameaças que colocam em risco a garantia dos quesitos fundamentais da segurança da informação (confidencialidade, disponibilidade e integridade) e o considerável número de usuários que acessam de maneira direta ou indireta os ativos tecnológicos e de informação, observou-se a necessidade de estabelecer métodos eficazes e eficientes de proteção.

Mediante a necessidade de proteger os ativos tecnológicos e de informação presentes no ICEA, viu-se a importância de elaborar e implantar uma PSI que atendesse as necessidades observadas. Para criação da proposta do modelo de documento apresentada nesse estudo foram levantadas a priori algumas informações como:

- Estudo da Norma NBR ISO 17799, uma vez que, esta Norma é definida como o código de prática para a gestão e garantia da segurança da informação.
- Estudos sobre a viabilidade da implementação de uma PSI que tivesse foco no contexto ICEA.
- Informações relevantes sobre os principais pontos de ameaças existentes no ICEA, com base na identificação da infraestrutura tecnológica do instituto.
- Apoio nos modelos de processo do ITIL
- Estudos de modelos de segurança da Informação:
    - Modelo de PSI do Instituto Federal do Norte de Minas Gerais (IFNMG, 2013).
    - Modelo de PSI do Santander (SANTANDER, 2013).
    - Modelo de PSI da Advocacia Geral da União (AGU, 2013).

4.1 Planejando uma Política de Segurança da Informação para o ICEA

Considerando-se que o ICEA é um *campus* situado na cidade de João Monlevade e que é subordinado a UFOP, em primeira instância optou-se por certificar se a universidade em questão possuía alguma Política de Segurança da Informação em vigência para que fosse adaptada uma política que atenderia o contexto ICEA. Para isso, um *email,* foi encaminhado ao NTI/UFOP como pode ser visto no Anexo A. Porém, em resposta constatou-se que a universidade não possui uma PSI em vigência, possui apenas um Comitê Gestor de Segurança da Informação e Comunicação (CGSIC) localizado na cidade de Ouro Preto criado com a finalidade de elaborar uma PSI que seria adotada pela UFOP. Ressalta-se que a portaria de criação do comitê responsável pela confecção da PSI no contexto UFOP ainda não foi publicada, e por questões éticas não foi anexada a essa monografia.

Uma vez constatada a inexistência de uma PSI em vigência no ambiente da UFOP, optou-se por elaborar uma política atendendo as necessidades de segurança tecnológicas e de informações. Para isso, como primeira etapa do planejamento, observou-se quais seriam as principais vulnerabilidades acerca do ambiente institucional que colocavam em riscos os serviços prestados. Desse modo, realizou-se a seleção de um grupo específico composto por: laboratórios de computadores para uso geral, laboratórios de computadores destinados a ensino (Redes, Programação e Otimização), os principais equipamentos tecnológicos presentes no bloco administrativo (Impressoras, Cabos de Rede, *Voice Panel*[1], *Patch Panel*[2], *Transceiver*[3]), a sala no qual o NTI/ICEA mantém sua instalação e dos *data shows* presentes em todas as salas de aula do instituto. Justifica-se pela escolha o fato de serem considerados ambientes fundamentais para a continuidade dos serviços oferecidos, sendo assim, pontos chaves para práticas maliciosas.

Definindo a importância de avaliar a infraestrutura do instituto, como segunda etapa do planejamento, realizou-se uma coleta de informações consideradas cruciais para a

[1] *Voice Panel*: é um painel de conexões destinado ao espalhamento de centrais telefônicas e à posterior distribuição de sinais de voz. Sua configuração depende da sua aplicação.

[2] *Patch Panel*: são equipamentos tecnológicos utilizados para organizar os cabos de rede, possibilitam uma fácil identificação dos pontos de rede no *rack*. São utilizados para realizar a conexão entre o cabeamento que sai do *rack* e chegam às tomadas, ou até mesmo em outro *patch panel*.

[3] *Transceiver*: é um dispositivo que combina um transmissor e um receptor utilizando componentes comuns, com o propósito de fornecer ambas as funções em um único equipamento.

estruturação da PSI. Para tal, elaborou-se um documento, no qual foi possível identificar todos os pontos de vulnerabilidades detectados no grupo preestabelecido, além de propor modelos de melhorias para solucionar tais problemas. Todavia, por questões éticas e em respeito a este instituto, o documento em questão não será anexado a esta monografia. Ressalta-se que a coleta e documentação das informações descritas, foi realizada pela própria autora e posteriormente encaminhado para a direção do ICEA.

Por fim, em uma terceira etapa do planejamento destacou-se que existe uma preocupação pertinente relacionada a sala no qual o NTI/ICEA mantem sua instalação, por ser considerado um departamento fundamental para o instituto, o mesmo deve ser protegido de possíveis vulnerabilidades que coloque em risco o serviço por ele prestado. Considerando que é um prestador das tecnologias e dos serviços de manutenção dessas Ciclo de Vida de uma informação, sua interrupção acarreta problemas aos demais departamentos presentes. Desse modo, elaborou-se um questionário que foi respondido pelos técnicos do NTI/ICEA, conforme pode ser visto no Apêndice A. Este questionário identificava quais as principais responsabilidades atribuídas a este departamento e quais as principais dificuldades enfrentadas.

Dentre as dificuldades apresentadas pelos técnicos do NTI/ICEA destaca-se o acesso a rede sem fio estudantil e administrativa, que devida a altas demandas em alguns horários os pontos de acessos muitas vezes são insuficientes, causando a falta de disponibilidade do serviço.

Ressalta-se que um planejamento bem estruturado tem a finalidade de apresentar justificativas plausíveis para a elaboração de uma Política de Segurança da Informação mediante a direção. Uma vez que, é necessário solicitar a aprovação da produção e posterior implantação do documento por parte da diretoria do instituto.

4.2 Criação de Normas, Diretrizes e Procedimentos

Um modo de garantir a aplicabilidade dos quesitos fundamentais da segurança da informação, dar-se pela maneira como as normas serão caracterizadas. A correta elaboração e estruturação das normas, diretrizes e procedimentos, estabelece a maneira pela qual os usuários deverão utilizar os ativos tecnológicos presentes dentro do ambiente institucional. De um modo geral, as normas têm por finalidade definir caminhos e instruções pelos quais os usuários devem seguir a fim de atingir os objetivos esperados. No caso do ICEA, as normas foram estabelecidas de acordo com as necessidades definidas no planejamento realizado anteriormente.

Optou-se por criar normas especificas de cada ambiente do ICEA, de modo a compor o documento da PSI, um exemplo disso, foi a criação de normas para acesso aos laboratórios de computadores destinados a ensino. Para sua definição, levou-se em consideração o constante uso dos mesmos por parte de professores e alunos por meio das aulas práticas das disciplinas ofertadas nos quatro cursos de graduação. Avaliou-se a possibilidade de elaborar diretrizes e normas de acesso para o departamento do NTI/ICEA, devido ao grau de criticidade que este apresenta para o instituto.

4.2.1 Normas de acesso aos laboratórios de computadores

Tendo em vista o constante uso dos laboratórios de computadores por meio das aulas práticas, viu-se a necessidade de garantir a segurança dos ativos tecnológicos presentes. Para isso, procurou-se certificar a existência de algum documento que orientasse os usuários ao uso dos recursos presentes. Em resposta, obteve-se o conhecimento da utilização de um “guia” que apresentava o modo como os usuários deveriam acessar os recursos disponíveis nos laboratórios.

Porém, observou-se que o documento utilizado não era suficiente para garantir a segurança dos recursos presentes nos laboratórios de computadores, desse modo, foi então proposto a reestruturação do documento, adicionando a ele normas de acesso e conduta específicas. Para sua criação, foram estudadas algumas normas destinadas a segurança da informação e tecnologia, além de modelos a serem seguidos, conforme apresentadas no Capítulo 2:

- Estudo da Norma NBR ISO/IEC 17799[4].
- Estudo da Norma NBR ISO/IEC 27001.
- *Framework* ITIL.

Sua estrutura baseou-se na necessidade de garantir que os recursos presentes pudessem ser acessados de maneira segura, além de fornecer informações claras e objetivas aos seus usuários, conforme pode ser visto no Apêndice B.

[4] NBR ISO/IEC 17799 tem por objetivo ``*estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.* ´´ [NBR IEC/17799:2005, p.1]

4.2.2 Avaliação do acesso ao NTI/ICEA

O NTI/ICEA é responsável por garantir o acesso e a manutenção dos recursos tecnológicos presentes no instituto, bem como, sua disponibilidade em tempo integral. Possui em seu ambiente servidores, computadores e recursos de redes, o que o torna um local propício a praticas maliciosas. Por ser considerado um ambiente crucial para o correto funcionamento dos recursos tecnológicos do ICEA, é importante estabelecer mecanismos que garantam sua segurança.

Considerando-se a importância que este departamento possui para o ICEA, avaliou-se a possibilidade de elaboração de diretrizes e normas para acesso à sala do NTI/ICEA. Dentre as medidas propostas, pensou-se na possibilidade de restringir o acesso de maneira direta, para tal, algumas possibilidades foram apresentadas, tais quais:

- Criar uma antessala na parte da frente como modo de restringir o acesso ao local no qual está inserido o NTI/ICEA, uma vez que, a sala, por não possuir uma recepção para atender as requisições solicitadas junto ao departamento, obriga as pessoas adentrarem diretamente ao local. Isso pode expor o ambiente a ameaças e a ataques aos equipamentos e às informações restritas nele contidos. Além disso, as conversas entre funcionários do departamento no momento podem ser confidenciais, e devem ser protegidas de pessoais não relacionadas com o setor. Por exemplo, uma pessoa alheia ao setor pode estar no NTI/ICEA enquanto são discutidas estratégias de segurança e infraestrutura, códigos, senhas e proteções, dentre outros.
- Estabelecer políticas de descarte seguro para os lixos gerados dentro do NTI/ICEA.
- Definir um acesso controlado dos técnicos na sala do NTI/ICEA. Ex: Criar recursos que inviabilizem o acesso físico direto, ou seja, somente os técnicos de informática e bolsistas do NTI teriam acesso à sala. Esse controle poderia ser feito de trancas elétricas, biométricas ou solicitações de senhas.

Destaca-se que os pontos apresentados tratam-se apenas de uma proposta para sanar o problema que o NTI/ICEA atualmente apresenta. Desse modo, a estruturação das normas, diretrizes e procedimentos para acesso ao departamento em questão ficará como trabalho futuro.

4.3 Estruturação de uma Política de Segurança da Informação no contexto ICEA

Seguindo as recomendações da Norma ABNT NBR ISO/IEC 17799 (ABNT 2005), iniciou-se a criação do documento da PSI, de acordo com as diretrizes para a implementação, os seguintes passos foram seguidos:

- A definição da segurança da informação aplicada ao contexto ICEA, bem como, suas metas, seu escopo e princípios da segurança da informação.
- Comprometimento por parte da direção para a aprovação das metas, diretrizes, normas e procedimentos estabelecidos.
- Estabelecimento dos objetivos de controle, avaliações/análises do gerenciamento de risco.
- A descrição de normas, princípios, requisitos de conformidade, definições de termos chaves da tecnologia, além da inclusão de requisitos de regulamentação, requisitos de conscientização, treinamento dos usuários para a nova cultura que será implantada e consequências da não adequação a política imposta.
- Definição de responsabilidades.

A Política de Segurança da Informação do ICEA abrange itens que estão relacionados com as principais necessidades apresentadas durante a fase de planejamento, desse modo, sua estrutura na versão inicial proposta contempla: o escopo, conceitos e definições, a estrutura geral da PSI, diretrizes, normas e procedimentos gerais, e as competências e responsabilidades, que serão discutidas nas seções seguinte.

4.3.1 Escopo

Esse tópico visa apresentar a finalidade pela qual a Política de Segurança da Informação é empregada, os objetivos principais de sua implantação e o estabelecimento de sua abrangência dentro do contexto ICEA. Ou seja, apresentar a política identificando seus propósitos e conteúdo de modo a identificar de maneira resumida e coesa as diretrizes, Normas e procedimentos. Além de identificar qual será a amplitude que terá em relação ao ambiente, indivíduos, departamentos e afins.

4.3.2 Conceitos e definições

Esse tópico visa definir conceitos abrangentes ao contexto tecnológico. De modo a compor o documento da Política de Segurança da Informação, foram definidos termos utilizados em sua conjuntura. Dentre eles, por exemplo: acessos lógicos, ameaças, senhas e demais.

4.3.3 Estrutura Geral da Política de Segurança da Informação

Esse tópico visa definir a classificação da informação levando em consideração o contexto ao qual está sendo aplicada, apresentar informações sobre acesso aos recursos de rede, autenticação de senhas, utilização de recursos de informação, utilização de equipamentos particulares dentro dos laboratórios e direitos de acesso ao ambiente institucional.

4.3.4 Diretrizes Gerais

Esse tópico visa apresentar em primeira instância as Normas de acesso aos laboratórios de uso geral, estabelecidas no processo de criação das Normas, diretrizes e procedimentos.

4.3.5 Competências e Responsabilidades

Por fim, esse tópico visa apresentar quais as principais responsabilidades e competências estabelecidas aos usuários dos recursos de informação e tecnológicos presentes no ambiente institucional. Assim, serão destinadas de acordo com sua classificação, sendo elas:

- Diretoria.
- Docente
- Discente.
- Técnico Administrativo

Observa-se que cada nível de classificação apresenta uma responsabilidade diferente ao que diz respeito à segurança institucional.

4.4 Implantação da Política de Segurança da Informação

Considerando a importância em proteger as informações presentes em um ambiente institucional, bem como, os recursos tecnológicos, foi então proposta a implantação de uma PSI no contexto ICEA. Como resultado dessa proposta, foi então estruturado um documento contendo o escopo, documentos que integram a PSI do ICEA, regulamentações e normativas, diretrizes, e responsabilidade, conforme pode ser visto no Apêndice C.

Todos os documentos gerados durante o processo foram encaminhados a direção do instituto. Uma vez que, é de suma importância o aval da diretoria para que todos aceitem, respeitem as normas e procedimentos vinculados na PSI. Uma vez de posse dos documentos, a direção do ICEA optou por apresentá-los em uma reunião do conselho institucional. Devido a uma decisão do conselho departamental do ICEA, criou-se um comitê gestor da informação responsável pela análise do documento e posterior implantação no instituto.

O comitê gestor da informação criado é composto por três professores do Departamento de Engenharia da Computação e Sistemas de Informação ficará a cargo do comitê, a responsabilidade de revisar o documento proposto, bem como a norma de acesso aos laboratórios de computadores destinados a ensino, e então juntamente com a direção promover a conscientização do seu uso por meio de informativos, palestras, elaboração de guias rápidos, e caso se aplique, treinamentos. Além da elaboração de mecanismos de adequação sempre que aplicável, uma vez que, em se tratando de recursos tecnológicos e de informação, é corriqueiro que mudanças sempre aconteçam.

Para auxiliar no processo de aceitação dos usuários para a nova política proposta a ICEA poderia realizar palestras de maneira a conscientizar a importância da segurança e instruir a comunidade acadêmica e os funcionários a importância de seguir as Normas estabelecidas. Essas palestras podem ser realizadas por técnicos de informática, pelo comitê gestor da segurança, ou pela própria direção com intuito de informar quais os riscos eminentes que o instituto poderá estar exposto, caso não sejam seguidas as recomendações dos documentos. Os computadores dos laboratórios de ensino, por exemplo, deveriam ser utilizados apenas para fins acadêmicos. Deve-se ressaltar a necessidade de realizar essas palestras pelo menos uma vez a cada semestre, já que alunos novos chegam ao ICEA nos dois semestres.

Deste modo, espera-se que a política proposta contribua para a garantia da segurança dentro do instituto, servindo como um guia para a correta utilização dos ativos tecnológicos presentes, bem como, a correta manipulação de suas informações. Ressalta-

se, todavia, que até o presente momento, não obteve-se nenhuma deliberação do comitê referentes aos documentos entregues, e que por esse motivo, a PSI, bem como, o documento de normas para acesso aos laboratórios de computadores, não estão em vigência.

4.5 Considerações Finais

Este capítulo apresentou a finalidade para a implantação de uma PSI acerca do ICEA, bem como, os passos seguidos para sua estruturação, de modo a alcançar os objetivos estabelecidos. A PSI proposta para o instituto visa criar mecanismos de proteção para os ativos tecnológicos e de informação presentes. Conforme apresentado, existe todo um planejamento a ser feito para a concepção do documento final, além, de dispor do apoio da direção. Foram identificadas as principais necessidades de segurança do ICEA, para então estabelecer uma PSI que melhor adequasse aos pontos observados.

A PSI proposta para o ICEA apoiou-se nas recomendações da Norma ABNT NBR ISO/IEC 17799, tendo em vista, a importância que os recursos presentes possuem para a continuidade dos serviços prestados. Sua estrutura baseou-se na criação de um escopo que identificava a razão pela qual a PSI é empregada, os objetivos principais de sua implantação e o estabelecimento de sua abrangência dentro do contexto ICEA. Além da definição de conceitos utilizados na conjuntura da política criada, normativas e regulamentações pela qual a PSI embasava-se e por fim as responsabilidades definidas a cada usuário dos recursos presentes no ICEA.

Ressalta-se que foram estabelecidas normas de acesso aos laboratórios de computadores destinados a ensino, de modo a orientar os usuários, a correta utilização dos recursos presentes. Todavia, os documentos propostos ainda não se encontram em vigência uma vez que necessita-se da aprovação da direção e do comitê da segurança. Diante à essas burocracias, foi criado um comitê gestor da informação em uma reunião departamental e este será responsável pela a validação e implantação tanto da PSI, quanto das normas estabelecidas. A seguir, no Capítulo 5, será abordada a auditoria interna dos recursos tecnológicos e de informações realizada no ICEA, de maneira a apresentar as inconformidades do instituto com a PSI proposta.

5 AUDITORIA TECNOLÓGICA NO ICEA

Com o objetivo de verificar a conformidade, a qualidade, a eficácia e a efetividade da área de TI dentro do instituto acordadas pela PSI proposta, foi sugerida a realização de uma auditoria interna. Considerando que o lCEA conta atualmente com um número relativamente alto de usuários que fazem acesso aos recursos tecnológicos presentes, incluindo diretamente: docentes, discentes, técnicos administrativos, anistiados e terceirizados. Totalizando aproximadamente 1545 usuários diretos até março de 2017, viu-se a necessidade de investigar a existência de vulnerabilidades nos recursos tecnológicos e de informação presentes.

O instituto conta com servidores, computadores, *data show*s, cabeamentos de rede, equipamentos de rede e diversos outros tipos de tecnologias, além de uma quantidade considerada de informações, em sua maioria de cunho confidencial, que circulam dentro do ICEA. Devido a esses quesitos é fundamental que a garantia da segurança seja uma preocupação constante. A realização de uma auditoria, ajuda a identificar pontos de vulnerabilidade que colocam em risco essa segurança e por consequência a quebra da integridade, disponibilidade e confidencialidade.

Logo, a auditoria foi realizada após a estruturação da PSI e seus resultados seguiram os seguintes passos: planejamento, identificação do ambiente, execução, análise dos resultados e ações pós-auditoria, que podem ser observados a seguir.

5.1 Planejamento

Durante o planejamento da auditoria no ICEA algumas informações foram levantadas afim de compor as próximas etapas a serem realizadas no processo. Dentre essas informações foram estabelecidos alguns pontos:

- **Áreas a serem auditadas**: para tal selecionou-se áreas especificas oriundas de um ataque malicioso, de modo a comprometer as principais atividades do ICEA.
- **O escopo da auditoria**: pretende-se atingir ao final da auditoria, uma excelência nos processos e ambientes auditados, e a conclusão de um trabalho proposto pela autora. Além de basear-se na Norma NBR ISO/IEC 27002 e nos processos de maturidade da metodologia COBIT para tal. Alinhando as expectativas aos negócios da instituição.
- **Nome do auditado**: Instituto de Ciências Extadas e Aplicadas;

- **Nome do Auditor**: foi definido que a responsável pela auditoria seria a própria autora.
- **Ferramentas Utilizadas**: para a realização da auditoria foi acordado que um questionário serviria como guia para o levantamento das informações.

5.2 Identificação do Ambiente

Considerando-se o planejamento para a realização da auditoria no ICEA, foi feita a identificação do local para que a auditoria pudesse ser executada. Para tal, selecionou-se um grupo composto por equipamentos tecnológicos presentes no bloco administrativo, laboratórios de computadores destinados a ensino e a sala no qual o NTI/ICEA mantém sua instalação, como visto, o ambiente em questão trata-se do mesmo utilizado para o planejamento da PSI. Considerando-se que estes são propícios à praticas maliciosas.

O ambiente para a aplicação de uma auditoria deve ser criteriosamente selecionado, uma vez que, é durante um processo de auditoria que é possível mencionar os principais pontos falhos de uma organização, de modo, a propor as melhores soluções para a resolução dos problemas apresentados. Desse modo, procurou-se identificar os locais com maiores probabilidades de incidência de um ataque malicioso, que por consequência comprometeria o andamento dos serviços por eles oferecidos.

5.3 Preparação e Execução da Auditoria

Uma vez identificado o ambiente para avaliação, foram feitos estudos sobre o melhor modo de averiguar como anda o quesito segurança dentro do ICEA. Para isso, levou-se em consideração o crescente aumento das maneiras de ameaça que a tecnologia vem sofrendo mediante a sua constante evolução.

Para o desenvolvimento da auditoria foi utilizado um questionário, conforme pode ser visto no Apêndice D. Um dos conjuntos de questões define o nível de acesso, dos equipamentos e ambientes auditados. Outro conjunto de questões define qual a probabilidade de uma interrupção do serviço oferecido acontecer, caso exista a possibilidade de um ataque malicioso. As demais questões levantadas estão relacionadas ao grau de segurança presente nas instalações e equipamentos auditados e a busca por sugestões de melhorias, caso se aplique.

Durante o processo de auditoria, foram identificados pontos importantes referente a segurança que podem ser descritos abaixo:

- Observou-se impacto de um risco/ameaça para o ambiente institucional.

- A probabilidade de acontecer um incidente que interrompe a segurança estabelecida.
- O nível de segurança imposto dentro do instituto atualmente.
- Como anda o funcionamento dos serviços de redes, servidores e equipamentos tecnológicos.
- A probabilidade de acessos indevidos, o que acarretaria a impossibilidade do funcionamento.
- O nível dos sistemas de *Firewall.*
- A probabilidade de acessos indevidos em equipamentos e informações de teor confidencial, principalmente dos equipamentos presentes na sala do NTI/ICEA.
- Funcionamento dos controles de acesso físicos.
- Avaliação dos riscos sobre a estrutura tecnológica do instituto.
- Verificação da necessidade de implantação de novos controles de acesso dentro do instituto.

Ressalta-se que em todas as questões levantadas no questionário, tinha por principal objetivo era averiguar quais dos quesitos da segurança da informação e das tecnologias (confidencialidade, disponibilidade e integridade) não estavam sendo validados.

5.4 Análise dos Resultados Obtidos Pela Auditoria

Por meio do questionário utilizado na auditoria, foram levantadas informações que de modo direto identificavam as principais vulnerabilidades acerca do instituto.

De modo geral, os locais e equipamentos auditados foram avaliados separadamente, o que gerou respostas diversificadas. Porém, em todos eles as preocupações com os quesitos fundamentais da segurança foram levadas em consideração. Após realizada a avaliação do local selecionado, criou-se uma tabela com todas as respostas obtidas durante o processo de auditoria.

A partir das respostas recebidas, foi feita a sumarização dos dados apresentados. Para tal, utilizou-se os seguintes passos propostos pela autora:

- Em cada questão levou-se em consideração os quesitos de confidencialidade, disponibilidade e integridade. Por exemplo: o nível de proteção dos equipamentos/ambientes avaliados, deixam a desejar na: confidencialidade, disponibilidade e integridade. Sendo que era possível selecionar mais de uma opção.

- Foram avaliados diferentes tipos de ambientes/equipamentos. Todos considerados de extrema importância para a continuidade dos serviços prestados.
- O questionário foi composto por questões diversas, sendo que, todas consideravam os quesitos acima apresentados.

Tendo em vista esses dados observados, foi feita a quantificação das informações obtidas. Para tal, considerou-se o conjunto de equipamentos/ambientes avaliados e em cada um desses, foram levantadas as questões descritas no questionário proposto. Com isso, foi possível perceber que em cada ambiente/equipamento totalizavam uma quantidade de treze possibilidades de incoerência ou infração a cada quesito da segurança. Ao final, observa-se pela Tabela 2, que o quesito disponibilidade possui o maior número de possibilidades de ocorrer dentro do ambiente institucional.

Os dados apresentados basearam-se na seguinte formulação:

- Foram considerados nove ambientes/equipamentos a serem avaliados (sala do NTI/ICEA, data shows das salas de aula, laboratórios de computadores destinados a ensino (Redes, Programação, Otimização), laboratório de computadores de uso geral, impressoras, transceiver, patch painel, voice painel, cabos de rede).
- O questionário utilizado foi composto por treze questões, todas consideravam a possibilidade da não adequação aos quesitos fundamentais da segurança (confidencialidade, disponibilidade e integridade).
- Considerando que foram examinados nove ambientes/equipamentos e em cada um desses foram avaliadas as treze questões propostas, obteve-se com isso, um total de cento e dezessete possibilidades de não adequação à cada quesito da segurança da informação descritos acima, o que representaria cem por cento do percentual total avaliado.
- Tendo em vista todos as informações descritas, por exemplo: as impressoras alocadas no bloco administrativo, apresentou durante o processo de auditoria doze ocorrências de quebra de confidencialidade, nove de integridade e seis de confidencialidade no decorrer das questões vistas. Fato esse preocupante.
- Ressalta-se que os dados apresentados na tabela acima, foram considerados de um modo geral, conforme pode ser visto.

Tabela 2 - Apresentação dos resultados gerados pela auditoria.

Quesito	Quantidade	Percentual %
Confidencialidade	32	27.35
Disponibilidade	82	70.08
Integridade	71	60.68

Fonte: Elaborado pela autora

Os resultados apresentados, mostram que existe um considerável número de vulnerabilidades acerca do ambiente institucional, devido a não conformidade dos pontos avaliados, além de não haver a conscientização da importância em garantir a segurança dentro do ICEA. Logo, coloca em riscos os recursos tecnológicos e as informações presentes, fato esse alarmante.

5.5 Ações Pós Auditória

Tendo em vista os resultados obtidos durante a execução da auditoria, optou-se por documentar os principais pontos levantados como maneira de estabelecer níveis de criticidade para os problemas identificados. Uma vez, identificado e classificado, realizou-se a formalização das ações, de modo a sanar os problemas identificados.

Desse modo, foi elaborado um documento contendo todas as vulnerabilidades observadas, bem como, o que acarretaria para o instituto caso o problema de fato fosse consumado. Além, de um conjunto de ações corretivas a serem implantadas para tornar o ambiente um local mais seguro, ressalta-se, que o documento gerado foi encaminhado a direção do ICEA como modo conscientizá-los sobre os ameaças à segurança das tecnologias e das informações acerca do instituto, todavia, considerando o elevado grau de confidencialidade que tais documentos apresentam e por questões éticas, o documento não será anexado a esta monografia. Logo, espera-se que ações preventivas sejam tomadas em conjunto, pela direção juntamente com o departamento de informática o NTI/ICEA de modo a criar um planejamento estratégico e priorizar os investimentos na segurança de seus ativos.

No que diz respeito a segurança da informação, acredita-se que a incidência de ameaças que colocam em risco os quesitos fundamentais da segurança da informação no ICEA, se dá pelo fato de não possuir uma PSI em vigência. O uso constante desses ativos

por parte de professores, alunos e até técnicos administrativos sem a devida preocupação com a segurança e a ausência de normas e diretrizes de acesso aos recursos, tende a contribuir para o surgimento de riscos, que de uma maneira direta ou indireta, expõe o instituto a ataques que comprometem seu funcionamento correto.

Para que a segurança seja garantida o ICEA, recomenda-se adotar práticas e ações que estimulem os usuários a perceberem a importância em garantir a segurança. Sugere-se a promoção de palestras para conscientização ou até mesmo criações de novos projetos sobre o tema destacado. Deve-se ressaltar a necessidade de realizar essas palestras pelo menos uma vez a cada semestre, já que alunos novos chegam ao ICEA nos dois semestres. Outro fator crucial para a excelência da segurança, é o apoio e comprometimento da direção para que ações conjuntas possam ser tomadas para minimizar as ocorrências de ameaças. Computadores.

5.6 Considerações Finais

Este capitulo apresentou a importância da realização de uma auditoria dos recursos tecnológicos e de informações presentes no ICEA. Para tal, realizou-se um planejamento, de modo a identificar quais os principais objetivos a serem alcançados ao final desta. Durante o processo de auditoria, identificou-se as principais dificuldades em garantir a aplicabilidade dos conceitos fundamentais da segurança da informação (confidencialidade, disponibilidade e integridade). Os resultados apresentados foram sumarizados, e a partir disso, notou-se que existe um considerável número de vulnerabilidades acerca do ambiente institucional, devido a não conformidade dos pontos avaliados. Desse modo, um documento foi redigido e entregue a direção do ICEA para que ações corretivas pudessem ser tomadas a fim de sanar as ameaças detectadas. O próximo capítulo apresentará as contribuições e trabalhos futuros.

6 CONSIDERAÇÕES FINAIS

O presente trabalho propôs-se a avaliar o nível de segurança da informação e das tecnologias presentes no campus ICEA/UFOP, buscando identificar os principais pontos de vulnerabilidades, que colocariam em evidência os pilares fundamentais da segurança (confidencialidade, disponibilidade e integridade). Por meio de observações exploratórias nos principais ambientes e equipamentos do instituto foi possível alcançar os objetivos estabelecidos nesse trabalho.

A dependência gradual que as organizações retêm sobre recursos tecnológicos, as tornam cada vez mais propícias a ameaças, que de uma maneira direta ou indireta comprometem a continuidade dos serviços por elas prestadas. Não diferente destes problemas corriqueiros, o ICEA, é detentor de um considerável número de ativos tecnológicos que são acessados diariamente por diferentes tipos de usuários (professores, alunos e técnicos), logo, ser frequentemente acompanhados, de modo, a garantir sua segurança. Além de possuir uma vasta quantidade de informações, muitas vezes de cunho confidencial, que circulam diariamente em seu meio.

Mediante aos problemas enfrentados, viu-se a necessidade de criar métodos que pudessem contribuir para a garantia da segurança acerca do ICEA. Para isso, foram observados os principais pontos de vulnerabilidades, de modo, estabelecer quais seriam os mecanismos de proteção, que melhor atenderiam às carências do instituto. A priori, observou-se, que o instituto não possuía uma Política de Segurança da Informação que orientasse seus usuários diretos para o correto uso dos ativos informacionais e tecnológicos presentes. Logo, isso contribuía significativamente para a ocorrência atos maliciosos.

Considerando que a PSI é a base para todas as questões pertinentes à proteção da informação, além de contribuir para a segurança da informação, optou-se, pela sua implantação no contexto ICEA.

Para o desenvolvimento do modelo de PSI, em primeira instância identificou-se, quais as principais necessidades que o instituto apresentava. Uma vez identificada as necessidades, utilizou-se de alguns conceitos e modelos, tais quais: Norma NBR ISO/IEC 17799 para o planejamento e posterior estruturação da política proposta, modelos de maturidade do COBIT e modelos de políticas de instituições e organizações de renome (IFNMG, AGU e Santander). Ressalta-se, que política proposta, tem por finalidade o esclarecimento do usuário para o correto uso dos ativos tecnológicos e de informação.

Além disso, considerando o constante uso dos laboratórios de computadores por parte de professores e alunos, em decorrência das aulas práticas, foram elaboradas normas

de acesso aos recursos neles presentes, de modo, a guiar os usuários para seu correto uso. A norma proposta irá compor a PSI.

Considerando a importância em garantir a segurança dos recursos tecnológicos e de informação mediante o contexto ICEA, realizou-se ao final da elaboração da PSI uma auditoria interna tecnológica, cujo proposito foi identificar a conformidade entre a política proposta e a infraestrutura tecnológica do instituto. Para tal, foi feito todo um planejamento para a elaboração da auditoria. Primeiramente, selecionou-se um grupo composto por ambientes/equipamentos considerados propícios a ataques maliciosos, no qual foram identificadas as probabilidades de ocorrência da quebra dos quesitos fundamentais da segurança, em seguida, com os dados gerados foram sumarizados e anexados a um relatório que posteriormente foi entregue a direção do ICEA.

Todavia, algumas barreiras foram identificadas, um exemplo disso, foi a não implantação imediata, tanto das normas de acesso aos laboratórios de computadores, que por questões burocráticas, os documentos elaborados foram entregues a direção do instituto para validação, que por meio de uma reunião do conselho departamental, viu-se a necessidade da criação de um comitê gestor da segurança, dando a este a responsabilidade pela validação e posterior vigência dos mesmos. Porém, até o presente momento não se obteve nenhuma deliberação quanto a aplicabilidade dos documentos apresentados.

Outro problema identificado no ICEA, foi a não conscientização por parte dos usuários para a constante proteção dos recursos presentes, o que contribui em sua maioria para a ocorrência de vulnerabilidades.

Portanto, o objetivo geral do trabalho, que é avaliar o nível de segurança das informações e tecnologias presentes no ambiente institucional e propor por consequência métodos que minimizem a ocorrência de ataques maliciosos, foi alcançado. Como prova disso, foi a documentação das vulnerabilidades detectadas e a elaboração de modelos que garantam a segurança dos recursos e informações acerca do instituto.

No entanto, como foi observado o trabalho possui algumas limitações que retardam a eficácia e eficiência dos modelos propostos. Uma vez que, com a não implantação da política e das normas propostas, não é possível saber se de fato foram elaboradas de modo a garantir a segurança no ICEA.

6.1 Trabalhos Futuros

Espera-se que a PSI proposta para o ICEA juntamente com documentos de regras e normas de conduta a serem seguidos por parte de todas as pessoas que, de modo

direto ou indireto, compõem o ambiente institucional, sejam implantadas o mais breve, considerando a constante necessidade proteger os ativos. Espera-se também que todos aqueles que fazem parte do instituto contribuam para a aplicação dessa política proposta no trabalho, uma vez que, isso trará benefícios ao instituto.

A elaboração de normas, diretrizes para acesso a sala no qual o NTI/ICEA possui sua instalação, seria fortemente recomendada considerando a criticidade que o ambiente apresenta para o instituto. Além da elaboração de normas para acesso aos recursos de redes, normas para uso de computadores pessoais, normas de acesso a rede móveis, entre outros.

A aplicação de uma segunda auditoria, após a vigência da PSI e das normas de acesso aos laboratórios de computadores, seria recomendada de modo a identificar as principais incoerências identificadas no que foi proposto pela política que não estão sendo aplicadas adequadamente. Além de propor a elaboração de projetos, palestras ou afins, que contribuam para a conscientização de todos para a importância em garantir a segurança tecnológica e de informação dentro no ICEA.

Uma auditoria do sistema de reserva dos laboratórios também poderia ser realizada, de modo a identificar possíveis inconsistências presentes o impossibilitaria o seu correto funcionamento. Ressalta-se, que uma auditoria contribui para a identificação e controle dos riscos eminentes e devem ser realizadas sempre que uma organização julgar necessária.

Referências

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

AGU. **Política de Segurança da Informação e das Comunicações**: Diretrizes e Normas. Advocacia Geral da União: Departamento de Tecnologia da Informação – Gerência Executiva de Segurança da Informação e das Comunicações, Brasília, 2013.

CARDOSO, F. E.; OLIVEIRA, P. C., (2012). **Política de Segurança da Informação nas Empresas**. Brasília: Faculdade de Tecnologia de Ourinhos, 2012.

CAUBIT, R. C. Segurança como Norma. 2002. Disponível em: <http://www.inovarse.org/filebrowser/download/9237 >. Acesso em: 16 Set 2016.

COLWILL, C. R. Human factors in information security: The insider threat Who can you trust these days? **Information Security Technical Report**, p. 186-196, 2009.

COSTA, A. Riscos, Ameaças e Vulnerabilidades. Recife: Faculdade dos Guararape, 2010. Disponível em:< http://www.aeciocosta.com.br/wp-content/uploads/FG/Introducao%20a%20Seguranca%20da%20Informacao%202014-1/5-ISI-Riscos,%20Ameacas%20e%20Vulnerabilidades.pdf>. Acesso em: 23 Nov 2016.

DANTAS, M. **Segurança da Informação: Uma Abordagem Focada em Gestão de Riscos**. 1 ed. Olinda: Livro rápido, 2011.

DESPENET. O Modelo do Ciclo de Vida do Serviço. 2015. Disponível em: < http://www.despnet.com/ciclo-de-vida-servico-conheca-o-modelo/ >. Acesso: 12 Fev 2017.

FREITAS, F.; ARAÚJO, M. **Políticas de Segurança da Informação:** Guia Prático para Elaboração e Implementação. 2ª. ed. Rio de Janeiro: Ciência Moderna LTDA, 2008.

FONTES, L. G. **Alinhamento da Segurança da Informação com as Áreas de Negócio – Contribuição da NBR ISO/IEC 27002:2013.** International Conference on Information Systems and Technology Managment, São Paulo, 1991, p. 1521.

HAROLD, F. T.; KRAUSE, M. **Information Security Management Handbook**. 6ª. ed. New Work: CRC Press Taylor & Francis Group, v. II, 2008.

IFNMG**. Política de Segurança da Informação e das Comunicações** – POSIC. Comitê da Segurança da Informação e Comunicações, Minas Gerais, 2013.

INFOSEC COUNCIL. Formação da Cultura em Segurança da Informação. 2005. Disponível em: < http://computerworld.com.br/estaticas/downloads/catalogo_parte1.pdf >. Acesso: 10 Jan 2017.

ITGI – IT GOVERNANCE INSTITUTE. CobiT 4.1 - Control Objectives for Information and related Technology - Framework. Rolling Meadows - USA: [s.n.], 2007. Disponível em <http://www.isaca.org/Knowledge- Center/cobit/Pages/Downloads.aspx>. Acesso em: 12 Set 2016.

KOVACICH, J., Ph.D. (1998)**. Interview with Nick Houtman**. University of Maine Department of Public Affairs, Orono, Maine. August 7, 1998.

LAUNDON, K. C.; LAUDON, J. P. Sistemas de Informação Gerenciais. 11ª ed. Rio de São Paulo: Pearson, 2014.

LAUREANO, M. A. P. Gestão da Segurança da Informação, 2005. Disponível em: < http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acessado em: 14 de Dez 2016.

LENTO, L. O. B. Conceitos, Tipos, e Características de Auditorias da Segurança da Informação. 2012. Disponível em: <http://www.diegomacedo.com.br/conceito-tipos-e-caracteristicas-de-auditoria-de-seguranca-da-informacao/>. Acesso: 14 Jan 2017.

LOUREIRO, L. C. & PENHA, P. A. & NASCIMENTO, J. M. **Relacionamento das Melhores Práticas do COBIT e ITIL para Governança de TI**. Simpósio de Excelência em Gestão e Tecnologia. v. IX, 2012.

LOUREIRO, S. C. **Segurança da Informação**: Preservação das Informações Estratégicas com Foco em Segurança. 2008. Especialização – Departamento de Ciências da Computação, Universidade de Brasília, Brasília, 2008.

MACEDO, D. Política de Segurança da Informação: Como Fazer. Belém: Diego Macedo – Analista de TI,2013. Disponível em:< http://www.diegomacedo.com.br/politica-de-seguranca-da-informacao-como-fazer/>. Acesso em: 24 Fev 2017.

MARCONDES, J. S., Conceitos de Segurança da Informação Organizacional. São Paulo: Blog Gestão da Segurança Privada, 2015. Disponível em: <http://www.gestaodesegurancaprivada.com.br/conceito-de-seguranca-da-informacao-organizacional/>. Acesso em: 20 Out 2016.

MELLO, Agostinho de Oliveira. Instituto dos auditores internos do Brasil. **Organização básica da auditoria interna**. Biblioteca Técnica de Auditoria Interna, 2005.

MENDES, R.; MOREIRA, A. R. **ITIL na Gestão da Segurança da Informação**. International Conference on Information Systems and Technology Managment, São Paulo, 2008, p. 2.

NBR ISO/IEC 17799:2005. **NBR ISO/IEC 17799 – Tecnologia da Informação – Técnicas de Segurança – Códigos para a Gestão da Segurança da Informação**. ABNT – Associação de Normas Técnicas, Rio de Janeiro, 2005.

NBR ISO/IEC 27002:2005. **Tecnologia da informação – Técnicas de segurança - Código de Práticas para Gestão da Segurança da Informação**. 120 p. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2005.

NBR ISO/IEC 27002:2013. **Tecnologia da Inforamação - Tecnicas de Segurança - Códigos de Prática para a Gestão da Segurança da Informação**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

NTI/OUROPRETO. Núcleo de Tecnologia da Informação. Ouro Preto: NTI/UFOP, 2011. Disponivel em: <http://nti.ufop.br/apresentacao>25 Julho 2016.

OLIVEIRA, P. C. Política de Segurança da Informação: Definição, Importância, Elaboração e Implementação. 2013. Disponível em: <https://www.profissionaisti.com.br/2013/06/politica-de-seguranca-da-informacao-definicao-importancia-elaboracao-e-implementacao/>. Acesso: 22 Fev 2017.

PILZ. Resumo de Normas Básicas. São Bernardo do Campo: The Spirit of Safety. Disponível em: <http://www.pilz.com/knowhow/standards/standards/index.pt.jsp>. Acesso: 17 out. 2016.

REIS, B.; MOTA, J. C.; OLIVEIRA, P. P. B. (2001). **Classificação da Informação**. Brasília: SGAN 916, 2001.

RIBEIRO, E. ITIL e Segurança da Informação. 2012. Disponível em: < https://www.tiespecialistas.com.br/2012/08/itil-e-seguranca-da-informacao/ >. Acesso: 28 Dez 2016.

RIBEIRO, F. S. G. **Estratégicas Tecnológicas em PMEs:** Auditorias Tecnológicas. 2000. Dissertação– Departamento de Engenharia Eletrotécnica e de Computadores, Faculdade de Engenharia da Universidade do Porto, Porto, 2000.

RIGON, E. A.; WESTPHALL, C. M. **Modelo de Avaliação da Maturidade da Segurança da Informação.** VII Simpósio Brasileiro de Sistemas de Informação. Bahia. 2004.

SANTANDER. REF.: Política de Segurança da Informação para Correspondentes Bancários do Santander. 2013. Disponível em: <https://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf>. Acesso: 14 Ago 2016.

SÊMOLA, M. **Gestão da Segurança da Informação:** Visão Executiva da Segurança da Informação. Rio de Janeiro: Elsevier, 2003.

SENAC. PSI- Política de Segurança da Informação: Documentos de Diretrizes e Normas Administrativas. São Paulo, 2013. Disponível em: <http://www.sp.senac.br/Normasadministrativas/psi_Normas_administrativas.pdf>. Acesso: 03 Mar 2017.

SMITH, R. ITIL – Benefícios Associados à Segurança da Informação. 2012. Disponível em: <https://blogs.technet.microsoft.com/ronaldosjr/2010/01/05/itil-benefcios-associados-segurana-da-informao/>. Acesso: 20 Jan 2017.

SPANCESKI, F. R. **Política de Segurança da Informação**: Desenvolvimento de um Modelo Voltado para Instituições de Ensino. 2004. Dissertação (Graduação) – Departamento de Informática, Instituto Superior de Tupy, Joinville, 2004.

STAIR, R. M.; REYNOLDS, G. W. **Principios de Sistemas de Informação**. Rio de Janeiro: LTC Editora, 2002.

STEFANINI. Gestão de Riscos e Segurança da Informação. Stefanini Powering Your Business, 2016. Disponível em: < https://stefanini.com/br/2014/01/gestao-riscos-seguranca-informacao/>. Acessado em 17 de Jan 2017.

APÊNDICE A – Questionário de Avaliação do NTI/ICEA

1. Como é composta a estrutura organizacional do NTI/ICEA (Ex: Coordenador, técnicos, supervisor, etc)?

R: Composta por 3 técnicos, sendo: um Técnico de Laboratório, um Assistente de Tecnologia da Informação e um Técnico de Tecnologia da Informação.

2. Qual o número de servidores do NTI/ICEA? Existe bolsistas? Em caso afirmativo, quantos?

R: Não existe uma divisão de setores. O setor possui 2 bolsistas.

3. Quem são os usuários diretos dos recursos tecnológicos do ICEA?

R: Alunos, Professores e Técnicos.

4. Como é dividida a infraestrutura tecnológica do ICEA atualmente (número de computadores, domínios, recursos tecnológicos)?

R: Não dá para listar tudo em detalhes, pois equipamentos vem e vão, mas de modo geral:

- Laboratórios supervisados diretamente pelo NTI/ICEA:
    - Laboratório de Programação, com 35 máquinas;
    - Laboratório de Bando de Dados e Redes, com 35 máquinas;
    - Laboratório de Expressão Gráfica, com 35 máquinas;
    - Laboratório de Otimização, com 28 máquinas;
    - Laboratório de Uso Geral 1, com 20 máquinas;
    - Laboratório de Uso Geral 2, com 20 máquinas.
- Laboratórios não supervisionados diretamente pelo NTI/ICEA:
    - Laboratório de Pesquisa;
    - Laboratórios de Elétrica;
    - Laboratórios de Iniciação Científica.

Em média é usado um *Rack* e um *Switch* por andar no bloco administrativo. Nos blocos de laboratórios é usado um *Rack* ou mais *Racks* por andar e em média um *switch* por laboratório.

Nos blocos exclusivos de salas de aulas, normalmente é utilizado apenas um *Rack* e um *switch* por bloco.

Na sala do NTI/ICEA contamos com 3 servidores de virtualização em funcionamento, sendo um deles dedicado a MINHAUFOPWIFI, e dois para erviços internos e externos do ICEA, como domínios, *firewall*, servidor HTTP e Banco de Dados, entre outros.

Contamos com um domínio na rede para controle de acesso aos laboratórios de aula. O ICEA possui 4 laboratórios de aulas que atendem a todos os cursos, além de alguns

laboratórios específicos para pesquisa e para determinado curso ou disciplina. Além de também oferecer dois laboratórios de uso geral para os alunos.

5. Qual o número de laboratórios de computadores destinados a ensino e de uso geral presentes atualmente no ICEA?

R: Quatro laboratórios, sendo três deles contendo 35 computadores cada e um contendo 25 computadores.

6. Qual o tipo de rede utilizada no ICEA?

R: Cabeada e sem fio. Sendo que os blocos são ligados por fibra óptica e e a rede interna de cada bloco se divide entre Ethernet tradicional CAT5 e CAT6 e a rede sem fio.

7. È utilizado algum sistema acadêmico? Em caso afirmativo, qual e quem é o responsável por sua manutenção?

R: O sistema Moodle é utilizado por alguns professores do ICEA, mas é gerido pelo NTI de Ouro Preto. Além deste existe o sistema de reserva de laboratórios, sistema de abertura de chamados, e sistema para solicitação de acesso a rede acadêmica, estes geridos pelo NTI/ICEA.

8. Quais são as responsabilidades do NTI/ICEA?

R: Gerência e manutenção da infraestrutura de rede e afins, como manutenção de máquinas, equipamentos de multimídia, impressoras, entre outros.

9. Existe uma Política de Segurança em vigência?

R: Não.

10. Quais os maiores problemas enfrentados pelo NTI/ICEA?

R: Pontos de acesso para rede sem fio estudantil e administrativa são insuficientes para a demanda, causando alguns transtornos em horários de alta demanda.

Falta de equipamentos para manutenção ou peças para reposição. Má utilização por parte da comunidade acadêmica dos recursos tecnológicos. Vide casos de laboratórios onde cabos de rede são retirados e deixados fora de lugar, furte de mouses e adaptadores de energia, entre outros.

Problemas com equipamentos multimídia, especialmente *data shows* em salas de aula, onde especificamente os cabos de conexão constantemente são trocados ou reparados.

APÊNDICE B – Normas de Acesso aos Laboratórios de Computadores

MINISTERIO DA EDUCAÇAO
Universidade Federal de Ouro Preto – UFOP
Instituto de Ciências Exatas e Aplicadas
Núcleo de Tecnologia da Informação – NTI/ICEA

NORMAS PARA USO E ACESSO DOS LABORATÓRIOS DE INFORMÁTICA

1. DO REGULAMENTO E SUA APLICAÇÃO

Art. 1º - O presente documento possui Normas que regem e orientam usuários as condições corretas de utilização dos Laboratórios da Informação.

Art. 2º - Ficam sujeitos ao correto uso deste regulamento todos os usuários diretos e indiretos do Laboratório de Informática.

§ único - Ficam a cargo do Núcleo de Tecnologia da Informação (NTI/ICEA) do campus quaisquer casos não esclarecidos, bem como casos omissos que não estão presentes neste documento.

2. DA POLÍTICA DE ACESSO AOS RECURSOS TECNOLÓGICOS

Art. 3º - Os Laboratórios de Informática estão vinculados ao Núcleo de Tecnologia da Informação, na qual adequará sua utilização de maneira na qual estejam sempre disponíveis para alunos e professores.

Art. 4º - A gestão de uso dos laboratórios de informática é feita por meio do sistema de agendamento e de reservas, podendo ser acessado diretamente em http://200.239.152.5/reserva. Para efetivação do uso do laboratório, os mesmos deverão ser agendados exclusivamente por meio do sistema supracitado:

a) Somente Professores e Técnicos de Informática poderão fazer a reserva do laboratório de Ensino. Para acesso ao sistema os usuários em questão deverão entrar com o ***login*** e senha utilizados no **MINHA UFOP**.

b) Para os demais usuários **não** será permitido o acesso para agendamento do laboratório de ensino.

Art. 5º - Requisições para instalações de novos softwares devem ser encaminhados ao NTI/ICEA, na qual será feita a análise da solicitação pelos técnicos responsáveis e sua posterior efetivação caso se aplique.

Art. 6º - São considerados usuários dos laboratórios de informática destinados a ensino técnicos administrativos, professores e alunos do instituto;

Art. 7º- Todos os usuários sem exceção, para ter acesso os computadores deverão seguir as regras abaixo citadas:

I. Usuários no Windows e Linux: CPF **(somente números);**

II. Senha: **Para todos os usuários a senha temporária é composta pela data de nascimento (ddmmaaaa);**

III. A troca da senha deve ser feita no Windows:

a. Após logado, pressione Ctrl + Alt + Delete (Alterar senha).

Art. 8º- É de responsabilidade do servidor que solicitou a reserva do laboratório, a garantia da integridade dos recursos tecnológicos presentes durante o período reservado, mesmo este não estando presente.

Art. 9º- A identificação de qualquer defeito nos equipamentos durante uma aula deve ser comunicada pelo professor/coordenador do projeto ao responsável do laboratório por meio do http://200.239.152.5/sisnti/web/ .

Art 10º- Os equipamentos devem ser desligados pelos alunos, ao término do seu uso, seguindo o seguinte roteiro de procedimentos:

a) Fechar todos os programas;

b) Finalizar o sistema operacional;

3. DAS PROIBIÇÕES NAS INSTALAÇÕES

Art 11º- É proibido fumar e consumir alimentos nas instalações do laboratório.

Art. 12º- É expressamente proibido nos laboratórios de informática destinado a ensino, exceto com permissão do professor responsável:

1) Instalar e desinstalar ***softwares*** sem permissão do professor e/ou do técnico responsável pelo laboratório;
2) Instalar ***software*** não licenciado;
3) Violar lacres de segurança presentes nos computadores;
4) Abrir, desmontar, consertar e reconfigurar qualquer equipamento presente nos laboratórios;
5) Danificar qualquer equipamento presente no laboratório;
6) Utilizar equipamentos particulares, salvo dispositivo de armazenamento removível, como ***pendrives*** ou ***notebook*** pessoal;
7) Utilizar equipamento sem a autorização do NTI/ICEA;
8) Desenvolver e disseminar vírus nos computadores presentes nos laboratórios;
9) Utilizar jogos no ambiente laboratorial;
10) Acessar páginas com conteúdo pornográfico;
11) Utilizar os computadores para fins que não estejam de acordo com os objetivos das tarefas acadêmicas;
12) Desorganizar o ambiente laboratorial;
13) Retirar mouse, teclado, monitor e/ou qualquer outro equipamento de lugar;
14) Fazer transferências de arquivos extensos via internet (***Torrent, Streaming*** de vídeos e músicas, dentre outros de comum finalidade);

15) Desrespeitar, agredir e humilhar fisicamente ou verbalmente outras pessoas presentes no ambiente laboratorial;

16) Tornar público assuntos pessoais alheios, conteúdo de correspondências eletrônicas particulares sem a devida autorização;

17) Publicar ou enviar trabalhos, violando direitos autorais;

18) Utilizar aparelhos celulares, salvo com a autorização explicita do professor responsável;

19) Assumir identidade de outra pessoa, ainda que com seu consentimento, para ter acesso aos laboratórios ou aos Recursos neles instalados;

20) Permitir que alguém assuma sua identidade para acesso aos laboratórios ou aos Recursos neles instalados.

§ único - No caso do item 6, o professor responsável não se responsabilizará pelo suporte no caso de o aluno optar pela utilização do notebook pessoal.

4. DAS PENALIDADES

Art. 13º- O não cumprimento das regras estabelecidas neste regulamento implica, ao usuário infrator as seguintes sanções:

a) Suspensão temporária do direito a acesso aos recursos presentes nos laboratórios de informática;

b) Reposição do equipamento deteriorado;

c) Sanções disciplinares previstas no Regimento do ICEA;

Art, 14º- No caso de dúvida quanto a correta utilização deve-se consultar o professor responsável.

5. DAS BOAS PRÁTICAS DE UTILIZAÇÃO DOS LABORATÓRIOS

Art.15º- Algumas recomendações constituem as boas práticas de utilização dos Laboratórios de Informática:

a) Não tente resolver problemas por conta própria;
b) Utilize a rede com responsabilidade e **não** faça downloads de arquivos sem direitos autorais, dentre outros;
c) Sugestões ou críticas deverão ser encaminhados para:

suporteinformatica@decea.ufop.br

d) Após a utilização das máquinas no laboratório de ensino **salve seus arquivos**, pois os mesmos serão excluídos 24 horas após sua criação;
e) Ao término das atividades nos laboratórios os computadores deverão ser desligados pelos próprios usuários e conferidos posteriormente pelo professor-responsável;
f) Organização de cadeiras após o uso do laboratório;
g) Zelar pela boa utilização dos computadores, cadeiras, mesas e demais equipamentos dos laboratórios de ensino.

João Monlevade, 22 de setembro de 2016

Núcleo de Tecnologia da Informação

Instituto de Ciências Exatas e Aplicadas

APÊNDICE C – Política de Segurança da Informação Proposta para O ICEA

Universidade Federal de Ouro Preto – UFOP

Instituto de Ciências Exatas e Aplicadas – ICEA

Política de Segurança da informação– PSI

1. ESCOPO

A Política de Segurança da informação e Comunicação (POSIC) do Instituto de Ciências Exatas e Aplicadas (ICEA) tem como propósito orientar e estabelecer Normativas acerca da Instituição provendo o compromisso mediante a proteção das informações de sua propriedade e/ou de sua guarda.

Tendo como objetivo estabelecer diretrizes, Normas, procedimentos, e responsabilidades que se adequam ao correto manuseio, manipulação, tratamento, controle e proteção das informações geridas e pertinentes sejam elas tangíveis ou intangíveis.

Essa política deve ser aplicada a todos os servidores, discentes e prestadores de serviços que exerçam atividades no âmbito do ICEA.

2. CONCEITOS E DEFINIÇÕES

Para fins desta política, considera-se:

- **Acesso Lógico** – acesso a redes de computadores, sistemas e estações de trabalho por meio de autenticação;
- **Acesso Remoto** – ingresso, por meio de uma rede, aos dados de um computador que se encontra fisicamente distante da máquina do usuário;
- **Agente Responsável** – Servidor Público ocupante do cargo efetivo, direta ou indireta responsável por chefiar e gerenciar a Equipe de Tratamento e Manutenção das Redes de Computadores e Recursos Tecnológicos no âmbito do Instituto;
- **Ameaça** – conjunto de fatores internos ou externos que são potenciais causadores de incidentes não desejados, causando danos para sistemas presentes no Instituto;
- **Análise/Avaliação de Risco** – processo completo de análise e avaliação de riscos;
- **Ativo** – qualquer bem, considerado tangível ou intangível, que apresente valor para o Instituto;
- **Ativo de Informação** – meios de armazenamento, transmissão e processamento, sistemas de informação, bem como locais no qual esses meios estão dispostos e às pessoas que a eles possuem acesso;

- **Ativo sigiloso** - qualquer bem tangível ou intangível que possui conteúdo sigiloso que, acessados por pessoas não autorizadas, podem causar danos significativos para o Instituto;

- **Auditoria -** verificar e avaliar sistemas, recursos tecnológicos e procedimentos internos com o objetivo de reduzir fraudes, erros e práticas ineficientes ou ineficazes;

- **Autenticação** - diz respeito ao ato de confirmar que algo ou alguém de fato é autêntico, ou seja, garantia uma garantia de alegação de ou sobre um objetivo é verdadeira;

- **Autenticidade** - propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

- **Bloqueio de acesso** - processo cuja finalidade é suspender temporariamente ou de forma definitiva o acesso ao recurso tecnológico;

- **Classificação da informação** - atribuição, pela autoridade competente, de grau de sigilo da informação, documento, material, área ou instalação;

- **Confidencialidade** - propriedade na qual a informação não esteja disponível ou apresentada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada ao acesso;

- **Contingência** - descrevem medidas tomadas por uma empresa, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou em um estado minimamente aceitável, o mais rápido possível, evitando por consequência uma paralisação prolongada que possa gerar maiores à corporação;
- **Controle de acesso** - conjunto de procedimentos, recursos e meios a serem utilizados cuja finalidade é conceder ou bloquear determinado acesso. Inclui políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

- **Cópia de Segurança (Backup)** - cópia de dados em um meio separado do original, de forma a resguardar sua integridade de qualquer eventualidade. Essencial para dados importantes;

- **Correio eletrônico** - consisti no método que permite compor, enviar e receber mensagens a partir de sistemas eletrônicos de comunicação;

- **Credenciais ou contas de acesso** - permissões, concedidas por autoridade competente após o processo de credenciamento, ao qual habilitam determinada pessoa, sistema ou organização ao acesso. As credenciais podem ser apresentadas de forma física como crachás, cartão e selo ou lógica como identificação de usuário e senha;

- **CGSIC** - Comitê Gestor de Segurança da Informação e Comunicação da UFOP;
- **Dado** - sequência de símbolos quantificados ou quantificáveis;
- **Diretriz** - são instruções ou indicações para estabelecer um plano, uma ação ou um negócio;
- **Disponibilidade:** Propriedade da informação que permite que ela esteja acessível e utilizável sempre que requisitada sobre uma pessoa física ou determinado sistema, órgão ou entidade;
- **Download** - copiar arquivo de um servidor (site) para um computador pessoal ou compartilhado;
- **FTP (File Transfer Protocol):** é definido como um protocolo de internet para transferência de arquivos**;**
- **Hardware:** É a parte física do computador, conjunto de componentes eletrônicos, circuitos integrados e periféricos, impressoras, teclados, mouses e demais;
- **HTTP (Hyper Text Transfer Protocol):** Linguagem utilizada para a troca de informação entre servidores e clientes;
- **HTTPS (Hyper Text Transfer Protocol Secure):** Linguagem utilizada para a troca de informação entre servidores e clientes da rede, com recursos de criptografia, autenticação e integridade;
- **Incidente de Segurança:** É qualquer evento que vai contra as Normativas de segurança, seja tentativa ou ato consumado, está relacionado a sistemas de informação e equipamentos de rede;
- **Informação:** São dados processados ou não, que podem ser utilizados para a geração do conhecimento, contidos em diferentes meios;
- **Informação Crítica:** São informações de extrema importância para a sobrevivência da informação;
- **Informação Sigilosa**: São Informações restrita ao acesso público por razões da sua importância para a organização, são aquelas abrangidas pelas demais hipóteses legais de sigilo;
- **Integridade:** Propriedade da Informação que indica que ela não foi modificada, destruída ou modificada de maneira proposital ou não autorizada;
- **Internet:** Rede mundial de computadores;
- **Internet Protocol (Protocolo de Internet):** É o protocolo de comunicação utilizado por duas ou mais máquinas em rede para a troca de dados;
- **Intranet:** Rede de computadores privada que faz uso dos mesmos protocolos da internet. Rede interna de uma organização;
- **Login**: Processo de identificação e autenticação nos recursos de tecnologia. Pessoal e intransferível;
- **On-Line:** Em se tratando de internet é definido como o ato ou efeito de estar disponível para acesso imediato;

- **Perfil de Acesso**: Conjunto de atributos de um usuário, utilizados para seu credenciamento;
- **Política de Segurança da Informação**: Documento cujo objetivo é prover Normas, diretrizes e procedimentos para o correto uso e acesso dos recursos tecnológicos e de informação;
- **Protocolo**: Padrão que possibilita uma conexão, comunicação, transferência de dados entre dois sistemas computacionais;
- **Proxy**: Serviço intermediário entre as estações de trabalho de uma rede e a Internet. Permite acesso rápido, bloqueio de páginas;
- **Quebra de Segurança:** Ação ou omissão, seja de maneira proposital ou não, que compromete a segurança;
- **Recursos Computacionais:** Recursos que processam, armazenam e/ou transmitem, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;
- **Rede Corporativa**: Conjunto de todas as redes locais sob a organização;
- **Rede Pública**: Rede de acesso a todos;
- **Roteador**: Equipamento que permite a troca de informações pela rede;
- **Segurança da Informação**: Ação de garantir a confidencialidade, disponibilidade e integridade dos recursos tecnológicos e da informação;
- **Servidor de Rede:** Recurso de TI com a finalidade de disponibilizar ou gerenciar serviços ou sistemas informáticos;
- **Tratamento da Informação:** Processos para a recepção. produção, reprodução, utilização e descarte da informação;
- **Usuários:** Técnicos, professores e alunos que fazem acessos aos recursos tecnológicos;
- **VLAN (Virtual Local Area Network ou Virtual LAN) – (Rede Local Virtual):** Agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local;
- **VPN (Virtual Private Network) – (Rede Privada Virtual):** Rede de dados privada que faz uso das infraestruturas públicas de telecomunicações, preservando a privacidade, logo é a extensão de uma rede privada que engloba conexões com redes compartilhadas ou públicas.
- **Vulnerabilidades:** Fatores internos que podem resultar em risco a organização;
- **Wireless (rede sem fio)**: Rede que permite a conexão entre computadores e outros dispositivos por meio da transmissão e recepção de sinais de rádio.

3. FUNDAMENTAÇÃO LEGAL E NORMATIVA

1. NBR ISO/IEC 17799:2005 – Código de Práticas para a Gestão da Segurança da Informação**;**

2. NBR/ISO/IEC 27002/2005, que institui o código de melhores práticas para gestão de segurança da informação;

3. COBIT (Control Objectives for Information and Related Technology).

4. DIRETRIZES GERAIS

1. Garantir os quesitos os quesitos fundamentais da segurança que são definidos como confidencialidade, disponibilidade e integridade dos dados presentes no Instituto de Ciências Exatas e Aplicadas (ICEA);
2. Continuidade do Negócio;
3. Responsabilização do usuário pelos atos que comprometam a segurança da tecnologia e da informação;
4. É dever do ICEA prover para toda comunidade acadêmica o acesso aos recursos tecnológicos e fontes de informação, de maneira a prover um ambiente de produção e alcance dos objetivos propostos por seus usuários;
5. O ICEA, como usuário dos serviços providos pela (RPN) Rede Nacional de Pesquisa, é, assíduo às suas Normas e diretrizes;
6. Usuários internos e externos devem observar:
    1. Que o acesso os recursos tecnológicos estão sob as Normativas de acesso e devem ser rigorosamente cumpridas;
    2. Que os recursos disponibilizados pelo ICEA, tem o propósito único de apoiar as atividades desenvolvidas internamente;
    3. Que as Normas para o tratamento da informação gerada dentro do ambiente institucional está sob pena e cuidado exclusivo do ICEA;
7. Segurança Física: Controles que monitorem é certifiquem a segurança dos recursos físicos presentes no ambiente institucional e que garantam a segurança ao acesso aos recursos apenas por parte de pessoas previamente autorizadas, proibindo o acesso de visitantes aos recursos de equipamentos e mídias.
8. Uso de e-mail: O serviço de correio eletrônico disponibilizado pelo ICEA constitui recurso do Instituto disponibilizado na rede para aumentar a agilidade, segurança e economia da comunicação oficial e informal.
9. Acesso a Internet: Técnicos, docentes e discentes têm o direito de acesso à internet, com utilização exclusiva para fins diretos e complementares às atividades do setor, para o enriquecimento intelectual de seus usuários ou como ferramenta para busca por informações que venham contribuir para o desenvolvimento de seus trabalhos.
10. Equipamentos Privados- Particulares: Equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, devem ser usados de forma controlada e autorizada para armazenar ou processar informações relacionadas com as atividades, e só devem ser conectados às redes cabeadas da instituição mediante a um documento de solicitação de acesso junto ao NTI-ICEA, prescrito pelo professor. Salvo para situações de projeto de extensão, iniciação científica e afins.

11. O acesso aos recursos dos laboratórios de computadores destinados a ensino deverá ser realizado de acordo com a Norma de acesso aos laboratórios que compõem este documento;
12. É comprometimento de todos os usuários dos recursos tecnológicos e de informação o zelo e atendimento às Normas propostas;
13. É de responsabilidade do usuário conhecer a legislação e cumprir os requisitos legais, Normas e padrões locais vigentes.

5. COMPETÊNCIAS E RESPONSABILIDADES

É de responsabilidade de cada usuário, seja aluno, técnico administrativo, professores ou terceirizados, atentar-se à política, normativas, diretrizes e procedimentos estabelecidos pela Política de Segurança da Informação. É fundamental o compreendimento por parte de cada usuário sobre o papel da garantia da segurança durante o desenvolvimento de suas respectivas atividades.

Todas as atividades executadas no ambiente ICEA, deverá estar de acordo com os padrões estabelecidos pelas políticas e pelas normas impostas, uma que, o principal foco é a garantia da segurança acerca do presente instituto.

APÊNDICE D – Questionário para a Auditoria da Segurança Tecnológica do ICEA

Questionário para auditoria da segurança tecnológica do ICEA	
Equipamento:	Data da auditoria:
Qual o nível de proteção do equipamento em análise: Fraco ( ) Médio ( ) Forte ( ) Muito Forte ( )	
Qual tipo de proteção adotada no equipamento?	
Como é feito o acesso ao equipamento?	
Quem tem acesso ao equipamento?	
Quem deveria ter acesso ao equipamento?	
O equipamento é passivo de ser removido? Se sim, com qual facilidade?	
O equipamento é passivo de ser atacado?	
Existe algum aviso identificando quem pode ter acesso ao equipamento? Sim ( ) Não ( )	
Quais pontos de falhas podem ser observados no equipamento?	
O local onde o equipamento é bem protegido?	
Quais riscos o equipamento está exposto?	
Existe algum tipo de conscientização para o correto uso dos equipamentos? Se sim, cite-os.	
Existe documentação para acesso ao equipamento?	
De quem é a responsabilidade da segurança do equipamento?	
É possível monitorar o uso do equipamento (quem está usando, com que frequência, etc) ?	

No instituto existe um gerenciamento periódico dos principais riscos de tecnologia da informação e comunicação que afetam os objetivos do negócio?
Sugestões de melhoria:

ANEXO A – Email Encaminhado ao NTI/ICEA

Politica de Segurança da Informação Entrada x

Fernanda Rocha <fernandalfrocha@gmail.com> 24/06/2016

para atendimento, suporteinforma.

Prezados(as) senhores(as), boa tarde!

Meu nome é Fernanda Lara Ferreira Rocha, sou aluna da Universidade Federal de Ouro Preto, curso de Sistemas de Informação, campus João Monlevade.

Em virtude do grande volume de informações e de novas tecnologias, emerge a preocupação com a segurança de tais elementos. Essas questões são de extrema importância para qualquer tipo de organização. Pensando nisso, optei pela realização do meu TCC voltado para a segurança das tecnologias implantadas no ICEA e pela segurança das informações do instituto. O tema proposto é o "Estudo de metodologias para a avaliação e a auditoria da segurança de informação e das tecnologias no ICEA", e tem como orientador o Prof. Fernando Bernardes de Oliveira (em cópia).

O trabalho tem como objetivo avaliar como questões de segurança da informação do instituto, observando questões sobre infraestrutura, os processos e demais itens relacionados. A partir dessa avaliação, propor uma política de segurança da informação para o instituto, documentando diretrizes e regras.

Para isso, peço, por gentileza, a colaboração do NTI, considerando que o departamento de informática do ICEA (em cópia) é vinculado ao departamento de Ouro Preto. É necessário identificar se existe alguma política de segurança de informação elaborada pelo NTI que esteja vigente, e se esse documento pode ser disponibilizado para estudo.

Além disso, é necessário identificar quais são os domínios e as responsabilidades do departamento de informática do ICEA, quais tarefas desenvolvidas por eles e as que estão atribuídas ao NTI/Ouro Preto.

Agradeço desde já a atenção acerca deste assunto, e toda ajuda será muito apreciada.

Estou à disposição para quaisquer esclarecimentos.

Atenciosamente,

Pedro Henrique <diretor@nti.ufop.br> 05/07/2016

para mim, Fábio

Prezada Fernanda,

Boa noite. Desculpe a demora em responder, mas vamos lá.

O departamento de informática do ICEA não é vinculado ao NTI e responde diretamente à diretoria do instituto, assim como os núcleos de informática de outras unidades.

Ainda não temos uma política de segurança da informação, apesar de ser obrigatória. A cerca de um mês, foi instituído o Comitê Gestor de Segurança da Informação e Comunicação (CGSIC), de caráter CONSULTIVO e PROPOSITIVO, cujo uma das atribuições é a criação da Política de Segurança da Informação e Comunicação (POSIC) da UFOP. Eu faço parte do comitê e, ele ainda não foi reunido pois depende da indicação de alguns membros ainda pelo Comitê Gestor de TI, instituído na mesma data.

Em anexo, envio-lhe a minuta da portaria de criação do comitê.

Com relação às atribuições, isso não está documentado. Mas se você quiser me ligar, posso lhe repassar os serviços pelos quais o NTI e o Suporte de Informática do DECEA são responsáveis. Meu telefone é (31) 3559-1415. Se você não conseguir falar comigo, você pode também conversar com o Abelard (Gerente da Infraestrutura Computacional) no mesmo ramal.

Att,
--