INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

GILLYANE MEDEIROS

# GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO DOS INSTITUTOS FEDERAIS DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA.

NATAL-RN
2016

GILLYANE MEDEIROS

# GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO DOS INSTITUTOS FEDERAIS DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA.

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Redes de Computadores.

Orientador: Prof. M.Sc.Francisco Sales de Lima Filho.

NATAL-RN
2016

M488g Medeiros, Gillyane.
Gestão de segurança da informação : um estudo de caso dos Institutos Federais de Educação, Ciência e Tecnologia / Gillyane Medeiros. – 2016.
46 f. ; il.

Orientador: Prof. Me. Francisco Sales de Lima Filho.
Trabalho de Conclusão de Curso (Tecnologia em Rede de Computadores) — Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, 2016.

1. Segurança da informação - Gestão. 2. Instituto Federal de Educação, Ciência e Tecnologia. 3. NBR ISO 27001. I. Lima Filho, Francisco Sales de. II. Título.

CDU 004.7

Ficha elaborada pelo Setor de Informação e Referência da Biblioteca Sebastião Fernandes do IFRN.

GILLYANE MEDEIROS

# GESTÃO DE SEGURANÇA DA INFORMAÇÃO: UM ESTUDO DE CASO DOS INSTITUTOS FEDERAIS DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA.

Trabalho de Conclusão de Curso apresentado ao Curso Superior de Tecnologia em Redes de Computadores do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Redes de Computadores.

Trabalho de Conclusão de Curso apresentado em 10/03/2016, pela seguinte Banca Examinadora:

BANCA EXAMINADORA

_____

Prof. M.Sc. Francisco Sales de Lima Filho – Orientador
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

_____

Prof. M.Sc. Alex Fabiano de Araújo Furtunato
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

_____

Prof. M.Sc. Galileu Batista de Sousa
Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte

*Dedico todo esse trabalho a Jackson Bezerra Ferreira, meu amado esposo, que acompanhou de perto minhas dificuldades e apoiou nos momentos mais difíceis, me incentivando a prosseguir mesmo nos momentos mais duros da jornada.*

## AGRADECIMENTOS

Agradeço a meu Deus por nunca ter me desamparado, mostrando sempre Sua presença ao meu lado, me protegendo e ajudando a superar as adversidades da vida, enfrentando os desafios.

Em seguida, agradeço a minha mãe por nunca desistir de seus filhos, por ter me ensinado os valores da educação e do amor, e nos momentos de tristeza ter ensinado a olhar pra frente com um sorriso no rosto e a alegria no coração. Ao meu pai, que enquanto em vida, me mostrou com seu exemplo como vencer os obstáculos da vida. E aos meus irmãos que sempre estão ao meu lado em qualquer situação.

Agradeço aos meus colegas de turma que principalmente na reta final do curso, deram as mãos motivando uns aos outros para a sua conclusão, partilhando conhecimentos em quaisquer atividades.

Aos professores do Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte (IFRN) que mostraram quais as direções corretas a tomar, compartilhando seus conhecimentos e experiências.

Ao Professor Sales Filho, por ser meu orientador, por sua disponibilidade e paciência durante todo o trabalho, colaborando de forma muito significativa para a conclusão deste curso.

Por fim, agradeço ao meu afetuoso esposo, Jackson, que soube me entender e me ajudou a superar os desafios, me motivando nos momentos em que parecia não me haver mais forças. Agradeço muito a Deus por ter colocado ele em minha vida.

**SUMÁRIO**

## LISTA DE SIGLAS E ABREVIATURAS

| | |
|---|---|
| GSI | Gestão de Segurança da Informação |
| GTI | Gestão da Tecnologia da Informação |
| IFRN | Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte |
| ISO | *International Organization for Standarzation* |
| MEC | Ministério da Educação |
| PDTI | Plano Diretor de Tecnologia da Informação |
| SGSI | Sistema de Gestão de Segurança da Informação |
| SI | Segurança da Informação |

## LISTA DE ILUSTRAÇÕES

## LISTA DE TABELAS

## RESUMO

Este trabalho de conclusão de curso foi realizado no Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte, com o intuito de verificar o panorama atual da gestão da segurança da informação nos Institutos Federais de Educação e em seguida, avaliar a conformidade do IFRN com a norma ABNT NBR ISO 27001 Anexo A. Para este estudo foram utilizados questionários simplificados específicos, enviados aos gestores de tecnologia da informação dos institutos, seguido da análise destes dados coletados. Constam também no presente trabalho, outras informações sobre os Institutos Federais, como sua história e gestão. Espera-se com isso, proporcionar um comparativo, de forma não exaustiva, da gestão da segurança da informação do Instituto Federal do Rio Grande do Norte em relação aos demais Institutos Federais de Educação, bem como apresentar a conformidade do IFRN com a norma ISO 27001 Anexo A.



Palavras-chave: Gestão da segurança da informação. Institutos Federais de Educação, Ciência e Tecnologia. Norma NBR ISO 27001 Anexo A.

## ABSTRACT

This is the final paper made in the Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte in order to verify the current situation of information security management in the federal education institutes and then evaluate the conformity of the IFRN with the Standard ABNT NBR ISO 27001 Annex A. In this study were used specific and simplified questionnaires, sent to the information technology managers of the federal institutes, followed by analysis of the collected data. There is also included in this paper other informations about the federal institutes, like its history and administration. The aim of this paper is to provide a comparative of the information security management, in a not tiring way, between the Instituto Federal do Rio Grande do Norte and the others federal institutes, and also to present the IFRN's conformity with the Standard ABNT NBR ISO 27001 Annex A.



Keywords: Information security management. Institutos Federais de Educação, Ciência e Tecnologia. Standard ABNT NBR ISO 27001 Annex A.

# 1 INTRODUÇÃO

Atualmente, com o crescimento e evolução das tecnologias, a informação passou a estar por toda a parte, impressa ou digital, sendo um grande diferencial nos negócios, necessitando de proteção.

O Instituto Federal está dentre estes negócios, onde a informação possui grande valia. Portanto, para que esta informação seja protegida, é necessária uma gestão adequada e planejada, que possua critérios de segurança da informação em conformidade com as leis e regulamentos vigentes.

Neste trabalho, será apresentado o panorama atual da gestão da segurança da informação nos Institutos Federais de Educação, Ciência e Tecnologia, suas dificuldades e desafios, bem como será identificada, através de um procedimento não exaustivo, a conformidade do IFRN com a norma NBR ISO 27001 Anexo A.

## 1.1 OBJETIVOS

Este trabalho tem como objetivo recolher informações sobre a gestão da segurança da informação, através de revisão bibliográfica, em seguida, realizar um estudo direcionado sobre o panorama da gestão da segurança da informação nos Institutos Federais de Educação, Ciência e Tecnologia. Logo depois, avaliar a situação do Instituto Federal do Rio Grande do Norte em relação à conformidade com a norma NBR ISO 27001 Anexo A, anexo normativo.

### 1.1.1 Objetivo Geral

Coletar, identificar e apresentar as condições atuais da gestão da segurança da informação nos Institutos Federais de Educação e, especialmente do Instituto Federal do Rio Grande do Norte, bem como apresentar de forma comparativa a situação do IFRN perante as demais Instituições do Brasil, mostrando também a sua adequação à norma NBR ISO 27001 Anexo A.

### 1.1.2 Objetivos Específicos

Realizar um mapeamento quanto à adoção das boas práticas de gestão da segurança da informação nos Institutos Federais de Educação através da análise de dados coletados por meio de pesquisa eletrônica feita pela internet, enviada a gestores de tecnologia da informação destes institutos em todo o Brasil.

Constatar, de forma generalista, a conformidade do Instituto Federal de Educação do Rio Grande do Norte com a norma NBR ISO 27001 Anexo A, através de questionários aplicados a gestores da área de Tecnologia da Informação nos campi do Rio Grande do Norte.

## 1.2 ESTRUTURA DO TRABALHO

O capítulo 2 começa fazendo uma contextualização teórica sobre a gestão da segurança da informação, apresentando conceitos, definições, características e requisitos.

A seguir, no capítulo 3, será exibido um breve histórico dos Institutos Federais de Educação, Ciência e Tecnologia; a gestão organizacional e a gestão da segurança da informação nestes institutos.

No capítulo 4 serão apresentados e discutidos os dados sobre a gestão da segurança da informação nos institutos federais no sentido amplo, bem como uma avaliação específica de conformidade do IFRN com a NBR ISO 27001 Anexo A, através de questionários simplificados.

Por fim, no capítulo 5, serão elencadas as considerações finais deste trabalho, contendo a conclusão da situação da gestão da segurança da informação nos Institutos Federais de Educação, Ciência e Tecnologia, sendo apresentadas algumas sugestões e recomendações para eventuais trabalhos futuros.

# 2 REFERENCIAL TEÓRICO

Atualmente, as informações estão por toda a parte: impressas, escritas, digitalizadas, em ondas no ar; estas informações podem ser capturadas a todo instante e de forma indetectável.

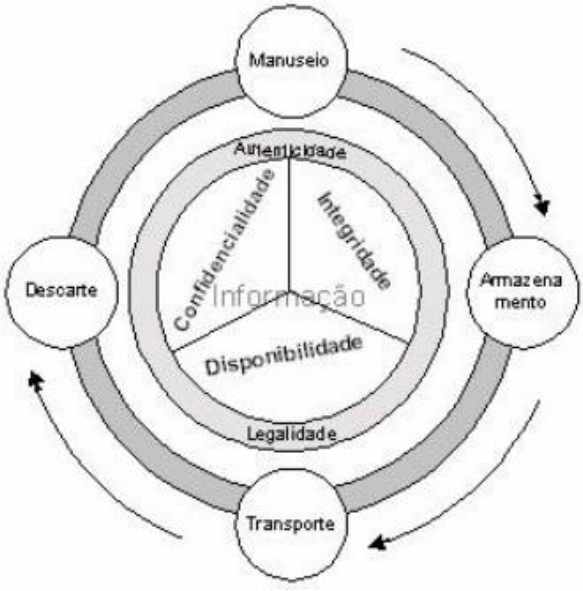
As informações são importantes para o desenvolvimento de qualquer instituição, neste sentido, Sêmola (2003) afirma que “A informação representa a inteligência competitiva dos negócios e é reconhecida como ativo crítico para a continuidade operacional e saúde da empresa”.

## 2.1 INFORMAÇÃO E SUAS CARACTERÍSTICAS

Como a informação é um bem valioso das empresas, temos que separar todos os aspectos ligados à segurança da informação, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle, e, principalmente, os momentos que fazem parte de seu ciclo de vida. (SÊMOLA, 2003)

O ciclo de vida da informação é apresentado na Figura 1, apontando os momentos deste ciclo.

Figura 1 - Ciclo de vida da informação.




Fonte: Extraído de Sêmola (2003).

O COBIT 5 (ISACA, 2012) afirma que a informação, desde sua criação, passa por sua vida útil/operacional até chegar ao descarte, sendo este o seu ciclo de vida.

Quanto ao ciclo de vida, “Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, os equipamentos em que ela é manuseada, transportada e descartada” (SÊMOLA, 2003).

Sêmola (2003) completa dizendo que “Basicamente, na SI[1] lidamos com um tipo específico de ativo que chamamos de **ativo da informação**, isto é, ativos que geram, processam, manipulam, transmitem e armazenam informações, além das informações entre si”.

## 2.2 SEGURANÇA DA INFORMAÇÃO: PRINCÍPIOS, CONCEITOS E REQUISITOS

Para que as organizações se atentem aos problemas de segurança, boas práticas surgiram, e posteriormente leis e regulamentações. A organização ISO (*International Organization for Standarzation*) têm se dedicado na construção de normas técnicas que trazem boas práticas para a segurança da informação. O conjunto de recomendações para segurança da informação é a família da ABNT NBR ISO/IEC 27000. A ISO 27000 foi criada no ano 2000 tomando como base a norma britânica BS 7799-1:1999, que só foi revisada em 2005 quando houve a inserção de um capítulo sobre a gestão de incidentes de segurança da informação. A norma ABNT NBR ISO/IEC 17799 que trata da gestão da segurança da informação foi atualizada, renumerada e incluída na família ISO como ABNT NBR ISO/IEC 27002.” (GUALBERTO, 2010)

Esta norma britânica possui uma segunda parte, BS779-2, que define como as recomendações da primeira parte devem ser avaliadas pelas empresas, sendo utilizada para definir se empresa segue ou não as boas práticas. A ISO 27001 foi a transformação desta segunda parte em ISO e serve para que organizações certifiquem as práticas de gestão de segurança da informação já adotadas na empresa. (RAMOS et al., 2008)

---

[1] Segurança da Informação

A NBR ISO 27002 define como segurança da informação a preservação da confidencialidade, da integridade e da disponibilidade da informação; e a estas podem ser somadas outras propriedades que podem também estar envolvidas, como autenticidade, responsabilidade, não repúdio e confiabilidade.

Conforme Gualberto (2010) é preciso proteger a informação "[...], preservando-a assim em suas propriedades, quais sejam disponibilidade, integridade, confidencialidade e autenticidade dentre outras".

As definições desses requisitos de segurança são introduzidas por ISACA (2012) e Ramos et al. (2008):

- A **confidencialidade** é o sigilo da informação, então preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-la. Diferentes tipos de informação terão diferentes necessidades em termos de confidencialidade;
- A preservação da **integridade** envolve proteger as informações contra alterações em seu estado original. Essas alterações podem ser tanto intencionais quanto acidentais;
- Uma informação **disponível** é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam.

Segundo a ABNT NBR ISO/IEC 27001:2006, a segurança da informação só é obtida quando há a implementação de um conjunto de controles, que incluem políticas de segurança, processos internos, procedimentos, estrutura organizacional e funções de *software* e *hardware*.

Mesmo com conjunto de controles, "A todo instante os negócios, seus processos e ativos físicos, tecnológicos e humanos são alvo de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar sua ação. Quando essa possibilidade aparece, a quebra de segurança é consumada." (SÊMOLA, 2003)

"Como se pode ver, o que chamamos de segurança da informação deve assumir a forma de um conjunto de processos integrados que têm objetivos locais específicos, mas estão intimamente alinhados a um único objetivo corporativo: gerir dinamicamente mecanismos de controle abrangentes - considerando os processos,

tecnologias e pessoas - que agreguem valor ao negócio, permitindo sua operação com risco controlado" (SÊMOLA, 2003)

Ramos et al. (2008) define os seguintes conceitos com relação à segurança da informação:

- **Ameaça**: Algo que possa causar dano à informação (ativo). Entre as ameaças possíveis, podemos citar *hackers* e vírus;
- **Vulnerabilidade**: é um ponto de fragilidade da empresa que necessita de proteção. Por exemplo: servidores conectados à internet;
- **Incidente**: Quando a ameaça que explora alguma vulnerabilidade consegue êxito.

Para melhor compreensão, a Figura 2 apresentada por Sêmola (2003) quantifica de forma visual os conceitos apresentados por Ramos et al. (2008).

Figura 2 - Diagrama apresentando a equação do risco de segurança da informação.


Fonte: Extraído de Sêmola (2003).

"O **risco** é a probabilidade de que agentes, que são as **ameaças**, explorem **vulnerabilidades**, expondo os **ativos** a perdas de confidencialidade, integridade e disponibilidade, e causando **impactos** nos negócios. Estes impactos são limitados por **medidas de segurança** que protegem os ativos, impedindo que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco." (SÊMOLA, 2003)

Com relação às medidas de segurança, Ramos et al. (2008) esclarece que "são práticas, procedimentos ou mecanismos que podem proteger os ativos contra ameaças, reduzir ou eliminar vulnerabilidades, limitar o impacto de um incidente ou ajudar na sua detecção, facilitando a correção e a recuperação dos estragos causados. "

Ramos et al. (2008) diz que "A proteção fornecida pela segurança é desejada por uma razão muito simples: evitar e minimizar prejuízos [...]", sendo assim, Sêmola

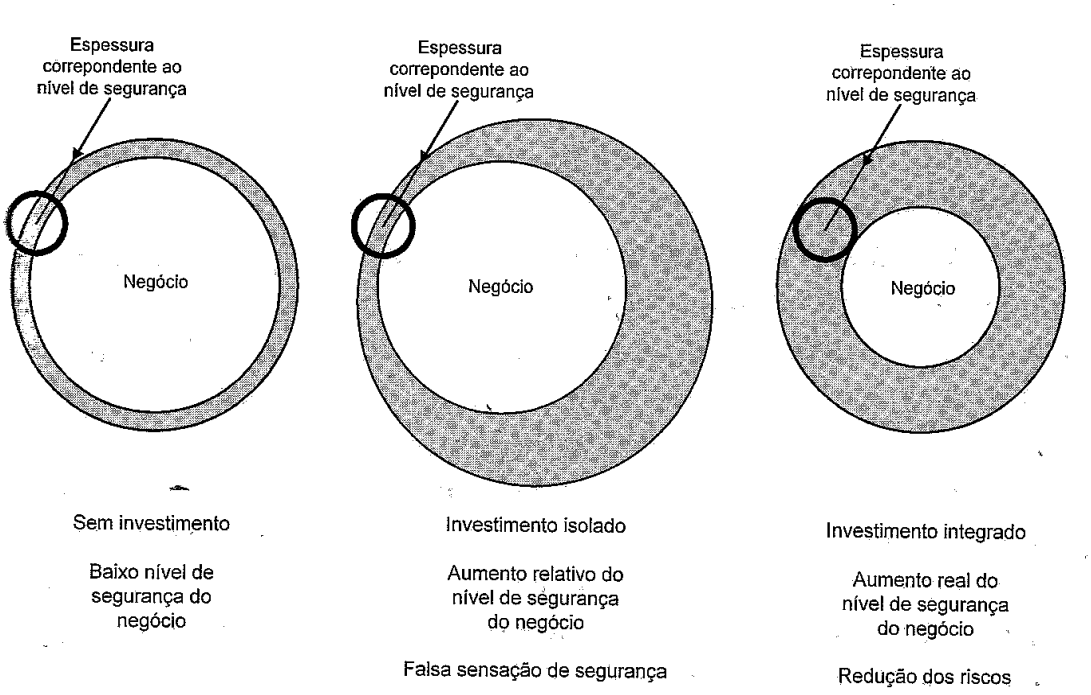
(2003) afirma que “[...] é preciso ter uma visão corporativa capaz de viabilizar uma ação consistente e abrangente, levando a empresa a atingir o nível de segurança adequado à natureza do seu negócio”.

## 2.3 GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Sêmola (2003) afirma que “Segurança é administrar riscos. Toda empresa possui características próprias, objetivos e planos específicos; por isso, precisa encontrar o nível de risco mais adequado para operar. [...] a análise de riscos deve fazer parte de um processo contínuo de gestão [...]”.

A Figura 3 apresenta a espessura correspondente ao nível de segurança de um negócio quando não há investimento, quando o investimento é isolado e quando o investimento é integrado, respectivamente.

Figura 3 - Ilustração dos estágios e do principal objetivo da solução corporativa de segurança da informação.




Fonte: Extraído de Sêmola (2003).

É possível verificar na Figura 3 que quando o investimento é feito de forma a integrar todas as áreas envolvidas, o negócio passa a ter uma maior segurança.

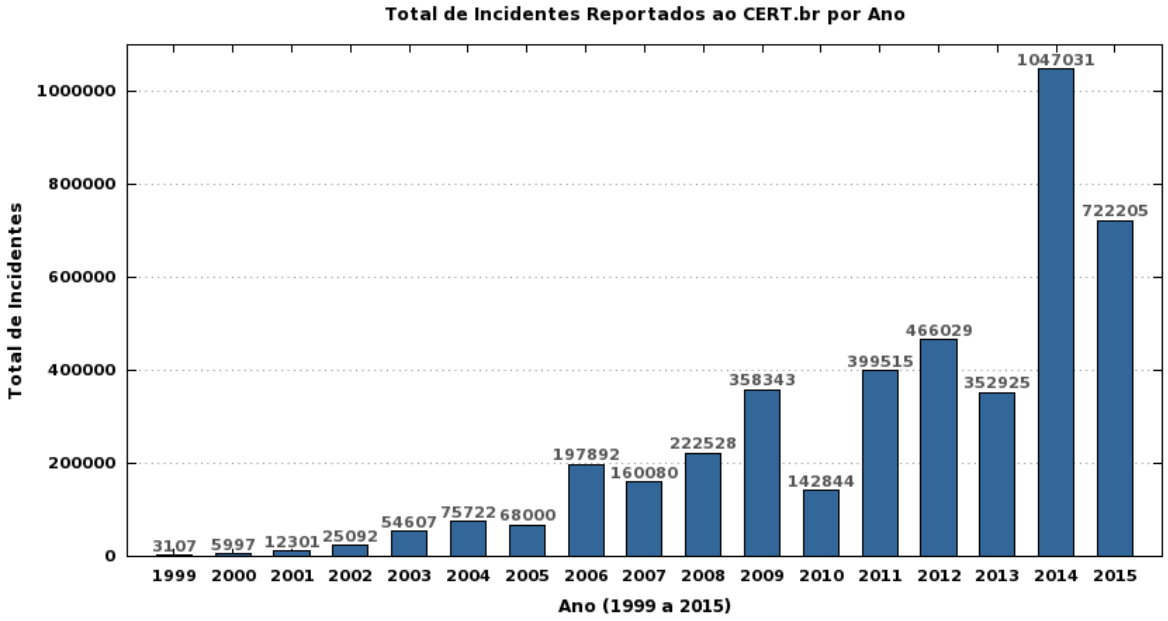
Quando há um investimento isolado, uma área fica mais coberta do que outra, e quando não existe investimento, o nível de segurança é muito menor. Por isto, Sêmola (2003) afirma que “O nível de segurança de uma empresa está diretamente associado à segurança oferecida pela ‘porta’ mais fraca. Por isso, é preciso ter uma visão corporativa capaz de viabilizar uma ação consistente e abrangente, levando a empresa a atingir o nível de segurança adequado à natureza do seu negócio”.

Sêmola (2003) e Gualberto (2010) concordam no que diz respeito à sistematização de processos e alinhamento às diretrizes estratégicas da empresa, sendo necessária uma estrutura organizacional definida, possuindo uma visão corporativa, global e ampla, potencializando a identificação e correção de pontos fracos.

Ramos et al. (2008) alerta que “A conformidade com a legislação e marcos regulatórios é um ponto normalmente fora de discussão dentro das organizações. O não-cumprimento dessas obrigações costuma implicar um risco muito grande levando, normalmente, à necessidade de investimentos e adequação. Além disso, muitos dos pontos levantados e implementados em marcos regulatórios ou exigidos por lei levam as organizações a aprimorar sua gestão, seus processos internos e sua transparência, fatores considerados importantes no atual cenário de gestão corporativa”.

O CERT.br (2016), Centro de Estudos, Resposta e Tratamento à Incidentes, lançou uma estatística quanto aos incidentes de segurança reportados, mostrando que vem crescendo exponencialmente estes incidentes: em 2013 foram reportados 352.925 (trezentos e cinquenta e dois mil, novecentos e vinte e cinco), em 2014 houve 1.047.031 (um milhão, quarenta e sete mil e trinta e  um) reportes e em 2015 houve 722.215 (setecentos e vinte e dois mil, duzentos e quinze) reportes. Como mostra a Figura 4.

Figura 4 - Total de incidentes reportados ao CERT.br por ano




Fonte: Extraído do site CERT.br (2016), disponível em <http://www.cert.br/stats/incidentes/>. Acesso em: 02 mar. 2016.

"[...] A segurança da informação é promovida por meio de um conjunto de controles (tais como procedimentos, estruturas organizacionais, políticas, etc) com objetivos específicos. Um Sistema de Gestão de Segurança da Informação (SGSI) visa (com base na análise avaliação e tratamento de riscos) justamente permitir que a organização que o implementa alcance seus objetivos relativos à segurança da informação" (RAMOS et al., 2008).

Todavia, "[...] uma das premissas básicas da segurança é o fato de que não existe segurança total ou completa. O que torna algo seguro ou não está muito mais ligado à gerência de uma série de fatores [...]" (RAMOS et al., 2008), como boas práticas, políticas de segurança e gerenciamento.

Ramos et al. (2008) mostra o porque de uma boa gestão empregar políticas, pois "servem como linhas-mestras para todas as atividades de SI desempenhadas em uma organização. São de extrema importância, pois é por meio delas que a estratégia de SI é montada e passada para todas as áreas envolvidas nas mais diversas esferas. As políticas também demonstram o comprometimento da alta direção da organização com a segurança, ponto fundamental para que ela possa ser gerida de forma eficaz, contando com o apoio da maior quantidade possível de colaboradores".

Uma boa política “Estabelece padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações dentro do nível de segurança estabelecido sob medida pela e para a empresa; portanto, a política deve ser personalizada” (SÊMOLA, 2003).

Além de ter uma política, é fundamental que haja revisões programadas visando adequar o regramento à situação da empresa. “Em linhas gerais, a revisão anual atende grande parte das organizações, sendo o prazo de dois anos recomendado para as de grande porte” (RAMOS et al., 2008).

Ramos et al.(2008) completa que “a Gestão de Segurança da Informação visa justamente permitir que a organização que o implementa alcance seus objetivos relativos à segurança da informação.”

# 3 GESTÃO DE SEGURANÇA DA INFORMAÇÃO NOS INSTITUTOS FEDERAIS DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA DO BRASIL

## 3.1 BREVE HISTÓRIA DOS INSTITUTOS FEDERAIS

Em 23 de setembro de 1909, o presidente do Brasil, Nilo Peçanha assina o Decreto nº 7.566, criando dezenove “Escolas de Aprendizes Artífices”, destinadas ao ensino profissional, primário e gratuito.

No ano de 1937, em 13 de Janeiro, foi assinada a Lei 378, transformando as Escolas de Aprendizes e Artífices em Liceus Profissionais, destinados ao ensino profissional de todos os ramos e graus.

As Escolas de Aprendizes e Artífices foi transformada em Escolas Industriais e Técnicas em 25 de fevereiro de 1942, através do decreto nº 4.127, oferecendo agora formação profissional em nível equivalente ao do secundário.

No ano de 1959, as Escolas Industriais e Técnicas são transformadas em autarquias com o nome de Escolas Técnicas Federais. As instituições ganham autonomia didática e de gestão, intensificando a formação técnica.

A Lei nº 6.545 assinada em 1978, tornou as três Escolas Técnicas Federais (Paraná, Minas Gerais e Rio de janeiro) em Centros Federais de Educação Tecnológica – CEFET. A partir de então, recebendo a nova função de formar engenheiros de operação e tecnólogos. Em 1994 foi assinada a Lei n 8.948, de 8 de dezembro, dispondo sobre a respectiva mudança para as demais Escolas Técnicas.

Somente em 2008 os Centros Federais se tornaram Institutos Federais de Educação, Ciência e Tecnologia, com a assinatura da Lei nº 11.892 do dia 29 de dezembro, sendo esta instituição vinculada ao Ministério da Educação.

Este histórico dos Institutos Federais pode ser consultado na íntegra no portal do MEC[2], e as Leis e Decretos mencionados podem ser acessados através do Portal da Legislação do Governo Federal[3].

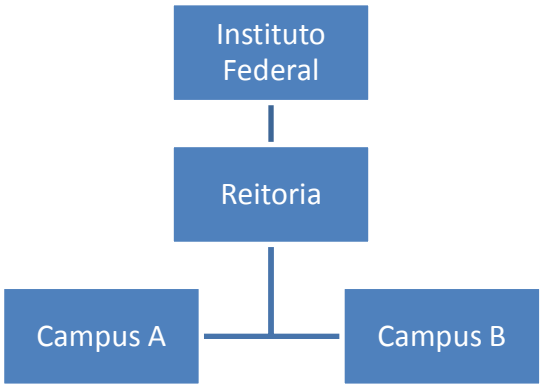
## 3.2 DA GESTÃO NOS INSTITUTOS

Os Institutos começaram a ganhar autonomia de gestão no ano de 1959, hoje somando 57 anos desde transformação em autarquia. Esta autonomia didática, administrativa e financeira se firmou tonando-se referência na qualidade de ensino.

Fernandes (2009) observou que cada Instituto Federal, de uma determinada extensão territorial, possui uma reitoria e vários *Campi*[4] com interdependência de gestão entre ambos. Em cada estado, a reitoria tem a função de controlar, supervisionar e definir políticas.

Na Figura 5 é possível verificar, de forma geral, a estrutura administrativa do Instituto Federal de uma determinada extensão territorial.

Figura 5 - Organograma base nas extensões territoriais




Fonte: Elaborado pela autora (2016).

[2]Dados extraídos do site http://portal.mec.gov.br/setec/arquivos/centenario/historico_educacao_profissional.pdf, acesso em 11 de Fevereiro de 2016.

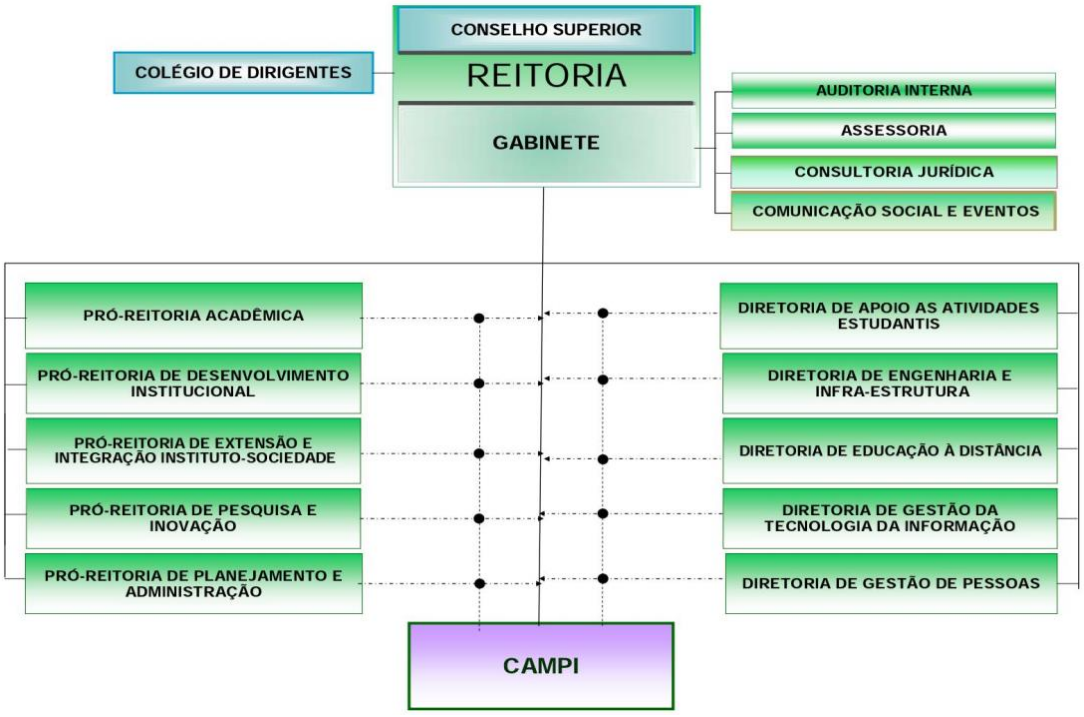
[3] http://www4.planalto.gov.br/legislacao

[4] Plural de campus.

Os Institutos Federais possuem estruturação sistêmica, sendo um conjunto de Unidades com gestões interdependentes entre reitoria e *Campi*, com único projeto político-pedagógico e princípios institucionais estratégicos. Na Lei nº 11.892 de 2008 é afirmado que os Institutos Federais terão como órgão executivo a reitoria (FERNANDES, 2009).

A Figura 6 desenvolvida por Fernandes (2009) ilustra, com maior riqueza de detalhes, o modelo referencial de uma estrutura administrativa para Reitoria dos Institutos Federais.

Figura 6 - Modelo referencial da estrutura administrativa para Reitoria dos Institutos Federais.




Fonte: Extraído do artigo de Fernandes (2009), disponível em http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/viewFile/267/187.

“Dessa forma a estrutura compreende as cinco pró-reitorias previstas na legislação, cujas atuações são requeridas para as principais áreas de estrutura e funcionamento da instituição, a saber: acadêmica (denominação própria em função da especificidade da oferta verticalizada de ensino, que vai da educação continuada à pós-graduação, associada à pesquisa e extensão em todo o trajeto da formação acadêmica); de pesquisa e inovação; de extensão e integração instituto-sociedade; de desenvolvimento institucional; e de planejamento e administração. Conta ainda com cinco diretorias de atuação sistêmica, conforme segue: apoio às atividades

estudantis (ação assumida como instrumento de inclusão, acompanhamento e manutenção dos estudantes na escola); engenharia e infraestrutura; educação à distância; gestão da tecnologia da informação; e gestão de pessoas – unidades necessárias ao atingimento do escopo funcional do Instituto" (FERNANDES, 2009).

## 3.3 GESTÃO DA TECNOLOGIA DA INFORMAÇÃO NOS INSTITUTOS FEDERAIS

Com a expansão e modernização dos Institutos Federais, há uma crescente preocupação com a informação, tendo em vista que estes institutos oferecem diversos cursos em seus *campi*, atuando também na modalidade à distância. (SOUSA, 2015)

Sousa (2015) observou a necessidade de um planejamento de TI, para que assim haja um alinhamento aos objetivos e metas estabelecidas pelos Institutos. "E o instrumento de planejamento que norteia a gestão da Tecnologia da Informação dos Institutos Federais é o Plano Diretor de Tecnologia da Informação - PDTI, sendo que o mesmo deve estar em consonância com o Plano de Desenvolvimento Institucional – PDI, dos IFs."

Dentro do Plano Diretor, devem estar as diretrizes, baseadas em normas, que devem ser seguidas pela instituição. Esta medida favorece a segurança da informação, pois são tomadas medidas neste sentido, tais como a aprovação e atualização da Política de Segurança da Informação. (SOUSA, 2015)

Existem ainda outros instrumentos que auxiliam na gestão da tecnologia da informação nos Institutos Federais de Educação, que são os acórdãos do Tribunal de Contas da União – TCU. Trazendo orientações aos gestores, para que estes adotem procedimentos padronizados e em conformidade com a legislação vigente, principalmente em relação a contratações de equipamentos e soluções de TI. (SOUSA, 2015)

No Instituto Federal do Rio Grande do Norte, já existe um PDTI, que possui as diretrizes apresentadas na Tabela 1.

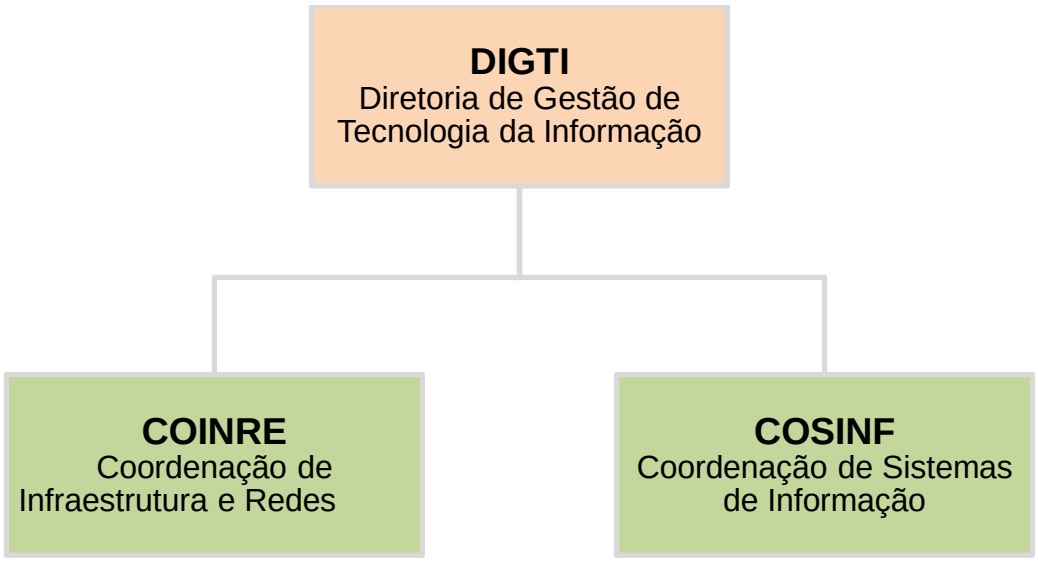
Tabela 1 - Diretrizes do PDTI do Instituto federal do Rio Grande do Norte.

| Diretriz | Descrição |
|---|---|
| D1 | Promover a governança de TI no IFRN |
| D2 | Buscar excelência, inovação e criatividade na gestão. |
| D3 | Garantir que as propostas orçamentárias de TIC sejam elaboradas com base em planejamentos e alinhadas com os objetivos de negócio. |
| D4 | Garantir a disponibilidade e integridade da informação. |
| D5 | Estabelecer, gerir, incentivar e manter políticas públicas por meios eletrônicos. |
| D6 | Investir no aumento da produtividade e otimização dos recursos de TI. |
| D7 | Promover a melhoria dos sistemas de informação do IFRN. |
| D8 | Estimular a adoção de metodologia de desenvolvimento de sistemas, procurando assegurar padronização, integridade e segurança. |
| D9 | Adotar padrões abertos no desenvolvimento de tecnologia da informação e comunicação. |
| D10 | Garantir a segurança da informação e comunicações. |
| D11 | Buscar a melhoria contínua da infraestrutura de TI. |
| D12 | Manter os processos internos de TI mapeados, formalizados, mensurados e otimizados. |
| D13 | Promover capacitação / formação de servidores de TI no IFRN. |

Fonte: PDTI – Instituto Federal do Rio Grande do Norte. Disponível em http://portal.ifrn.edu.br/conselhos/consup/resolucoes/2014/resolucao-no-23-2014, acesso em 16 de Fevereiro de 2016.

Na Figura 7, de forma ilustrativa, é possível verificar a Diretoria de Gestão de Tecnologia da Informação com as suas coordenações: A Coordenação de Infraestrutura e Redes; e a Coordenação de Sistemas de Informação.

Figura 7 - Organograma da Diretoria de Gestão de Tecnologia da Informação (DIGTI).




Fonte: Extraído do site do IFRN, disponível em http://portal.ifrn.edu.br/tec-da-informacao acesso em 07 de Fevereiro de 2016.

As informações organizacionais apresentadas neste capítulo são insumos importantes para a compreensão do estudo de caso descrito no capítulo 4.

# 4 ESTUDO DE CASO SOBRE A GESTÃO DA SEGURANÇA DA INFORMAÇÃO NOS INSTITUTOS FEDERAIS DE EDUCAÇÃO CIÊNCIA E TECNOLOGIA

Neste capítulo será apresentado o atual cenário da gestão da segurança da informação encontrado nos Institutos Federais, bem como mostrar uma breve análise de conformidade com a ISO 27001 Anexo A no Instituto Federal do Rio Grande do Norte.

## 4.1 METODOLOGIA

### 4.1.1 Enquadramento da metodologia

Este trabalho apresenta um estudo qualitativo do tipo estudo de caso exploratório, baseado em conceitos e metodologias definidas por Flick (2009), tendo destaque os enquadramentos a seguir:

I. Postura teórica definida: Interacionismo simbólico, pela busca por significados que os indivíduos atribuem à gestão praticada em seu ambiente de trabalho;
II. Métodos de coleta de dados: Revisão bibliográfica, Entrevistas estruturadas, através da internet (pesquisa “*on line*”);
III. Métodos de análise dos dados: Análise do material bibliográfico e dos seguintes documentos:
    a. Sites dos Institutos Federais do Brasil;
    b. Políticas de segurança da informação dos Institutos Federais que foram publicadas;
    c. Organogramas;
    d. Análise das respostas dos questionários aplicados.
IV. Campos de aplicação desta pesquisa: Análise da gestão da Tecnologia da Informação no IFRN através da aplicação de questionário baseado no Anexo A da Norma ABNT NBR ISO/IEC 27001.

### 4.1.2 Descrição dos procedimentos da pesquisa

A metodologia traçada por esta pesquisa foi desenvolvida em 3 etapas. A primeira foi a revisão bibliográfica, a segunda, feita em paralelo com a primeira, duas entrevistas do tipo pesquisa "*on line*", a terceira e última, a análise dos documentos e dados coletados.

#### 4.1.2.1 Revisão Bibliográfica

O estudo foi realizado com base em livros de tecnologia e gestão da informação publicados pelas editoras: Elsivier, *Módulo Security Solutions* e da Universidade de Brasília; bem como pesquisa nas bases de artigos científicos da Holos e Normas norteadoras dos temas:

- Segurança da informação;
- Gestão da segurança da informação;
- Gestão da segurança da informação nos Institutos Federais.

#### 4.1.2.2 Revisão Documental

Diante da documentação disponibilizada, foi realizado o estudo, com o propósito de buscar informações relevantes no conteúdo dos documentos para responder às questões da pesquisa. Abaixo seguem alguns documentos:

- Políticas de segurança da informação;
- Site dos Institutos Federais e das Universidades Federais;
- Artigos publicados no site da revista Holos e no periódico Capes.

#### 4.1.2.3 Entrevista estruturada através de correio eletrônico e ferramenta de *web survey*[5]

Abaixo seguem alguns aspectos utilizados para os questionários:

- Gestores de TI;
- Percepção sobre a gestão no órgão;
- Percepção da influência da GTI na Instituição;
- Percepção dos benefícios de Política de Segurança;
- Percepções sobre adequações às normas técnicas.

---

[5] Pesquisa através de ferramentas online na internet

#### 4.1.2.4 Da amostragem

A análise da bibliografia foi executada através da leitura de livros, pesquisa ao site da revista Holos e da Capes, bem como os sites das Universidades Federais e das reitorias dos Institutos Federais de cada extensão territorial.

Foram realizadas duas entrevistas "*on-line*", a primeira encaminhada para cada gestor da área de tecnologia da informação dos *campi* do Brasil que possuíam as informações de e-mail no site da instituição, totalizando 21 gestores, dos quais 38% responderam à pesquisa. Já a segunda, foi encaminhada para os gestores de tecnologia da informação da reitoria e *campi* específicos, onde 100% responderam à pesquisa.

#### 4.1.2.5 Das condições de confidencialidade

Quanto aos entrevistados, os seus nomes não serão revelados, pois as informações apresentadas possuem um grau elevado de confidencialidade, sendo primordial que estes tenham absoluto sigilo.

#### 4.1.2.6 Das entrevistas

As entrevistas foram realizadas por meio de *web survey*, disponibilizadas na internet através de um formulário. Esta etapa foi desenvolvida de forma paralela ao das análises bibliográfica e documental, de forma a aperfeiçoar os resultados.

#### 4.1.2.7 Análise dos dados

A análise dos dados foi realizada por meio de estudo bibliográfico visando contextualizar o tema, bem como a análise de dados das respostas aos questionários que foram realizados.

No estudo bibliográfico, foi feito o levantamento qualitativo de informações referente à gestão da segurança da informação e a adequação do IFRN às normas ISO que referenciam o tema.

## 4.2 RESULTADOS E DISCUSSÕES

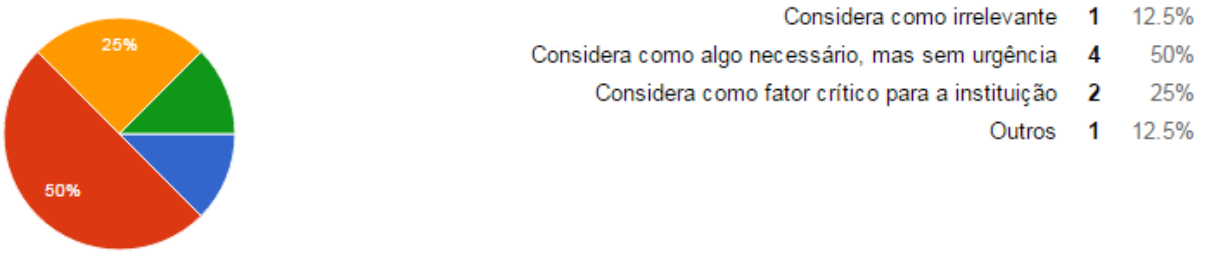
Com base nos questionários contidos nos Anexos A e B, seguem nas subseções 4.2.1 e 4.2.2 a compilação das respostas obtidas.

### 4.2.1 QUANTO À GESTÃO DA TECNOLOGIA DA INFORMAÇÃO DOS INSTITUTOS FEDERAIS DE EDUCAÇÃO DO BRASIL

As respostas desta subseção foram obtidas través do questionário do Anexo A, aplicado aos gestores dos Institutos Federais de Educação do país, que trata sobre gestão e política de segurança da informação.

Quando questionados sobre a visão da administração quanto à gestão da segurança da informação, as respostas obtidas estão ilustradas na Figura 8, onde 50% dos gestores responderam que a administração considera a gestão da segurança da informação algo necessário, mas sem urgência. Outros 25% dos gestores apontaram que a alta administração considera a gestão da segurança da informação um fator crítico para a instituição. Apenas 12,5% consideram como irrelevante e 12,5% apontam que há outras visões.

Figura 8 – Gráfico de respostas ao questionamento quanto à visão da administração sobre a gestão da segurança da informação.




Fonte: Elaborado pela autora (2016).

Quando questionados sobre possuir uma política de segurança da informação, os resultados, conforme mostrados na Tabela 2, apontam que 12,5% não possuem políticas, 25% estão com política em desenvolvimento e 62,5% possuem política ativa.

Tabela 2 - Respostas ao questionamento quanto ao Instituto Federal possuir política de segurança da informação.

| **QUANTO AO INSTITUTO FEDERAL POSSUIR POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** | |
|---|---|
| **Resposta** | **%** |
| Não possui | 12,5 % |
| Possuem política de segurança | 62,5 % |
| Ainda em andamento | 25 % |

Fonte: Elaborado pela autora (2016).

Dos institutos que ainda não possuem uma política de segurança da informação ativa (37,5%), apenas 12,5% não souberam informar se há um período programado para revisão, as demais instituições, mesmo as que estavam em fase de desenvolvimento da política, já possuíam um período programado para este fim.

No que diz respeito ao incentivo da alta administração a respeitar a política de segurança da informação, e levando em consideração que três instituições que responderam o questionário ainda não tinham política, ou estavam em desenvolvimento, para efeito de cálculo, nos dados da Tabela 3 só foram consideradas as respostas dos gestores que possuíam política ativa.

Tabela 3 - Respostas ao questionamento de se a alta administração incentiva os servidores e alunos a respeitar as instruções e normas descritas pela política de segurança da informação e de que forma incentivam.

| **QUANTO AO QUESTIONAMENTO SE A ALTA ADMINISTRAÇÃO INCENTIVA OS SERVIDORES E ALUNOS A RESPEITAR AS INSTRUÇÕES E NORMAS DESCRITAS PELA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DE QUE FORMA INCENTIVAM** | |
|---|---|
| **Resposta** | **%** |
| Não sabe informar | 20 % |
| Não incentiva | 20 % |
| Incentiva através de portarias, campanhas de divulgação como palestras e *worshop's* | 40 % |
| Acredita que incentivará | 20 % |

Fonte: Elaborado pela autora (2016).

Quando questionados se a política de segurança foi (será) elaborada com a participação de todas as partes envolvidas, 62,5% responderam que sim e 37,5% responderam que não, conforme apresentado na Figura 9. Das instituições que responderam que não, apenas uma ainda não elaborou e nem está desenvolvendo a política.

Figura 9 - Gráfico de respostas quanto se a política de segurança foi (será) elaborada com a participação de todas as partes envolvidas.


Fonte: Elaborado pela autora (2016).

Diante dos dados obtidos, foi observado que na visão dos gestores de TI a alta administração, em sua maioria, vê a gestão da segurança da informação como algo necessário, mas ainda não compreendem completamente a sua importância, inclusive menos da metade da alta administração destes institutos incentivam o respeito e cumprimento da política.

Os institutos, de forma geral, já possuem política de segurança da informação, não houve presença de todas as partes envolvidas em sua elaboração, muito embora haja períodos programados para que possam ser adicionadas informações relevantes não incluídas no texto inicial da política.

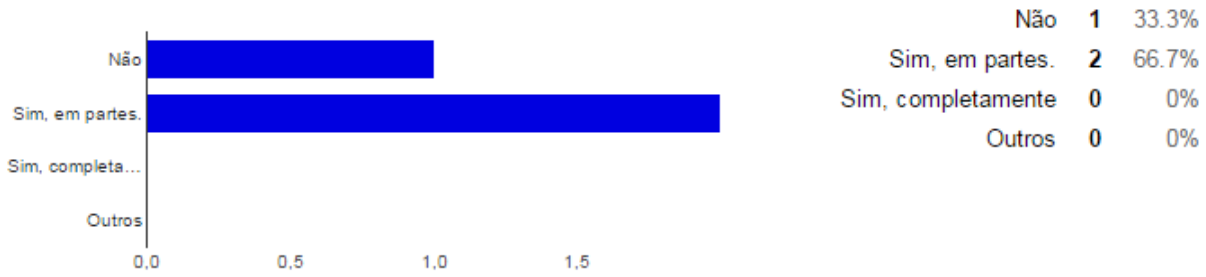
### 4.2.2 QUANTO À GESTÃO E CONFORMIDADE COM A NORMA NBR ISO 27001 ANEXO A NO IFRN

As respostas desta subseção foram obtidas través do questionário do Anexo B, aplicado aos gestores do IFRN, que trata sobre a gestão da segurança da informação e sua conformidade com a ISO 27001.

Quando questionados quanto à administração (incluindo a direção) compreender que a Infraestrutura da Tecnologia da Informação (TI) é um fator crítico e estratégico para o crescimento/desenvolvimento do instituto, foi estimado que

33,3% não compreendem e que 66,7% compreendem apenas em partes, conforme pode ser visto na Figura 10.

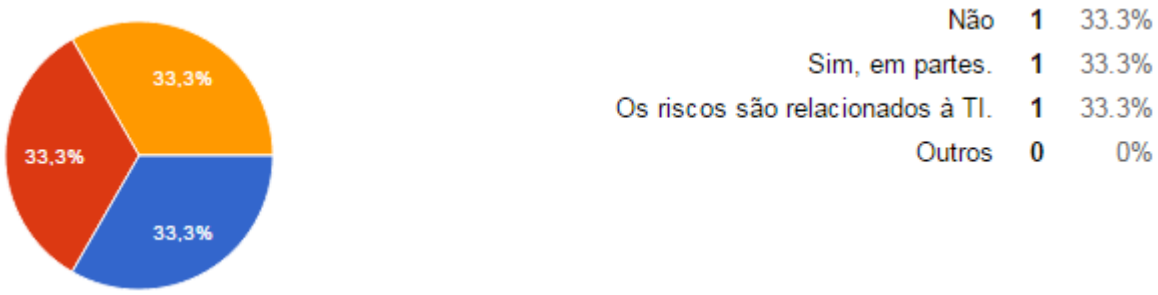
Figura 10 - Respostas à pergunta quanto se a administração (incluindo a direção) compreende que a Infraestrutura da Tecnologia da Informação (TI) é um fator crítico e estratégico para o crescimento/desenvolvimento do instituto.




Fonte: Elaborado pela autora (2016).

Quando questionados sobre os riscos organizacionais serem relacionados a TI ou à GTI, as respostas obtidas dos gestores de TI foram que 33,3% não relacionam, 33,3% só relacionam em partes e 33,3% e os que afirmam que os riscos são relacionados a TI somam 33,3%. Na Figura 11 é apresentado o gráfico desta estatística.

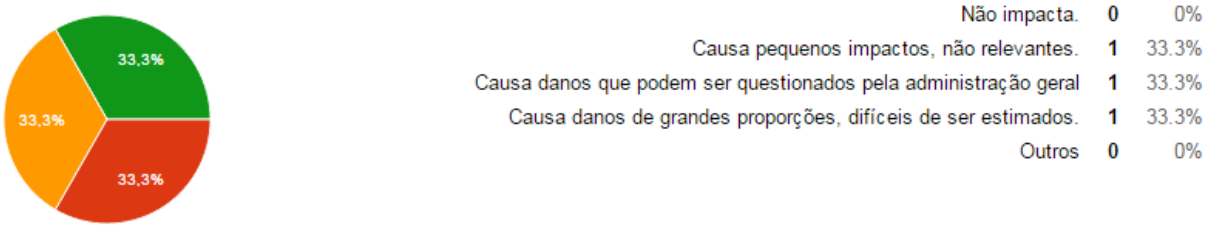
Figura 11 - Respostas quanto aos riscos organizacionais serem relacionados à TI ou à Gestão da TI (GTI).




Fonte: Elaborado pela autora (2016).

Já no que diz respeito ao impacto causado ao instituto quando há falhas na infraestrutura de TI, as respostas obtidas podem ser observadas na Figura 12, onde aponta que 33,3% informaram que causa pequenos impactos, não relevantes; 33,3% responderam que causam danos que podem ser questionados pela administração geral; e 33,3% que causam danos de grandes proporções, difíceis de ser estimados.

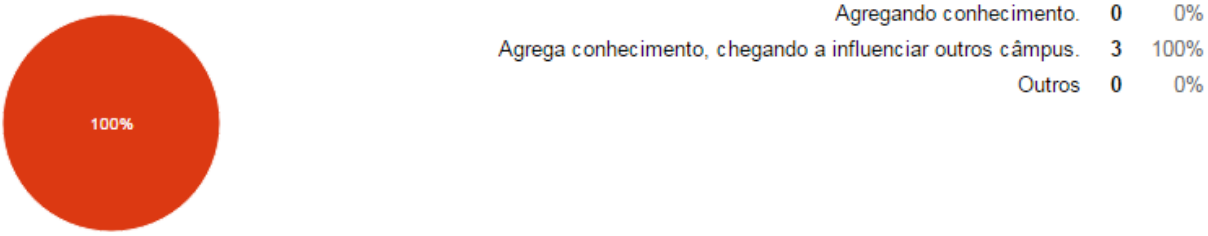
Figura 12 - Resposta a pergunta de como as falhas na infraestrutura da TI impactam a imagem do Instituto.




Fonte: Elaborado pela autora (2016).

No questionamento sobre como uma boa gestão e organização da TI pode corroborar para o crescimento da organização, a resposta obtida por 100% dos entrevistados aponta que agrega conhecimento, chegando a influenciar outros *campi*. O gráfico estatístico está representado na Figura 13.

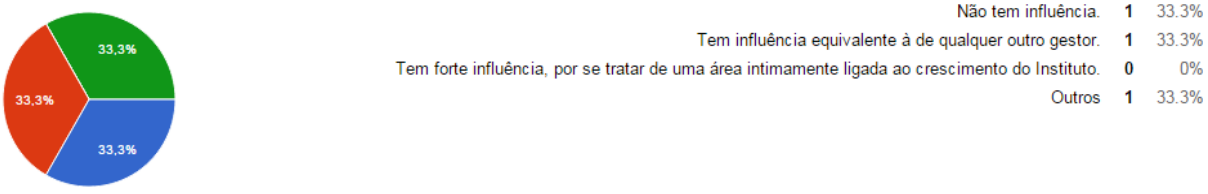
Figura 13 - Respostas ao questionamento de sobre como uma boa gestão e organização da TI podem corroborar para o crescimento da organização.




Fonte: Elaborado pela autora (2016).

Porém, quando questionados sobre a influência da GTI no instituto, as respostas obtidas estão apontadas na Figura 14, onde 33,3% responde que não tem influência, 33,3% apontam que tem influência equivalente a de qualquer outro gestor, e 33,3% informam que tem influência, mas com uma visão da Alta gestão de um setor de infraestrutura (descrita na opção “Outros”).

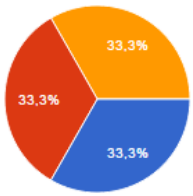
Figura 14 - Respostas quanto ao questionamento de qual a influência da GTI no Instituto.




Fonte: Elaborado pela autora (2016).

Sobre os aspectos mais importantes para a alta administração na gestão da tecnologia da informação, 33,3% responderam que o mais importante é economizar no orçamento, 33,3% que o mais importante é gerir de forma a otimizar os recursos, melhorando a qualidade dos serviços de TI; e 33,3% que dar fluidez à dinâmica do dia-a-dia, garantindo a resposta rápida à incidentes. Estas respostas estão ilustradas na Figura 15.

Figura 15 - Resposta quanto aos aspectos mais importantes para a alta administração no que diz respeito à GTI.




| | | |
|---|---|---|
| Economizar no orçamento. | 1 | 33.3% |
| Gerir de forma a otimizar os recursos, melhorando a qualidade dos serviços de TI. | 1 | 33.3% |
| Dar fluidez à dinâmica do dia-a-dia, garantindo a resposta rápida à incidentes. | 1 | 33.3% |
| Outros | 0 | 0% |

Fonte: Elaborado pela autora (2016).

O IFRN possui política de segurança da informação, mas não tem intervalos programados para revisão.

Quanto à conformidade com a Norma NBR ISO 27001 Anexo A, a Tabela 4 apresenta o resultado obtido, tomando como base as respostas dos entrevistados para cada tema.

Foram feitas 11 perguntas sobre a conformidade com a NBR ISO 27001, uma para cada tema da norma. Como na norma não há uma forma de julgar a porcentagem de conformidade (como também não tem em outras fontes pesquisadas), a forma adotada foi elaborar uma questão para cada tema, onde os temas possuem pesos iguais (no final é feita soma aritmética).

Para o tema política de segurança todos os gestores responderam que tinham política de segurança, mas que não haviam revisões programadas, com isso não atenderam em 100% ao item, recebendo 50% de conformidade.

No tema organizando a segurança da informação, quando a resposta assinalada foi de que não havia comprometimento com a segurança, o gestor recebeu 0% de conformidade, no caso de ter respondido que há comprometimento com a segurança, mas não há pessoas responsáveis por ela, o gestor recebeu 50%.

Quanto à gestão de ativos, todos os gestores responderam que há a gestão dos ativos, mas não há a classificação da informação, sendo assim receberam 50% por não estarem totalmente conforme com o tema.

Já no quesito segurança em recursos humanos, os gestores que informaram que há um controle na contratação, mudança de função ou encerramento de atividades de funcionários, receberam 100% de conformidade, aqueles que responderam que só havia este controle na segurança apenas em alguns casos, receberam 50%.

No que diz respeito a segurança física e do ambiente, os gestores que responderam que há a prevenção quanto ao acesso físico não autorizado à equipamentos e instalações, possuindo ainda o equipamento uma proteção contra danos ou furtos, o gestor recebe 100% de conformidade, já no caso de possuir controle aos ambientes, mas de não haver proteção no equipamento contra furtos, o gestor recebe 50% de conformidade.

Para os temas de gerenciamento das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas da informação; gestão de incidentes de segurança da informação, gestão de continuidade do negócio e o tema conformidade, cada gestor respondia sim ou não, onde para sim, alcançava 100% e para não a porcentagem obtida foi de 0% de conformidade com a norma.

Tabela 4 - Respostas às perguntas baseadas na Norma 27001 Anexo A.

| Tema | Gestor 1 | Gestor 2 | Gestor 3 | Média |
|---|---|---|---|---|
| Política de segurança | 50% | 50% | 50% | 50% |
| Organizando a segurança da informação | 0% | 50% | 0% | 17% |
| Gestão de ativos | 50% | 50% | 50% | 50% |
| Segurança em recursos humanos | 100% | 50% | 100% | 83% |
| Segurança física e do ambiente | 100% | 50% | 50% | 67% |
| Gerenciamento das operações e comunicações | 0% | 100% | 100% | 67% |
| Controle de acessos | 100% | 100% | 100% | 100% |
| Aquisição, desenvolvimento e manutenção de sistemas de informação | 0% | 100% | 100% | 67% |
| Gestão de incidentes de segurança da informação | 0% | 0% | 0% | 0% |
| Gestão da continuidade do negócio | 0% | 0% | 0% | 0% |
| Conformidade | 0% | 0% | 50% | 17% |
| **Média total** | | | | **47%** |

Fonte: Elaborado pela autora (2016).

Desta forma, fazendo a análise dos dados, após calcular a média de cada tema, em seguida realizando a média de todas as médias, com a metodologia adotada, o IFRN obteve 47% de conformidade.

Diante do exposto, foi verificado que os riscos organizacionais ainda não são bem compreendidos pela alta administração, não os relacionando à infraestrutura da tecnologia da informação, bem como não é visto como fator crítico e estratégico para o crescimento/desenvolvimento da organização. Ainda não há mensurado, por parte dos gestores de TI, de forma unificada, os impactos causados à imagem do instituto quando ocorrem falhas na infraestrutura e disponibilidade.

Os dados apontam que a boa gestão de TI no IFRN corrobora para o crescimento da organização, agregando conhecimento ao ponto de influenciar positivamente outros *campi*.

No que diz respeito ao IFRN seguir a NBR ISO 27001 Anexo A, foi atingido um total de 47% de conformidade, sendo necessário averiguar quais providências podem ser tomadas para que este índice seja melhorado.

# 5 CONSIDERAÇÕES FINAIS

Neste capítulo serão apresentadas as conclusões deste trabalho de conclusão de curso, partindo de normas técnicas e das pesquisas "*web survey*" que foram realizadas para a elaboração deste projeto no Instituto Federal de Educação, Ciência e Tecnologia do Rio Grande do Norte.

## 5.1 CONCLUSÃO

Ao longo deste trabalho buscou-se atingir o objetivo de identificar a situação atual da gestão da segurança da informação nos Institutos Federais de Educação do Brasil, e especificamente do IFRN, fazendo um comparativo destes dados, verificando o posicionamento do Instituto Federal do Rio Grande do Norte em relação aos demais institutos do Brasil. A seguir trataremos sinteticamente do que foi concluído nestas pesquisas.

No período de realização deste trabalho foi verificado que um dos maiores problemas encontrados é o fato de a alta administração dos IF's de todo o Brasil, incluindo o IFRN, ainda não compreender claramente a necessidade da gestão da segurança da informação.

Os Institutos Federais de Educação, Ciência e Tecnologia, em sua maioria, possuem política de segurança da informação, e quase que completamente já há um período programado para a revisão desta. O IFRN, especificamente, também já possui está política, porém, com revisões não programadas e sem classificação das informações. Para que isto seja corrigido, é necessário que haja aditivos ao texto principal incluindo estas revisões.

Na ótica dos gestores da tecnologia da informação e segundo a metodologia aplicada, o IFRN possui apenas 47% de conformidade com a NBR ISO 27001. Como sugestão de melhoria, pode ser adotada a própria norma como base, agregando mais qualidade à gestão e proporcionando maior segurança às informações da organização, sendo um dos objetivos estratégicos do PDTI do IFRN

adequar a gestão da área de TI às novas exigências de governança e promover a segurança da informação e comunicação.

Não foram encontrados dados de normas, instituições ou pesquisas, que evidenciem que esse valor de 47% de conformidade seja bom ou ruim, para que assim fossem feitas comparações.

Após analisar e identificar os pontos fracos e sugerir melhorias, percebe-se a importância da contribuição que este trabalho pode oferecer ao Instituto federal como um todo. E no caso de os Institutos Federais de Educação adotarem as normas técnicas e boas práticas de segurança da informação, as informações da instituição serão tratadas com maior segurança.

## 5.2 TRABALHOS FUTUROS

Como sugestão para trabalhos futuros e buscando aperfeiçoamento da gestão da segurança da informação, podem-se realizar novos estudos de caso sobre a gestão de segurança da informação nos Institutos Federais de Educação, Ciência e Tecnologia com os gestores da alta administração e ainda com alunos, servidores e terceirizados, realizando um comparativo de dados.

Também pode ser feito um novo projeto de conformidade com a NBR ISO 27001 Anexo A, sendo que abrangendo todo o território nacional de forma a minimizar os pontos fracos da segurança da informação nos Institutos Federais de Educação de todo o Brasil.

## REFERÊNCIAS

Associação Brasileira de Normas Técnicas - ABNT. **Norma NBR-ISO/IEC 27001:2006**.

CERT.BR (Org.). **Estatísticas dos Incidentes Reportados ao CERT.br.** 2016. Disponível em: <http://www.cert.br/stats/incidentes/>. Acesso em: 02 mar. 2016.

FERNANDES, Francisco das Chagas Mariz. Gestão dos Institutos Federais: O Desafio do Centenário da Rede Federal de Educação Profissional e Tecnológica. **HOLOS**, [S.l.], v. 2, p. 3-9, out. 2009. ISSN 1807-1600. Disponível em: <http://www2.ifrn.edu.br/ojs/index.php/HOLOS/article/view/267>. Acesso em: 15 fev. 2016. doi:http://dx.doi.org/10.15628/holos.2009.267.

FLICK, Uwe; **Introdução à pesquisa qualitativa**; 3a edição / Tradução: Joice Elias Costa; Porto Alegre/ RS; Artmed, 2009; ISBN 978-85-363-1711-3

GUALBERTO, Éder Souza. **Um estudo de caso sobre a gestão da segurança da informação em uma organização pública.** 2010. 112 f. TCC (Graduação) - Curso de Bacharelado em Ciência da Computação, Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2010.

ISACA. **COBIT 5:** Modelo Corporativo para Governança e Gestão de TI da Organização. Estados Unidos da América: ISACA, 2012.

RAMOS, Anderson et al. **Security Officer - 1:** guia oficial para formação de gestores em segurança da informação. 2. ed. Porto Alegre, Rs: Zouk, 2008. (Módulo Security Solutions).

SÊMOLA, Marcos. **Gestão da segurança da informação:** visão executiva da segurança da informação. 12. ed. Rio de Janeiro: Elsevier, 2003.

SOUSA, Edilson Leite de. **Investigação do Processo de Aplicação das Tecnologias da Informação e Comunicação na Gestão dos Institutos Federais de Educação, Ciência e Tecnologia.** 2015. 129 f. Dissertação (Mestrado) - Curso de Mestrado Profissional em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2015. Disponível em: <http://www.repositorio.ufpe.br/bitstream/handle/123456789/14224/Dissertação_Versão_06_Digital.pdf?sequence=1&isAllowed=y>. Acesso em: 16 fev. 2016.

## ANEXO A – QUESTIONÁRIO DE GESTÃO E POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

**01. O seu Instituto Federal possui Política de Segurança da Informação?**

a. Sim
b. Não
c. Em desenvolvimento.

**02. Esta política foi (será) elaborada com participação de todas as partes envolvidas?**

a. Sim
b. Não
c. Outro:

**03. Para a revisão da Política de Segurança da Informação, há (haverá) algum período programado para revisão?**

Ex.: A cada dois anos ou sempre que ocorrem mudanças de gestão

**04. Os colaboradores foram (serão) conscientizados sobre a importância da política de segurança da informação?**

a. Sim
b. Não
c. Outro:

**05. No documento da política de segurança. está formalizado a responsabilidade e o dever da instituição quanto à informação?**

a. Sim
b. Não
c. Em partes
d. Outro:

**06. Qual a visão da administração sobre a gestão da segurança da informação?**

a. Considera como irrelevante
b. Considera como algo necessário, mas sem urgência
c. Considera como fator crítico para a instituição

d. Outro:

**07. A alta administração incentiva (incentivará) os servidores e alunos a respeitar as instruções e normas descritas pela política de segurança da informação? De que forma isto é (será) realizado?**

## ANEXO B – QUESTIONÁRIO DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO NO IFRN E SUA CONFORMIDADE COM A ISO 27001

1. **De qual campus do IFRN você faz parte?**
    a. Natal-Central
    b. Reitoria
2. **A administração (incluindo a direção) compreendem que a Infraestrutura da Tecnologia da Informação (TI) é um fator crítico e estratégico para o crescimento/desenvolvimento do instituto?**
    a. Não
    b. Sim, em partes.
    c. Sim, completamente.
    d. Outro: ☐
3. **Os riscos organizacionais são relacionados à TI ou à Gestão da TI (GTI)?**
    a. Não
    b. Sim, em partes
    c. Os riscos são relacionados à TI.
    d. Outro: ☐
4. **Como as falhas na infraestrutura da TI impactam a imagem do Instituto?**
    a. Não impacta.
    b. Causa pequenos impactos, não relevantes.
    c. Causa danos que podem ser questionados pela administração geral
    d. Causa danos de grandes proporções, difíceis de ser estimados.
    e. Outro: ☐
5. **Qual a influência da GTI no Instituto?**
    a. Não tem influência.
    b. Tem influência equivalente à de qualquer outro gestor.
    c. Tem forte influência, por se tratar de uma área intimamente ligada ao crescimento do Instituto.
    d. Outro: ☐

6. **Como uma boa gestão e organização da TI pode corroborar para o crescimento da organização?**
    a. Agregando conhecimento.
    b. Agrega conhecimento, chegando a influenciar outros *campi*.
    c. Outro: ☐
7. **Quais são os aspectos mais importantes para a alta administração no que diz respeito à GTI?**
    a. Economizar no orçamento.
    b. Gerir de forma a otimizar os recursos, melhorando a qualidade dos serviços de TI.
    c. Dar fluidez à dinâmica do dia-a-dia, garantindo a resposta rápida à incidentes.
    d. Outro: ☐
8. **O campus possui uma política de Segurança da Informação? Ela possui intervalos programados de revisão?**
    a. Não possui política.
    b. Possui uma política mas não tem revisões programadas
    c. Possui política de segurança da informação e é revisada periodicamente, sendo alterada também quando mudanças significativas ocorrem, como mudança de direção.
    d. Outro: ☐
9. **No quesito organização, existe comprometimento da administração com a segurança? Existem pessoas responsáveis pela segurança da Informação?**
    a. Não há comprometimento com a Segurança.
    b. Há comprometimento da administração com a segurança, mas não existem pessoas responsáveis por ela.
    c. Há o comprometimento da administração com a segurança da Informação. E também existem pessoas responsáveis por esta segurança.
    d. Outro: ☐

10. **Quanto à gestão de ativos, existe a identificação dos ativos e regras de uso? A informação do IF é classificada?**
    a. Não existe identificação dos ativos, regras de uso e nem classificação da informação.
    b. Há a gestão dos ativos, mas a classificação.
    c. Os ativos são gerenciados e a informação é classificada.
    d. Outro: ☐
11. **No quesito segurança em recursos humanos, há um controle na contratação, mudança de função ou encerramento da atividades de funcionários?**
    a. Não.
    b. Sim.
    c. Apenas em alguns casos.
    d. Outro: ☐
12. **Existe a prevenção quanto acesso físico não autorizado à equipamentos e instalações? No caso de um indivíduo conseguir acesso a um destes locais, o equipamento tem alguma proteção contra danos ou furtos?**
    a. Há um controle aos ambientes com equipamentos, mas não especificamente aos equipamentos
    b. Existe controle a ambientes e a equipamentos.
    c. Outro: ☐
13. **Quanto ao Gerenciamento das operações e comunicações, existe algum controle de disponibilidade e integridade de serviços e sistemas?**
    a. Sim
    b. Não
    c. Outro: ☐
14. **No quesito controle de acessos à informação, existe controle de acesso à sistemas, à rede, aos sistemas operacionais e aplicações?**
    a. Sim
    b. Não

c. Outro:

15. **Quanto ao item Aquisição, desenvolvimento e manutenção de sistemas de informação; existem requisitos de segurança e controles que protejam a confidencialidade e integridade das informações?**
    a. Sim
    b. Não
    c. Outro:
16. **Na Gestão de incidentes de segurança da informação, existem notificações de fragilidades e melhorias na gestão de incidentes?**
    a. Sim
    b. Não
    c. Outro:
17. **No que diz respeito à gestão da continuidade do negócio, existem aspectos da gestão da continuidade do negócio relacionados à segurança da informação?**
    Ex. Como avaliação dos riscos
    a. Não
    b. Sim
    c. Outro:
18. **Quanto à conformidade, as legislações civis, normas técnicas e auditoria de sistemas são praticadas?**
    a. Não
    b. Sim
    c. Outro: