UNIVERSIDADE DO SUL DE SANTA CATARINA

RAFAEL ALVES DE SOUZA

SEGURANÇA DA INFORMAÇÃO NO SERVIÇO PÚBLICO: A REALIDADE DA SEGURANÇA DA INFORMAÇÃO NO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO

Palhoça

2017

RAFAEL ALVES DE SOUZA

SEGURANÇA DA INFORMAÇÃO NO SERVIÇO PÚBLICO: A REALIDADE DA SEGURANÇA DA INFORMAÇÃO NO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação,** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Prof. MSc. Horácio Dutra Mello

Palhoça

2017

RAFAEL ALVES DE SOUZA

SEGURANÇA DA INFORMAÇÃO NO SERVIÇO PÚBLICO: A REALIDADE DA SEGURANÇA DA INFORMAÇÃO NO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Palhoça, _____ de _____ de _____.

Prof. e orientador Horácio Dutra Mello, MSc

Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço a Universidade do Sul de Santa Catarina pelo desafio proposto para a elaboração deste Estudo de Caso.

Agradeço ao Professor MSc. Horácio Dutra Mello, por sua paciência e compreensão da importância acadêmica e profissional deste trabalho.

Agradeço o apoio dos tutores que sempre estiveram disponíveis *on-line* mesmo não solicitando suas ajudas com regularidade.

Agradeço à minha família por ser o maior e mais belo patrimônio existente.

RESUMO

Este trabalho surgiu como uma proposta a ser aplicada no Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro. Os conceitos iniciais que motivaram o seu desenvolvimento ocorreram após serem observadas divergências entre as Coordenações de Tecnologia da Informação e Comunicação dos campi com a Diretoria de Gestão de Tecnologia da Informação e Comunicação na Reitoria, nas questões relacionadas à Segurança da Informação.

Após a apresentação dos principais conceitos, é realizada uma pesquisa com as CSTIC dos campi e com a DGTIC de modo a compreender as relações entre as entidades e suas abordagens para a Segurança da Informação.

Com os resultados obtidos, é possível observar divergências na implementação de diretrizes e uma ausência de política de Segurança da Informação na Instituição. Essas principais diferenças foram observadas em questões como a falta de treinamento para a equipe de TI, distanciamento e ausência de reuniões para discussão de ações e estratégias institucionais, etc.

Apesar dos conhecimentos sobre a Segurança da Informação não serem plenos, é possível observar que as entidades estão trabalhando com qualidade.

É proposto a reunião com todas as equipes de TI para a discussão de apresentação de propostas para a definição de um plano de diretrizes que deverá se tornar a política de Segurança da Informação institucional.

Palavras-chave: Segurança da Informação. Política. Sistema de Informação. Serviço Público.

LISTA DE ILUSTRAÇÕES

Quadro 1 – Quadro de Instrumento de coleta de dados 13
Gráfico 1 – Atividades de um sistema de informações 17
Figura 1 – Componentes da abordagem sociotécnica de sistemas de informação 18
Figura 2 – Representação de uma rede com *firewall* 30
Figura 3 – Dimensões da Segurança da Informação. 33
Figura 4 – Estrutura hierárquica do IFRJ. 39
Figura 5 – Nova estrutura organizacional do Campus Rio de Janeiro. 41

LISTA DE TABELAS

Tabela 1 – Questionário aplicado às CSTIC. 45
Tabela 2 – Questionário aplicado à DGTIC. 49
Tabela 3 – Resultados coletados das CSTIC. 54
Tabela 4 – Resultados coletados da DGTIC. 58

SUMÁRIO

1 INTRODUÇÃO 10

2 TEMA 11

3 OBJETIVOS 12

3.1 OBJETIVO GERAL 12

3.2 OBJETIVOS ESPECÍFICOS 12

4 PROCEDIMENTOS METODOLÓGICOS 13

4.1 CAMPO DE ESTUDO 13

4.2 INSTRUMENTO PARA COLETA DE DADOS 13

5 FUNDAMENTAÇÃO TEÓRICA 14

5.1 INTRODUÇÃO 14

5.2 DADO, INFORMAÇÃO E CONHECIMENTO 14

5.2.1 Contextos no uso da informação 14

5.2.2 Características da informação de qualidade 15

5.3 SISTEMA DE INFORMAÇÃO 16

5.3.1 Conceitos de sistema 16

5.3.2 Características de um sistema de informação 16

5.3.3 Abordagem sociotécnica 18

5.4 SEGURANÇA DA INFORMAÇÃO 19

5.4.1 Conceitos de segurança da informação 19

5.4.2 A importância da segurança da informação nas organizações 20

5.4.3 Características da segurança da informação 20

5.4.4 Vulnerabilidades e ameaças 21

5.4.5 Ataques à segurança da informação 22

5.4.5.1 Etapas dos ataques 22

5.4.5.2 Modelos de ataques 23

5.4.5.3 Tipos de ataques 23

5.4.6 Criptografia 26

5.4.6.1 Conceitos de criptografia 26

5.4.6.2 Tipos de criptografia 26

5.4.6.2.1 Criptografia de chave simétrica e de chaves assimétricas 26

5.4.6.2.2 Função Hash 28

5.4.6.2.3 Assinatura digital 28

5.4.6.2.4 Certificação digital *28*
5.5 DISPOSITIVOS DE SEGURANÇA 29
5.5.1 *Firewall* **29**
5.5.2 Serviços de *proxy* **30**
5.5.3 Network Address Translation **31**
5.5.4 Intrusion Detection System **31**
5.6 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO 31
5.6.1 Conceitos básicos **31**
5.6.2 Objetivos da política de segurança da informação **32**
5.6.3 Arquitetura da política de segurança da informação **32**
6 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA **35**
6.1 O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO 35
6.1.2 Histórico, visão e missão **35**
6.1.3 Estrutura organizacional **37**
6.1.3.1 Estrutura administrativa da Reitoria 37
6.1.3.2 Estrutura administrativa dos campi 40
6.1.4 Competência da Direção de Gestão de Tecnologia da Informação e Comunicação **41**
6.1.5 Competência das Coordenações de Suporte de Tecnologia da Informação e Comunicação **42**
6.2 APLICAÇÃO DE QUESTIONÁRIO E ANÁLISE DOS DADOS OBTIDOS 44
6.2.1 Definição do questionário **44**
6.2.2 Aplicação do questionário **44**
6.2.3 Resultados do questionário aplicado aos Campi **54**
6.2.4 Resultados do questionário aplicado à DGTIC **58**
6.2.5 Análise dos resultados dos Campi **63**
6.2.6 Análise dos resultados da DGTIC **68**
7 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA **70**
7.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA 70
7.2 RESULTADOS ESPERADOS 71
7.3 VIABILIDADE DA PROPOSTA 71
8 CONSIDERAÇÕES FINAIS **72**

1 INTRODUÇÃO

A Segurança da Informação tem sido alvo de diversos estudos em áreas acadêmicas e organizacionais por se tratar de um tema crescente em sua importância.

Com a globalização e consequente aumento no fluxo de informações, tornou-se fundamental que houvesse algum tipo de controle dos dados, uma vez que muitas decisões importantes puderam ser tomadas com base nos conteúdos disponíveis. É importante destacar que paralelamente a isso, as informações tornaram-se o ativo das organizações e um bem precioso a preservar. Desse modo, existe uma preocupação com a segurança dessas informações pois ameaças externas ocorrem com frequência e a perda desse bem pode comprometer a organização e prejudicar o seu posicionamento no mercado.

Nesse Estudo de Caso, buscou-se compreender a Segurança da Informação pela visão das Coordenações de Suporte de Tecnologia da Informação e Comunicação (CSTIC) e Diretoria de Gestão de Tecnologia da Informação e Comunicação (DGTIC) do Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro. Foram analisadas as relações existentes entre as duas entidades quanto os aspectos da Segurança da Informação e também o entendimento individual do assunto.

O trabalho que segue é um importante elemento a ser avaliado na Instituição para a definição de uma sólida política de Segurança da Informação e um norteador para a discussão de melhores práticas e futuros estudos que beneficiem a qualidade e excelência profissional institucional.

2 TEMA

A Segurança da Informação tem sido objeto de diversos estudos devido a sua importância nos meios na qual se aplica. Com uma economia global em constantes transformações e novas informações sendo criadas, transformadas e trocadas entre pessoas e organizações, torna-se fundamental obter o controle desse conteúdo de modo a preservar características da Segurança da Informação segundo Landwehr, Bishop, Russell e Gangemi (2001, 2003, 1991 apud LENTO, 2011, p. 23) de confidencialidade, integridade e disponibilidade.

No contexto apresentado, este trabalho acadêmico terá como tema central a realidade da Segurança da Informação no Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro (IFRJ). Sendo assim, o presente trabalho pretende responder algumas perguntas, tais como: “De que forma as coordenações de tecnologia da informação dos campi do IFRJ lidam com os aspectos de Segurança da Informação? ”; “Como se dá a relação da Diretoria de Gestão de Tecnologia da Informação e Comunicação do IFRJ (DGTIC) com as outras coordenações de tecnologia da informação dos campi a ela subordinados no que diz respeito aos aspectos da Segurança da Informação? ”.

Estas e outras questões serviram de base para a elaboração deste trabalho, uma vez que foi possível observar a falta de padronização em algumas questões relacionadas ao armazenamento, recuperação e apresentação de informações possivelmente sigilosas. Esse fato pôde ser observado nas coordenações de tecnologia da informação e em diferentes ocasiões pela DGTIC.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Explorar o modo como a Segurança da Informação é tratada nas coordenações de tecnologia da informação do Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro e identificar possíveis vulnerabilidades no acesso, armazenamento e apresentação das informações, servindo também como proposta para adoção de políticas sólidas e unificadas de Segurança da Informação a nível institucional.

3.2 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho acadêmico são os seguintes:

- Verificar como as coordenações de tecnologia da informação e comunicação dos campi do IFRJ criam, acessam e armazenam as informações potencialmente sigilosas;
- Verificar o modo como as coordenações de tecnologia da informação e comunicação e diretoria de gestão de tecnologia da informação lidam com questões inerentes à segurança da informação;
- Analisar o modo como as informações potencialmente sigilosas são tratadas por cada campus;
- Analisar a relação de comunicação dos aspectos de Segurança da Informação da Diretoria de Gestão de Tecnologia da Informação e Comunicação do IFRJ com as coordenações de TI dos outros campi a ela subordinados;
- Propor mudanças nas políticas de Segurança da Informação da Instituição que se apresentarem incompatíveis com os requisitos mínimos de segurança.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

Neste trabalho acadêmico, será realizado uma pesquisa na forma de Estudo de Caso do tipo exploratória, uma vez que se pretende obter maior familiaridade com as questões que envolvem a Segurança da Informação entre a Diretoria de Gestão de Tecnologia da Informação e Comunicação e suas coordenações de tecnologia da informação nos campi a ela subordinados. Além disso, será utilizado uma abordagem quantitativa para análise dos dados, pois com base em comparações serão propostas possíveis soluções nas políticas adotadas pela Instituição.

4.2 INSTRUMENTO PARA COLETA DE DADOS

O instrumento para a coleta dos dados deste Estudo de Caso se dará através de entrevista fechada na forma de questionário com questões fechadas e de múltipla escolha. A coleta dos dados ocorrerá por meio digital com uso de ferramentas integradas ao sistema de comunicação da Instituição.

O instrumento para coleta de dados adotado neste trabalho é descrito no quadro a seguir:

Quadro 1 – Quadro de Instrumento de coleta de dados

Instrumento de coleta de dados	Universo pesquisado	Finalidade do Instrumento
Entrevista fechada (questionário *online*)	O universo a ser pesquisado compreenderá todos os coordenadores de tecnologia da informação dos campi ou os seus representantes e a direção de gestão tecnologia da informação do Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro. Ao todo, espera-se pesquisar treze campi.	A finalidade da entrevista fechada em forma de questionário é para a obtenção dos dados necessários à elaboração deste estudo com o apoio de bibliografia especializada no tema da segurança da informação.

Fonte: Cavalcanti e Moreira (2008).

5 FUNDAMENTAÇÃO TEÓRICA

5.1 INTRODUÇÃO

Antes de iniciarmos o Estudo de Caso, convém entendermos a importância da Segurança da Informação e os aspectos que a caracterizam. Serão, portanto, definidos os conceitos fundamentais da informação de modo que a compreensão deste trabalho se dê com maior clareza.

Convém ainda destacar que os fundamentos teóricos que guiarão este trabalho não objetivam um grande aprofundamento no assunto, mas permitir que sirvam de referência aos assuntos abordados no decorrer do estudo.

5.2 DADO, INFORMAÇÃO E CONHECIMENTO

De acordo com Mulbert e Ayres (2010), o dado pode ser apresentado em diversas formas como números, palavras, imagens ou mesmo sons. Porém, o dado individualmente não nos conduz a uma compreensão sobre um fato ou situação. Sendo assim, o dado é apenas uma representação de um elemento em seu estado bruto.

A informação corresponde aos dados já coletados, organizados e ordenados, os quais são atribuídos contextos e significado. Sendo assim, a informação é o resultado trabalhado dos dados brutos.

O conhecimento está relacionado ao tratamento da informação de modo que podemos obter conclusões baseado no contexto, síntese e experiências.

5.2.1 Contextos no uso da informação

A informação é um bem muito valioso para as organizações pois permite extrair dela conhecimentos para a tomada de decisões. Se uma organização dispõe de grande volume de dados e não atua diretamente neles para obter informações relevantes, está desperdiçando a oportunidade de analisar os dados e conseguir, a partir disso, melhorar sua atuação interna e externa.

De acordo com Mulbert e Ayres (2010), as informações têm como propósito habilitar a organização a alcançar os seus objetivos. Para isso, a informação pode estar situada em alguns contextos de modo a proporcionar ganhos às organizações como:

- A informação como apoio à decisão permite que as decisões possam ser tomadas com maior segurança;

- A informação como apoio à produção permite que novas tecnologias possam ser desenvolvidas, agregando valores aos produtos e serviços oferecidos aos clientes;

- A informação como fator de sinergia permite que os departamentos da organização troquem informações de qualidade e interajam adequadamente, garantindo produtos e serviços de qualidade;

- A informação como fator determinante de comportamento irá gerar entre os indivíduos tanto internos quanto externos comportamentos diversos, sejam positivos ou negativos, mas permitirão que fluam em todos os elementos que se relacionam com a organização.

5.2.2 Características da informação de qualidade

Tendo em vista que a informação pode se dar de diversas formas e em diferentes contextos, é fundamental que ela possua qualidade. Essa característica definirá sua relevância na aplicação, portanto, algumas características relacionadas a qualidade da informação são destacadas por Mulbert e Ayres (2010), tais como:

- A informação deve ser precisa para que não haja erros;

- A informação deve ser completa de modo que inclua todos os detalhes importantes;

- Para que a informação possa ser viável, é importante que seja econômica, mas com a qualidade necessária;

- A informação deve ser flexível de modo a ser utilizada em diferentes contextos;

- A informação deve ser confiável. Isso significa que depende de dados exatos e de uma fonte segura;

- A informação precisa ser relevante para que possa ser utilizada em decisões;

- A simplicidade de uma informação torna seu entendimento mais fácil e oportuno;

- A informação deve ser pontual para que seja obtida quando necessário e sem esforço;

- A informação também deve ser verificável, de modo a ser conferida sempre que necessário, assegurando que está correta.

5.3 SISTEMA DE INFORMAÇÃO

5.3.1 Conceitos de sistema

Os conceitos de sistema são muito abrangentes e têm aplicações a diversas situações do mundo real. Podemos aplicar os mesmos conceitos a sistemas matemáticos, políticos, sociais, etc.

De acordo com Bio (1985 apud MULBERT e AYRES, 2010, p. 19), “sistema é um conjunto de elementos interdependentes, ou um todo organizado, ou partes que interagem formando um todo unitário e complexo”.

Um sistema também possui um objetivo a ser atingido pois cada elemento que se relaciona com o outro objetiva algo. Como exemplos, podemos observar que o sistema digestivo humano, através dos órgãos, desempenha cada um seu papel e todos objetivam o processamento do alimento. Já um sistema computacional, por meio dos diversos elementos que interagem com os dados, é capaz de armazenar, recuperar, calcular e exibir resultados desejados através do processamento eletrônico.

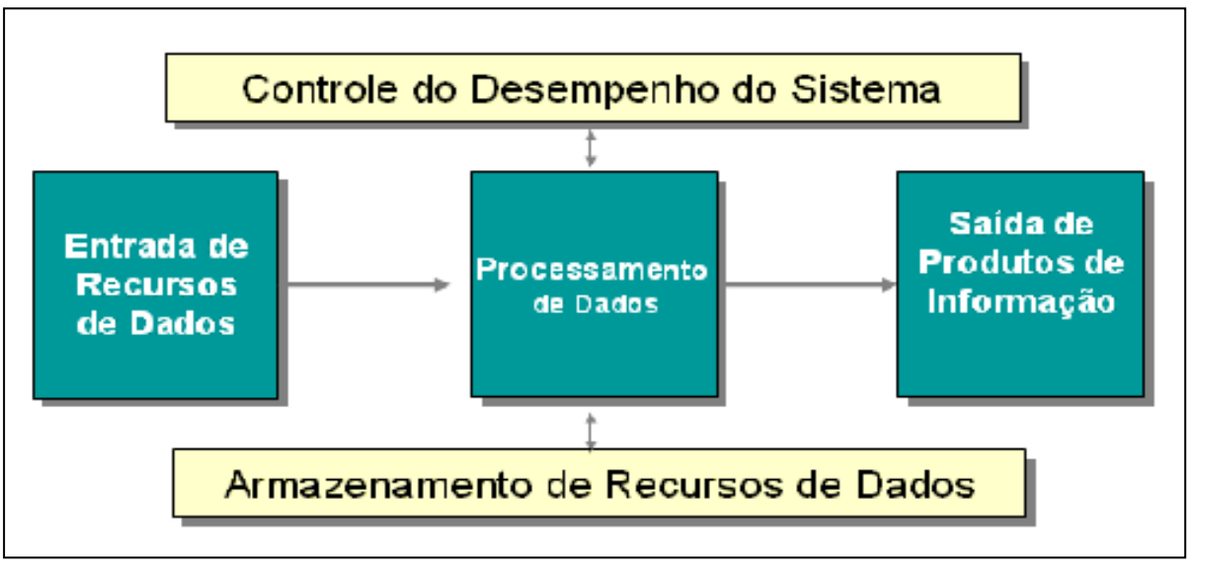
5.3.2 Características de um sistema de informação

Seguindo o mesmo raciocínio para a definição de sistema, um sistema de informação segundo Laudon e Laudon (1999 apud MULBERT e AYRES, 2010, p. 23) é definido como:

> Sistema de informação é um conjunto de componentes inter-relacionados, desenvolvidos para coletar, processar, armazenar e distribuir informação para facilitar a coordenação, o controle, a análise, a visualização e o processo decisório.

Sendo assim, todo sistema de informação basicamente é composto por elementos de entrada, processamento, saída, armazenamento e controle. O gráfico abaixo resume as atividades de um sistema de informação:

Gráfico 1 – Atividades de um sistema de informações



Fonte: Elaboração do autor (2017).

Com base no gráfico acima, podemos definir cada atividade da seguinte forma:

- **Entrada de recursos de dados** – Todos os dados primários devem ser capturados e preparados para posterior processamento. O tipo de entrada de dados é determinado pela saída desejada do sistema;

- **Processamento de dados** – Os dados são submetidos ao processamento como cálculos, análises, classificação, etc. Nessa etapa os dados são manipulados e convertidos para o destino desejado. O produto dessa etapa deve ser adequado aos usuários finais desse sistema;
- **Saída de produtos de informação** – Nesta etapa obtemos a disponibilidade da informação aos usuários finais;

- **Controle do desempenho do sistema** – A importância desta etapa é o monitoramento e avaliação sobre o desempenho do sistema, de modo que os

resultados esperados estejam de acordo com o desejado. Caso o resultado não atenda aos requisitos desejados, deve-se corrigir os problemas para que o sistema cumpra seu papel adequadamente;

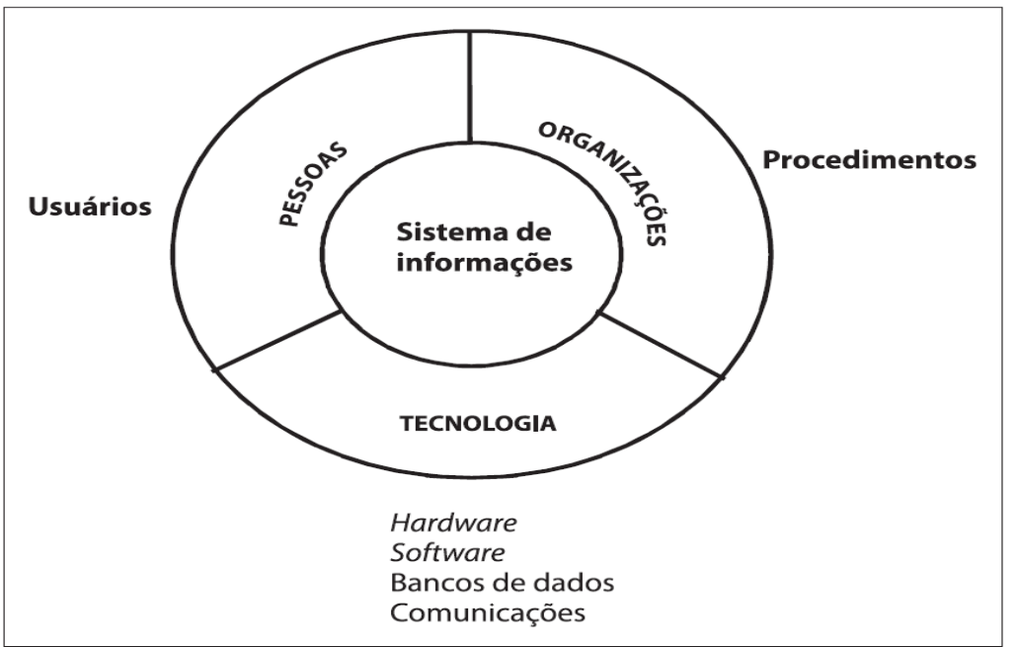
- **Armazenamento de recursos de dados** – Tem como objetivo a retenção da informação de forma organizada para posterior utilização quando necessária.

5.3.3 Abordagem sociotécnica

Conforme descrito por Kinjo (2014), após a Segunda Guerra Mundial, as organizações sob influência das novas mudanças políticas, econômicas e sociais, passaram a aperfeiçoar seus sistemas técnicos e operacionais e permitiram que os trabalhadores tivessem uma participação democrática dentro das organizações. Foi a partir disso que o conceito de abordagem sociotécnica surgiu. Com isso, as organizações deixaram de ser vistas como um sistema fechado e isolado e passaram a ter maior importância no meio social, político e econômico em que estava inserida, sendo compreendidas como um sistema aberto e influenciada tanto interna quanto externamente.

Sob a visão sociotécnica, um sistema de informações pode ser visto como um produto de três componentes segundo Laudon e Laudon (2001 apud MULBERT e AYRES, 2010, p. 26):

Figura 1- Componentes da abordagem sociotécnica de sistemas de informação



Fonte: Laudon e Laudon (2001 apud MULBERT e AYRES, 2010, p. 26).

Com base na figura acima, podemos descrever os elementos componentes da abordagem sociotécnica da seguinte forma:

- **Pessoas** – Os sistemas de informação devem ser adequados aos usuários que irão utilizar o sistema. São eles os responsáveis pelas entradas, utilização das saídas, enfim, fazem com que todo o sistema seja produtivo. Assim, o ambiente de trabalho das pessoas deve ser propício a um maior ganho de produtividade;

- **Organizações** – Diversos processos estão relacionados nas organizações, sejam operacionais ou administrativos. Esses processos devem estar inseridos em um sistema de informações para que os procedimentos possam ser melhor compreendidos e organizados adequadamente. A maneira como uma organização trata seus processos e procedimentos afeta diretamente seu funcionamento no meio que está inserida;

- **Tecnologia** – Através dos recursos tecnológicos as organizações podem implementar seus sistemas de informação. Ela deve servir de suporte aos processos e tomadas de decisões para seus usuários. É através da tecnologia que a comunicação pode ser melhor difundida e utilizada para suportar a produtividade crescente nas organizações.

5.4 SEGURANÇA DA INFORMAÇÃO

5.4.1 Conceitos de segurança da informação

A segurança da informação vem ganhando a cada dia mais importância e preocupação para as organizações. Uma vez que os fluxos de informações não estão limitados ao ambiente organizacional apenas, é fundamental que sejam aplicadas técnicas e procedimentos que visem a garantia de informações confidenciais e manipulação adequada destas. Sob esta perspectiva, ABNT NBR ISO/IEC 27002 (2013 apud COELHO 2011) diz:

> Segurança da Informação compreende a proteção das informações, sistemas, recursos e demais ativos contra desastres, erros (intencionais ou não) e manipulação não autorizada, objetivando a redução da probabilidade e do impacto de incidentes de segurança.

A segurança da informação também é responsável, de acordo com Coelho (2011), em proteger a informação dos variados tipos de ameaças que podem comprometer a organização. É sua responsabilidade garantir a continuidade do negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócios.

Segundo a autora, a segurança da informação é obtida como um resultado da implementação de políticas, processos, procedimentos, controles, funções de hardware e software nas organizações.

5.4.2 A importância da segurança da informação nas organizações

A informação é um patrimônio de grande valor às organizações atuais e ela deve ser protegida para que possa agregar valor ao negócio e ajudar na toma de decisão.

De acordo com Moreira (2013), diferentemente do passado onde os documentos e arquivos das organizações eram mantidos fisicamente em armários e depósitos específicos, hoje na sociedade da informação e graças ao desenvolvimento tecnológico, os dados são armazenados eletronicamente. Mesmo utilizando este novo formato de armazenamento ainda há preocupação com esses dados pois estão sujeitos a diversas ameaças que podem comprometer a organização.

Devido ao grande número de ameaças na Internet, as organizações precisam estar atentas para estes riscos e buscar oferecer os seus produtos e serviços com qualidade mantendo a preocupação com as necessidades de segurança para não sofrer no futuro com a perda do negócio.

5.4.3 Características da segurança da informação

Quando nos referimos às características e propriedades da segurança da informação, alguns autores como Landwehr, Bishop, Russell e Gangemi (2001, 2003, 1991 apud LENTO, 2011, p. 23); Coelho (2011, p. 6-7) e Amatte e Peixinho (2013, p. 2), descrevem adequadamente estas características conforme abaixo:

- **Confidencialidade** – Garante que somente as pessoas autorizadas podem ter acesso a informação. Sistemas seguros devem buscar manter o sigilo das informações dos que não têm os direitos para tal;

- **Integridade** – Manter a integridade da informação significa preservar seu conteúdo armazenado de pessoas não autorizadas de modo que não seja corrompida de forma acidental ou intencional;

- **Disponibilidade** – Garante que as pessoas e processos que possuam autorização tenham acesso a informação sempre que precisarem;

- **Autenticidade** – Preocupa-se em garantir que a origem e o destino da informação são quem deveriam ser, ou seja, devem ser devidamente identificados;

- **Não repúdio** – Compreende serviços que previnem que origem e destino neguem a transmissão da informação;

- **Conformidade** – A informação e seus recursos devem estar em conformidade com a legislação vigente, regras contratuais e corporativas e demais regulamentos impostos;

- **Controle de acesso** – Limita e controla os acessos físicos e lógicos aos sistemas por meio de identificação, autenticação e autorização, buscando proteger os recursos de acessos não autorizados;

- **Auditabilidade** – As ações que utilizam a informação devem ser capazes de serem rastreadas e analisadas.

5.4.4 Vulnerabilidades e ameaças

Todo sistema de informação está sujeito a variados tipos de violações entre os quais podemos citar, segundo Lento (2011):

- **Físicas** – Quando há acesso indevido a compartimentos protegidos;

- **Naturais** – Provocados por desastres naturais;

- **Equipamentos e softwares** – Falhas em equipamentos podem comprometer a segurança assim como erros no desenvolvimento de softwares podem

permitir que intrusos tenham acessos indevidos e possam roubar informações e/ou modificá-las;

- **Emanação** – Equipamentos diversos e também os que são mal projetados podem prejudicar as comunicações devido a possíveis radiações eletromagnéticas ou mesmo interceptações nas comunicações;

- **Comunicação** – Todo sistema que está conectado em uma rede está vulnerável a invasão e interceptação de dados;

- **Humana** – Usuários que acessam sistemas estão sujeitos a cometerem erros prejudicando todo o sistema ou parte dele.

A ameaça corresponde a qualquer potencialidade que venha a violar a segurança da informação. Não há ameaça sem que exista uma vulnerabilidade e uma vez detectada uma vulnerabilidade a ameaça pode se transformar em um ataque, causando perdas ao negócio e aos sistemas de informação das organizações.

5.4.5 Ataques à segurança da informação

O ataque a um sistema de informação corresponde a efetivação da ameaça sobre este sistema. Este ataque pode comprometer todo um sistema causando prejuízos ao negócio de diversas maneiras.

Os ataques podem ocorrer através de escutas e monitoramento de transmissões de dados com o objetivo de coletar informações relevantes. Eles também podem ocorrer com alteração dos dados, negação de serviço e até mesmo com a criação de objetos falsificados conforme descrito por Coelho (2011, p. 4-5).

As organizações devem estar atuantes não apenas nas possíveis ameaças pelas quais os seus sistemas estão vulneráveis mas devem possuir capacidade para se recuperar de um ataque e saber defender seus ativos e informações.

5.4.5.1 Etapas dos ataques

Melo (2006 apud LENTO, 2011, p. 32-33) diz que um ataque é composto em três etapas como *footprint*, *fingerprint* e enumeração:

- A etapa de *footprint* é caracterizada pela organização das ideias de modo a se obter um perfil completo do alvo a ser atacado;

- A etapa de *fingerprint* objetiva identificar o sistema operacional utilizado pela vítima;

- A etapa de enumeração consiste na coleta de informação do alvo e identificação de vulnerabilidades da vítima.

5.4.5.2 Modelos de ataques

Além das etapas de ataques, há quatro possíveis modelos de ataques à segurança da informação:

> "**Interrupção**: quando um ativo é destruído ou torna-se indisponível (ou inutilizável), caracterizando um ataque contra a disponibilidade;
>
> **Interceptação**: quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), caracterizando um ataque contra a confidencialidade;
>
> **Modificação**: quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador) e ainda alterado, caracterizando um ataque contra a integridade.
> **Fabricação**: quando uma parte não autorizada (pessoa, programa ou computador) insere objetos falsificados em um ativo, caracterizando um ataque contra a autenticidade" (COELHO, 2011, p. 3-4).

5.4.5.3 Tipos de ataques

Muitos são os tipos de ataques realizados a computadores e sistemas nas organizações. Convém destacar que existem medidas para prevenir ou mesmo solucionar essas ameaças de prejudicarem o negócio.

Com base no Comitê Gestor da Internet no Brasil (2012), podemos citar 9 tipos de ameaças comuns relacionadas à segurança da informação que serão detalhadas a seguir:

- ***Phishing*** – Método que busca obter dados financeiros da vítima por meio de mensagens eletrônicas solicitando confirmação de dados, acesso a links para regularizar pendências, induzindo o alvo a fornecer dados pessoais e financeiros e algumas vezes sendo direcionados a páginas *Web* falsas contendo programas maliciosos.

Alguns exemplos de situações envolvendo *phishing* podem ser: páginas *Web* falsas de *e-commerce*, redes sociais ou de banco; mensagens que contenham *links* para códigos maliciosos disfarçados de algo relevante; solicitação de recadastramento para a coleta de dados da vítima, etc.;

- ***E-mail spoofing*** – Método que consiste em alterar propriedades do cabeçalho de um *e-mail* com o objetivo de parecer ter sido enviado de uma fonte confiável.
  Alguns exemplos deste ataque são mensagens de alguém supostamente conhecido solicitando o acesso a um *link* determinado; de banco, solicitando o fornecimento dos dados bancários para confirmação de algo; o serviço de *e-mail* utilizado, ameaçando a confirmação de dados para não perder a conta utilizada;

- ***Sniffing*** – É uma técnica que utiliza *softwares* para inspecionar o tráfego em uma rede. Neste caso, convém destacar que as ferramentas que se utilizam desta técnica podem ser utilizadas tanto por administradores de redes, com o objetivo de analisar a performance do tráfego quanto por pessoas mal-intencionadas, para captura de informações como senhas e outras informações potencialmente sigilosas e relevantes;

- ***Brute force*** – O ataque de força bruta consiste em buscar adivinhar por tentativa e erro os dados de acesso a um sistema para se aproveitar do acesso conquistado. Qualquer computador e sistema que possui conectividade em rede está sujeito a ataques de *brute force*.
  Recomenda-se que todo sistema que possua credenciais de acesso tenha uma senha complexa o suficiente para evitar possíveis descobertas. Senhas com letras, números e caracteres especiais são desejadas para a segurança;

- ***Distributed Denial of Service (DDoS)*** – O ataque de negação de serviço distribuído consiste em utilizar diversos computadores para acessar um determinado servidor e fazer que este seja sobrecarregado de solicitações, ficando, portanto, indisponível aos outros que precisarem dos serviços. Normalmente não se pratica tal ataque com o objetivo de coletar informações confidenciais e sim a indisponibilidade do serviço apenas;

- **Vírus** – Em computação, um vírus representa um software que possui código malicioso que é capaz de se multiplicar e fazer parte de outros programas e arquivos.
  Para que o vírus seja ativado e realize as funções que foi projetado ele precisará ser acionado. Este acionamento pode ocorrer em data específica ou após ações da vítima.
  Os vírus podem ser encontrados em *e-mails*, em linguagens *script* e macro, em telefone celular, *flash drives*, *CDs* e em diversas outras mídias;

- ***Worm*** – Os *worms* diferentemente dos vírus têm a capacidade de se multiplicarem automaticamente sem a necessidade do usuário. Eles costumam consumir muitos recursos do equipamento onde estão alocados devido ao processo de multiplicação.
  O processo de infecção e propagação dos *worms* pode ocorrer com a identificação dos computadores alvos; com envio de cópias de si mesmo após a identificação do alvo; com sua ativação automática ou acionada e através do reinício do processo de infecção e propagação;

- ***Spyware*** – Este *software*, após a sua instalação, objetiva o monitoramento das atividades do sistema e envio de dados a terceiros. Assim como o *sniffing* pode ser utilizado tanto para uso legítimo quanto malicioso.
  Alguns exemplos de uso de *spyware* podem ser através de *keylogger*, capaz de registrar todos os dados digitados pelo teclado do usuário. Existe também o *screenlogger*, capaz de armazenar a área da tela onde o mouse do usuário clicou e com isso ser capaz de saber as ações realizadas. Por fim, temos o *adware*, utilizado para exibição de propagandas, mas em alguns casos ser utilizado para esconder códigos maliciosos;

- ***Trojan-horse*** – Os *trojan-horses* precisam da participação do usuário para que desempenhe suas funções. Estes programas podem estar escondidos em protetores de tela, cartões virtuais entre outros recursos.
  Diversos podem ser os usos destes programas, mas objetivam manipular os dados das vítimas, coletar informações e até mesmo interferir fisicamente no computador. Muitos ataques em computadores podem incluir a instalação do *trojan-horse*, de modo que o atacante possa retornar a praticar suas ações em outros momentos oportunos sem o consentimento da vítima.

Apesar das grandes ameaças que os computadores estão vulneráveis, convém estar atento a todo tipo de ação realizada pelo usuário para que este não comprometa seus dados ou mesmo a organização na qual esteja inserido. *Softwares* antivírus, *firewalls* e outros mecanismos permitem a proteção de ameaças comumente encontradas nos meios digitais, principalmente no uso da Internet.

5.4.6 Criptografia

5.4.6.1 Conceitos de criptografia

Segundo Amatte e Peixinho (2013), a criptografia consiste na ciência de ler e escrever mensagens cifradas. Para isso, ela é fundamentada em complexos modelos matemáticos que buscam obter uma mensagem de difícil compreensão, deixando para o destinatário a responsabilidade de ler este conteúdo quando estiver de posse da chave correta para decifrar.

Atualmente muitas aplicações de segurança utilizam criptografia como base para seus sistemas. Essas técnicas garantem, segundo Lento (2011), três aspectos nas mensagens como confidencialidade, autenticidade e integridade.

No aspecto da confidencialidade, os usuários que não compartilham a mesma chave não podem ler o conteúdo da mensagem. Na autenticidade, com razoável certeza podemos crer que a mensagem de origem é autêntica, uma vez que somente ela possui a chave criptográfica. Por fim, no aspecto da integridade, podemos ter certeza de que não foi modificada durante o envio, visto que precisaria ser descriptografada com outra chave.

5.4.6.2 Tipos de criptografia

5.4.6.2.1 Criptografia de chave simétrica e de chaves assimétricas

Os métodos criptográficos podem ser subdivididos em duas categorias, como criptografia de chave simétrica e assimétrica.

De acordo com o Comitê Gestor da Internet no Brasil (2012), na criptografia de chave simétrica, a chave é utilizada tanto para codificar quanto para decodificar as informações, dessa forma, podemos garantir a confidencialidade dos dados.

Nos casos onde a informação precisa ser codificada e decodificada pela mesma pessoa, não há necessidade de compartilhar a chave secreta. No entanto, a chave deverá ser previamente combinada por meio de canal de comunicação seguro se estas operações envolverem pessoas ou equipamentos diferentes.

Alguns exemplos de criptografias simétricas são:

- *Eletronic Code Book*;
- *Cipher Block Chaining*;
- *Cipher Feed Back*;
- *Output Feedback*;
- *Data Encryption Standard*;
- *Triple DES*;
- *RivestChipher4*;
- *International Data Encryption Algorithm*;
- *Advanced Encryption Standard*;
- *Diffie-Hellman Algorithm*.

Na criptografia assimétrica são utilizadas duas chaves distintas: uma pública, que pode ser divulgada ao interessado e uma privada, que deve ser mantida em segredo pelo dono.

No processo de codificação, utiliza-se uma das chaves e para decodificar utiliza-se a outra. A chave privada pode ser armazenada em diversas formas, como um arquivo no computador ou mesmo num dispositivo *token*.

Alguns exemplos de criptografias assimétricas são:

- RSA;
- DAS;
- El Gamal;
- DSS.

É importante compreender que a criptografia de chave simétrica, comparada a assimétrica é mais indicada para garantir a confidencialidade em grandes volumes de dados, pois tem a capacidade de processar mais rapidamente. Porém ela se torna menos importante quando é utilizada para o compartilhamento de informações por se tornar mais complexa.

Apesar de possuir um processamento mais lento que a criptografia de chave simétrica, a criptografia de chave assimétrica pode resolver esses problemas. O ideal é que se utilize uma combinação de ambas as criptografias como ocorre nos navegadores *Web* e em *softwares* clientes de *e-mails*.

5.4.6.2.2 Função Hash

Segundo o Comitê Gestor da Internet no Brasil (2012, p. 69), uma função *Hash* pode ser definida como:

> [...] é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho que ela tenha, gera um resultado único e de tamanho fixo, chamado *hash*.

Desse modo, uma função *hash* pode ser utilizada para verificar a integridade de um arquivo, de modo que erros na transmissão ou armazenamento possam ser detectadas. Podemos também utilizar as funções *hash* para gerar assinaturas digitais.

Exemplos de algoritmos de função *hash* são:

- *Message Digest* (MD5);
- *Secure Hash Algorithm* (SHA).

5.4.6.2.3 Assinatura digital

A assinatura digital está baseada no fato de que somente o dono da chave privada tem o conhecimento dela e se ela foi utilizada para codificar uma informação, logo o dono certamente é o responsável. Com isso, a verificação da assinatura digital é realizada com a chave pública correspondente.

Para solucionar a baixa eficiência da criptografia de chaves assimétricas, a codificação é realizada sobre a função *hash*.

Será através dos certificados digitais que haverá a garantia de autenticidade e confidencialidade.

5.4.6.2.4 Certificação digital

O uso de certificação digital permite que se possa distinguir uma entidade da outra e associar uma chave pública para elas. É interessante o uso de certificados digitais para garantir que somente as pessoas comprovadamente identificadas possam se comunicar, impedindo assim que impostores falsifiquem a identidade e tenham acesso a informações confidenciais.

A autenticidade deve ser garantida pela Autoridade Certificadora que também tem como função atualizar constantemente a lista de certificados que não tem mais validade, permitindo assim maior segurança.

5.5 DISPOSITIVOS DE SEGURANÇA

5.5.1 Firewall

Segundo Zwicky, Cooper e Chapman (2000 apud LENTO, 2011, p. 89-91), os *firewalls* são definidos como mecanismos de bloqueio cuja finalidade é a proteção dos recursos e ameaças à organização, de intrusos que possam tentar comprometer informações vitais. Este mecanismo está normalmente situado entre a rede interna, ou seja, a rede privada da organização e entre a rede externa.

Sendo o *firewall* um dispositivo que visa a proteção das informações do meio externo, convém destacar as razões de sua implementação e seus objetivos, tais como:

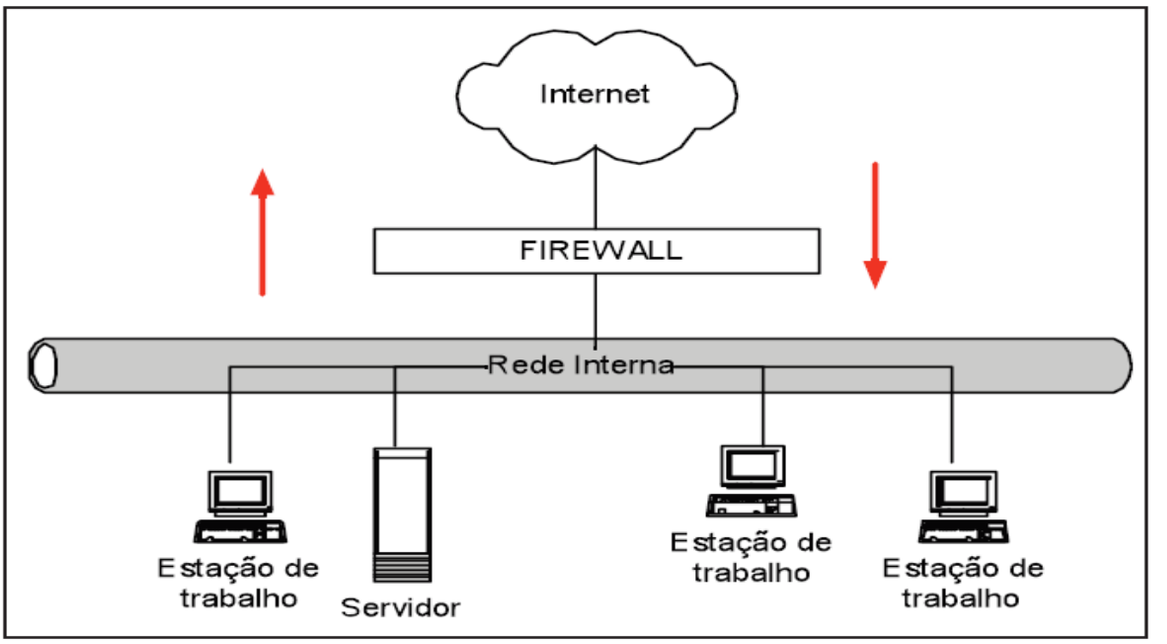
- **Dados** – Estes devem estar devidamente protegidos pois representam valiosíssimos recursos para a organização. O dispositivo de proteção deve garantir que os dados tenham confidencialidade, integridade e disponibilidade;

- **Recursos** – Os recursos são os próprios ativos físicos da organização. A proteção destes evita o uso de funcionalidades restritas e impede que possíveis danos físicos possam ocorrer nos equipamentos;

- **Reputação da Organização** – A reputação reflete a qualidade e confiabilidade da organização. Seu posicionamento pode ser afetado caso algum uso indevido ocorra e possa causar impacto tanto interno como externo. É de fundamental importância que todos os acessos sejam legítimos e identificados para não correr o risco com roubo de informações.

O uso de *firewalls* traz muitos benefícios às organizações impedindo que usuários de redes externas tenham acesso a informações da rede interna. Ao mesmo tempo, os usuários da organização podem ter restrições de acesso a *sites* externos que possam causar ameaças, contribuindo dessa forma com a segurança da informação.

Figura 2 – Representação de uma rede com *firewall*.



Fonte: Zwicky, Cooper e Chapman (2000 apud LENTO, 2011, p. 91).

Apesar do *firewall* implementar diversas regras de segurança, ele não é capaz de impedir que usuários mal-intencionados possam comprometer a segurança da organização ou mesmo que novas ameaças realizem seus ataques.

5.5.2 Serviços de *proxy*

Segundo Lento (2011, p. 98-100), os serviços de *proxy* são aplicações de servidores que basicamente recebem requisições de serviços de clientes, analisa e redireciona os pedidos aos servidores necessários. Dessa forma, os serviços de *proxy* permitem que os clientes requisitantes não estabeleçam uma conexão direta com estes servidores. Ocorre um mascaramento das informações do cliente e da rede na qual está inserido, uma vez que a conexão ocorrerá entre o *proxy* e o servidor da Internet.

Além da segurança proporcionada pelos serviços de *proxy*, estes permitem um maior desempenho no tráfego da rede, pois estes servidores possuem um armazenamento chamado *cache* que retém os pedidos de conexão externa para uso posterior. Com isso, caso uma nova requisição seja feita, não será necessário enviá-la ao *proxy* e então ao servidor externo. Esta requisição será atendida pelo próprio *cache* do *proxy*, evitando assim um consumo maior de conexão.

5.5.3 Network Address Translation

Ainda de acordo com Lento (2011, p. 101-102), o *Network Address Translation (NAT)* realiza basicamente a tradução de endereços de rede internos e externos de modo que eles não se pareçam com os originais. Essa técnica não provê segurança mas permite que as características da rede interna sejam preservadas. Resumidamente, quando um equipamento deseja se comunicar com uma rede externa, o *NAT* modificará este endereço de modo que não seja reconhecível como pertencente à rede do remetente. O mesmo ocorrerá com um endereço externo que terá suas informações modificadas quando chegar na rede interna de destino.

5.5.4 Intrusion Detection System

Um *Intrusion Detection System (IDS)*, segundo Lento (2011, p. 102-109) tem o propósito de fornecer ao administrador da rede informações sobre questões de segurança da informação. Este sistema, que pode ser baseado em *software* e/ou *hardware*, monitora possíveis tentativas de ataques a sistemas computacionais e até mesmo ataques ocorridos, de modo que sirva como um bom mecanismo para análise dos acontecimentos da rede organizacional.

Um *IDS* auxilia a organização a identificar e melhorar os sistemas disponíveis com base nos dados coletados. Esses registros permitem que tomadas de decisões sobre alguma tecnologia sejam efetivas de modo a corrigir falhas e inclusive melhorar a administração da rede corporativa.

5.6 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

5.6.1 Conceitos básicos

Segundo o Tribunal de Contas da União (2012 apud FONTES, 2014), a política de segurança da informação pode ser definida como:

> Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações (BRASIL, TCU, 2012, p. 10).

Dessa forma, é importante que a política seja seguida por todos os colaboradores da organização uma vez que ela pode ser vista como um documento jurídico.

A política de segurança da informação ainda pode conter outras regras específicas como políticas de senhas, *backup*, privacidade, confidencialidade, etc.

É importante destacar que segundo Amatte e Peixinho (2013, p. 138, 142), não existe uma regra geral para a elaboração de uma política de segurança. Cada organização deve, com base em suas características, elaborar as suas regras de modo que atendam aos seus objetivos de negócio.

5.6.2 Objetivos da política de segurança da informação

Segundo Coelho (2011), o objetivo da política de segurança da informação é o provimento de orientação à direção da organização e o apoio desta para a segurança da informação com base nos requisitos do negócio e também nas leis e regulamentos vigentes. Essa política deve ser clara e objetiva e alinhada com o negócio.

Nesta política serão definidos as diretrizes, os limites, as responsabilidades e os objetivos dos controles que deverão ser implementados para garantir os requisitos de proteção da segurança da informação na organização.

5.6.3 Arquitetura da política de segurança da informação

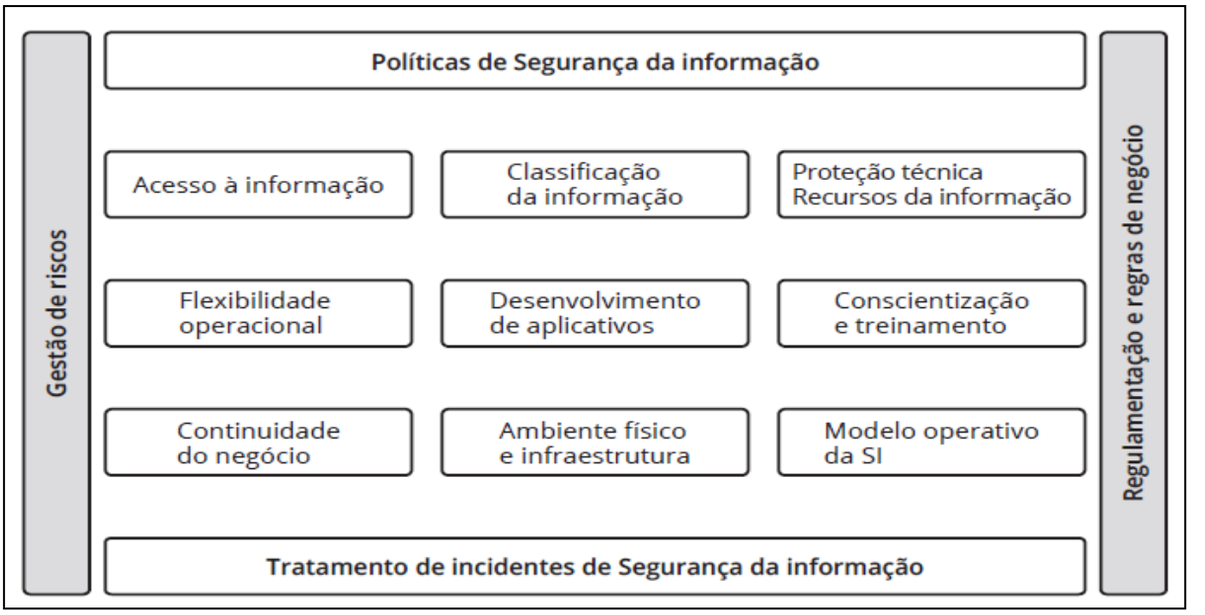
A proteção da informação é de responsabilidade da organização e ela deve se consolidar pela atuação dos seus gestores. A segurança da informação existe para proteger os recursos de informação de modo que atinjam os objetivos do negócio.

Uma vez que não existe uma arquitetura padrão para a definição das políticas de segurança, deve ser definido uma que seja adequada à organização e à sua cultura.

De acordo com Coelho (2011) e Fontes (2014), podemos ter uma dimensão da segurança da informação que corresponde os aspectos que devem ser considerados em um processo de segurança da informação, considerando a Família NBR ISO/IEC 27000 de normas de segurança da informação.

A figura abaixo ilustra as Dimensões da Segurança da Informação:

Figura 3 – Dimensões da Segurança da Informação.



Fonte: Coelho (2011, p. 73) e Fontes (2014, p. 5).

Apesar destas políticas serem consideradas como necessárias à segurança, cada organização deve adequar da melhor forma ao seu negócio.

É importante destacar que cada dimensão tem sua importância no processo e a maturidade da organização valerá pela eficiência e efetividade deste conjunto de dimensões.

Será descrito a seguir o objetivo de cada dimensão:

- **Gestão de Riscos** – Definição, implantação e manutenção da gestão de riscos da segurança da informação para o monitoramento e tratamento das ameaças que podem gerar impactos financeiros, operacionais ou qualquer outro impacto nos recursos de informação que possa comprometer os objetivos e atividade da organização;

- **Políticas de Segurança da Informação** – Desenvolvimento, implantação e manutenção dos regulamentos para que a organização possua um bom processo de segurança de informação. Nesse regulamento são definidas as regras para o uso e controle da informação e que esteja em conformidade com as leis vigentes e demais regras que a organização deve cumprir;

- **Acesso à Informação** – Garante um adequado uso para o acesso à informação, definindo regras e responsabilidades aos participantes;

- **Classificação da Informação** – Define o padrão de sigilo que deverá ser utilizado na informação da organização;

- **Proteção Técnica de Recursos de Informação** – Garante que haja uma gestão técnica para os recursos de tecnologia da informação da organização. Garante também medidas para atualização da proteção da informação;

- **Flexibilidade Operacional** – Busca garantir a existência e efetividade da Gestão de Mudanças, Gestão de Problemas, Gestão de Ativos e Gestão de Capacidade para os recursos de informação;

- **Desenvolvimento ou Aquisição de Sistemas** – Garante que o desenvolvimento e aquisição de *softwares* estejam de acordo com os requisitos de segurança. Também inclui a manutenção de tais *softwares* e a dependência de desenvolvedores, de modo que garanta a continuidade desse aplicativo ao longo do tempo;

- **Conscientização e Treinamento de Usuário** – Desenvolver atividades para o treinamento e conscientização dos usuários participantes da organização;

- **Continuidade de Negócio** – Garantir a continuidade do negócio no que se refere aos recursos de informação quando alguma indisponibilidade ocorrer;

- **Ambiente Físico e Infraestrutura** – Garantir a proteção física da infraestrutura onde existem recursos de informação e ao mesmo tempo garantir a existência dessa infraestrutura;

- **Modo Operativo da Segurança da Informação** – Definição, implantação e monitoramento da estrutura organizacional da segurança da informação. Deve buscar manter um bom relacionamento com seus parceiros tanto interna como externamente;

- **Tratamento de Incidente de Segurança da Informação** – Garantir um adequado controle dos incidentes de segurança da informação, de modo a reduzir a probabilidade de comprometer as operações do negócio e ameaças à organização.

Temos ainda a **Dimensão Política de Segurança da Informação** que objetiva desenvolver, implantar e manter atualizados os regulamentos necessários para que a organização possua um efetivo processo de segurança da informação. Esses regulamentos definem como a organização deseja que a informação seja utilizada, controlada e tenha seu uso responsabilizado.

Essa dimensão se caracteriza por regulamentar todas as outras dimensões, ou seja, ela serve de base para um efetivo processo organizacional de segurança da informação. Ela é também considerada como uma dimensão estrutural pois garante o controle da cada dimensão, de modo que ela apenas defina características de regulamentação.

Não cabe neste trabalho o detalhamento da norma internacional ISO/IEC 27002 mas apenas destacar os pontos considerados adequados para o propósito deste estudo de caso.

6 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

O objeto de estudo deste trabalho é o Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro nas suas relações com as questões referentes a Segurança da Informação. Antes de apresentar as questões apropriadas ao estudo, suas análises e recomendações, convém apresentar o IFRJ a partir do seu histórico, seus princípios, estrutura hierárquica, catálogo de cursos, entre outros dados básicos. Sendo assim, poderemos compreender a importância da Instituição no país e sua responsabilidade com a educação pública de qualidade.

6.1 O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO

6.1.2 Histórico, visão e missão

Com base no Relatório de Avaliação e-MEC/INEP (2015), a história do IFRJ tem início em 1942 quando houve a criação da Escola Técnica de Química, por meio do Decreto-Lei nº. 4.127, que passou a funcionar em 6 de dezembro de 1945, após a aprovação do curso Técnico de Química Industrial, pelo Decreto-Lei nº. 8.300. A Instituição estava fisicamente instalada nas dependências da Escola Nacional de Química da Universidade do Brasil, hoje Universidade Federal do Rio de Janeiro, até 1946. Foi transferida em 1946 para as dependências da Escola Técnica Nacional, onde funciona o Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (CEFET-RJ).

A Lei nº. 3.552 conferiu à Instituição a condição de autarquia federal, passando a ser denominada Escola Técnica de Química e posteriormente a ser denominada Escola Técnica Federal de Química.

Foi em 1985 que a Instituição teve espaço físico próprio e passou a ser denominada Escola Técnica Federal de Química do Rio de Janeiro, localizada no bairro do Maracanã, onde hoje está instalado o campus Rio de Janeiro.

Em 1988, foi criado o curso Técnico em Biotecnologia. Seguindo o plano de expansão em 1990, a Instituição criou a Unidade de Ensino Descentralizada de Nilópolis, na qual foram instalados os cursos Técnicos em Química e Técnico em Saneamento.

Foi em dezembro de 1994, com a promulgação da Lei nº. 8.948, que criou o Sistema Nacional de Educação Tecnológica, que possibilitou que as escolas técnicas federais fossem transformadas em Centros Federais de Educação Tecnológica. Em 1999, a Instituição foi transformada em Centro Federal de Educação Tecnológica de Química de Nilópolis, tendo suas finalidades ampliadas e mudança de sede para o município de Nilópolis, Região Metropolitana do Rio de Janeiro.

Devido a Lei de Diretrizes e Bases da Educação Tecnológica, Lei nº. 9394 de 1996, do Decreto nº 2208 de 1997 e da Portaria MEC nº. 646/97, as Instituições Federais de Educação Tecnológica foram autorizadas a manter o Ensino Médio desde que suas matrículas fossem independentes da Educação Profissional, dessa maneira, elas deveriam encerrar os cursos integrados. Com a promulgação do Decreto nº. 5.514, tal situação foi revertida em 2005, de modo que o CEFETQ passa, novamente, a oferecer o Ensino Médio integrado ao Ensino Técnico.

Com a publicação dos Decretos nº. 5.224 os CEFET's como Instituições Federais de Ensino Superior, foram autorizados a oferecer cursos de graduação, sendo estimulados a participar ativamente da pesquisa e da pós-graduação. Na fase inicial do desenvolvimento, projetos de pesquisa que aconteciam informalmente, passaram a ser formalizados e proporcionaram a criação de grupos de pesquisas, cadastrados na instituição e no CNPq. Foi então criado o primeiro curso de pós-graduação *lato sensu*, na Unidade Rio de Janeiro, sendo criado outros cursos posteriormente.

Foi em 2005, com a publicação do Decreto nº. 5.478, criando o Programa de Integração da Educação Profissional ao Ensino Médio na Modalidade de Educação de Jovens e Adultos (PROEJA) que se planejou para no ano de 2006 oferecer uma nova formação profissional e modalidade de escolarização.

Em 2007, foi criado o primeiro programa de pós-graduação *stricto sensu*, com a oferta do curso de Mestrado Profissional em Ensino de Ciências.

No dia 29 de dezembro de 2008, através da Lei nº. 11.892, o Centro Federal de Educação Tecnológica de Química de Nilópolis é transformado em Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro (IFRJ).

Muitos campi foram implantados antes e após a transformação do IFRJ, sendo atualmente uma referência no ensino médio, graduação, pós-graduação em nível *lato sensu* e *stricto sensu* sendo em todo o Estado.

Ainda com base em seu *site*, para a visão e missão temos:

> Missão: Promover a formação profissional e humana, por meio de uma educação inclusiva e de qualidade, contribuindo para o desenvolvimento do país nos campos educacional, científico, tecnológico, ambiental, econômico, social e cultural.
>
> Visão: O IFRJ se consolidará como instituição de referência em educação profissional, científica e tecnológica, integrando as ações de ensino, pesquisa e extensão, com ênfase na disseminação da cultura inovadora e em consonância com as demandas da sociedade (INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO, 2011).

6.1.3 Estrutura organizacional

6.1.3.1 Estrutura administrativa da Reitoria

Conforme o seu Regimento Geral, o IFRJ está organizado em uma estrutura multicampi e atualmente possui quinze unidades espalhadas pelo estado do Rio de Janeiro. Além da Reitoria, órgão com função executiva para a Instituição e administração central desta, temos os campi Arraial do Cabo, Belford Roxo, Duque de Caxias, Engenheiro Paulo de Frontin, Mesquita, Nilópolis, Niterói, Paracambi, Pinheiral, Realengo, Resende, Rio de Janeiro, São Gonçalo, São João de Meriti e Volta Redonda.

A Reitoria é o órgão executivo do IFRJ, cabendo-lhe a administração, a coordenação e a supervisão de todas as atividades da Autarquia.

O órgão compreende, de acordo o Regimento Geral do IFRJ:

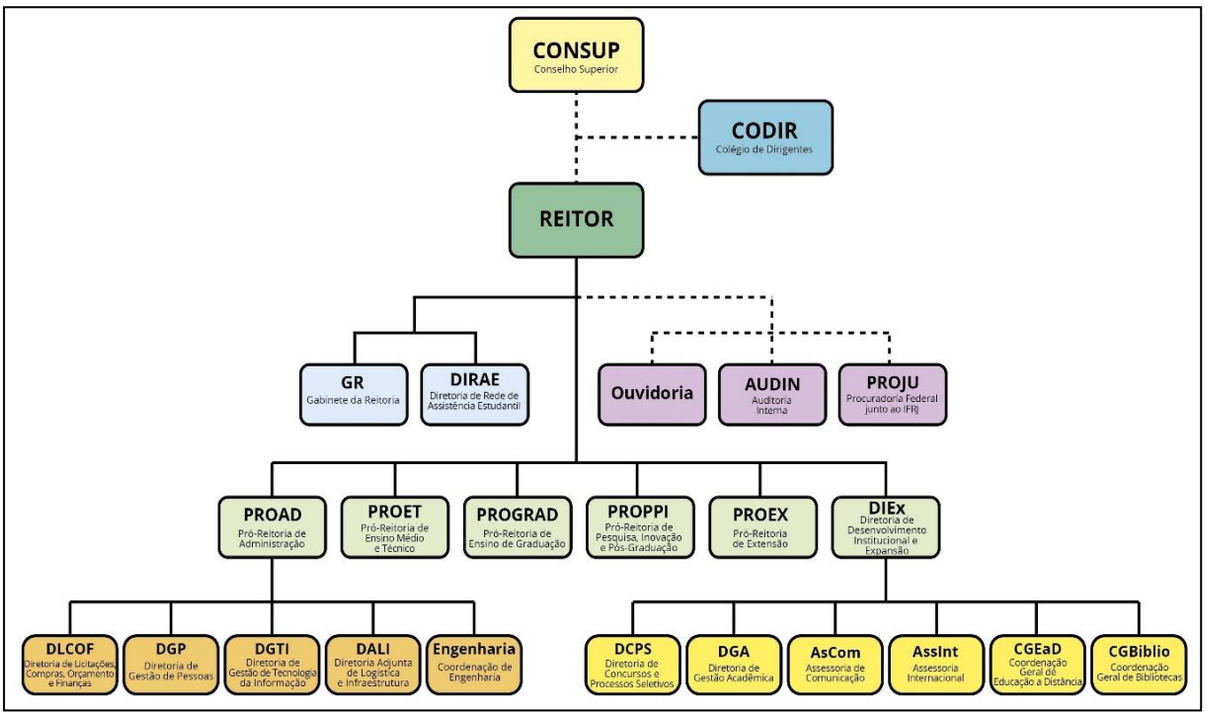
- O Reitor;
- O Gabinete da Reitoria;
- As Pró-Reitorias;
- As Diretorias Sistêmicas;
- A Auditoria Interna;
- A Procuradoria Federal;
- Os Órgão de Assessoramento.

Para um melhor detalhamento da hierarquia e das divisões temos:

- Conselho Superior – CONSUP
- Colégio de Dirigentes – CODIR
- Reitor do IFRJ
- Gabinete da Reitoria – GR
- Diretoria de Rede de Assistência Estudantil – DIRAE
- Ouvidoria
- Auditoria Interna – AUDIN
- Procuradoria Federal junto ao IFRJ – PROJU
- Pró-Reitoria de Administração – PROAD
- Pró-Reitoria de Ensino Médio e Técnico – PROET
- Pró-Reitoria de Ensino de Graduação – PROGRAD
- Pró-Reitoria de Pesquisa, Inovação e Pós-Graduação – PROPPI
- Pró-Reitoria de Extensão – PROEX
- Diretoria de Desenvolvimento Institucional e Expansão – DIEx
- Diretoria de Licitações, Compras, Orçamento e Finanças – DLCOF
- Diretoria de Gestão de Pessoas – DGP
- Diretoria de Gestão de Tecnologia da Informação e Comunicação – DGTIC
- Diretoria Adjunta de Logística e Infraestrutura – DALI
- Coordenação de Engenharia – Engenharia
- Diretoria de Concursos e Processos Seletivos – DCPS
- Diretoria de Gestão Acadêmica – DGA
- Assessoria de Comunicação – AsCom
- Assessoria Internacional – AssInt
- Coordenação Geral de Educação a Distância – CGEaD
- Coordenação Geral de Bibliotecas – CGBiblio

O gráfico abaixo ilustra a estrutura hierárquica principal da Reitoria:

Figura 4 – Estrutura hierárquica do IFRJ.



Fonte: Prestação de Contas Ordinárias Anual. Relatório de Gestão do Exercício de 2015 (2015).

Desse modo, no artigo 34 do Regimento Geral da Instituição, à Reitoria compete as seguintes atribuições:

> I - Administrar de forma geral o IFRJ, bem como supervisionar a execução das políticas de gestão educacional, de pessoal, orçamentária, financeira e patrimonial, visando ao aperfeiçoamento, ao desenvolvimento e à excelência das atividades de ensino, pesquisa e extensão;
>
> II - Formular as propostas orçamentárias, encaminhando-as para a aprovação dos órgãos competentes;
>
> III - planejar as estratégias de desenvolvimento da Instituição, conforme previsto o Plano de Desenvolvimento Institucional - PDI;
>
> IV - Coordenar e supervisionar a execução das políticas aprovadas pelo Conselho Superior, adotando medidas para seu cumprimento e avaliação dos resultados;
>
> V - Promover o relacionamento e o permanente intercâmbio com as instituições congêneres;
>
> VI - Promover o planejamento, a integração e a cooperação mútua entre as unidades organizacionais que compõem o IFRJ, (REGIMENTO GERAL DO IFRJ, 2011, p.15).

6.1.3.2 Estrutura administrativa dos campi

Os Campi do IFRJ são dirigidos por Diretores-Gerais nomeados pelo Reitor para o mandato de quatro anos, permitida uma recondução, após o processo de consulta do respectivo campus.

O processo de escolha dos Diretores-Gerais dos campi é coordenado por uma Comissão Eleitoral, aprovada no Conselho Superior e nomeada pelo Reitor.

Uma vez que o Regimento Geral da Instituição define a estrutura organizacional para cada Campus, podem haver pequenas diferenças entre eles.

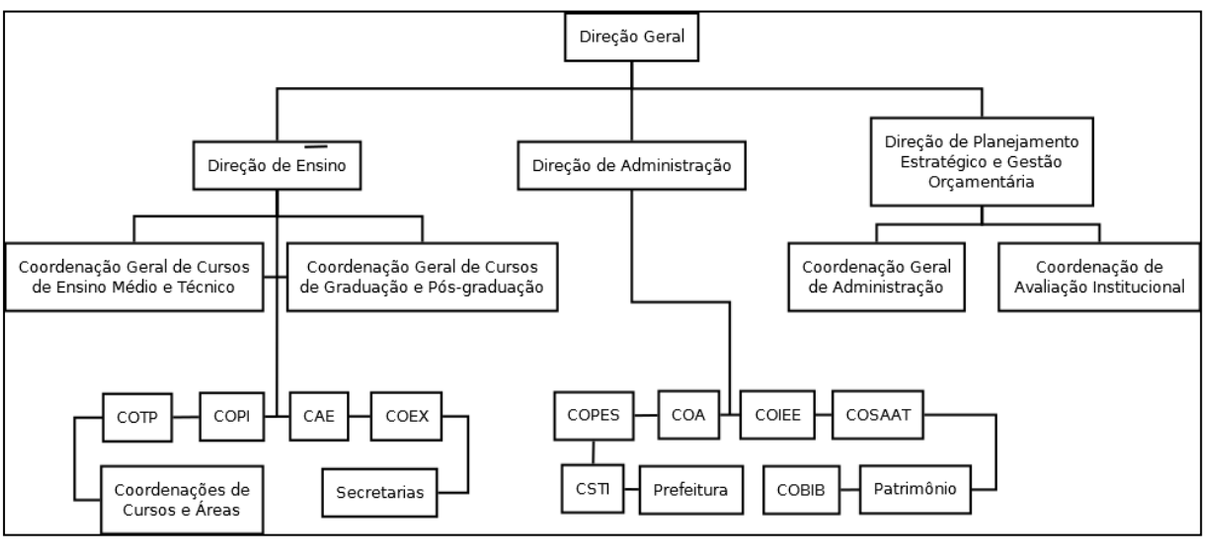
Desse modo, segundo o Regimento, os Campi poderão ser compostos pela estrutura a seguir:

> I - Diretoria Geral do Campus (DG);
>
> II - Diretoria de Administração (DA);
>
> III - Diretoria de Ensino (DE);
>
> IV - Diretoria a ser definida por cada campus em seu regimento interno;
>
> V - Secretaria da direção Geral (SecDG);
>
> VI - Assessoria de Comunicação (AsCom);
>
> VII - Coordenação das Disciplinas Básicas (CoDB);
>
> VIII - Coordenação de Biblioteca (CoBib);
>
> IX - Coordenação de Extensão (CoEx);
>
> X - Coordenação de Integração Escola-Empresa (CoIEE);
>
> XI - Coordenação de Pesquisa e Inovação (CoPI);
>
> XII - Coordenação de Segurança e Administração de Ambientes Tecnológicos (CoSAAT);
>
> XIII - Coordenação de Suporte de Tecnologia da Informação e Comunicação (CSTIC);
>
> XIV - Coordenação de Turno (CoTur);
>
> XV - Coordenação Técnico Pedagógica (CoTP);
>
> XVI - Coordenações de Curso;
>
> XVII - Prefeitura do Campus (PrefCampus);
>
> XVIII - Secretarias Acadêmicas por níveis de ensino:
>
> a) Secretaria do Ensino Médio e Técnico (SEMT);
>
> b) Secretara do Ensino de Gradução (SEG);
>
> c) Secretaria do Ensino de Pós-Graduação (SEPG);

> XIX - Serviço de Saúde (SerSa);
>
> XX - Coordenação de Almoxarifado (CoAlm);
>
> XXI - Coordenação de Compras (CoComp);
>
> XXII - Coordenação de Gestão de Pessoas (CoGP);
>
> XXIII - Coordenação de contratos e convências (CoCC);
>
> XXIV - Coordenação de Orçamento e Financeiro (COF);
>
> XXV - Coordenação de Patrimônio (CoPat);
>
> XXVI - Setor de Protocolo (SeProt);
>
> XXVII - Setor de Recursos didáticos (SeRD);
>
> XXVIII - Núcleo de Apoio às pessoas com necessidades educacionais especiais (NAPNE);
>
> XXIX - Núcleo Docente Estruturante (NDE), (REGIMENTO GERAL DO IFRJ, 2011, p.37).

Através do gráfico abaixo é apresentada a estrutura administrativa do Campus Rio de Janeiro como exemplo. Convém observar que nem todas as coordenações e setores foram detalhados no gráfico, uma vez que a nova proposta de gestão do Campus integrou alguns desses setores a outros.

Figura 5 – Nova estrutura organizacional do Campus Rio de Janeiro.



Fonte: Elaboração do autor, 2017.

6.1.4 Competência da Direção de Gestão de Tecnologia da Informação e Comunicação

Apesar da DGTIC estar fisicamente localizada na Reitoria e possuir papel de destaque quanto a inovação tecnológica no suporte a sistemas acadêmicos e administrativos, apoio

a gerenciamento de projetos e de infraestrutura entre tantas outras atribuições importantes, não há no Regimento Geral do IFRJ a descrição das competências da DGTIC. Não foi também localizada no *site* institucional informações de destaque que pudessem ser citadas neste trabalho para melhor esclarecer as atribuições da DGTIC.

Com base no conhecimento do autor pelas relações entre a CSTIC e DGTIC, convém destacar algumas atribuições percebidas desempenhadas pela DGTIC:

- Gerenciamento de sistemas integrados de gestão de atividades acadêmicas e administrativas;
- Gerenciamento de contas de usuários institucionais;
- Gerenciamento de plataforma de ensino a distância;
- Apoio a pesquisa e comunicação;
- Gerenciamento de licenças de softwares;
- Gerenciamento de infraestrutura de tecnologia;
- Gerenciamento de serviços de comunicação;
- Parcerias com instituições de tecnologia para a disseminação de conhecimentos técnicos a alunos, professores e servidores administrativos;
- Consultoria aos outros Campi.

Muitas outras atribuições não puderam ser destacadas devido à falta de informações disponíveis publicamente, sendo necessário um contato mais próximo com a DGTIC para maiores esclarecimentos sobre as atividades desempenhadas.

6.1.5 Competência das Coordenações de Suporte de Tecnologia da Informação e Comunicação

Com base no Artigo 127 do Regimento Geral do IFRJ, compete às CSTIC de todos os Campi as seguintes atribuições:

> I - Atuar no Suporte de primeiro nível de TIC, que compreende o atendimento ao usuário final *on site* (no local);
>
> II - Realizar a manutenção preventiva nos equipamentos do Campus;
>
> III - Cadastrar usuários no servidor do serviço de Diretório;
>
> IV - Encaminhar criação de e-mail para suporte de e-mail;
>
> V - Realizar a avaliação na rede física de dados com a orientação da Diretoria de Tecnologia da Informação e Comunicação e fornecer informações sobre qualquer anomalia;

> VI - Responder pelo bom funcionamento diário da rede de dados e de telefonia do Campus, com a orientação da DGTIC, informando sobre qualquer anomalia;
>
> VII - Responder pelo suporte de primeiro nível dos sistemas do IFRJ;
>
> VIII - Propor, coordenar e acompanhar os planos estratégicos de tecnologia da informação e comunicação no âmbito do campus, no que concerne à tecnologia a ser implementada;
>
> IX - Propor programas de capacitação e desenvolvimento de recursos humanos em tecnologia da informação e comunicação;
>
> X - Administrar a infraestrutura tecnológica e os serviços de rede existentes no campus;
>
> XI - Propor normas, procedimentos e padrões para a utilização dos recursos de tecnologia da informação e comunicação no Campus;
>
> XII - Acompanhar tecnicamente contratos e convênios relativos à tecnologia da informação e comunicação;
>
> XIII - Oferecer suporte técnico aos usuários no que diz respeito a aplicativos, sistemas gestores e manutenção de equipamentos no âmbito do Campus;
>
> XIV - Propor a especificação técnica para a aquisição de equipamentos, periféricos, suprimentos de tecnologia da informação e comunicação;
>
> XV - Promover, orientar e controlar a execução dos serviços de manutenção e atualização dos recursos de tecnologia da informação e comunicação do Campus;
>
> XVI - Realizar e acompanhar, em articulação com a Prefeitura do Campus, Adequações e ampliações de instalações físicas para utilização de equipamentos de tecnologia da informação e comunicação, (REGIMENTO GERAL DO IFRJ, 2011, p.43).

É importante observar que as CSTIC são dependentes da DGTIC em muitos aspectos devendo buscar conformidade com as recomendações e exigências, não sendo possível em alguns casos adquirir autonomia para as tarefas internas que podem gerar divergências de opiniões e atraso técnico e gerencial entre os Campi.

6.2 APLICAÇÃO DE QUESTIONÁRIO E ANÁLISE DOS DADOS OBTIDOS

6.2.1 Definição do questionário

Para a definição do questionário deste estudo, foi utilizado as normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27002:2013 em conjunto com os materiais presentes na bibliografia que resumem a norma, de modo a facilitar a compreensão e aplicabilidade na pesquisa.

O questionário é composto para a Diretoria de Gestão de Tecnologia da Informação e Comunicação, de um total de 57 questões objetivas, sendo permitida uma única resposta. Da mesma forma, o questionário elaborado para as Coordenações de Suporte de Tecnologia da Informação e Comunicação foi composto por 57 questões objetivas, sendo permitida uma única resposta.

Os dois questionários foram elaborados individualmente e possuem relação contextual entre si, buscando confrontar opiniões e experiências vividas pelos entrevistados.

O meio utilizado para a interação com o questionário ocorreu através de formulário eletrônico, utilizando a mesma plataforma de software do *e-mail* institucional. Este questionário foi enviado para as contas de *e-mail* institucionais dos coordenadores de campus e para o coordenador da CSTIC na DGTIC.

Convém observar que os questionários foram enviados após o contato telefônico com os coordenadores e tendo sido esclarecidos os propósitos da pesquisa e em acordo com estes participantes.

O prazo definido para a participação na pesquisa foi de 7 (sete) dias úteis, tendo como base a quantidade de questões e o tempo médio para a conclusão que foi estimado em 20 (vinte) minutos.

6.2.2 Aplicação do questionário

O questionário foi enviado para 13 (treze) campi a saber:

- Rio de Janeiro;
- Nilópolis;
- Caxias;
- Volta Redonda;
- Realengo;
- Pinheiral;

- Mesquita;
- Paulo de Frontin;
- Arraial do Cabo;
- Resende;
- Niterói;
- São João de Meriti;
- Paracambi.

Apenas 5 (cinco) campi responderam à pesquisa e conforme suas respostas foram sendo enviadas, foi realizado uma classificação dos dados para facilitar a compreensão de tabelas.

Convém destacar que não se busca avaliar a opinião individual dos coordenadores de cada campus, mas o conjunto CSTIC e suas relações internas e externas com a DGTIC.

Será exposto abaixo os dois questionários e suas possíveis respostas, iniciando com as questões destinadas às CSTIC:

Tabela 1 – Questionário aplicado às CSTIC.

(continua)

Item	Questão aplicada	Respostas possíveis
1	A CSTIC possui uma política de Segurança da Informação?	Não.
		Sim. Através de prática informal.
		Sim. Através de documentação formal.
2	Na CSTIC existe profissional responsável pela Segurança da Informação?	Não.
		Sim. Um profissional responsável.
		Sim. Todos são responsáveis.
3	São aplicados cursos, palestras ou treinamentos sobre Segurança da Informação na CSTIC?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
4	São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação à comunidade do Campus?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
5	A CSTIC tem conhecimento pleno das vulnerabilidades e ameaças à Segurança da Informação no Campus?	Não.
		Sim. Parcialmente.
		Sim. Plenamente.

Tabela 1 – Questionário aplicado às CSTIC.

(continuação)

6	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por acidentes naturais (tempestades, incêndios, etc.)?	Não.
		Sim. Poucas vezes.
		Sim. Muitas vezes.
7	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas no fornecimento de energia elétrica?	Não.
		Sim. Poucas vezes.
		Sim. Muitas vezes.
8	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por roubo de equipamentos ou erro humano?	Não.
		Sim.
9	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *hardware* local ou remoto?	Não.
		Sim.
10	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *software*?	Não.
		Sim.
11	Na sua opinião, a comunidade do IFRJ (funcionários e professores) têm conhecimento dos riscos de Segurança da Informação que podem estar sujeitos no cotidiano?	Não.
		Sim.
12	São aplicadas técnicas de segurança de acesso físico aos equipamentos de Tecnologia da Informação (Ex: Cadeados, alarmes, etc.)?	Não.
		Sim.
13	O acesso físico aos equipamentos de Tecnologia da Informação ocorre exclusivamente por funcionários da Instituição?	Não.
		Sim.
14	O acesso físico aos equipamentos de Tecnologia da Informação ocorre mediante autorização ou algum processo de autenticação?	Não.
		Sim.
15	São registradas ameaças ou ataques aos sistemas de Tecnologia da Informação da Instituição?	Não.
		Sim.
16	Após a ciência de ameaças ou ataques aos sistemas de Tecnologia da Informação são analisados os fatores que causaram ou propiciaram o evento?	Não.
		Sim. Eventualmente.
		Sim. Sempre.
17	Há sistemas (*sites*, aplicações, etc.) de acesso externo e/ou interno sem criptografia aplicada?	Não.
		Sim.
18	O gerenciamento de senhas de acesso ocorre mediante o uso de *software* específico?	Não.
		Sim.
19	As senhas de acesso são de conhecimento de todos os funcionários de Tecnologia da Informação?	Não.
		Sim.
20	Existe algum tipo de classificação ou definição para a geração de senhas de acesso?	Não.
		Sim.
21	As senhas de acesso aos sistemas de Tecnologia da Informação são atualizadas regularmente?	Não.
		Sim.
22	As senhas de acesso aos sistemas de Tecnologia da Informação são passíveis de memorização pelos funcionários de Tecnologia da Informação?	Não.
		Sim.

Tabela 1 – Questionário aplicado às CSTIC.

(continuação)

23	Existe conscientização para o sigilo de senhas de acesso aos funcionários de Tecnologia da Informação?	Não.
		Sim.
24	Existe conscientização para o sigilo de senhas de acesso aos usuários da Instituição?	Não.
		Sim.
25	As senhas de acesso aos sistemas de Tecnologia da Informação são divulgadas verbalmente?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
26	Existe algum tipo de mapeamento ou documentação sobre os pontos críticos relacionados a Segurança da Informação (acesso físico, sistemas online, funcionários autorizados, etc.)?	Não.
		Sim.
27	Existe na CSTIC algum controle efetivo na identificação de funcionários e/ou visitantes?	Não.
		Sim.
28	Existe na Instituição algum controle efetivo de entrada/saída de equipamentos?	Não.
		Sim.
29	A CSTIC está alinhada com a coordenação de recursos humanos para o gerenciamento de recursos e sistemas aos funcionários e/ou visitantes?	Não.
		Sim. Superficialmente.
		Sim. Totalmente.
30	O ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) possui organização e limpeza periódicos?	Não.
		Sim.
31	No ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) há algum tipo de manutenção preventiva?	Não.
		Sim.
32	Nos equipamentos de Tecnologia da Informação disponíveis aos usuários são realizadas manutenções preventivas e/ou corretivas?	Não.
		Sim.
33	Existe política formal para realização de *backups* de dados importantes da CSTIC?	Não.
		Sim.
34	A definição de aplicações de *softwares* para uso na CSTIC ocorre mediante análise e reunião entre os funcionários?	Não.
		Sim.
35	Em um processo de mudança, existe avaliação do impacto antes da implementação?	Não.
		Sim. Eventualmente.
		Sim. Sempre.
36	Os procedimentos operacionais da CSTIC são formalmente documentados?	Não.
		Sim.
37	São gerenciados os incidentes e requisições de Tecnologia da Informação na CSTIC?	Não.
		Sim.
38	A CSTIC utiliza *software* antivírus nos equipamentos de Tecnologia da Informação?	Não.
		Sim.

Tabela 1 – Questionário aplicado às CSTIC.

(continuação)

39	A CSTIC realiza o monitoramento das operações e comunicações de acordo com a legislação vigente?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
40	Os usuários dos sistemas de Tecnologia da Informação são devidamente identificados para o acesso aos recursos?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
41	São revisados regularmente os acessos atribuídos aos usuários dos serviços de Tecnologia da Informação?	Não.
		Sim.
42	A CSTIC dispõe de sistema de proteção contra quedas de energia elétrica?	Não.
		Sim.
43	A CSTIC dispõe de mecanismos de proteção contra incêndios?	Não.
		Sim.
44	A CSTIC possui controle formal e atualizado dos ativos de Tecnologia da Informação da Instituição?	Não.
		Sim.
45	Na sua opinião, os usuários dos recursos de Tecnologia da Informação têm conhecimento sobre suas responsabilidades no uso dos serviços e equipamentos da Instituição?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
46	A CSTIC possui algum plano de análise de riscos e continuidade de negócios?	Não.
		Sim.
47	A CSTIC realiza auditoria com a finalidade de avaliar o sistema de Segurança da Informação existente?	Não.
		Sim.
48	A CSTIC do Campus possui reuniões periódicas com as outras CSTIC para troca de experiências e definição de novos projetos?	Não.
		Sim.
49	A CSTIC realiza cursos, palestras ou treinamentos sobre Segurança da Informação por recomendação ou patrocínio da DGTIC?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
50	A DGTIC orienta a CSTIC do Campus no uso dos recursos e serviços de Tecnologia da Informação?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
51	A DGTIC delega tarefas à CSTIC do Campus quando necessário?	Não.
		Sim.
52	A DGTIC interfere, se necessário, nas decisões da CSTIC do Campus?	Não.
		Sim.
53	A CSTIC possui plena conformidade nas decisões tomadas internamente?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
54	As decisões tomadas pela DGTIC que afetam a CSTIC do Campus são compreendidas plenamente por esta?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.

Tabela 1 – Questionário aplicado às CSTIC.

(conclusão)

55	As definições de Segurança da Informação da DGTIC são seguidas plenamente pela CSTIC do Campus?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
56	A DGTIC se reúne com a CSTIC do Campus para discutir entre outros assuntos a Segurança da Informação?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
57	A CSTIC do Campus tem liberdade para definir sua política de Segurança da Informação com base na sua realidade local?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.

Fonte: Elaboração do autor, 2017.

Abaixo temos o questionário aplicado à DGTIC:

Tabela 2 – Questionário aplicado à DGTIC.

(continua)

Item	Questão aplicada	Respostas possíveis
1	A DGTIC possui uma política de Segurança da Informação?	Não.
		Sim. Através de prática informal.
		Sim. Através de documentação formal.
2	Na DGTIC existe profissional responsável pela Segurança da Informação?	Não.
		Sim. Um profissional responsável.
		Sim. Todos são responsáveis.
3	São aplicados cursos, palestras ou treinamentos sobre Segurança da Informação na DGTIC?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
4	São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação à comunidade da Reitoria?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
5	A DGTIC tem conhecimento pleno das vulnerabilidades e ameaças à Segurança da Informação na Reitoria?	Não.
		Sim. Parcialmente.
		Sim. Plenamente.

Tabela 2 – Questionário aplicado à DGTIC.

(continuação)

6	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por acidentes naturais (tempestades, incêndios, etc.)?	Não.
		Sim. Poucas vezes.
		Sim. Muitas vezes.
7	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas no fornecimento de energia elétrica?	Não.
		Sim. Poucas vezes.
		Sim. Muitas vezes.
8	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por roubo de equipamentos ou erro humano?	Não.
		Sim.
9	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *hardware* local ou remoto?	Não.
		Sim.
10	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *software*?	Não.
		Sim.
11	Na sua opinião, a comunidade da Reitoria (funcionários e professores) têm conhecimento dos riscos de Segurança da Informação que podem estar sujeitos no cotidiano?	Não.
		Sim.
12	São aplicadas técnicas de segurança de acesso físico aos equipamentos de Tecnologia da Informação (Ex: Cadeados, alarmes, etc.)?	Não.
		Sim.
13	O acesso físico aos equipamentos de Tecnologia da Informação ocorre exclusivamente por funcionários da Instituição?	Não.
		Sim.
14	O acesso físico aos equipamentos de Tecnologia da Informação ocorre mediante autorização ou algum processo de autenticação?	Não.
		Sim.
15	São registradas ameaças ou ataques aos sistemas de Tecnologia da Informação da Instituição?	Não.
		Sim.
16	Após a ciência de ameaças ou ataques aos sistemas de Tecnologia da Informação são analisados os fatores que causaram ou propiciaram o evento?	Não.
		Sim. Eventualmente.
		Sim. Sempre.
17	Há sistemas (*sites*, aplicações, etc.) de acesso externo e/ou interno sem criptografia aplicada?	Não.
		Sim.
18	O gerenciamento de senhas de acesso ocorre mediante o uso de software específico?	Não.
		Sim.

Tabela 2 – Questionário aplicado à DGTIC.

(continuação)

19	As senhas de acesso são de conhecimento de todos os funcionários de Tecnologia da Informação?	Não.
		Sim.
20	Existe algum tipo de classificação ou definição para a geração de senhas de acesso?	Não.
		Sim.
21	As senhas de acesso aos sistemas de Tecnologia da Informação são atualizadas regularmente?	Não.
		Sim.
22	As senhas de acesso aos sistemas de Tecnologia da Informação são passíveis de memorização pelos funcionários de Tecnologia da Informação?	Não.
		Sim.
23	Existe conscientização para o sigilo de senhas de acesso aos funcionários de Tecnologia da Informação?	Não.
		Sim.
24	Existe conscientização para o sigilo de senhas de acesso aos usuários da Instituição?	Não.
		Sim.
25	As senhas de acesso aos sistemas de Tecnologia da Informação são divulgadas verbalmente?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
26	Existe algum tipo de mapeamento ou documentação sobre os pontos críticos relacionados à Segurança da Informação (acesso físico, sistemas online, funcionários autorizados, etc.)?	Não.
		Sim.
27	Existe na DGTIC algum controle efetivo na identificação de funcionários e/ou visitantes?	Não.
		Sim.
28	Existe na Instituição algum controle efetivo de entrada/saída de equipamentos?	Não.
		Sim.
29	A DGTIC está alinhada com a coordenação de recursos humanos para o gerenciamento de recursos e sistemas aos funcionários e/ou visitantes?	Não.
		Sim. Superficialmente.
		Sim. Totalmente.
30	O ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) possui organização e limpeza periódicas?	Não.
		Sim.
31	No ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) há algum tipo de manutenção preventiva?	Não.
		Sim.
32	Nos equipamentos de Tecnologia da Informação disponíveis aos usuários são realizadas manutenções preventivas e/ou corretivas?	Não.
		Sim.

Tabela 2 – Questionário aplicado à DGTIC.

(continuação)

33	Existe política formal para realização de *backups* de dados importantes da DGTIC?	Não.
		Sim.
34	A definição de aplicações de *softwares* para uso na DGTIC ocorre mediante análise e reunião entre os funcionários?	Não.
		Sim.
35	Em um processo de mudança, existe avaliação do impacto antes da implementação?	Não.
		Sim. Eventualmente.
		Sim. Sempre.
36	Os procedimentos operacionais da DGTIC são formalmente documentados?	Não.
		Sim.
37	São gerenciados os incidentes e requisições de Tecnologia da Informação na DGTIC?	Não.
		Sim.
38	A DGTIC utiliza *software* antivírus nos equipamentos de Tecnologia da Informação?	Não.
		Sim.
39	A DGTIC realiza o monitoramento das operações e comunicações de acordo com a legislação vigente?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
40	Os usuários dos sistemas de Tecnologia da Informação são devidamente identificados para o acesso aos recursos?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
41	São revisados regularmente os acessos atribuídos aos usuários dos serviços de Tecnologia da Informação?	Não.
		Sim.
42	A DGTIC dispõe de sistema de proteção contra quedas de energia elétrica?	Não.
		Sim.
43	A DGTIC dispõe de mecanismos de proteção contra incêndios?	Não.
		Sim.
44	A DGTIC possui controle formal e atualizado dos ativos de Tecnologia da Informação da Reitoria?	Não.
		Sim.

Tabela 2 – Questionário aplicado à DGTIC.

(conclusão)

45	Na sua opinião, os usuários dos recursos de Tecnologia da Informação têm conhecimento sobre suas responsabilidades no uso dos serviços e equipamentos da Instituição?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
46	A DGTIC possui algum plano de análise de riscos e continuidade de negócios?	Não.
		Sim.
47	São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação aos Campi subordinados?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
48	A DGTIC orienta as CSTIC dos Campi no uso dos recursos e serviços de Tecnologia da Informação?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
49	A DGTIC delega tarefas às CSTIC dos Campi quando necessário?	Não.
		Sim.
50	A DGTIC interfere, se necessário, nas decisões das CSTIC dos Campi?	Não.
		Sim.
51	A DGTIC possui plena conformidade nas decisões tomadas internamente?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
52	As decisões tomadas pela DGTIC que afetam as CSTIC dos Campi são compreendidas plenamente por estas?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
53	As definições de Segurança da Informação da DGTIC são seguidas plenamente pelas CSTIC dos Campi?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
54	A DGTIC reúne as CSTIC dos Campi para discutir entre outros assuntos a Segurança da Informação?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
55	As CSTIC dos Campi têm liberdade para definir sua política de Segurança da Informação com base na sua realidade local?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
56	A DGTIC realiza auditoria com a finalidade de avaliar o sistema de Segurança da Informação existente?	Não.
		Sim.
57	A DGTIC promove reuniões periódicas com as outras CSTIC para troca de experiências e definição de novos projetos?	Não.
		Sim.

Fonte: Elaboração do autor, 2017.

6.2.3 Resultados do questionário aplicado aos Campi

Nesta seção serão detalhadas as questões respondidas pelos campi e com isso destacar as respostas mais frequentes dentre as opções.

Convém observar que foi destacado em vermelho as escolhas em maior quantidade e apresentadas em percentual de modo a facilitar a compreensão.

Tabela 3 – Resultados coletados das CSTIC.

(continua)

Item	Questão aplicada	Resposta escolhida	%
1	A CSTIC possui uma política de Segurança da Informação?	Não.	20
		Sim. Através de prática informal.	**60**
		Sim. Através de documentação formal.	20
2	Na CSTIC existe profissional responsável pela Segurança da Informação?	**Não.**	**60**
		Sim. Um profissional responsável.	0
		Sim. Todos são responsáveis.	40
3	São aplicados cursos, palestras ou treinamentos sobre Segurança da Informação na CSTIC?	**Não.**	**80**
		Sim. Eventualmente.	20
		Sim. Regularmente.	0
4	São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação à comunidade do Campus?	**Não.**	**80**
		Sim. Eventualmente.	20
		Sim. Regularmente.	0
5	A CSTIC tem conhecimento pleno das vulnerabilidades e ameaças à Segurança da Informação no Campus?	Não.	20
		Sim. Parcialmente.	**80**
		Sim. Plenamente.	0
6	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por acidentes naturais (tempestades, incêndios, etc.)?	Não.	20
		Sim. Poucas vezes.	**40**
		Sim. Muitas vezes.	**40**
7	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas no fornecimento de energia elétrica?	Não.	20
		Sim. Poucas vezes.	**40**
		Sim. Muitas vezes.	**40**
8	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por roubo de equipamentos ou erro humano?	**Não.**	**80**
		Sim.	20

Tabela 3 – Resultados coletados das CSTIC.

(continuação)

9	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *hardware* local ou remoto?	Não.	20
		Sim.	**80**
10	A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *software*?	**Não.**	**60**
		Sim.	40
11	Na sua opinião, a comunidade do IFRJ (funcionários e professores) têm conhecimento dos riscos de Segurança da Informação que podem estar sujeitos no cotidiano?	**Não.**	**100**
		Sim.	0
12	São aplicadas técnicas de segurança de acesso físico aos equipamentos de Tecnologia da Informação (Ex: Cadeados, alarmes, etc.)?	**Não.**	**60**
		Sim.	40
13	O acesso físico aos equipamentos de Tecnologia da Informação ocorre exclusivamente por funcionários da Instituição?	**Não.**	**60**
		Sim.	40
14	O acesso físico aos equipamentos de Tecnologia da Informação ocorre mediante autorização ou algum processo de autenticação?	**Não.**	**60**
		Sim.	40
15	São registradas ameaças ou ataques aos sistemas de Tecnologia da Informação da Instituição?	**Não.**	**80**
		Sim.	20
16	Após a ciência de ameaças ou ataques aos sistemas de Tecnologia da Informação são analisados os fatores que causaram ou propiciaram o evento?	**Não.**	**60**
		Sim. Eventualmente.	20
		Sim. Sempre.	20
17	Há sistemas (*sites*, aplicações, etc.) de acesso externo e/ou interno sem criptografia aplicada?	Não.	40
		Sim.	**60**
18	O gerenciamento de senhas de acesso ocorre mediante o uso de *software* específico?	**Não.**	**60**
		Sim.	40
19	As senhas de acesso são de conhecimento de todos os funcionários de Tecnologia da Informação?	**Não.**	**20**
		Sim.	80
20	Existe algum tipo de classificação ou definição para a geração de senhas de acesso?	Não.	20
		Sim.	**80**
21	As senhas de acesso aos sistemas de Tecnologia da Informação são atualizadas regularmente?	**Não.**	**80**
		Sim.	20
22	As senhas de acesso aos sistemas de Tecnologia da Informação são passíveis de memorização pelos funcionários de Tecnologia da Informação?	Não.	0
		Sim.	**100**
23	Existe conscientização para o sigilo de senhas de acesso aos funcionários de Tecnologia da Informação?	Não.	0
		Sim.	**100**
24	Existe conscientização para o sigilo de senhas de acesso aos usuários da Instituição?	Não.	20
		Sim.	**80**

Tabela 3 – Resultados coletados das CSTIC.

(continuação)

25	As senhas de acesso aos sistemas de Tecnologia da Informação são divulgadas verbalmente?	**Não.**	**40**
		Sim. Eventualmente.	**40**
		Sim. Regularmente.	20
26	Existe algum tipo de mapeamento ou documentação sobre os pontos críticos relacionados à Segurança da Informação (acesso físico, sistemas online, funcionários autorizados, etc.)?	**Não.**	**100**
		Sim.	0
27	Existe na CSTIC algum controle efetivo na identificação de funcionários e/ou visitantes?	**Não.**	**60**
		Sim.	40
28	Existe na Instituição algum controle efetivo de entrada/saída de equipamentos?	Não.	40
		Sim.	**60**
29	A CSTIC está alinhada com a coordenação de recursos humanos para o gerenciamento de recursos e sistemas aos funcionários e/ou visitantes?	Não.	40
		Sim. Superficialmente.	**60**
		Sim. Totalmente.	0
30	O ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) possui organização e limpeza periódicos?	Não.	40
		Sim.	**60**
31	No ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) há algum tipo de manutenção preventiva?	**Não.**	**60**
		Sim.	40
32	Nos equipamentos de Tecnologia da Informação disponíveis aos usuários são realizadas manutenções preventivas e/ou corretivas?	Não.	20
		Sim.	**80**
33	Existe política formal para realização de *backups* de dados importantes da CSTIC?	**Não.**	**60**
		Sim.	40
34	A definição de aplicações de *softwares* para uso na CSTIC ocorre mediante análise e reunião entre os funcionários?	**Não.**	**60**
		Sim.	40
35	Em um processo de mudança, existe avaliação do impacto antes da implementação?	Não.	20
		Sim. Eventualmente.	**60**
		Sim. Sempre.	20
36	Os procedimentos operacionais da CSTIC são formalmente documentados?	**Não.**	**60**
		Sim.	40

Tabela 3 – Resultados coletados das CSTIC.

(continuação)

37	São gerenciados os incidentes e requisições de Tecnologia da Informação na CSTIC?	Não.	40
		Sim.	**60**
38	A CSTIC utiliza *software* antivírus nos equipamentos de Tecnologia da Informação?	Não.	0
		Sim.	**100**
39	A CSTIC realiza o monitoramento das operações e comunicações de acordo com a legislação vigente?	Não.	20
		Sim. Parcialmente.	**40**
		Sim. Totalmente.	**40**
40	Os usuários dos sistemas de Tecnologia da Informação são devidamente identificados para o acesso aos recursos?	Não.	0
		Sim. Parcialmente.	40
		Sim. Totalmente.	**60**
41	São revisados regularmente os acessos atribuídos aos usuários dos serviços de Tecnologia da Informação?	Não.	40
		Sim.	**60**
42	A CSTIC dispõe de sistema de proteção contra quedas de energia elétrica?	Não.	20
		Sim.	**80**
43	A CSTIC dispõe de mecanismos de proteção contra incêndios?	**Não.**	**60**
		Sim.	40
44	A CSTIC possui controle formal e atualizado dos ativos de Tecnologia da Informação da Instituição?	Não.	0
		Sim.	**100**
45	Na sua opinião, os usuários dos recursos de Tecnologia da Informação têm conhecimento sobre suas responsabilidades no uso dos serviços e equipamentos da Instituição?	**Não.**	**40**
		Sim. Parcialmente.	**40**
		Sim. Totalmente.	20
46	A CSTIC possui algum plano de análise de riscos e continuidade de negócios?	**Não.**	**100**
		Sim.	0
47	A CSTIC realiza auditoria com a finalidade de avaliar o sistema de Segurança da Informação existente?	**Não.**	**80**
		Sim.	20
48	A CSTIC do Campus possui reuniões periódicas com as outras CSTIC para troca de experiências e definição de novos projetos?	**Não.**	**80**
		Sim.	20
49	A CSTIC realiza cursos, palestras ou treinamentos sobre Segurança da Informação por recomendação ou patrocínio da DGTIC?	**Não.**	**80**
		Sim. Eventualmente.	20
		Sim. Regularmente.	0
50	A DGTIC orienta a CSTIC do Campus no uso dos recursos e serviços de Tecnologia da Informação?	Não.	20
		Sim. Eventualmente.	**40**
		Sim. Regularmente.	**40**
51	A DGTIC delega tarefas à CSTIC do Campus quando necessário?	Não.	0
		Sim.	**100**

Tabela 3 – Resultados coletados das CSTIC.

(conclusão)

52	A DGTIC interfere, se necessário, nas decisões da CSTIC do Campus?	Não.	40
		Sim.	**60**
53	A CSTIC possui plena conformidade nas decisões tomadas internamente?	Não.	0
		Sim. Parcialmente.	40
		Sim. Totalmente.	**60**
54	As decisões tomadas pela DGTIC que afetam a CSTIC do Campus são compreendidas plenamente por esta?	Não.	20
		Sim. Parcialmente.	**60**
		Sim. Totalmente.	20
55	As definições de Segurança da Informação da DGTIC são seguidas plenamente pela CSTIC do Campus?	Não.	0
		Sim. Parcialmente.	20
		Sim. Totalmente.	**80**
56	A DGTIC se reúne com a CSTIC do Campus para discutir entre outros assuntos a Segurança da Informação?	**Não.**	**100**
		Sim. Eventualmente.	0
		Sim. Regularmente.	0
57	A CSTIC do Campus tem liberdade para definir sua política de Segurança da Informação com base na sua realidade local?	**Não.**	**40**
		Sim. Parcialmente.	**40**
		Sim. Totalmente.	20

Fonte: Elaboração do autor, 2017.

6.2.4 Resultados do questionário aplicado à DGTIC

Nesta seção serão detalhadas as questões respondidas pela DGTIC e com isso destacar as respostas mais frequentes dentre as opções. Os gráficos em formato de pizza para estas questões foram inseridos no anexo deste trabalho para consulta.

Tabela 4 – Resultados coletados da DGTIC.

(continua)

Item	Questão aplicada	Resposta escolhida
1	A DGTIC possui uma política de Segurança da Informação?	Não.
		Sim. Através de prática informal.
		Sim. Através de documentação formal.
2	Na DGTIC existe profissional responsável pela Segurança da Informação?	Não.
		Sim. Um profissional responsável.
		Sim. Todos são responsáveis.

Tabela 4 – Resultados coletados da DGTIC.

(continuação)

3	São aplicados cursos, palestras ou treinamentos sobre Segurança da Informação na DGTIC?	**Não.**
		Sim. Eventualmente.
		Sim. Regularmente.
4	São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação à comunidade da Reitoria?	**Não.**
		Sim. Eventualmente.
		Sim. Regularmente.
5	A DGTIC tem conhecimento pleno das vulnerabilidades e ameaças à Segurança da Informação na Reitoria?	Não.
		Sim. Parcialmente.
		Sim. Plenamente.
6	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por acidentes naturais (tempestades, incêndios, etc.)?	Não.
		Sim. Poucas vezes.
		Sim. Muitas vezes.
7	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas no fornecimento de energia elétrica?	Não.
		Sim. Poucas vezes.
		Sim. Muitas vezes.
8	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por roubo de equipamentos ou erro humano?	**Não.**
		Sim.
9	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *hardware* local ou remoto?	Não.
		Sim.
10	A DGTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de *software*?	Não.
		Sim.
11	Na sua opinião, a comunidade da Reitoria (funcionários e professores) têm conhecimento dos riscos de Segurança da Informação que podem estar sujeitos no cotidiano?	Não.
		Sim.
12	São aplicadas técnicas de segurança de acesso físico aos equipamentos de Tecnologia da Informação (Ex: Cadeados, alarmes, etc.)?	Não.
		Sim.
13	O acesso físico aos equipamentos de Tecnologia da Informação ocorre exclusivamente por funcionários da Instituição?	Não.
		Sim.
14	O acesso físico aos equipamentos de Tecnologia da Informação ocorre mediante autorização ou algum processo de autenticação?	Não.
		Sim.

Tabela 4 – Resultados coletados da DGTIC.

(continuação)

15	São registradas ameaças ou ataques aos sistemas de Tecnologia da Informação da Instituição?	Não.
		Sim.
16	Após a ciência de ameaças ou ataques aos sistemas de Tecnologia da Informação são analisados os fatores que causaram ou propiciaram o evento?	Não.
		Sim. Eventualmente.
		Sim. Sempre.
17	Há sistemas (*sites*, aplicações, etc.) de acesso externo e/ou interno sem criptografia aplicada?	Não.
		Sim.
18	O gerenciamento de senhas de acesso ocorre mediante o uso de *software* específico?	**Não.**
		Sim.
19	As senhas de acesso são de conhecimento de todos os funcionários de Tecnologia da Informação?	**Não.**
		Sim.
20	Existe algum tipo de classificação ou definição para a geração de senhas de acesso?	Não.
		Sim.
21	As senhas de acesso aos sistemas de Tecnologia da Informação são atualizadas regularmente?	**Não.**
		Sim.
22	As senhas de acesso aos sistemas de Tecnologia da Informação são passíveis de memorização pelos funcionários de Tecnologia da Informação?	Não.
		Sim.
23	Existe conscientização para o sigilo de senhas de acesso aos funcionários de Tecnologia da Informação?	Não.
		Sim.
24	Existe conscientização para o sigilo de senhas de acesso aos usuários da Instituição?	Não.
		Sim.
25	As senhas de acesso aos sistemas de Tecnologia da Informação são divulgadas verbalmente?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
26	Existe algum tipo de mapeamento ou documentação sobre os pontos críticos relacionados à Segurança da Informação (acesso físico, sistemas online, funcionários autorizados, etc.)?	Não.
		Sim.
27	Existe na DGTIC algum controle efetivo na identificação de funcionários e/ou visitantes?	**Não.**
		Sim.

Tabela 4 – Resultados coletados da DGTIC.

(continuação)

28	Existe na Instituição algum controle efetivo de entrada/saída de equipamentos?	Não.
		Sim.
29	A DGTIC está alinhada com a coordenação de recursos humanos para o gerenciamento de recursos e sistemas aos funcionários e/ou visitantes?	Não.
		Sim. Superficialmente.
		Sim. Totalmente.
30	O ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) possui organização e limpeza periódicas?	Não.
		Sim.
31	No ambiente onde se localizam os equipamentos de processamento de dados (Centro de Processamento de Dados, Sala de Equipamentos, *Data Center*, etc.) há algum tipo de manutenção preventiva?	Não.
		Sim.
32	Nos equipamentos de Tecnologia da Informação disponíveis aos usuários são realizadas manutenções preventivas e/ou corretivas?	Não.
		Sim.
33	Existe política formal para realização de *backups* de dados importantes da DGTIC?	Não.
		Sim.
34	A definição de aplicações de *softwares* para uso na DGTIC ocorre mediante análise e reunião entre os funcionários?	Não.
		Sim.
35	Em um processo de mudança, existe avaliação do impacto antes da implementação?	Não.
		Sim. Eventualmente.
		Sim. Sempre.
36	Os procedimentos operacionais da DGTIC são formalmente documentados?	Não.
		Sim.
37	São gerenciados os incidentes e requisições de Tecnologia da Informação na DGTIC?	Não.
		Sim.
38	A DGTIC utiliza *software* antivírus nos equipamentos de Tecnologia da Informação?	Não.
		Sim.
39	A DGTIC realiza o monitoramento das operações e comunicações de acordo com a legislação vigente?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
40	Os usuários dos sistemas de Tecnologia da Informação são devidamente identificados para o acesso aos recursos?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
41	São revisados regularmente os acessos atribuídos aos usuários dos serviços de Tecnologia da Informação?	Não.
		Sim.

Tabela 4 – Resultados coletados da DGTIC.

(continuação)

42	A DGTIC dispõe de sistema de proteção contra quedas de energia elétrica?	Não.
		Sim.
43	A DGTIC dispõe de mecanismos de proteção contra incêndios?	Não.
		Sim.
44	A DGTIC possui controle formal e atualizado dos ativos de Tecnologia da Informação da Reitoria?	Não.
		Sim.
45	Na sua opinião, os usuários dos recursos de Tecnologia da Informação têm conhecimento sobre suas responsabilidades no uso dos serviços e equipamentos da Instituição?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
46	A DGTIC possui algum plano de análise de riscos e continuidade de negócios?	Não.
		Sim.
47	São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação aos Campi subordinados?	**Não.**
		Sim. Eventualmente.
		Sim. Regularmente.
48	A DGTIC orienta as CSTIC dos Campi no uso dos recursos e serviços de Tecnologia da Informação?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.
49	A DGTIC delega tarefas às CSTIC dos Campi quando necessário?	Não.
		Sim.
50	A DGTIC interfere, se necessário, nas decisões das CSTIC dos Campi?	Não.
		Sim.
51	A DGTIC possui plena conformidade nas decisões tomadas internamente?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
52	As decisões tomadas pela DGTIC que afetam as CSTIC dos Campi são compreendidas plenamente por estas?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
53	As definições de Segurança da Informação da DGTIC são seguidas plenamente pelas CSTIC dos Campi?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
54	A DGTIC reúne as CSTIC dos Campi para discutir entre outros assuntos a Segurança da Informação?	Não.
		Sim. Eventualmente.
		Sim. Regularmente.

Tabela 4 – Resultados coletados da DGTIC.

(conclusão)

55	As CSTIC dos Campi têm liberdade para definir sua política de Segurança da Informação com base na sua realidade local?	Não.
		Sim. Parcialmente.
		Sim. Totalmente.
56	A DGTIC realiza auditoria com a finalidade de avaliar o sistema de Segurança da Informação existente?	**Não.**
		Sim.
57	A DGTIC promove reuniões periódicas com as outras CSTIC para troca de experiências e definição de novos projetos?	Não.
		Sim.

Fonte: Elaboração do autor, 2017.

6.2.5 Análise dos resultados dos Campi

Algumas respostas se fazem importantes discutir neste trabalho, uma vez que não estão de acordo com uma política adequada de Segurança da Informação. Outros detalhes também serão destacados para se fazer entender algumas divergências com a DGTIC que, por suas atribuições e responsabilidades, não estão alinhadas com os campi subordinados.

Na questão 1, "*A CSTIC possui uma política de Segurança da Informação?* ", apesar de ter sido em sua maioria afirmativa, não corresponde ao desejado em uma instituição de ensino com milhares de usuários. É fundamental que um plano inicial seja desenvolvido de modo a se iniciar um delineamento das diretrizes básicas para a Segurança da Informação institucional.

Na questão 2, "*Na CSTIC existe profissional responsável pela Segurança da Informação?* ", é desejável que mesmo não havendo um profissional dedicado ao assunto, todos possam se responsabilizar em coordenar essas questões. Quando todos os profissionais se preocupam com a Segurança da Informação na instituição não será difícil implementar políticas e elaborar processos que facilitem o cumprimento de regras em favor da comunidade acadêmica.

Na questão 3, "*São aplicados cursos, palestras ou treinamentos sobre Segurança da Informação na CSTIC?* ", fica evidente que um esclarecimento sobre as questões inerentes à Segurança da Informação se torna necessário. É importante que todos os envolvidos com a TI dos campi estejam qualificados e cientes dos riscos com as informações e com os bens de comunicação.

Na questão 4, "*São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação à comunidade do Campus?* ", assim como a questão anterior, se faz necessário que a comunidade dos campi também tenha conhecimento dos riscos e deveres com o uso dos equipamentos de comunicação. Esse treinamento trará benefícios aos usuários da instituição e

espera-se que outros também sejam conscientizados através das relações sociais. Uma vez que os profissionais de TI não são capacitados adequadamente, entendemos que os usuários também serão afetados pelos serviços e orientações gerais sobre o uso e responsabilidades com a tecnologia.

Nas questões 6 e 7, "*A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por acidentes naturais (tempestades, incêndios, etc.)?* " e "*A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas no fornecimento de energia elétrica?* ", observa-se certa vulnerabilidade quanto os fenômenos naturais que interferem no pleno funcionamento dos serviços da instituição. É recomendável que seja realizada vistorias técnicas com profissionais capacitados para reduzir ao mínimo os riscos e impactos com as possíveis interrupções dos serviços.

Na questão 9, "*A CSTIC já teve interrupção dos serviços de Tecnologia da Informação causados por falhas de hardware local ou remoto?* ", observa-se que grande parte dos entrevistados afirmam que houve problemas com interrupção. Como a questão não objetivava discriminar os motivos principais que determinava o evento, podemos entender que se torna necessário o acompanhamento dos equipamentos participantes das comunicações de dados da instituição. Para isso, recomenda-se a realização de manutenções preventivas, de modo a reduzir as chances de um incidente prejudicar os serviços ativos. Ao mesmo tempo, é recomendável que os incidentes sejam devidamente documentados e analisados para prevenir possíveis erros no futuro.

Na questão 11, "*Na sua opinião, a comunidade do IFRJ (funcionários e professores) têm conhecimento dos riscos de Segurança da Informação que podem estar sujeitos no cotidiano?* ", observamos que as CSTIC não acreditam no conhecimento relacionado à Segurança da Informação da comunidade acadêmica. Desse modo, podemos inferir que não há conscientização, palestras, cursos, etc., que altere a visão dos coordenadores de TI. Podemos também observar que não há iniciativa das CSTIC em alterar esse cenário observado de desconhecimento dos riscos de Segurança da Informação.

Na questão 12, "*São aplicadas técnicas de segurança de acesso físico aos equipamentos de Tecnologia da Informação (Ex: Cadeados, alarmes, etc)?* ", não há em sua maioria a aplicação de técnicas que proteja o acesso físico aos equipamentos institucionais de pessoas sem autorização. Isso deve ser uma preocupação para as equipes de TI pois um intruso pode comprometer a infraestrutura de dados por diversas intenções e a recuperação do desastre pode não ser tão rápida como desejado.

Na questão 14, "*O acesso físico aos equipamentos de Tecnologia da Informação ocorre mediante autorização ou algum processo de autenticação?* ", há relação também com a questão 12. Se não existir um processo formal de registro de autenticação ou para acesso aos

equipamentos, não há como saber inicialmente se um possível incidente ocorreu por um usuário indevido ou por erros de *software*. Ter registros de acesso permite avaliar os responsáveis e manter a segurança dos equipamentos.

Nas questões 15 e 16, "*São registradas ameaças ou ataques aos sistemas de Tecnologia da Informação da Instituição?* " e "*Após a ciência de ameaças ou ataques aos sistemas de Tecnologia da Informação são analisados os fatores que causaram ou propiciaram o evento?* ", vemos que não existe uma preocupação com as ameaças e ataques que ocorrem nos sistemas de TI na instituição. Podemos considerar preocupante esse modo de agir das CSTIC uma vez que não se busca verificar o que causou o incidente. Não havendo a análise dos eventos causadores e, por conseguinte a sua correção, os sistemas de TI continuarão sujeitos aos mesmos eventos. Não é desejado que uma ameaça ou ataque ocorra novamente e as CSTIC devem tratar com seriedade esse assunto para não expor dados privados a intrusos.

Na questão 18, "*O gerenciamento de senhas de acesso ocorre mediante o uso de software específico?* ", observa-se que de algum modo as senhas de acesso aos sistemas da instituição são armazenadas. É importante compreender que o armazenamento de senhas de acesso em sistemas simples como papel, documento de texto no computador ou outro meio simples, pode comprometer a segurança dos sistemas. É recomendável que as senhas de acesso sejam armazenadas em sistemas seguros e com criptografia.

Na questão 21, "*As senhas de acesso aos sistemas de Tecnologia da Informação são atualizadas regularmente?* ", temos que a grande maioria das coordenações afirmam que suas senhas não são atualizadas com regularidade. Ainda com relação à questão 18, o uso de aplicações de *software* para o armazenamento seguro de senhas de acesso permite na maioria dos casos a redefinição de senhas facilmente. Como podemos observar, a retenção de senhas de acesso é um grande risco à Segurança da Informação pois funcionários e/ou estagiários, ao deixarem a CSTIC ainda terão conhecimento de informações privilegiadas. É recomendável que haja uma política onde inclua a renovação periódica de senhas e que estas sejam seguramente armazenadas "fora" da cabeça dos seus usuários.

Na questão 25, "*As senhas de acesso aos sistemas de Tecnologia da Informação são divulgadas verbalmente?* ", temos certamente um erro comum em muitas organizações: expor verbalmente dados sigilosos. Isso, de fato é um grave hábito que muitas vezes não é percebido pelo praticante. Deve-se criar uma rotina, com base nos funcionários autorizados, a ter acesso a alguma aplicação de armazenamento de senhas, de modo que não seja divulgada as senhas verbalmente. Deve-se também ter em mente que um usuário sem autorização pode ouvir o "código secreto" e com isso se aproveitar do privilégio e possivelmente obter informações confidenciais.

Na questão 27, "*Existe na CSTIC algum controle efetivo na identificação de funcionários e/ou visitantes?* ", apesar de não haver um controle efetivo por parte da CSTIC, esta também poderá definir regras junto às Diretorias e equipe de segurança institucional que viabilizem o registro e controle de funcionários e pessoas externas à instituição. No caso da questão, buscou-se o entendimento do controle de usuários que de algum modo precisam usufruir dos serviços ou equipamentos de TI nos campi.

Na questão 29, "*A CSTIC está alinhada com a coordenação de recursos humanos para o gerenciamento de recursos e sistemas aos funcionários e/ou visitantes?* ", apesar de ser positiva a resposta, é sempre fundamental estreitar os laços com a coordenação de recursos humanos através de uma boa comunicação e diretrizes. Quando ambas as coordenações estão alinhadas, o controle de funcionários e os serviços disponibilizados, podem ser melhor gerenciados, proporcionando assim uma maior fluidez e satisfação dos usuários.

Na questão 33, "*Existe política formal para realização de backups de dados importantes da CSTIC?* ", poucos responderam haver uma política para a cópia de dados importantes da instituição. Tendo como base as respostas anteriores onde não há considerável estabilidade elétrica, uma interrupção de energia pode corromper e até danificar os meios de armazenamento de dados. Essas perdas devem ser consideradas e avaliadas e sem dúvida, uma ação para resguardar as informações precisa ser posta em prática.

Levando em consideração que muitas informações da instituição são de interesse público, a perda destas pode causar sérios transtornos e prejudicar a visão da comunidade sobre a instituição.

Na questão 34, "*A definição de aplicações de softwares para uso na CSTIC ocorre mediante análise e reunião entre os funcionários?* ", grande parte das respostas das CSTIC não ocorrem após uma reunião ou acordo entre seus membros. Isso não é benéfico aos funcionários de TI pois a troca de experiências profissionais sempre é favorável ao crescimento das coordenações. Quando uma decisão é tomada sem a prévia consulta e análise dos seus colaboradores, podem ser geradas insatisfações e diminuição na qualidade dos serviços prestados. Ao mesmo tempo, uma prévia avaliação pode ser vital para evitar um problema no futuro.

Na questão 36, "*Os procedimentos operacionais da CSTIC são formalmente documentados?* ", temos um caso comum a muitas organizações e que afeta não apenas a área de Tecnologia da Informação. Não se espera que uma coordenação retenha todo o seu conhecimento de modo tácito, mas que documente e oriente os funcionários a fazerem o mesmo. São muitos os aspectos que propiciam este comportamento, mas o desejado é que os procedimentos e conhecimentos sejam reutilizados por todos os envolvidos mesmo quando houver a saída de um funcionário. Quando uma organização não atua para transformar o conhecimento tácito em explícito ela estará colocando em risco seu maior patrimônio que é o conhecimento.

Na questão 37, "*São gerenciados os incidentes e requisições de Tecnologia da Informação na CSTIC?* ", ainda temos campi sem o gerenciamento dos incidentes que ocorrem na instituição. São grandes as preocupações que geram a partir disso, como a falta de uma visão global das necessidades de TI, os problemas que precisam ser quantificados e analisados, o gerenciamento das tarefas e projetos de TI, etc. É interessante destacar que todas as CSTIC possuem autorização para utilizar um sistema de gerenciamento de tarefas, projetos e ativos de TI, mas nesta pesquisa poucos são adeptos ao uso desta aplicação. Cabem às CSTIC, que ainda não adotaram este gerenciamento, o contato com a DGTIC para uma possível orientação e treinamento adequado.

Na questão 43, "*A CSTIC dispõe de mecanismos de proteção contra incêndios?* ", é de fundamental importância que as CSTIC manifestem preocupação com a segurança física dos funcionários e com os equipamentos de TI. Uma vez que todas as CSTIC possuem uma padronização tecnológica adotada pela DGTIC, não é seguro manter equipamentos de grande valor e com funcionamento ininterrupto sem uma correta proteção, de modo a evitar possíveis danos causados por incêndio.

Na questão 45, "*Na sua opinião, os usuários dos recursos de Tecnologia da Informação têm conhecimento sobre suas responsabilidades no uso dos serviços e equipamentos da Instituição?* ", compete às CSTIC orientar e propor treinamento aos usuários dos serviços de Tecnologia da Informação. Quando os usuários estão capacitados e conscientes das suas responsabilidades, fica mais fácil propor melhorias aos sistemas existentes. Da mesma forma, considerando os usuários finais como um elo fraco à Segurança da Informação, quanto mais capacitados e preocupados com os riscos e ameaças existentes, melhor será a segurança institucional.

Nas questões 48 e 56, "*A CSTIC do Campus possui reuniões periódicas com as outras CSTIC para troca de experiências e definição de novos projetos?* " e "*A DGTIC se reúne com a CSTIC do Campus para discutir entre outros assuntos a Segurança da Informação?* ", percebemos um grande distanciamento entre as CSTIC dos campi e a DGTIC quanto ao relacionamento e comunicação. É fundamental que as coordenações discutam seus processos e troquem experiências vividas no cotidiano pois nem todos os campi possuem as mesmas atividades. É importante um maior contato entre toda a equipe de TI, de modo a reduzir as diferenças nos procedimentos e visões dos processos, buscando maior convergência de conhecimento.

Verificando que sob o ponto de vista das CSTIC quanto a ausência de reuniões propostas pela DGTIC, fica claro que novas definições, processos e ações ocorrem impessoalmente. Deve ser posto em prática reuniões periódicas para tratar do desenvolvimento e aperfeiçoamento dos serviços e planos estratégicos de TI entre as CSTIC e DGTIC.

6.2.6 Análise dos resultados da DGTIC

Com base na Tabela 4, pode-se observar que a DGTIC está mais alinhada com as questões sobre a Segurança da Informação se comparada às CSTIC. Sendo assim, tendo a Tabela 3 sido analisada na seção anterior, será confrontado algumas questões no que diz respeito a ambas entidades.

Na questão 47, "*São ministrados cursos, palestras ou treinamentos sobre Segurança da Informação aos Campi subordinados?* ", não há uma iniciativa pela DGTIC em propor treinamento e qualificação aos coordenadores de TI dos campi. O mesmo pôde ser confirmado na questão 49 feita às CSTIC.

É desejado que a DGTIC também incentive e promova a qualificação dos campi subordinados, uma vez que muitas atribuições são delegadas a estes. Isso propiciará maior produtividade aos coordenadores e melhor fluidez nas ações estratégicas da TI. Ao mesmo tempo, essa mudança comportamental também deve ser motivada pelos campi, de modo a definir novas diretrizes e independência em algumas ações, permitindo que haja institucionalmente maior sinergia entre a equipe de TI.

Na questão 48, "*A DGTIC orienta as CSTIC dos Campi no uso dos recursos e serviços de Tecnologia da Informação?* ", obtivemos uma afirmativa pela DGTIC, mas o mesmo não pôde ser confirmado pelas CSTIC na questão 50 onde houve uma afirmativa variável. De qualquer modo, é fundamental que essa interação seja constante e construtiva para que o ambiente institucional seja promissor e colaborativo. Tendo em vista que a DGTIC possui melhor compreensão sobre a Segurança da Informação, sem dúvida será importante sua participação na comunicação e orientações às unidades menores.

Nas questões 49 e 50, "*A DGTIC delega tarefas às CSTIC dos Campi quando necessário?* " e "*A DGTIC interfere, se necessário, nas decisões das CSTIC dos Campi?* ", temos exemplos de interação entre Diretoria e Coordenação. Essa interação, no caso, através de delegação de tarefas, demonstra um envolvimento benéfico a ambas as entidades. É através desse processo que as CSTIC podem adquirir conhecimento e propor mudanças se necessário, mas deve-se ter em mente que é indispensável a troca de experiências e propostas em reuniões bem definidas.

Na questão 54, "*A DGTIC reúne as CSTIC dos Campi para discutir entre outros assuntos a Segurança da Informação?* ", temos uma divergência se comparada com a questão 56 feita às CSTIC. No primeiro caso, é afirmado que ocorrem reuniões eventuais e no segundo, de forma unânime, não temos essa afirmativa. Partindo do fato que apenas 5 campi participaram da pesquisa, percebemos que nem todos possuem interação com a DGTIC como desejado.

Nesse ponto, mais uma vez, a prática de reuniões para discussão e propostas são fundamentais para estreitar os laços entre os campi.

Na questão 57, "*A DGTIC promove reuniões periódicas com as outras CSTIC para troca de experiências e definição de novos projetos?* ", a DGTIC afirma que promove reuniões periódicas, mas em contraste com a questão 56 feita às CSTIC não temos essa afirmação. Percebemos então que há algumas divergências entre as entidades, podendo, conforme já citado, que alguns campi não participem das reuniões promovidas pela DGTIC. De qualquer forma, uma boa comunicação e interação com as unidades menores se faz necessário para garantir a qualidade nos serviços prestados a toda a comunidade acadêmica da instituição.

7 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

7.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

Com base no Estudo de Caso aplicado em formato de questionário às Coordenações de Suporte de Tecnologia da Informação e Comunicação e à Diretoria de Gestão de Tecnologia da Informação e Comunicação, podemos compreender algumas divergências de opiniões mas ao mesmo tempo muitas ações estão alinhadas corretamente. Foi possível observar que uma efetiva comunicação entre as CSTIC e DGTIC precisa acontecer para reduzir as diferenças operacionais e estratégicas visto que na instituição objetiva-se uma conformidade e excelência profissional.

Uma política para a gestão da Segurança da Informação se faz necessária em ambas as entidades pois é possível observar que alguns aspectos cruciais não são considerados e isso pode ser um fator grave a longo prazo. É desejável que a DGTIC estabeleça diretrizes para uma política sólida e de acordo com todos os campi subordinados.

Conforme foi exposto, não ocorrem cursos e treinamentos para a capacitação da equipe técnica e de sua comunidade acadêmica. Isso propicia uma defasagem de conhecimento técnico uma vez que o campo tecnológico sofre constantes transformações. É desejável que os profissionais estejam qualificados e sejam submetidos a constantes avaliações para que o desempenho e produtividade sejam constantes. Ao mesmo tempo, os usuários dos serviços de Tecnologia da Informação precisam ter conhecimento, sejam através de cursos, palestras ou mesmo eventos, dos riscos e ameaças à Segurança da Informação. Além disso, a conscientização no uso dos equipamentos e sistemas favorece à comunidade, uma vez que a segurança na instituição pode ser melhorada.

Diferentemente da DGTIC, as CSTIC estão mais vulneráveis às ameaças naturais. As consequências podem ser desastrosas se não forem corrigidas. Conforme pôde ser observado, as frequentes quedas de energia, ausência de cópias de segurança de dados e um sistema de combate a incêndios ineficiente, são ingredientes perigosos à proteção da informação institucional. A partir disso, espera-se que haja maior preocupação com essas questões pois são fundamentais em uma instituição de ensino.

Foi visto também que não existe uma política de gerenciamento de senhas, ficando essas obsoletas e sujeitas a serem usadas por ex-funcionários ou mesmo intrusos.

É importante que as CSTIC e DGTIC criem mecanismos para o gerenciamento dos acessos por senhas através de alguma aplicação de *software*. A atualização lenta dessas senhas, passíveis de serem memorizadas, certamente compromete grande parte dos acessos lógicos aos sistemas.

Por fim, o questionário se mostra útil para analisarmos as opiniões de diversos coordenadores de TI e percebemos que a implementação de uma política eficiente de Segurança da Informação é indispensável para a correção de comportamentos e práticas das entidades avaliadas.

7.2 RESULTADOS ESPERADOS

Com o presente estudo espera-se apresentar a proposta às CSTIC e à DGTIC de modo a promover uma discussão sobre novas possibilidades de melhorias na segurança institucional. Sendo assim, o primeiro campus a ser submetido a uma avaliação interna de Segurança da Informação será o campus Rio de Janeiro, atualmente um dos mais ativos e mais próximos da DGTIC.

Espera-se também que este trabalho seja fundamental para esclarecer as principais dúvidas antes observadas internamente na instituição e que se torne eficaz nas reflexões e atividades cotidianas das coordenações.

Por fim, este Estudo de Caso busca contribuir com os serviços técnicos e gerenciais em atividades na instituição, para que a qualidade e excelência profissional seja mantida, uma vez que, como instituição pública de ensino, a comunidade acadêmica deverá o foco constante do empenho da TI.

7.3 VIABILIDADE DA PROPOSTA

A reunião com as equipes de TI se faz necessário para a exposição dos problemas e propostas de solução. Conforme pôde ser visto neste estudo, muitas ações e visões ainda são divergentes e a discussão com as CSTIC e DGTIC trará muitos benefícios à instituição.

É desejável acima de tudo que a proposta para um esboço das diretrizes de Segurança da Informação ocorra nas periódicas reuniões entre as entidades. Foi possível observar que a falta de comunicação é um dos fatores de distanciamento e desentendimentos entre as CSTIC e DGTIC.

Considerando viável a proposta deste trabalho, pode ser observado que não há indícios de impedimentos na sua implementação institucional. Uma vez que as coordenações precisam se qualificar, melhorar suas ações e interagir mais, ficará mais fácil iniciar as mudanças necessárias conforme a demanda de cada campus. Com isso, com uma comunicação participativa e produtividade, todas as equipes terão maior sinergia e como resultado, haverá maior conformidade e entendimento com as estratégias de TI.

8 CONSIDERAÇÕES FINAIS

Este Estudo de Caso buscou analisar as principais questões de Segurança da Informação envolvendo as coordenações de Tecnologia da Informação dos campi do Instituto Federal de Educação, Ciência e Tecnologia do Rio de Janeiro e a Diretoria de Gestão de Tecnologia da Informação e Comunicação, localizada na Reitoria. Nessa análise, foi possível constatar algumas divergências, mas que serão sanadas com reuniões para a discussão e implementação de melhorias.

Apesar do tempo curto para sua elaboração, muito trabalho foi realizado para se chegar em um nível desejado. Este trabalho permitiu uma nova forma de analisar questões antes informais na instituição e com isso, será uma peça importante em estudos acadêmicos a serem desenvolvidos.

REFERÊNCIAS

AMATTE, Fernando Pompeo e PEIXINHO, Ivo de Carvalho. **Introdução a segurança de redes**. 1. ed. Rio de Janeiro: Escola Superior de Redes, 2013.

BRASIL, Comitê Gestor da Internet no. **Cartilha de segurança para internet versão 4.0**. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil – CGI.BR, 2012.

CASSA, Mônica. **A importância e a implementação da segurança da informação no âmbito das atividades de negócios**. Disponível em: <http://www.techoje.com.br/site/techoje/categoria/detalhe_artigo/221>. Acesso em: 17 set. 2017.

CAVALCANTI, Marcelo e MOREIRA, Enzo. **Metodologia de estudo de caso**: livro didático. 3. ed. rev. e atual. Palhoça: UnisulVirtual, 2008.

COELHO, Flavia Estélia Silva. **Gestão da segurança da informação: NBR 27001 e NBR 27002**. 1. ed. Rio de Janeiro: Escola Superior de Redes, 2011.

FONTES, Edison Luiz Gonçalves. **Políticas de segurança da informação**. 1. ed. Rio de Janeiro: Escola Superior de Redes, 2014.

GARCIA, R. M. (1980). Abordagem Sócio-Técnica: Uma rápida avaliação. *Revista de Administração de Empresas*, 20(3), 71-77. Disponível em: <http://www.scielo.br/pdf/rae/v20n3/v20n3a06.pdf>. Acesso em: 15 set. 2017.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO DE JANEIRO. **Prestação de Contas Ordinárias Anual. Relatório de Gestão do Exercício de 2015**. Disponível em: <http://www.ifrj.edu.br/sites/default/files/webfm/images/RelatorioGestao%20TCU.pdf>. Acesso em: 07 out. 2017.

_____. **Regimento Geral do IFRJ**. Disponível em: <http://www.ifrj.edu.br/sites/default/files/webfm/images/REGIMENTO%20GERAL%20IFRJ.pdf>. Acesso em: 14 out. 2017.

_____. **Relatório de Avaliação e-MEC/INEP**. Disponível em: <http://www.ifrj.edu.br/sites/default/files/webfm/images/Recredenciamento_%20Rel-Avaliadores_INEP.pdf>. Acesso em: 13 out. 2017.

_____. **Visão e Missão**. Disponível em: <http://www.ifrj.edu.br/instituicao/visao-e-missao>. Acesso em: 13 out. 2017.

KINJO, Jacqueline. **Trabalho de G.E. – Taylor e Abordagem Sociotécnica**. Disponível em: <https://prezi.com/xebb14g8mano/trabalho-de-ge-taylor-e-abordagem-sociotecnica/>. Acesso em: 25 mar. 2014.

LENTO, Luiz Otávio Botelho. **Segurança da Informação**. 3. ed. Palhoça: UnisulVirtual, 2011.

LOHN, Joel Irineu. **Metodologia para elaboração e aplicação de projetos**: livro didático. 2 ed. rev. e atual. Palhoça: Unisul Virtual, 2005. 100 p.

MACHADO, Cristiane Salvan et al. **Trabalhos acadêmicos na Unisul**: apresentação gráfica. 2. ed. rev. e atual. Palhoça: Ed. Unisul, 2013.

MOREIRA, Ademilson. **A importância da segurança da informação**. Disponível em: <https://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao>. Acesso em: 23 jun. 2013.

MULBERT, Ana Luíza e AYRES, Nilce Miranda. **Fundamentos para Sistemas de Informação**. 3. ed. Palhoça: UnisulVirtual, 2010.

RAUEN, Fábio José. **Roteiros de investigação científica**. Tubarão: Unisul, 2002.

SISTEMA. In: WIKIPÉDIA, a enciclopédia livre. Flórida: Wikimedia Foundation, 2017. Disponível em: <https://pt.wikipedia.org/w/index.php?title=Sistema&oldid=50271861>. Acesso em: 15 nov. 2017.