



**PÓS-GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO**

**VICENTE DE PAULO BATISTA**

**UM ESTUDO SOBRE A ADERÊNCIA DAS INSTITUIÇÕES DA REDE  
FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E  
TECNOLÓGICA AO CORREIO ELETRÔNICO PROPOSTO NO DECRETO  
8.135/2013**



Universidade Federal de Pernambuco  
CIN - CENTRO DE INFORMÁTICA  
[posgraduacao@cin.ufpe.br](mailto:posgraduacao@cin.ufpe.br)  
[www.cin.ufpe.br/~posgraduacao](http://www.cin.ufpe.br/~posgraduacao)

RECIFE  
2017

**VICENTE DE PAULO BATISTA**

**UM ESTUDO SOBRE A ADERÊNCIA DAS INSTITUIÇÕES DA REDE  
FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E  
TECNOLÓGICA AO CORREIO ELETRÔNICO PROPOSTO NO DECRETO  
8.135/2013**

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação do Centro de Informática da Universidade Federal de Pernambuco como requisito parcial para obtenção do título de Mestre em Ciência da Computação.

Orientador: Prof. Fernando da Fonseca de Souza, PhD

RECIFE  
2017

Catálogo na fonte  
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

B333e Batista, Vicente de Paulo  
Um estudo sobre a aderência das instituições da Rede Federal de Educação Profissional, Científica e Tecnológica ao correio eletrônico proposto no Decreto 8.135/2013 / Vicente de Paulo Batista. – 2017.  
143 f.:il., fig., tab.

Orientador: Fernando da Fonseca de Souza.  
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CIn, Ciência da Computação, Recife, 2017.  
Inclui referências, apêndices e anexos.

1. Banco de dados. 2. Comunicação de dados. 3. Segurança da informação. I. Souza, Fernando da Fonseca (orientador). II. Título.

025.04 CDD (23. ed.) UFPE - MEI 2017-179

**Vicente de Paulo Batista**

**Um estudo sobre a aderência das instituições da Rede Federal de Educação Profissional, Científica e Tecnológica ao correio eletrônico proposto no Decreto 8.135/2013**

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestre Profissional em 14 de junho de 2017.

Aprovado em: 14/06/2017

**BANCA EXAMINADORA**

---

Prof.<sup>a</sup>. Carla Taciana Lima Lourenço Schuenemann  
Centro de Informática / UFPE

---

Prof. Sidney de Carvalho Nogueira  
Universidade Federal Rural de Pernambuco

---

Prof. Fernando da Fonseca de Souza  
Centro de Informática / UFPE  
(Orientador)

Este trabalho é dedicado aos meus pais  
Bernardino Batista e Maria Cecília (in memória)  
e a minha companheira Maiza Barros.

## AGRADECIMENTOS

Obrigado meu Deus por todas as vezes que me concedeste o dom da sabedoria.

A Maiza, minha eterna incentivadora com a qual compartilho a minha vida e os meus sonhos e que sempre está presente, acreditando e me fazendo crescer;

O meu muito obrigado ao professor Fernando, por acreditar no meu projeto e por tantas vezes dispensar o seu precioso tempo na orientação deste trabalho;

A Anny Kariny que foi luz na realização desse projeto e pela qual tenho uma imensa gratidão;

Aos colegas de instituto Helba, Eleudson, Fátima e Thiago (Reitoria) pela presteza e disposição em contribuir;

A Dackson, que sempre foi o amigo leal e com quem pude contar em todos os momentos;

Ao colega de mestrado Kleber que disponibilizou o seu precioso tempo para colaborar comigo na realização deste trabalho;

À minha irmã Cecília pela torcida e as orações.

À administração do IFCE *campus* Iguatu, por ter facilitado e colaborado com a realização deste mestrado;

Que Deus me permita ser alguém melhor a cada novo dia.

## RESUMO

Como resposta às denúncias feitas pelo o ex-técnico da CIA (Central Intelligence Agency), Edward Snowden, relatando o caso de espionagem contra o Brasil, foi sancionado o Decreto 8.135/2013, o qual dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e adota os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da administração pública, devendo possuir características que permitam a auditoria. Considerando tal normativa, este trabalho buscou efetuar um estudo sobre a aderência das instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica ao correio eletrônico nos moldes do decreto. Para tanto, utilizou-se de pesquisa bibliográfica e aplicação de questionário eletrônico, o qual foi enviado aos membros das Diretorias Gerais de Tecnologia da Informação (DGTI) das quarenta e duas (42) instituições da Rede Feral de Educação. Considerando a participação de 92% das instituições pesquisadas, os resultados obtidos com a pesquisa permitiram identificar a pouca adesão por parte dessas instituições à proposta do correio eletrônico auditável apresentada no decreto, pois somente 31% disseram utilizar um e-mail que permita a auditoria, como também a preferência de 69% dessas instituições pela utilização de um correio eletrônico não auditável, mesmo existindo o conhecimento por parte de 90% das instituições pesquisadas, quanto à existência da normativa. A respeito dos fatores considerados impeditivos para a adesão ao decreto, destaca-se a indicação feita por vinte e cinco (25) instituições que não aderiram à proposta do decreto, e 84% delas disseram que o motivo é por usarem atualmente uma ferramenta que atende às demandas e não gera custos para a instituição; 36% delas alegaram que é pela resistência dos usuários em adaptar-se a um novo correio eletrônico, e outros 36% alegaram que é por achar que a proposta do decreto não está bem definida. Outros fatores foram apresentados, somando 28% das indicações e todos eles estão relacionados à questões orçamentária. Com relação às sugestões apresentadas pelas vinte e cinco (25) instituições que responderam a pesquisa para que possa haver a adesão, 84% delas sugerem que o correio eletrônico proposto tenha um gerenciamento local, mas que não tenha custos para a instituição, enquanto que 68% não deseja ter nenhuma responsabilidade com o correio eletrônico. Outras sugestões apresentadas somaram 16% e dentre elas cita-se a necessidade de recursos orçamentários; que o gerenciamento seja feito por outros órgãos públicos e também cobrem a adesão massiva por parte dos órgãos do governo federal à proposta do decreto. Este estudo também propõe medidas para incentivar a adoção de um correio eletrônico auditável, mantido pela Rede Federal de Educação, de modo a amenizar os riscos com a segurança da informação na administração pública federal, e como forma de cumprimento da proposta do decreto.

**Palavras-Chave:** Comunicação de dados. Administração Pública Federal. Software Livre. Auditoria. Portaria 141/2014. Segurança da informação.

## ABSTRACT

In response to the denunciations made by the former CIA technician, Edward Snowden, reporting the espionage case against Brazil, Decree 8.135 / 2013, which provides for data communications of the direct federal public administration, autarchic and foundational, and adopts the electronic mail services along with their complementary functionalities offered by public administration bodies and entities, and must possess characteristics that allow the audit. Considering this normative, this work sought to carry out a study on the adherence of the institutions that take part in the Federal Network of Professional, Scientific and Technological Education to the electronic mail according to the decree. For this purpose, a bibliographic research and electronic questionnaire application was used, which was sent to the members of the Information Technology General Offices of the forty-two (42) institutions of the Federal Education Network. Considering the participation of 92% of the institutions surveyed, the results obtained with the research allowed the identification of the low adherence by such institutions to the proposal of the electronic mail presented in the decree, since only 31% said they use an e-mail that allows the audit, as well as the preference of 69% of these institutions for the use of non-auditable electronic mail, even though there was 90% knowledge of the institutions surveyed regarding the existence of regulations. Regarding the factors considered to impair adherence to the decree, the most noteworthy is the indication made by twenty-five (25) institutions that did not adhere to the proposal of the decree, and 84% of them said that the reason is for using currently a tool that meets demands and does not generate costs for the institution; 36% of them claimed that it is because of the resistance of users to adapt to a new e-mail, and another 36% claimed that it is because they think the proposal of the decree is not well defined. Other factors were presented, accounting for 28% of the indications and all of them are related to the budget issues. Concerning the suggestions presented by the twenty-five (25) institutions that answered the survey, 84% of them suggest that the proposed electronic mail should have local management, but that it may have no costs for the institution, while 68% do not wish to be held responsible for electronic mail. Other suggestions reached 16%, among them the need for budgetary resources; the management should be carried out by other public agencies that should also enforce a massive adhesion by the organs of the federal government to the decree. This study also proposes measures to encourage the adoption of an auditable electronic mail, maintained by the Federal Education Network, as a way to mitigate the risks to the safety of the federal public administration information, as well as a means to fulfill the decree.

**Keywords:** Auditable electronic mail. Data communication in the Federal Public Administration. Federal Education Network.



## LISTA DE GRÁFICOS

<b>Gráfico 1.1:</b> Clientes de e-mail utilizados nos Institutos Federais de Educação .....	18
<b>Gráfico 3.1:</b> Função na DGTI .....	57
<b>Gráfico 3.2:</b> Conhece o decreto 8.135/2013 .....	58
<b>Gráfico 3.3:</b> Usa e-mail auditável? .....	59
<b>Gráfico 3.4:</b> <i>E-mail</i> livre utilizado .....	61
<b>Gráfico 3.5:</b> Recursos positivos do Zimbra por região .....	62
<b>Gráfico 3.6:</b> Recursos positivos do Expresso por região.....	63
<b>Gráfico 3.7:</b> Recursos positivos do Rouncube por região .....	64
<b>Gráfico 3.8:</b> Recursos negativos do Zimbra por região.....	66
<b>Gráfico 3.9:</b> Recursos negativos do Expresso por região .....	67
<b>Gráfico 3.10:</b> Recursos negativos do Rouncube por região .....	68
<b>Gráfico 3.11:</b> Fator determinante para adesão ao e-mail livre .....	70
<b>Gráfico 3.12:</b> E-mail proprietário utilizado .....	71
<b>Gráfico 3.13:</b> Recursos positivos do Gmail por região .....	74
<b>Gráfico 3.14:</b> Recursos positivos do Exchange por região.....	75
<b>Gráfico 3.15:</b> Recursos positivos do Office 365 por região .....	76
<b>Gráfico 3.16:</b> Recursos negativos do Gmail por região .....	77
<b>Gráfico 3.17:</b> Recursos negativos do Exchange por região .....	78
<b>Gráfico 3.18:</b> Recursos negativos do Office 365 por região .....	79
<b>Gráfico 3.19:</b> Fatores que impedem a adesão ao decreto 8.135/2013 .....	80
<b>Gráfico 3.20:</b> Sugestões para adesão ao decreto 8.135/2013 .....	83
<b>Gráfico 4.1:</b> Orçamento da Rede Federal de Educação.....	93
<b>Gráfico 5.1:</b> Funções ocupadas nas DGTI (Validação) .....	101
<b>Gráfico 5.2:</b> Nível de aceitação à proposta apresentada (Validação) .....	102
<b>Gráfico 5.3:</b> Sugestões apresentadas (Validação) .....	104

## LISTA DE TABELAS

<b>Tabela 3.1:</b> Quantitativo de respostas obtidas com a pesquisa .....	50
<b>Tabela 3.2:</b> Quantitativo de campi por região .....	55

## LISTA DE QUADROS

<b>Quadro 2.1:</b> Instituições que compõem a Rede Federal de Educação .....	26
--	----

## LISTA DE ABREVIATURAS E SIGLAS

<b>ABIN</b>	Agência Brasileira de Inteligência
<b>APF</b>	Administração Pública Federal
<b>BACEN</b>	Banco Central do Brasil
<b>CDN</b>	Conselho de Defesa Nacional
<b>CEFET</b>	Centro Federal de Educação Profissional e Tecnológica
<b>CEFETMG</b>	Centro Federal de Educação Tecnológica de Minas Gerais
<b>CEFET-RJ</b>	Centro Federal de Educação Tecnológica Celso Suckow da Fonseca
<b>CEPESC</b>	Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações
<b>CGSI</b>	Gestor da Segurança da Informação
<b>CIA</b>	Central Intelligence Agency
<b>CISL</b>	Comitê de Implantação de <i>Software</i> Livre
<b>CONIF</b>	Conselho Nacional das Instituições da Rede Federal de Educação
<b>CP2</b>	Colégio Pedro II
<b>CPI</b>	Comissão Parlamentar de Inquérito
<b>CREDEN</b>	Câmara de Relações Exteriores e Defesa Nacional
<b>CTI</b>	Centro de Tecnologia da Informação
<b>CTIR</b>	Centro de Tratamento de Incidentes de Redes
<b>DATAPREV</b>	Empresa de Tecnologia e Informações da Previdência Social
<b>DGTI</b>	Diretorias Gerais de Tecnologia da Informação
<b>DICA</b>	Disponibilidade, Integridade, Confidencialidade e a Autenticidade
<b>DSIC</b>	Departamento de Segurança da Informação e Comunicações
<b>EGD</b>	políticas e estratégias de governança digital
<b>EGTIC</b>	Estratégia Geral de Tecnologia da Informação e Comunicações
<b>ePING</b>	Padrões de Interoperabilidade de Governo Eletrônico
<b>GCHQ</b>	Government Communications Headquarters
<b>GDS</b>	Government Digital Services
<b>GSI</b>	Gabinete de Segurança Institucional da Presidência da República
<b>GSTI-IF</b>	Grupo de Servidores de TI dos Institutos Federais
<b>GT</b>	Grupo de Trabalho
<b>ICA</b>	Instituto de Ciências Agrárias

<b>IF</b>	Instituto Federal
<b>IHC</b>	Interação Humano-Computador
<b>IRP</b>	Intenção de Registro de Preços
<b>ISSO</b>	International Organization for Standardization
<b>ISSN</b>	International Standard Serial Number
<b>LPM</b>	Licença Pública de Marca
<b>MC</b>	Ministério das comunicações
<b>MCTI</b>	Ministério das Ciências e Tecnologia
<b>MD</b>	Ministério da Defesa
<b>MF</b>	Ministério da Fazenda
<b>MP</b>	Ministério do planejamento, orçamento e gestão
<b>MPS</b>	Ministério da Previdência Social
<b>MRE</b>	Ministério das Relações Exteriores
<b>MRE</b>	Ministério das Relações Exteriores
<b>NSA</b>	National Security Agency
<b>NSC</b>	Núcleo de Segurança e Credenciamento
<b>PR</b>	Presidência da República
<b>RNP</b>	Rede Nacional de Pesquisa
<b>SAE</b>	Secretaria de Assuntos Estratégicos
<b>SegCiber</b>	Segurança Cibernética
<b>SEPIN</b>	Secretaria de Política de Informática
<b>SERPRO</b>	Serviço Federal de Processamento de Dados
<b>SIC</b>	Segurança da Informação e Comunicações
<b>SIOP</b>	Sistema Integrado de Planejamento e Orçamento
<b>SLTI</b>	Secretaria de Logística e Tecnologia da Informação
<b>TELEBRÁS</b>	Telecomunicações Brasileiras S.A
<b>TI</b>	Tecnologia da Informação
<b>TIC</b>	Tecnologia de informação e comunicação
<b>UFMG</b>	Universidade Federal de Minas Gerais
<b>UNED</b>	Unidade de Ensino Descentralizada
<b>USDS</b>	United States Digital Service
<b>UTFPR</b>	Universidade Tecnológica Federal do Paraná
<b>VOIP</b>	Voz sobre IP
<b>RFEPCT</b>	Rede Federal de Educação Profissional, Científica e Tecnológica

# SUMÁRIO

<b>1.</b>	<b>INTRODUÇÃO.....</b>	<b>16</b>
<b>1.1</b>	<b>As medidas contra as denúncias de espionagem .....</b>	<b>16</b>
<b>1.2</b>	<b>Pesquisa feita com os Institutos Federais sobre o correio eletrônico utilizado .....</b>	<b>17</b>
<b>1.3</b>	<b>Pergunta de pesquisa.....</b>	<b>19</b>
<b>1.4</b>	<b>Objetivos .....</b>	<b>19</b>
1.4.1	Objetivo Geral .....	19
1.4.2	Objetivos Específicos .....	19
<b>1.5</b>	<b>Metodologia de Pesquisa.....</b>	<b>19</b>
1.5.1	Participantes .....	21
1.5.2	Local da Pesquisa .....	21
1.5.3	Procedimentos .....	21
<b>1.6</b>	<b>Estrutura do trabalho .....</b>	<b>22</b>
<b>2.</b>	<b>COMUNICAÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL E A REDE FEDERAL DE EDUCAÇÃO.....</b>	<b>24</b>
<b>2.1</b>	<b>A Rede Federal de Educação.....</b>	<b>24</b>
2.1.2	Composição da Rede Federal de Educação .....	26
2.1.3	Expansão da Rede Federal de Educação .....	27
<b>2.2</b>	<b>Normativas sobre a comunicação de dados na Administração Pública Federal. ....</b>	<b>29</b>
2.2.1	O Decreto 8.135/2013 contra as denúncias de espionagem .....	30
2.2.2	A Portaria 141/2014 como normatização do Decreto 8.135/2013 .....	32
<b>2.3</b>	<b>Segurança da Informação na Rede Federal de Educação.....</b>	<b>37</b>
2.3.1	Cenário da segurança da informação na Administração Pública Federal .....	37

2.3.2	Estrutura do Departamento de Segurança da Informação e Comunicações .....	39
<b>2.4</b>	<b>Software livre na Administração Pública Federal .....</b>	<b>42</b>
2.4.1	As características do Software livre .....	43
2.4.2	O Software Público Brasileiro.....	44
2.4.3	A Estratégia de Governança Digital (EGD) brasileira .....	45
2.4.4	Estratégias de Governança Digital (EGD) internacionais .....	46
2.4.5	O uso do Software Proprietário na APF .....	47
<b>2.5</b>	<b>Considerações finais do capítulo .....</b>	<b>48</b>
<b>3.</b>	<b>O CORREIO ELETRÔNICO DA REDE FEDERAL DE EDUCAÇÃO. ....</b>	<b>50</b>
<b>3.1</b>	<b>Análise dos dados .....</b>	<b>53</b>
3.1.1	Identificação da Instituição e a função do respondente .....	53
3.1.2	O correio eletrônico livre e auditável utilizado .....	60
3.1.2.1	<u>Recursos positivos da ferramenta Zimbra</u> .....	62
3.1.2.2	<u>Recursos positivos da ferramenta Expresso</u> .....	63
3.1.2.3	<u>Recursos positivos da ferramenta Roundcube</u> .....	64
3.1.2.4	<u>Recursos negativos da ferramenta Zimbra</u> .....	66
3.1.2.5	<u>Recursos negativos da ferramenta Expresso</u> .....	67
3.1.2.6	<u>Recursos negativos da ferramenta Roundcube</u> .....	67
3.1.3	O correio eletrônico proprietário e não auditável utilizado .....	70
3.1.3.1	<u>Recursos positivos da ferramenta Gmail</u> .....	74
3.1.3.2	<u>Recursos positivos da ferramenta Exchange</u> .....	75
3.1.3.3	<u>Recursos positivos da ferramenta Office 365</u> .....	76
3.1.3.4	<u>Recursos negativos da ferramenta Gmail</u> .....	77
3.1.3.5	<u>Recursos negativos da ferramenta Exchange</u> .....	78
3.1.3.6	<u>Recursos negativos da ferramenta Office 365</u> .....	79

3.1.4	Fatores impeditivos para adesão ao decreto 8.135/2013 .....	79
3.1.5	Sugestões apresentadas para facilitar a adesão ao decreto 8.135/2013 .....	82
<b>3.2</b>	<b>Considerações finais do capítulo .....</b>	<b>85</b>
<b>4.</b>	<b>CONJUNTO DE RECOMENDAÇÕES.....</b>	<b>86</b>
<b>4.1</b>	<b>Fatores impeditivos para adesão ao correio eletrônico nos moldes do decreto e sugestões apresentadas na pesquisa.....</b>	<b>86</b>
4.1.1	Uso de uma ferramenta que atende às demandas e não gera custos .....	87
4.1.2	Resistência dos usuários em adaptar-se a um novo correio eletrônico.....	88
4.1.3	Por achar que a proposta do decreto não está bem definida .....	89
4.1.4	Fatores apresentados no campo Outro .....	91
4.1.5	Investimentos já feitos e/ou contratos ainda vigentes .....	94
4.1.6	Alternativa ao correio eletrônico do decreto .....	94
<b>4.2</b>	<b>Considerações finais do capítulo .....</b>	<b>96</b>
<b>5.</b>	<b>CONSIDERAÇÕES FINAIS DO TRABALHO .....</b>	<b>97</b>
<b>5.1</b>	<b>Limitações do trabalho.....</b>	<b>97</b>
<b>5.2</b>	<b>Sugestões de trabalhos futuros.....</b>	<b>98</b>
<b>5.3</b>	<b>Validação da proposta apresentada neste trabalho .....</b>	<b>98</b>
5.3.1	Identificação da instituição e do respondente da validação .....	100
5.3.2	Avaliação da proposta apresentada e sugestões do respondente .....	101
	<b>REFERÊNCIAS.....</b>	<b>105</b>
	<b>APÊNDICE A – Questionário utilizado na coleta de dados .....</b>	<b>110</b>
	<b>APÊNDICE B – Questionário utilizado na validação .....</b>	<b>115</b>
	<b>ANEXO A – Lei nº 11.892/2008 – Lei de instituição dos IFET.....</b>	<b>117</b>
	<b>ANEXO B – Decreto nº 8.135/2013 .....</b>	<b>131</b>
	<b>ANEXO C – Portaria 141/2014 .....</b>	<b>133</b>





## 1. INTRODUÇÃO

Neste capítulo serão apresentadas as denúncias feitas pelo ex-técnico da CIA (Central Intelligence Agency), Edward Snowden, sobre a espionagem americana que atingiu diretamente o governo brasileiro e as normativas criadas a partir dessas denúncias, visando garantir a segurança das informações na Administração Pública Federal (APF).

Serão apresentados ainda, a argumentação que justifica o desenvolvimento desse trabalho, os objetivos propostos e a metodologia a ser utilizada para o desenvolvimento do mesmo.

### 1.1 As medidas contra as denúncias de espionagem

Considerando as denúncias de espionagem do ex-técnico da CIA (Central Intelligence Agency), Edward Snowden, de que os Estados Unidos estariam monitorando *e-mails* e ligações telefônicas de brasileiros G1 (2014), o Governo Federal, visando obter uma infraestrutura de comunicação e informação confiável e após ouvir o Conselho de Defesa Nacional, assina o decreto no 8.135, de 4 de novembro de 2013.

O decreto dispõe sobre as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional e, também, sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional. BRASIL (2013).

O § 5º do referido decreto afirma que esse é um ato conjunto dos ministros de estado da defesa (MD), do planejamento, orçamento e gestão (MP) e das comunicações (MC) e que estes entes públicos estarão responsáveis por disciplinar o disposto neste artigo e estabelecerão procedimentos, abrangência e prazos de implementação.

No Artigo 1º, § 2º do mesmo decreto é afirmado que os órgãos e entidades da União a que se refere o caput deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da Administração Pública Federal. Segundo Veloso (2014), referindo-se ao serviço de correio eletrônico,

afirma que a APF terá uma contratação restrita a um único fornecedor, no caso, o Serviço Federal de Processamento de Dados – Serpro, uma vez ser essa a única empresa com capacidade de prover tais serviços para os órgãos e entidades, com a ferramenta Expresso<sup>1</sup>, que já é utilizada por vários órgãos federais.

Embora exista, por parte do governo federal, a necessidade de melhorar os serviços de comunicação de dados da APF, visando à segurança das informações, e em particular a possível utilização do sistema de correio eletrônico Expresso do Serpro, entende-se que a realidade atual é bem diversificada e também desafiadora, e necessitará de uma reestruturação para que se enquadre na proposta do decreto 8.135.

## **1.2 Pesquisa feita com os Institutos Federais sobre o correio eletrônico utilizado**

A partir do conhecimento das exigências apresentadas no Decreto 8.135/2014 quanto à utilização de um correio eletrônico auditável e considerando a existência do Grupo de Servidores de TI dos Institutos Federais, GSTI-IF (2016), e que o mesmo mantém uma planilha com os dados das soluções utilizadas por essas instituições, foi possível fazer uma análise prévia do cenário dos correios eletrônicos utilizados.

Os resultados da análise que pode ser visto no Gráfico 1.1, mostra a existência de uma diversidade de clientes de *e-mail* em uso nos Institutos Federais e esse cenário é caracterizado pela falta de padronização dos correios eletrônicos utilizados nas comunicações de dados da Administração Pública Federal.

Pode-se observar que a empresa Google, com o seu cliente Gmail<sup>2</sup>, ocupa o maior percentual de utilização desses clientes, seguido do Zimbra<sup>3</sup> com 20%, Exchange<sup>4</sup> com 15,6%, Expresso com 13,3% e numa fatia menor, o iRedmail<sup>5</sup> com apenas 2,2% do percentual de utilização nas instituições.

---

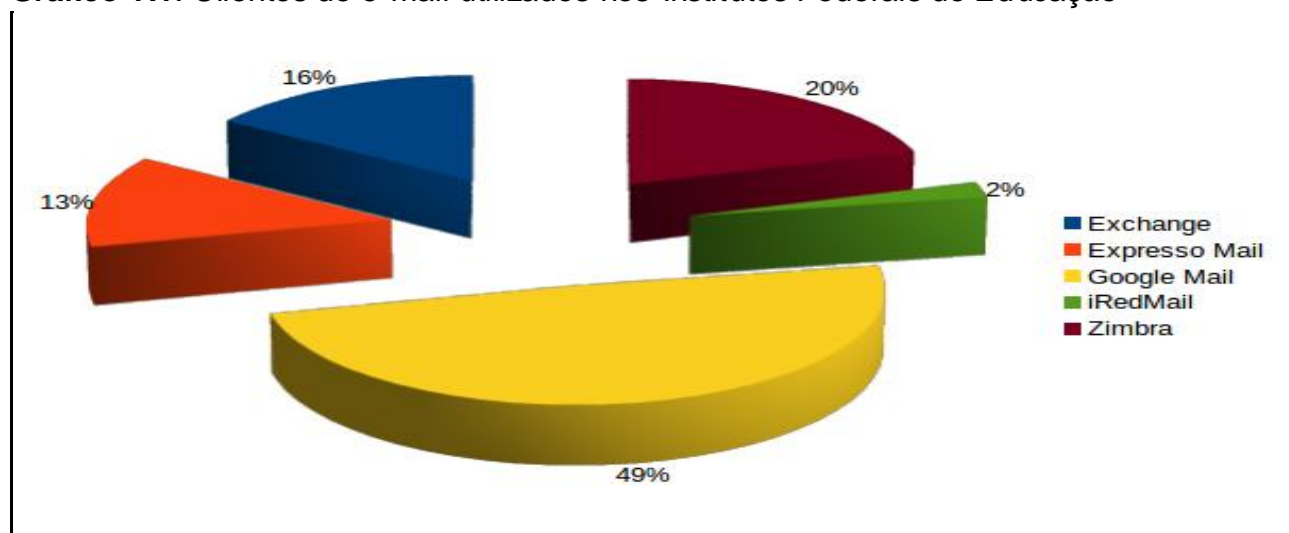
1 Suíte de comunicação Expresso - <http://comunidadeexpresso.serpro.gov.br/>

2 Sistema de correio eletrônico da Google - [www.gmail.com](http://www.gmail.com)

3 Sistema de correio eletrônico Open Source - [www.zimbra.org](http://www.zimbra.org)

4 Sistema de correio eletrônico da Microsoft - <https://products.office.com/pt-br/exchange/email>

5 Sistema de correio eletrônico Open Source - [www.iredmail.org](http://www.iredmail.org)

**Gráfico 1.1:** Clientes de e-mail utilizados nos Institutos Federais de Educação

Fonte: Fórum GSTI 2016

Observa-se ainda a existência de uma grande representatividade de programas proprietários para atender às demandas de correio eletrônico nas instituições pesquisadas, pois os clientes Gmail e Exchange, pertencentes respectivamente às empresas Google<sup>6</sup> e Microsoft<sup>7</sup>, são utilizados por um número significativo de instituições.

Merece atenção o fato do cliente Expresso do Serpro ser apontado como alternativa para atender as exigências do decreto 8.135/2013 e normativas geradas a partir dele, ocupar ainda uma parcela irrelevante, ficando com um percentual abaixo de outros clientes de *e-mail* pertencentes à categoria de *Software* livre, como é o caso do Zimbra, o que mostra ainda uma baixa adesão a essa ferramenta, por parte das instituições pesquisadas.

Diante do exposto acima, observa-se um quantitativo diversificado de clientes de *e-mail* que são utilizados nos Institutos Federais de Educação com o objetivo de atenderem as demandas de comunicação e em específico do sistema de correio eletrônico. No entanto, percebe-se uma falta de padronização desses clientes de *e-mail* e uma grande representatividade de clientes de *e-mails* proprietários, o que está em desacordo com o que orienta o decreto 8.135/2013.

<sup>6</sup> Sistema de busca na Internet - [www.google.com](http://www.google.com)

<sup>7</sup> Empresa de soluções de TI - [www.microsoft.com](http://www.microsoft.com)

### 1.3 Pergunta de pesquisa

Qual o nível de adesão e os fatores que influenciam a decisão das instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPECT) em aderir ou não à ferramenta de correio eletrônico que atenda aos critérios recomendados no Decreto 8.135/2013?

### 1.4 Objetivos

A proposta desse trabalho é apresentada de forma macro, por meio do objetivo geral e fragmentada em tópicos definidos nos objetivos específicos.

#### 1.4.1 Objetivo Geral

Analisar a aderência das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica ao correio eletrônico nos moldes do decreto 8.135/2013.

#### 1.4.2 Objetivos Específicos

- Identificar a natureza do correio eletrônico das instituições quanto a ser *Software* livre ou proprietário;
- Analisar se as características do correio eletrônico utilizado estão de acordo com a proposta do decreto;
- Identificar e avaliar os fatores determinantes das instituições, quanto a adesão ou não, ao correio eletrônico livre e auditável, de acordo com o decreto 8.135/2013;
- Propor um conjunto de recomendações que facilite a adesão das referidas instituições ao modelo de correio eletrônico proposto na referida lei.

### 1.5 Metodologia de Pesquisa

A pesquisa se caracteriza como sendo de natureza exploratória, que segundo Gil (2010), tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses.

O autor ainda relata que a grande maioria dessas pesquisas envolve: (a) levantamento bibliográfico; (b) entrevistas com pessoas que tiveram experiências práticas com o problema pesquisado; e, (c) análise de exemplos que estimulem a compreensão. Ainda segundo o mesmo autor, essas pesquisas podem ser classificadas como: pesquisa bibliográfica e estudo de caso.

Como estratégia de pesquisa será utilizada a revisão de literatura, da qual serão recolhidas as informações documentais sobre os conhecimentos já acumulados acerca do tema da pesquisa.

Adicionalmente será feita a análise dos formulários obtidos por meio da pesquisa com *Survey* que segundo Fonseca (2002, p. 33), referindo-se a esse tipo de pesquisa, afirma que pode ser considerada como sendo a “obtenção de dados ou informações sobre as características ou as opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo, utilizando um questionário como instrumento de pesquisa”.

Para Santos (1999), a pesquisa *Survey* busca informação diretamente com um grupo de interesse a respeito dos dados que se deseja obter. Trata-se de um procedimento útil, especialmente em pesquisas exploratórias e descritivas.

Quanto à abordagem, será utilizada a qualitativa e quantitativa, pois, segundo Fonseca (2002, p. 20), a utilização conjunta da pesquisa qualitativa e quantitativa, permite recolher mais informações do que se poderia conseguir isoladamente.

Deslauriers (1991, p. 58) diz que, na abordagem qualitativa o desenvolvimento da pesquisa é imprevisível e o conhecimento do pesquisador é parcial e limitado. O objetivo da amostra é de produzir informações aprofundadas e ilustrativas: seja ela pequena ou grande, o que importa é que ela seja capaz de produzir novas informações.

Fonseca (2002, p. 20) esclarece que na abordagem quantitativa, os resultados da pesquisa podem ser quantificados. Como as amostras geralmente são

grandes e consideradas representativas da população, os resultados são tomados como se constituíssem um retrato real de toda a população alvo da pesquisa. A pesquisa quantitativa se centra na objetividade.

Quando fala da atitude do pesquisador quanto ao objeto a ser estudado, Fonseca (2002, p. 33) diz que não existe a pretensão do mesmo de exercer uma intervenção sobre o objeto de estudo, mas revelá-lo como tal e como ele o percebe.

#### 1.5.1 Participantes

Os participantes da pesquisa correspondem aos membros das Diretorias Gerais de Tecnologia da Informação (DGTI) das instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica do Brasil.

#### 1.5.2 Local da Pesquisa

Instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica do Brasil.

#### 1.5.3 Procedimentos

Para a realização deste trabalho, inicialmente, será aplicado um questionário eletrônico (*survey*), que segundo Tanur apud Pinsonneault & Kraemer (1993), se referindo a esse tipo de pesquisa, diz que pode ser descrita como a obtenção de dados ou informações sobre características, ações ou opiniões de determinado grupo de pessoas, indicado como representante de uma população-alvo, por meio de um instrumento de pesquisa, normalmente um questionário.

Santos (1999), define como o tipo de pesquisa que busca informação diretamente com um grupo de interesse a respeito dos dados que se deseja obter. Trata-se de um procedimento útil, especialmente em pesquisas exploratórias e descritivas e Fonseca (2002, p. 33) se refere como o tipo de pesquisa que visa à obtenção de dados ou informações sobre as características ou as opiniões de determinado grupo de

peessoas, indicado como representante de uma população-alvo, utilizando um questionário como instrumento de pesquisa.

Esse questionário eletrônico será direcionado às Diretorias Gerais de Tecnologia da Informação (DGTI) das instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica do Brasil, visando coletar informações sobre a estrutura de correio eletrônico existente e sobre fatores influenciadores na adesão ou não adesão da instituição ao *e-mail* livre e auditável de acordo com que é sugerido decreto.

Após obtenção dos dados, as respostas dos questionários serão tabuladas, transformadas em gráficos e analisadas com base na fundamentação teórica, visando mapear a estrutura de comunicação via correio eletrônico que é utilizada por essas instituições e analisar a influência dos fatores determinantes da adesão ou não adesão ao modelo de correio eletrônico proposto no decreto 8.135/2013.

## **1.6 Estrutura do trabalho**

Este trabalho está dividido em cinco capítulos, e em seguida é apresentada a estrutura dos mesmos de acordo com o conteúdo abordado em cada capítulo.

No Capítulo 2, além do histórico da Rede Federal de Educação Profissional, Científica e Tecnológica, são apresentadas as normativas que dispõem sobre as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional e o que dizem os autores sobre a aplicação e adesão a essas normativas. Em seguida são apresentados ainda, os conceitos sobre segurança da informação a sua aplicação na comunicação de dados na Rede Federal de Educação e o uso do *Software* Livre na Administração Pública Federal.

No Capítulo 3, será apresentado o detalhamento do questionário aplicado junto as instituições, os resultado obtidos através do mesmo e as considerações do autor referente a análise desses dados de modo a construir um diagnóstico sobre a



aderência ou não aderência das instituições analisados ao serviço de correio eletrônico proposto no decreto 8.135/2013.

No Capítulo 4 será definido um conjunto de recomendações gerado a partir da análise dos dados realizada no Capítulo 3, que possa servir para solucionar problemas identificados na pesquisa, facilitar a adesão ao decreto 8.135/2013 e nortear as futuras ações relacionadas à utilização de ferramentas de correio eletrônico na Administração Pública Federal.

No Capítulo 5 serão destacadas as contribuições conseguidas a partir deste trabalho, as limitações identificadas e também serão apresentadas sugestões para trabalhos futuros que possam contribuir ainda mais com o tema pesquisado.

## **2. COMUNICAÇÃO DE DADOS NA ADMINISTRAÇÃO PÚBLICA FEDERAL E A REDE FEDERAL DE EDUCAÇÃO**

Neste capítulo será apresentado o histórico da Rede Federal de Educação Profissional, Científica e Tecnológica, as normativas que dispõem sobre as comunicações de dados da Administração Pública Federal Direta, Autárquica e Fundacional e opiniões de autores sobre a aplicação dessas normativas, como também, os conceitos sobre segurança da informação a sua aplicação na comunicação de dados na Rede Federal de Educação e o uso do *Software* Livre na Administração Pública Federal.

### **2.1 A Rede Federal de Educação.**

No portal da RFEPT<sup>8</sup>, é apresentado um histórico, que mostra desde o surgimento até o cenário atual da Rede Federal, e nesse histórico, o surgimento da Rede Federal se deu em 1909, por meio de ato do então Presidente da República, Nilo Peçanha, que inicialmente criou as 19 escolas de Aprendizes e Artífices e que, mais tarde, deram origem aos Centros Federais de Educação Profissional e Tecnológica (CEFET), (BRASIL, 2016a).

A Rede Federal de Educação Profissional, Científica e Tecnológica foi instituída pela Lei nº 11.892, de 29 de dezembro de 2008 (Anexo 1), que além de criar os Institutos Federais de Educação, Ciência e Tecnologia, dá outras providências BRASIL (2008).

No seu artigo 1º, é declarada a vinculação da Rede ao Ministério da Educação, e é apresentada a sua constituição com as seguintes instituições:

- I - Institutos Federais de Educação, Ciência e Tecnologia - Institutos Federais;
- II - Universidade Tecnológica Federal do Paraná – UTFPR;
- III - Centros Federais de Educação Tecnológica Celso Suckow da Fonseca - CEFET-RJ e de Minas Gerais – CEFET-MG;
- IV - Escolas Técnicas Vinculadas às Universidades Federais; e (Redação dada pela Lei nº 12.677, de 2012); BRASIL(2012)
- V - Colégio Pedro II. (Incluído pela Lei nº 12.677, de 2012)

---

<sup>8</sup> Rede Federal de Educação Profissional, Científica e Tecnológica: <http://redefederal.mec.gov.br/>

O portal da RFEPECT mostra o cenário atual com a existência de 38 Institutos Federais de Educação (IF), presentes em todos os estados, oferecendo cursos de qualificação, ensino médio integrado, cursos superiores de tecnologia e licenciaturas e ainda apresenta a estrutura da Rede com instituições que não aderiram ao processo de transformação dos Institutos Federais, mas também oferecem educação profissional em todos os níveis. São dois CEFET: (CEFET-RJ - Centro Federal de Educação Tecnológica Celso Suckow da Fonseca e CEFETMG - Centro Federal Minas Gerais), 25 escolas vinculadas a Universidades; Colégio Pedro II; e uma Universidade Tecnológica (UTFPR - Universidade Tecnológica Federal do Paraná).

O Artigo 1º da lei nº 11.892/2008 ainda possui um parágrafo único que apresenta as características das instituições mencionadas nos incisos I, II, III e V e dá a seguinte definição (BRASIL, 2008).

Parágrafo único. As instituições mencionadas nos incisos I, II, III e V do caput possuem natureza jurídica de autarquia, detentoras de autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar. (Redação dada pela Lei nº 12.677, de 2012)

O parágrafo acima não inclui o inciso IV da referida lei, que corresponde as Escolas Técnicas vinculadas às Universidades Federais, portanto, dá um tratamento diferenciado pois as mesmas não possuem natureza jurídica de autarquia, autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar, que é peculiar às demais instituições que compõem a Rede Federal de Educação Profissional e Tecnológica.

Segundo Pereira (2003), os Colégios Técnicos Vinculados às universidades, são instituições sem autonomia administrativa, financeira e orçamentária mantidas pelas universidades federais. Ministram o ensino médio e a educação profissional no nível técnico voltado para o setor industrial, agrícola e de serviços.

Dessa forma, as instituições citadas nos incisos II, III e V (Universidade Tecnológica Federal do Paraná – UTFPR, Centros Federais de Educação Tecnológica Celso Suckow da Fonseca - CEFET-RJ e de Minas Gerais – CEFET-MG e Colégio

Pedro II), não foram transformadas em Institutos Federais de Educação, mas fazem parte da Rede Federal de Educação Profissional, Científica e Tecnológica, oferecendo educação profissional em todos os níveis, além de possuírem natureza jurídica de autarquia, autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar.

### 2.1.2 Composição da Rede Federal de Educação

Atualmente, a RFEPCT está presente em todo o território nacional, conforme mostra o Quadro 2.1.

**Quadro 2.1:** Instituições que compõem a Rede Federal de Educação

N.	REGIÃO	CIDADE	SIGLA	INSTITUIÇÃO
1	Norte	Acre	IFAC	IF do Acre
2	Nordeste	Alagoas	IFAL	IF de Alagoas
3	Norte	Amapá	IFAP	IF do Amapá
4	Norte	Amazonas	IFAM	IF do Amazonas
5	Nordeste	Bahia	IFBA	IF da Bahia
6	Nordeste	Bahia	IFBAIANO	IF Baiano
7	Nordeste	Ceará	IFCE	IF do Ceará
8	Centro-Oeste	Distrito Federal	IFB	IF de Brasília
9	Sudeste	Espírito Santo	IFES	IF do Espírito Santo
10	Centro-Oeste	Goiás	IFG	IF de Goiás
11	Centro-Oeste	Goiás	IFGOIANO	IF Goiano
12	Centro-Oeste	Mato Grosso	IFMT	IF de Mato Grosso
13	Nordeste	Maranhão	IFMA	IF do Maranhão
14	Centro-Oeste	Mato Grosso do Sul	IFMS	IF de Mato Grosso do Sul
15	Sudeste	Minas Gerais	CEFETMG	Centro Federal de Educação Tecnológica de Minas Gerais
16	Sudeste	Minas Gerais	IFMG	IF de Minas Gerais
17	Sudeste	Minas Gerais	IFNMG	IF do Norte de Minas
18	Sudeste	Minas Gerais	IFSUDESTEMG	IF Sudeste de Minas Gerais
19	Sudeste	Minas Gerais	IFSULDEMINAS	IF do Sul de Minas
20	Sudeste	Minas Gerais	IFTM	IF do Triângulo Mineiro
21	Norte	Pará	IFPA	IF do Pará
22	Nordeste	Paraíba	IFPB	IF da Paraíba
23	Sul	Paraná	UTFPR	Universidade Tecnológica Federal do Paraná
24	Sul	Paraná	IFPR	IF do Paraná
25	Nordeste	Pernambuco	IFPE	IF de Pernambuco
26	Nordeste	Pernambuco	IFSERTAO-PE	IF do Sertão Pernambucano
27	Nordeste	Piauí	IFPI	IF do Piauí
28	Sudeste	Rio de Janeiro	CEFET-RJ	Centro Federal de Educação Tecnológica

N.	REGIÃO	CIDADE	SIGLA	INSTITUIÇÃO
				Celso Suckow da Fonseca
29	Sudeste	Rio de Janeiro	CP2	Colégio Pedro II
30	Sudeste	Rio de Janeiro	IFF	IF Fluminense
31	Sudeste	Rio de Janeiro	IFRJ	IF do Rio de Janeiro
32	Nordeste	Rio Grande do Norte	IFRN	IF do Rio Grande do Norte
33	Sul	Rio Grande do Sul	IFFARROUPILHA	IF Farroupilha
34	Sul	Rio Grande do Sul	IFRS	IF do Rio Grande do Sul
35	Sul	Rio Grande do Sul	IFSUL	IF Sul-Rio-Grandense
36	Norte	Rondônia	IFRO	IF de Rondônia
37	Norte	Roraima	IFRR	IF de Roraima
38	Sudeste	São Paulo	IFSP	IF de São Paulo
39	Sul	Santa Catarina	IFC	IF Catarinense
40	Sul	Santa Catarina	IFSC	IF de Santa Catarina
41	Nordeste	Sergipe	IFS	IF de Sergipe
42	Norte	Tocantins	IFTO	IF de Tocantins

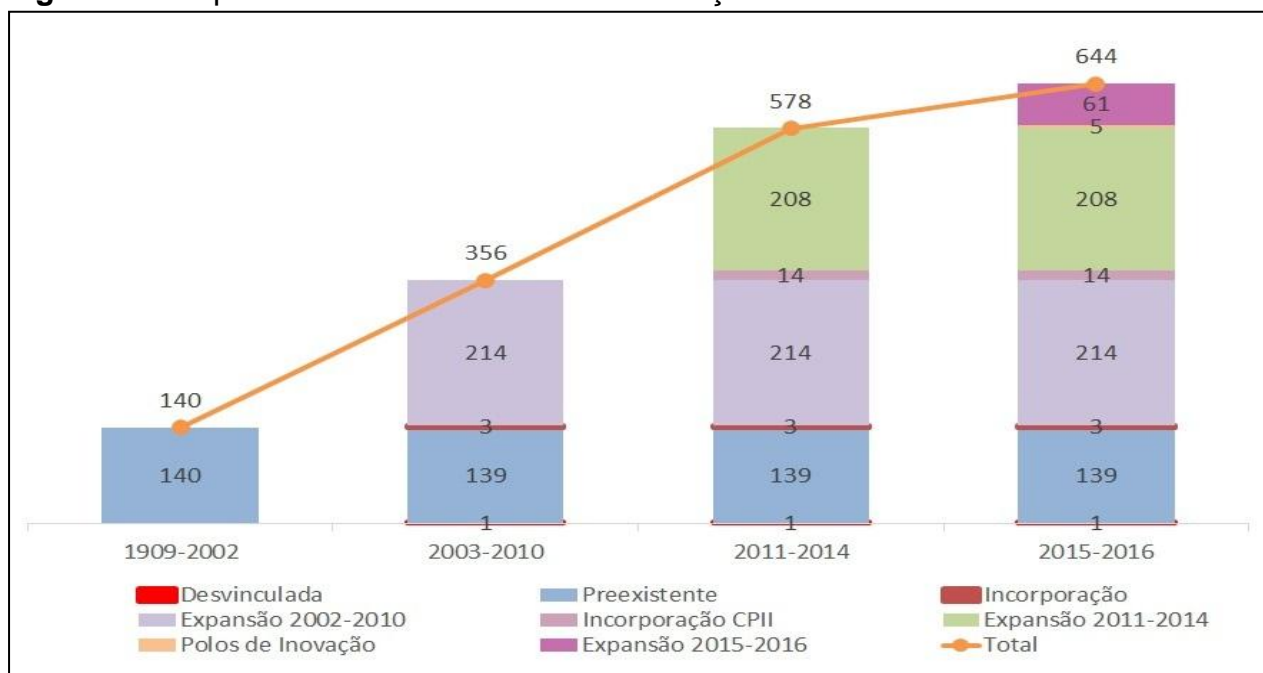
Fonte: Portal da Rede Federal de Educação Profissional, Científica e Tecnológica (2016)

O artigo 2º da lei nº 11.892/2008 apresenta os Institutos Federais de Educação, Ciência e Tecnologia como instituições de educação superior, básica e profissional, pluricurriculares e *multicampi*, especializadas na oferta de educação profissional e tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas, nos termos desta lei e os equipara às universidades federais.

Diante de um cenário econômico produtivo, surgido na década de 1980, com desenvolvimento de novas tecnologias agregadas à produção e à prestação de serviços, as Instituições de Educação Profissional vêm buscando a diversificação de programas e cursos que permitam elevar os níveis dos serviços ofertados e atualmente a Rede Federal de Educação cobre todo o território nacional com a sua missão de qualificar profissionais para os diversos setores da economia brasileira.

### 2.1.3 Expansão da Rede Federal de Educação

Quando se refere ao cenário de expansão atual da Rede Federal, seu portal na Internet apresenta como sendo a maior expansão de sua história e identifica as etapas dessa expansão no gráfico da Figura 2.1.

**Figura 2.1:** Expansão da Rede Federal de Educação

Fonte: Portal da Rede Federal de Educação Profissional, Científica e Tecnológica (2016).

A Nota Técnica nº 50/2016 de 06 de maio de 2016 faz um melhor detalhamento das etapas de expansão da Rede Federal de Educação e apresenta no item 1.11 a seguinte descrição (BRASIL, 2016b).

Antes da publicação da Lei nº 11.892/2008, a Rede Federal, apesar de não instituída formalmente, era composta por 140 unidades, sendo uma delas a Escola Técnica Vinculada ao Núcleo Avançado de Ciências Agrárias da Universidade Federal de Minas Gerais (UFMG). Em 2008, essa escola foi transformada em Instituto de Ciências Agrárias – ICA, e já não incorporou o rol de unidades listadas no Anexo III na Lei nº 11.892/2008. Em 2009, passou a ofertar cursos de graduação e foi incorporada como campus pela UFMG (Campus Montes Claros), ficando a Rede Federal com 139 unidades.

Com a transformação da Escola Técnica Vinculada ao Núcleo Avançado de Ciências Agrárias da Universidade Federal de Minas Gerais (UFMG) em Instituto de Ciências Agrárias – ICA, e posteriormente ter sido transformado em campus pela UFMG (Campus Montes Claros), o quantitativo inicial que compunha a Rede diminuiu de 140, para 139 instituições, como pode ser visto a partir da segunda coluna, na primeira linha do Gráfico 1, no qual a referida instituição é representada pelo número 1.

No item 1.12 da Nota Técnica nº 50/2016, é feita referência à incorporação de mais quatro (4) novas unidades à Rede Federal, e a narrativa é feita como se segue:

1.12. Na publicação da mesma Lei, houve a incorporação de três Escolas Técnicas Vinculadas: Escola Técnica de Artes da Universidade Federal de Alagoas, Colégio Universitário da Universidade Federal do Maranhão e a Escola Agrotécnica da Universidade Federal de Roraima.

Essas três (3) instituições estão representadas na segunda linha da segunda coluna do gráfico da Figura 1. Na segunda coluna ainda são apresentadas as 214 instituições incorporadas na expansão de 2003 a 2010.

Na terceira coluna do referido gráfico, tem-se ainda a incorporação das 14 unidades do Colégio Pedro II, que se deu por meio do art. 5º da Lei 12.677/2012, seguida da inclusão de mais 208 instituições, resultantes da expansão de 2011 a 2014.

Por último, na coluna quatro do gráfico da Figura 2.1, é apresentada a incorporação dos cinco (5) polos de inovação e mais 61 unidades integrantes da estrutura organizacional da Rede Federal, totalizando dessa forma, 644 unidades.

Enquanto num período de 93 anos (1909 a 2002), a Rede Federal teve a construção de apenas 140 unidades, uma grande expansão aconteceu em um curto período de 13 anos (2003 e 2016), no qual se deu a construção de mais 500 novas unidades, totalizando dessa forma, 644 *campi* em funcionamento, pertencentes à RFEPCT.

## **2.2 Normativas sobre a comunicação de dados na Administração Pública Federal.**

Segundo o site G1 (2014), o ex-técnico da CIA Edward Snowden, é acusado de espionagem por vazar informações sigilosas de segurança dos Estados Unidos e revelar em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana – utilizando servidores de empresas como Google, Apple<sup>9</sup> e Facebook<sup>10</sup> e vários países da Europa e da América Latina, entre eles o Brasil, inclusive

---

<sup>9</sup> Empresa que oferece soluções na área de TI – [www.apple.com](http://www.apple.com)

<sup>10</sup> Rede social – [www.facebook.com](http://www.facebook.com)

fazendo o monitoramento de conversas da então presidente Dilma Rousseff com seus principais assessores.

Segundo Harding (2014), a NSA<sup>11</sup> (National Security Agency) juntamente com o seu parceiro britânico, o GCHQ<sup>12</sup> (Government Communications Headquarters), visando espionar as comunicações mundiais, tinham ligado secretamente interceptadores de dados aos cabos de fibra ótica submarinos que circundam o globo. Além desses recursos, também contavam com tribunais secretos, que convenciam empresas de telecomunicações a entregar seus dados. O autor diz que a espionagem ia mais além, quando afirma que praticamente todo o Vale do Silício<sup>13</sup> estava envolvido com a NSA e a mesma alegava ter “acesso direto” aos servidores das gigantes da tecnologia.

#### 2.2.1 O Decreto 8.135/2013 contra as denúncias de espionagem

Esse vazamento de informações sigilosas; chamou a atenção do Governo Brasileiro para a questão da segurança das informações e comunicações do Brasil, e como resposta às denúncias de espionagem americanas, a então presidente da república Dilma Rousseff, após ouvir o Conselho de Defesa Nacional, assina o decreto nº 8.135, de 4 de novembro de 2013 (Anexo 2), o qual dispõe sobre as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional e, também, sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

Segundo Kuhn (2016), o Decreto 8.135/2013 mudou o patamar da Tecnologia da Informação (TI) no país, elevando-a ao patamar de segurança nacional e puxou pra dentro do estado a responsabilidade da comunicação e da TI. O autor alerta também que não se tem como confiar nas estruturas nas quais são colocados esses dados, pois as mesmas podem estar fora do país e sujeitas à legislação desses países.

---

<sup>11</sup> Agência de Segurança Nacional dos Estados Unidos - [www.nsa.gov](http://www.nsa.gov)

<sup>12</sup> Serviço de inteligência britânico - [www.gchq.gov.uk](http://www.gchq.gov.uk)

<sup>13</sup> Região localizada na Califórnia, EUA, onde está situado um conjunto de empresas como objetivo de gerar inovações científicas e tecnológicas.



No Artigo 1º do decreto 8.135/2013, fica determinado que toda comunicação de dados da Administração Pública Federal deverá ser realizada por redes de comunicações e serviços de tecnologia da informação (TI), fornecidos por entidades do Governo Federal. Com relação à contratação de programas e equipamentos que serão utilizados para esta comunicação, o § 3º do mesmo artigo, diz que deverão possuir as características que permitam a auditoria, como forma de defesa das comunicações de dados da Administração Pública Federal.

Quando se fala em auditoria em equipamentos, a situação torna-se mais complicada pelo fato de que muitos equipamentos que são geridos no Brasil, não são fabricados por aqui e possuem uma arquitetura fechada, o que impossibilita a auditoria dos mesmos. Referindo-se a essas dificuldades, Grossmann (2013) apresenta a fala do presidente do Serpro, Marcos Mazoni, que cita os equipamentos e aplicativos, como roteadores Cisco<sup>14</sup>, servidores Oracle<sup>15</sup> e programas Microsoft, e lamenta “uma série de componentes no ambiente que, embora gerido por nós, não são controlados por nós”.

Referindo-se à afirmativa contida no Decreto 8.135/2013, de que os órgãos e entidades da união deverão usar necessariamente, ferramentas de estatais, empresas públicas ou de economia mista, Grossmann (2016) afirma ainda que o referido Decreto também permite a contratação delas com dispensa de licitação, nos casos em que possam comprometer a segurança nacional.

Já para Moraes (2013), a contratação por dispensa de licitação, apresentada no decreto, reforça que existe uma obrigação positiva para a Administração Pública Federal, qual seja, os serviços enumerados no art. 1º, devem, e não podem, ser contratados de “órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias”, sendo um comando positivo impositivo exarado legitimamente pela Chefia do Poder Executivo Federal à Administração que lhe está subordinada.

---

<sup>14</sup> Empresa que oferece soluções para redes e comunicações – [www.cisco.com](http://www.cisco.com)

<sup>15</sup> Empresas que oferece soluções de TI - [www.oracle.com](http://www.oracle.com)

Considerando as regras da livre concorrência por meio das licitações realizadas no serviço público que visam à obtenção do menor preço e da qualidade do serviço prestado ou produto adquirido, Veloso (2014) afirma que tal situação pode ser considerada como desfavorável para os órgãos ou entidades da Administração Pública Federal, que passam a estar impedidos de realizar licitações abertas ao mercado de ampla concorrência.

Enquanto no decreto 8.135/2013 é apresentado o que deve ser feito como forma de garantia da segurança das informações do governo federal, a normatização do mesmo, com o detalhamento do que deverá ser feito, acompanhado de procedimentos, abrangência e prazos de implementação, são encontrados na Portaria Ministerial MP/MC/MD nº 141 de 02 de maio de 2014, a qual define normas de comunicação da rede federal visando obter uma infraestrutura de serviços confiáveis de comunicação e informação para o governo brasileiro (BRASIL, 2014a)

### 2.2.2 A Portaria 141/2014 como normatização do Decreto 8.135/2013

A Portaria Interministerial nº 141/2014 (Anexo 3), elaborada por grupos técnicos representativos do MP – Ministério do Planejamento<sup>16</sup>, MC – Ministério das Comunicações<sup>17</sup>, MD – Ministério da Defesa<sup>18</sup>, as empresas públicas SERPRO - Serviço Federal de Processamento de Dados<sup>19</sup>, DATAPREV - Empresa de Tecnologia e Informações da Previdência Social<sup>20</sup> e TELEBRÁS - Telecomunicações Brasileiras S.A.<sup>21</sup>, ouvindo representantes da RNP – Rede Nacional de Pesquisa, BACEN - Banco Central do Brasil<sup>22</sup>, GSI/PR- Gabinete de Segurança Institucional da Presidência da República<sup>23</sup> e MRE - Ministério das Relações Exteriores<sup>24</sup>, além do CTI/MCTI. Após a elaboração da Portaria, a mesma teve a aprovação das Secretarias Executivas do MP, MC e MD e em seguida, foi apresentada à direção do SERPRO, DATAPREV, TELEBRÁS, RNP e à

<sup>16</sup> Ministério do Planejamento, Desenvolvimento e Gestão - <http://www.planejamento.gov.br/>

<sup>17</sup> Ministério da Ciência, Tecnologia, Inovações e Comunicações <http://www.mcti.gov.br/>

<sup>18</sup> Ministério da Defesa - <http://www.defesa.gov.br/>

<sup>19</sup> Serviço Federal de Processamento de Dados - <http://www.serpro.gov.br/>

<sup>20</sup> Empresa de Tecnologia e Informações da Previdência Social - <http://portal.dataprev.gov.br/>

<sup>21</sup> Telecomunicações Brasileiras S.A - <http://www.telebras.com.br/>

<sup>22</sup> Banco Central do Brasil - <http://www.bcb.gov.br/>

<sup>23</sup> Gabinete de Segurança Institucional da Presidência da República - <http://www.gsi.gov.br/>

<sup>24</sup> Ministério das Relações Exteriores - <http://www.itamaraty.gov.br>

Casa Civil para fins de alinhamento estratégico com objetivos do Decreto no 8.135/2013 (BRASIL, 2015a)

A portaria 141/2014, apresenta no seu Art. 11, uma listagem dos serviços de tecnologia da informação que são abrangidos pela mesma:

- I - correio eletrônico;
- II - compartilhamento e sincronização de arquivos;
- III - mensageria instantânea;
- IV - conferência (teleconferência, telepresença e webconferência); e
- V - comunicação de voz sobre protocolo de internet (VoIP).

No Artigo 1º, § 1º da Portaria 141/2014, consta que o disposto no *caput* não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado e ao excluir esses serviços, Veloso (2014) afirma que o decreto permite o fornecimento de tais serviços por terceiros (empresas privadas) e que se pode considerar que isso se deve ao fato de que as empresas públicas e sociedades de economia mista não oferecerem tais produtos/serviços, e estão incapacitadas de assumirem tal responsabilidade.

No entanto, permitir que o fornecimento de serviços de telefonia fixa e móvel possa ser feito por empresas privadas, isso mostra a fragilidade na segurança das comunicações do governo, pois segundo a reportagem no site G1 (2014), os dados coletados por Snowden, mostraram que não só milhões de *e-mails* foram espionados, mas também, várias ligações de brasileiros e estrangeiros em trânsito no país foram monitoradas.

No Artigo 1º, § 2º da Portaria 141/2014, é apresentada a obrigatoriedade dos órgãos e entidades da União a que se refere o *caput* de adotarem os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da Administração Pública Federal. Para Veloso (2014), referindo-se ao serviço de comunicação via correio eletrônico como é apresentado no decreto, fica claro que a contratação ficará restrita a um único fornecedor, no caso o Serviço de Processamento de Dados - Serpro, com a sua ferramenta Expresso.

No Art. 1º, § 3º da Portaria 141/2014, é citado que os programas e equipamentos destinados às atividades de que trata o *caput* deverão possuir características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, e no inciso II do Art. 2º da mesma Portaria, é apresentada a seguinte definição para o termo auditoria:

II - auditoria: processos e procedimentos sistemáticos de levantamento de evidências que tem como objetivo verificar se os serviços de redes de telecomunicações e de tecnologia da informação atendem aos requisitos especificados previamente em termo de referência ou projeto básico para fins de garantia da disponibilidade, integridade, confidencialidade, autenticidade das informações;

Quanto às definições dos quatro atributos da segurança da informação, as mesmas podem ser encontradas respectivamente nos incisos III, VII, VIII e XIV do Art. 2º, como segue:

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

VII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VIII - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

XIV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

Referindo-se aos programas considerados auditáveis, é feita uma citação no Art. 14º, inciso II, § 3º da referida portaria, quando conclui que, para efeito da mesma, são considerados auditáveis o *Software* livre ou público brasileiro, e no Art. 2º, inciso XXII, é apresentada a seguinte definição para *Software* livre:

*Software* cujo modelo de licença livre atende a liberdade para executar o programa, estudar como o programa funciona e adaptá-lo para as suas necessidades, redistribuir cópias do programa e aperfeiçoar o programa e liberar os seus aperfeiçoamentos sem restrição.

Quanto ao que venha ser considerado como *Software* público brasileiro, ainda no Art. 2º, inciso XXIII, encontra-se a seguinte definição:

*Software público brasileiro: Software que adota um modelo de licença livre para o código-fonte, a proteção da identidade original entre o seu nome, marca, código-fonte, documentação e outros artefatos relacionados por meio do modelo de Licença Pública de Marca - LPM e é disponibilizado na Internet em ambiente virtual público, sendo tratado como um benefício para a sociedade, o mercado e o cidadão;*

Quanto ao prazo de adesão às prerrogativas dessa portaria, por parte dos órgãos que compõem a RFEPCT, o Art. 18º define um prazo de cinco anos, a contar da data de publicação desta portaria.

Art. 18. A migração dos serviços de redes de telecomunicações e de tecnologia da informação em operação ou ativos deve ocorrer no prazo máximo de sessenta meses a partir da vigência desta Portaria.

No entanto, para Grossmann (2016), referindo-se ao tempo de adesão a essas normas, o mesmo afirma que já se passaram mais de dois anos e meio da determinação de uso de redes e serviços de tecnologia da informação fornecidos por estatais, e que o uso de comunicações seguras pelo governo federal ainda atravessa o curso burocrático.

Após a publicação do decreto 8.135/2013 e como forma de regulamentação de parte desse decreto, foi criado um Grupo de Trabalho (GT) interministerial, temporário, que apresentou como um dos resultados dos trabalhos realizados nesse GT, a publicação da portaria 141/2014, e a elaboração dos seguintes documentos:

- Conjunto de Características, Critérios, Condições Mínimas e Medidas para Auditoria de Segurança da Informação em Programas e Equipamentos (BRASIL, 2015e);
- Cronograma para Implantação dos Critérios (BRASIL, 2015d); e
- Modelo de Governança e Gestão de Auditoria de Segurança da Informação em Programas e Equipamentos (BRASIL, 2015f).

Após o encerramento dos trabalhos do primeiro GT, foi publicada a Portaria nº 2, de 24 de fevereiro de 2015, na qual foi constituído o Grupo de Trabalho Permanente,

denominado GT-Auditoria, vinculado ao Segmento de Segurança da ePING<sup>25</sup> - Padrões de Interoperabilidade de Governo Eletrônico e que visa dar continuidade à regulamentação do restante do decreto (BRASIL, 2015b).

Este Grupo de Trabalho foi composto por servidores públicos de vários órgãos, com a finalidade de produzir, em conformidade com o que disciplina o Decreto 8.135/2013, e a Portaria Interministerial MP/MC/MD 141/2014, as seguintes ações que são apresentadas no Art. 1º da portaria 2/2015:

- Elaborar e zelar pelo seu regimento interno;
- Produzir o refinamento dos trabalhos realizados de acordo com a portaria slti/mp nº 54, de 6 de maio de 2014, considerando as contribuições recebidas em conformidade com o aviso de consulta pública nº 3, de 6 de novembro de 2014 (issn 1677-7069).
- Analisar e definir medidas necessárias para mitigar os riscos decorrentes de incidentes de segurança ou descoberta de vulnerabilidades nos serviços contratados de redes de comunicações e de tecnologia da informação;
- Consolidar um modelo de rede de colaboração envolvendo institutos de pesquisa e acadêmicos e órgãos e entidades da Administração Pública Federal para dar suporte na operação e na continuidade dos processos de auditoria em consonância com o disposto no decreto; e
- Prospectar, propor e coordenar iniciativas considerando que em seu art. 1º, § 3º, o decreto nº 8.135, de 4 de novembro de 2013, estabelece que os programas e equipamentos destinados às atividades de que trata o seu caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações.

As normativas apresentadas e que dispõe sobre as comunicações de dados da Administração Pública Federal, objetivam uma melhor segurança das informações e um maior controle sobre as mesmas. Na seção seguinte, será feita uma abordagem sobre como está sendo tratada a segurança das informações na Administração Pública Federal.

---

<sup>25</sup> ePING - define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da TIC na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.  
<http://eping.governoeletronico.gov.br>

## **2.3 Segurança da Informação na Rede Federal de Educação**

Considerando as espionagens denunciadas por Snowden e que afetaram diretamente a então presidente do Brasil e alguns órgãos federais, essas denúncias mostraram a existência de fragilidades na segurança das informações, bem como a necessidade de investimentos em ações que possam amenizar as fragilidades existentes, e que comprometem a segurança das informações na administração pública federal.

Embora os Estados Unidos justifiquem a maioria das suas ações de espionagem com o pretexto de proteção contra o terrorismo, segundo Kuhn (2016), a espionagem realizada contra o Brasil, foi por questão meramente econômica e não por terrorismo, e isso justifica a necessidade de maiores ações voltadas para a segurança da informação na administração pública.

### **2.3.1 Cenário da segurança da informação na Administração Pública Federal**

O “Guia básico de orientações ao gestor em segurança da informação e comunicações” na sua versão 2.0, referindo-se ao valor das informações da APF, diz que “as informações tratadas no âmbito da Administração Pública Federal, direta e indireta, são ativos valiosos para a eficiente prestação dos serviços públicos. Consequentemente, como ativo valioso e estratégico, a informação deve ser adequadamente tratada, armazenada e protegida” (BRASIL, 2016c, p. 14).

No “Livro Verde - Segurança Cibernética no Brasil” (BRASIL, 2010a, p.15), é apresentada a necessidade da construção de ambiente no país que permita sistematizar a identificação, a monitoração, a minimização e a mitigação de riscos cibernéticos. O mesmo apresenta ainda que tais ambientes contribuirão com a segurança das informações, impulsionando o desenvolvimento de ações preventivas, pró-ativas, reativas, e de repressão, a todo o tipo de ameaças, e que essas ações prescindem de Política de Estado, visando assegurar e defender os interesses do país e da sociedade brasileira.

A Segurança Cibernética é apresentada ainda como um desafio do século XXI, e que a mesma vem se destacando como função estratégica de Estado, e essencial à manutenção das infraestruturas críticas de um país, e que diante dos desafios, muitas nações vêm se preparando, para evitar ou minimizar ataques cibernéticos às redes e sistemas de informação de governo, bem como de todos os demais segmentos da sociedade (BRASIL, 2010a, p.13).

No referido livro, são destacados ainda os seguintes fenômenos da sociedade da Informação (BRASIL, 2010a, p.14).

- a) Elevada convergência tecnológica;
- b) Aumento significativo de sistemas e redes de informação, bem como da interconexão e interdependência dos mesmos;
- c) Aumento crescente e bastante substantivo de acesso à Internet e das redes sociais;
- d) Avanços das tecnologias de informação e comunicação (TIC);
- e) Aumento das ameaças e das vulnerabilidades de segurança cibernética; e,
- f) Ambientes complexos, com múltiplos atores, diversidade de interesses, e em constantes e rápidas mudanças”

Considerando os fenômenos da sociedade da Informação citados, vê-se que com o elevado aumento do uso da Internet e dos sistemas e redes de informação, aumenta também as vulnerabilidades e riscos à segurança da informação e referindo-se a isso, Coelho (2014, pag. 22), diz que “a segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizando os riscos e maximizando o retorno sobre os investimentos e as oportunidades de negócio”. Referindo-se a forma de obtê-la, o autor diz que a mesma é obtida como resultado da implementação de um conjunto de controles, compreendendo políticas, processos, procedimentos, estruturas organizacionais e funções de *hardware* e *Software*.

Algumas das fragilidades na área de segurança da informação são mostradas num Relatório final da Comissão Parlamentar de Inquérito, denominada CPI da Espionagem, no qual são apontadas fragilidades do Brasil frente à espionagem eletrônica Internacional. O mesmo relatório sugere medidas e propostas para a melhoria da segurança cibernética nacional, e evidencia a fragilidade do sistema de



telecomunicações brasileiro, como também do nosso sistema de inteligência e defesa cibernética (BRASIL, 2014b).

Referindo-se aos órgãos que tratam da Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas na Administração Pública Federal, O livro “Estratégia de segurança da informação e comunicações e de segurança cibernética da Administração Pública Federal 2015-2018: versão 1.0”, dá o seguinte relato (BRASIL, 2015c, pag. 17).

No Brasil, os assuntos relacionados à Segurança da Informação e Comunicações, Segurança Cibernética e Segurança das Infraestruturas Críticas vêm sendo tratados no âmbito do Conselho de Defesa Nacional (CDN) e da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), do Conselho de Governo, por intermédio do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que exerce as funções de Secretaria Executiva do citado Conselho e de Presidência daquela Câmara.

Anda são evidenciados os vários desafios enfrentados pelo Governo Federal, em especial a carência do estabelecimento de governança efetiva da Segurança da Informação e Comunicações (SIC), da Segurança Cibernética (SegCiber), da segurança dos ativos de informação críticas, e cita a carência de um órgão central que exerça coordenação executiva de tais temas, de forma sistêmica e participativa.

Como forma de representar o cenário a ser gerenciado na APF e que representa um importante desafio para a área de SIC e de SegCiber, é citado ainda que “na atualidade, são 39 ministérios, cerca de seis mil entidades governamentais, mais de um milhão de servidores federais, em torno de 320 grandes redes do Governo Federal, mais de 16,5 mil sítios de governo que superam 12 milhões de páginas WEB, e uma crescente participação e controle social” (BRASIL, 2015c, pag. 18)

### 2.3.2 Estrutura do Departamento de Segurança da Informação e Comunicações

Diante do cenário exposto a ser gerenciado, e para tratar das questões relacionadas à SIC e à SegCiber, o GSI/PR instituiu em 2006 o Departamento de

Segurança da Informação e Comunicações (DSIC), para atuar na APF, com a seguinte missão (BRASIL, 2009).

- I - orientar a implementação de ações de segurança da informação e comunicações, inclusive as de segurança cibernética, no âmbito da Administração Pública Federal;
- II - definir normativos e requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da Administração Pública Federal, no âmbito da Secretaria-Executiva do Conselho de Defesa Nacional;
- III - operacionalizar e manter o centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da Administração Pública Federal;
- IV - avaliar tratados, acordos ou atos internacionais relacionados ao tratamento e à troca de informação classificada;
- V - exercer, por meio do Núcleo de Segurança e Credenciamento, na qualidade de Órgão de Registro Central, atividades relacionadas ao credenciamento de segurança e ao tratamento de informação classificada; e
- VI - exercer outras atribuições que lhe forem determinadas pelo Assessor Chefe da Assessoria Especial da Secretaria-Executiva do Conselho de Defesa Nacional.

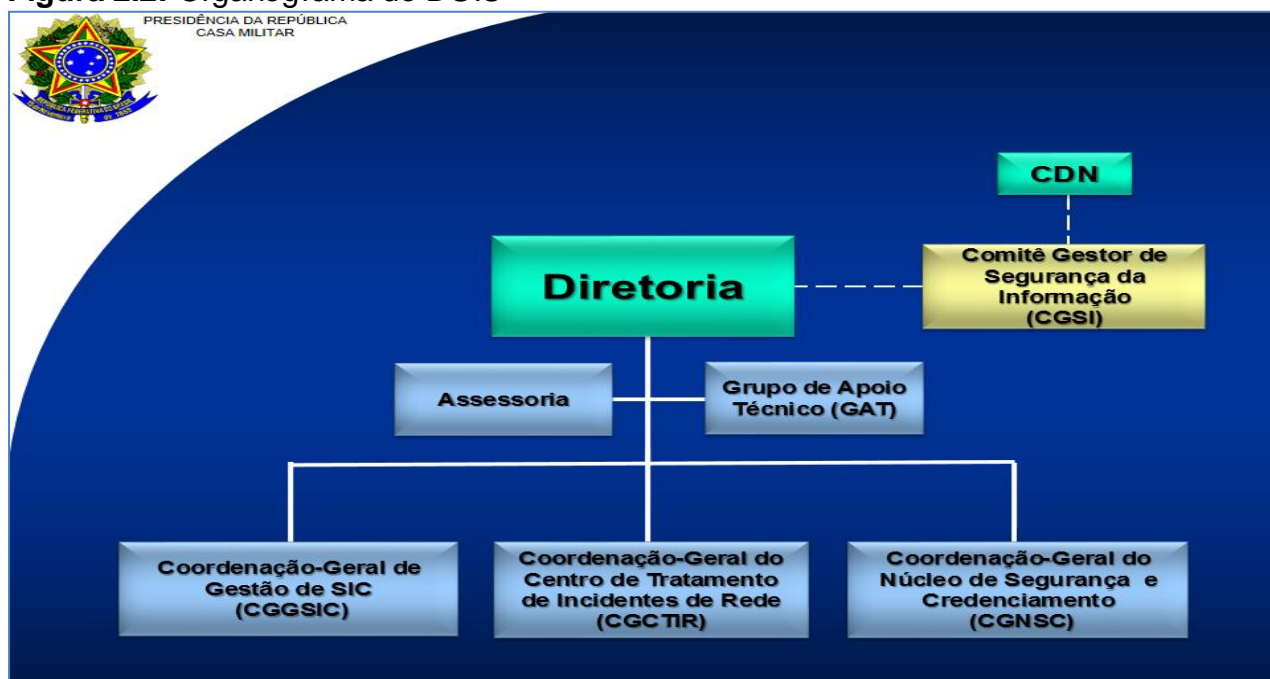
Para o cumprimento da missão apresentada anteriormente, o Departamento de Segurança da Informação e Comunicações (DSIC); possui três áreas finalísticas definidas, as quais são apresentadas na sequência e as respectivas coordenações que podem ser visualizadas no organograma do DSIC, representadas na Figura 2.2 (BRASIL, 2015c)

**Gestão de SIC** que executa o planejamento e a gestão orientada aos órgãos e entidades da APF e também é responsável pela gestão das reuniões do Comitê Gestor da Segurança da Informação (CGSI/CDN) [...];

**Centro de Tratamento de Incidentes de Redes da APF- (CTIR Gov)** que possui a missão de coordenar e acompanhar o tratamento e a resposta aos incidentes em redes computacionais da APF [...];

**Credenciamento de Segurança**, que após reformulação, estabeleceu-se o Núcleo de Segurança e Credenciamento (NSC) como órgão central da cadeia de credenciamento no âmbito do Poder Executivo Federal, com o objetivo de promover e regular o tratamento da informação classificada em qualquer grau de sigilo [...].

**Figura 2.2:** Organograma do DSIC



Fonte: <http://dsic.planalto.gov.br/organograma>

Ainda como órgão vinculado a GS/PR, é citada a Agência Brasileira de Inteligência (ABIN), e que possui na sua estrutura com o Centro de Pesquisas e Desenvolvimento para Segurança das Comunicações (CEPESC), com a finalidade de sanar deficiência do Brasil em garantir o sigilo dos canais de comunicação dos órgãos estratégicos da Administração Pública Federal (BRASIL, 2015, pag. 18)

Para Kuhn (2016), a administração pública federal brasileira não possui claramente um órgão responsável por centralizar a responsabilidade pela estrutura de TI do governo federal e cita os exemplos do SEPIN – Secretaria de Política de Informática no Ministério de Ciências e Tecnologia (MCT), SLTI - Secretaria de Logística e Tecnologia da Informação, no Ministério do Planejamento (MP), SERPRO - Serviço Federal de Processamento de Dados no Ministério da Fazenda (MF) e DATAPREV - Empresa de Tecnologia e Informações da Previdência Social no Ministério da Previdência Social (MPS)<sup>26</sup>.

Como forma de apresentar um pensamento estratégico para o futuro do Brasil, foi publicado em 2010, pela Secretaria de Estudos Estratégicos da Presidência da

<sup>26</sup> Ministério da Previdência Social - <http://www.previdencia.gov.br/>

República (SAE)<sup>27</sup>, o “Plano Brasil 2022”, que fixa metas para o ano de 2022, ano do bicentenário da independência brasileira. Desta forma, destacam-se abaixo algumas das metas a serem alcançadas para o centenário brasileiro (BRASIL, 2015c, pag. 19).

- I) **Economia**: modernizar o funcionamento da administração pública;
- II) **Sociedade**: universalizar o acesso aos bens e conteúdos culturais a todos os brasileiros;
- III) **Infraestrutura**: assegurar acesso integral à banda larga, à velocidade de 100 Mbps, a todos os brasileiros; e,
- IV) **Estado**: garantir pleno exercício do direito de acesso a informações públicas e consolidar a Internet como um terreno de liberdade de expressão.

Diante da evolução tecnológica e também das ameaças que comprometem a segurança da informação na APF, os temas de SIC e de SegCiber passaram a ser reconhecidos por vários atores do Governo Federal como sendo relevantes e de competência e coordenação político estratégica de órgão da Presidência da República, com abrangência para a APF, incluídas ações de segurança das infraestruturas críticas da informação.

## 2.4 Software livre na Administração Pública Federal

As denúncias apresentadas por Snowden mostraram as vulnerabilidades existentes na segurança das informações da APF, como também a necessidade urgente de ações que minimizem os riscos e que permitam uma maior segurança dessas informações;

O decreto 8.135/2013 apresenta a utilização de *Software* livre e auditável, como uma das medidas de proteção das informações trafegadas na APF, e Kuhn (2016), cita também o uso do *Software* livre como um reforço na questão de amenizar a espionagem, considerando que esses *Softwares* podem ser auditados e, portanto, permitem saber como os mesmos tratam as informações que são processadas.

---

<sup>27</sup> Presidência da República - <http://www2.planalto.gov.br/>

### 2.4.1 As características do *Software* livre

Conforme a definição da Free Software Foundation<sup>28</sup>, um *Software* se caracteriza como livre quando permite a seus usuários compartilhar, estudar e modificar e estabelece, por meio da licença de uso, quatro liberdades fundamentais para a utilização desse modelo de *Software*:

- Liberdade de executar o programa, para qualquer propósito (liberdade 0);
- Liberdade de modificar o programa para adaptá-lo às suas necessidades (liberdade 1). Para tornar essa liberdade efetiva na prática, é preciso ter acesso ao código fonte;
- Liberdade de redistribuir cópias gratuitamente ou mediante pagamento (liberdade 2); e
- Liberdade de distribuir versões modificadas do programa para que a comunidade possa se beneficiar de suas melhorias (liberdade 3).

Para Dias (2016), esse modelo de *Software* vem sendo aplicado ao longo das ultimas décadas também na esfera de governos e cita como principais razões, a questão da economia financeira com a libertação de licenças proprietárias; a possibilidade de modificação e adaptação do programa às necessidades da gestão e a reutilização em vários órgãos (o que vai ao encontro da liberdade 1 e liberdade 3), e por razões de segurança e soberania, considerando a possibilidade de estudar o código do programa e saber o que ele faz com os dados que manipula.

No âmbito do governo federal brasileiro, o *Software* livre teve a sua maior ascensão no governo de Luiz Inácio Lula da Silva, que criou um comitê técnico de implementação do *Software* livre e a partir de então, foram adotadas soluções de código aberto em muitos projetos de vários órgãos do governo. Como exemplo, Dias (2016) cita as consultas públicas que deram origem ao Marco Civil da Internet e à Reforma da Lei de Direitos Autorais, que foram feitas em uma plataforma Wordpress - livre - adaptada, a um custo baixo para o governo.

---

<sup>28</sup> Free Software Foundation. <http://www.fsf.org>

### 2.4.2 O Software Público Brasileiro

Também foi criado o Portal de *Software* Público Brasileiro<sup>29</sup>, onde são hospedados todos os programas de código aberto criados pelo governo e para serem utilizados pelo governo e que também permita a utilização desses programas por outros órgãos públicos e privados.

Para Germani (2016), na Portaria 46/2016 que dispõe sobre a disponibilização de *Software* Público Brasileiro, o Ministério do Planejamento propõe uma nova categoria de *Software* chamada “*Software* de governo”, que seria um *Software* que é compartilhado, sem ônus, entre órgãos governamentais, mas que, no entanto, não é licenciado como *Software* livre e que viria a legitimar uma prática já existente na APF, que é a cessão de *Software* entre órgãos. No entanto, essa nova categoria de *Software* é vista como uma tentativa de aproximação dessas soluções à lógica do *Software* livre, mas traz alguns riscos que são citados pelo autor como segue:

1. Em primeiro lugar, não se aproveita de toda a possibilidade de colaboração com a sociedade que se poderia ter com um *Software* livre, indo contra, inclusive, o princípio de Participação e Controle Social da Política de Governança Digital. Tampouco se estimula empresas nacionais a se tornarem prestadoras de serviço sobre aquela solução; e
2. O órgão que utiliza o *Software* cedido, e que passa a depender dele, se coloca em uma posição frágil e dependente, esperando que a “boa vontade” do cedente nunca termine [...].

Durante a gestão do governo Lula, podem ser citados como fatos relevantes relacionados ao uso de *Software* livre na APF, a criação do comitê técnico de implementação do *Software* livre e do portal, chamado *Software* Público Brasileiro.

Já o governo Dilma, após ser vítima de espionagem americana, chegou a encomendar soluções nacionais, abertas, para substituir os programas estrangeiros utilizados na comunicação do governo, o que gerou o decreto 8135/2013 e estes atos trouxeram esperanças para uma maior adesão às políticas de *Software* livre no governo brasileiro. No entanto, ainda no governo Dilma, o Ministério do Planejamento adotou para os seus servidores a solução de *e-mails* da Microsoft e aconteceu a extinção do

---

<sup>29</sup>Portal do Software Público Brasileiro: <https://softwarepublico.gov.br>

comitê técnico de Implantação do *Software* Livre, criado anteriormente no governo Lula e essas mudanças causaram enfraquecimento e mau exemplo para os demais órgãos da APF quanto à adesão da política de uso de *Software* livre.

O uso do *Software* livre no governo brasileiro vem sofrendo resistência e constantes mudanças ao longo do tempo. Dias (2016) afirma que as políticas a favor do *Software* livre cresceram na administração do governo Lula, mas sofreram retrocesso na gestão de Dilma e, agora, com Temer, tendem a perder ainda mais relevância, levando em conta as primeiras medidas do governo na área.

#### 2.4.3 A Estratégia de Governança Digital (EGD) brasileira

No início de 2016, as políticas de informática no governo passaram a ser centralizadas pela Secretaria de Tecnologia da Informação, (resultante do desmembramento da antiga SLTI), órgão do Ministério de Planejamento e juntamente com essa secretaria, por meio do decreto 8.638/2016, também foram criadas políticas e estratégias de governança digital (EGD), que segundo Germani (2016), substitui os comitês técnico e executivo de governo eletrônico, pois o mesmo decreto que instituiu a Política de Governança Digital, no seu Art. 15, revoga o comitê de governo eletrônico e seus comitês técnicos, entre eles, o de Implantação de *Software* Livre (CISL).

A Estratégia de Governança Digital (EGD) brasileira, “define conceitos, desafios, oportunidades, objetivos estratégicos, as metas, os indicadores e as iniciativas para implementar a Política de Governança Digital, instituída pelo Decreto no 8.638, de 15 de janeiro de 2016, e norteará programas, projetos, serviços, sistemas e atividades a ela relacionados” (BRASIL, 2016e).

Para Germani (2016), essa EGD substitui a atual Estratégia Geral de Tecnologia da Informação e Comunicações (EGTIC), utilizada para alinhar as iniciativas de TIC às estratégias do governo federal e traz princípios importantes, que segundo o autor, estão alinhados em grande parte com as melhores referências internacionais

como o Government Digital Services (GDS)<sup>30</sup>, do Reino Unido, e o US Digital Services, dos Estados Unidos (USDS)<sup>31</sup>.

No item 6.2 da EGD, são listadas as oportunidades encontradas, e entre elas é apresentado o Decreto no 8.135, de 4 de novembro de 2013, que reforça a Gestão da Segurança da Informação e das Comunicações do Governo Federal. Embora o decreto sugira o uso de *Software* livre e auditável como um dos meios de segurança das informações na APF, Germani (2016), alerta que em nenhum momento na EGD, é citada a adoção de *Software* livre pelas agências governamentais brasileiras.

#### 2.4.4 Estratégias de Governança Digital (EGD) internacionais

A utilização dessas importantes referências internacionais como inspiração para a construção EGD foi um ponto positivo, no entanto, quando se refere à utilização de *Software* livre e auditável, não foram seguidos os exemplos britânico e estadunidense, e referindo-se a esses modelos, Germani (2016) cita trechos do padrão de serviços digitais do GDS do Reino Unido, o qual diz:

“8. Faça com que todo novo código fonte seja aberto e reutilizável e publique-o sob licenças apropriadas (ou então dê uma explicação convincente de porque isso não pode ser feito para partes específicas do código fonte)”.

O autor apresenta ainda a orientação que é dada nos princípios de *design* de projetos da GDS britânica:

“Faça as coisas abertas: Devemos compartilhar o que estamos fazendo sempre que pudermos. Com colegas, com as pessoas que usam o serviço, com o mundo. Compartilhar código, design, ideias, intenções e falhas. Quanto mais gente olhando um serviço melhor ele fica – grandes erros são previstos, melhores alternativas são descobertas e a barra é levantada. Muito do que estamos fazendo só é possível devido a códigos abertos e a generosidade da comunidade de web design. Deveríamos pagar isso de volta.”

A exemplo da GDS britânica, o autor mostra um exemplo tirado da cartilha do US Digital Services, dos Estados Unidos (USDS), o qual diz:

<sup>30</sup> Government Digital Services do Reino Unido - <https://gds.blog.gov.uk/>

<sup>31</sup> US Digital Services, dos Estados Unidos - <https://www.whitehouse.gov/participate/united-states-digital-service>



“13. Aberto por padrão: Ao colaborar de maneira aberta e publicando dados abertos, simplifica-se o acesso do público aos serviços e informações governamentais, permite-se que qualquer pessoa contribua com facilidade e que o código seja reutilizado por empreendedores, organizações não governamentais, outros órgãos do governo, e pelo público em geral.”

Dessa forma, pode-se ver nessas renomadas referências internacionais a importância da utilização do *Software* livre como forma de segurança das informações na administração pública e a possibilidade que o mesmo proporciona por ter o seu código aberto para ser auditado e permitir saber como os dados são manipulados, diferentemente dos programas proprietários.

#### 2.4.5 O uso do *Software* Proprietário na APF

Mesmo com os exemplos apresentados nas conceituadas normas internacionais sobre a importância do uso do *Software* livre como garantia da segurança das informações, essa visão ainda sofre resistência no governo brasileiro, que indo na contramão das renomadas normativas estrangeiras, manifestou o seu interesse, por meio da Intenção de Registro de Preços 16/2016<sup>32</sup>, numa compra coletiva de programas proprietários para serem utilizados em vários órgãos federais.

Por sua vez, como forma de retomar o seu lugar de destaque como grande fornecedor de *Software* ao governo federal, a Microsoft inaugurou um centro de transparência, com os argumentos de “promover a computação segura” e “atender a necessidades específicas do poder público”, o qual permitem que governos revisem o código fonte dos seus programas e, dessa forma, tentar conhecer como são manipulados os dados por esses programas proprietários.

No entanto, Dias (2016) afirma que em muitas instâncias do governo, o uso do *Software* livre está bem consolidado, pois muitos órgãos migraram massivamente para servidores e sistemas operacionais Linux<sup>33</sup> e Germani (2016) reforça esse posicionamento citando como exemplo o Ministério da Cultura que oferece e utiliza *Software* livre em várias finalidades.

<sup>32</sup> IRP 16/2016 - <http://www.comprasgovernamentais.gov.br/noticias/26-10-2016-a-central-de-compras-em-conjunto-com-a-sti-informa-a-publicacao-da-irp-no-16-2016-com-prazo-de-manifestacao-ate-11-11-2016>

<sup>33</sup> Linux Foundation: <https://www.linuxfoundation.org/>

## 2.5 Considerações finais do capítulo

Desta forma, pelo exposto neste capítulo, vê-se que a utilização do *Software* livre na administração pública federal continuará sendo um grande desafio, e mesmo diante das muitas vantagens oferecidas por esse modelo de *Software*, sempre existirão questões comerciais e a resistência por parte de alguns usuários que dificultarão a adesão e utilização dos mesmos.

Esse capítulo apresentou inicialmente um histórico da Rede Federal de Educação Profissional, Científica e Tecnológica, e foi falado sobre as normativas que instituíram a rede federal de educação e normatizaram a sua expansão no Brasil. Foram apresentadas ainda as instituições que compõem a rede e onde estão distribuídas nas várias regiões do país e foi mostrada através de gráfico a cronologia da rede com o surgimento, evolução e cenário atual da mesma.

Na sequência, foi apresentado um breve histórico de como se deram as ações de espionagem americanas, que foram denunciadas por Snowden, e também foram apresentadas algumas normativas que visam a segurança da comunicação de dados na Administração Pública Federal, com ênfase nas normativas surgidas a partir das denúncias de espionagem do governo brasileiro e as observações de alguns autores sobre essas normativas.

Falou-se ainda sobre o cenário atual da segurança da informação na Administração Pública Federal e sobre a estrutura dos órgãos responsáveis pelo gerenciamento da informação e comunicação do governo brasileiro, e também foram apresentadas algumas literaturas voltadas para o tema que mostram o cenário atual da segurança da informação no Brasil, como também o que está sendo feito como forma de enfrentamento dos vários desafios existentes relacionados a segurança da informação na APF.

Como o decreto 8.135/2013 defende a utilização de *Softwares* livre e auditável como forma de amenizar os riscos com a segurança da informação, foram apresentadas também as características do *Software* livre e as liberdades fundamentais

para a utilização do mesmo. Em seguida, apresentou-se a trajetória do *Software* livre no governo brasileiro e falou-se da adoção de um padrão denominado de *Software* Público Brasileiro, que visa atender as demandas dos órgãos da APF.

Foram apresentados ainda alguns tópicos considerados relevantes das GDS britânica (Government Digital Service) e da USDS americana (US Digital Services) que são consideradas como importantes referências internacionais e que serviram de modelo para a construção da Estratégia de Governança Digital (EGD) brasileira. Também foi tratado nesse capítulo a forma como essas EGDs internacionais tratam o uso do *Software* livre na administração pública.

Como finalização do capítulo, falou-se sobre a utilização do *Software* livre e proprietário na Administração Pública Federal, e das estratégias de empresas privadas para continuar fornecendo programas para o governo brasileiro, frente as exigências do decreto 8.135.

No capítulo seguinte será apresentada a análise dos dados coletados por meio do questionário que foi enviado às instituições federais que compõem a Rede Federal de Educação Profissional e Tecnológica, visando fazer um diagnóstico do correio eletrônico utilizado e identificar os fatores determinantes para a adesão ou não adesão dessas instituições ao modelo de correio eletrônico apresentado no decreto 8.135/2013.

### 3. O CORREIO ELETRÔNICO DA REDE FEDERAL DE EDUCAÇÃO.

Com o objetivo de Avaliar a aderência das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica ao decreto 8.135/2013, e seguindo a metodologia proposta para este trabalho, esta pesquisa foi realizada com os membros Diretores de Tecnologia da Informação (DGTI) das 42 instituições que compõem a Rede.

O método utilizado para essa pesquisa foi o *Survey* e a coleta de dados se deu por meio de um questionário eletrônico, construído sob a plataforma do *Google Forms*, com 14 questões objetivas e subjetivas (Apêndice A). Todo o questionário foi enviado aos participantes da pesquisa por meio dos *e-mails* institucionais, aos quais foi solicitado o preenchimento das questões pelo próprio destinatário ou outro profissional pertencente à DGTI.

Com referência a análise dos dados coletados, GIL (2010, p. 113), diz que “é necessário também, à medida que os dados sejam agrupados, examiná-los para verificar se estão completos, claros, coerente e precisos”. Assim, o questionário utilizado na pesquisa (APÊNDICE A), ficou disponível no período de 04/07/2016 a 13/09/2016 e recebeu 55 respostas.

Em virtude de o questionário ter sido respondido por mais de um membro das Diretorias Geral de TI das instituições, foram identificadas 16 respostas em duplicidade e o descarte foi feito após análise das respostas e consultas efetuadas aos diretores de TI das instituições visando maiores esclarecimentos, cujas respostas foram utilizadas para determinar o descarte de respostas duplicadas. Assim, restaram 39 respostas consideradas válidas para análise e posterior interpretação, conforme pode ser visualizado na Tabela 3.1.

**Tabela 3.1:** Quantitativo de respostas obtidas com a pesquisa

Rede Federal de Educação Profissional, Científica e Tecnológica			
Instituições pesquisadas	Respostas		
	Recebidas	Duplicadas	Válidas
42	55	16	39

**Fonte:** Elaborada pelo autor (2017).

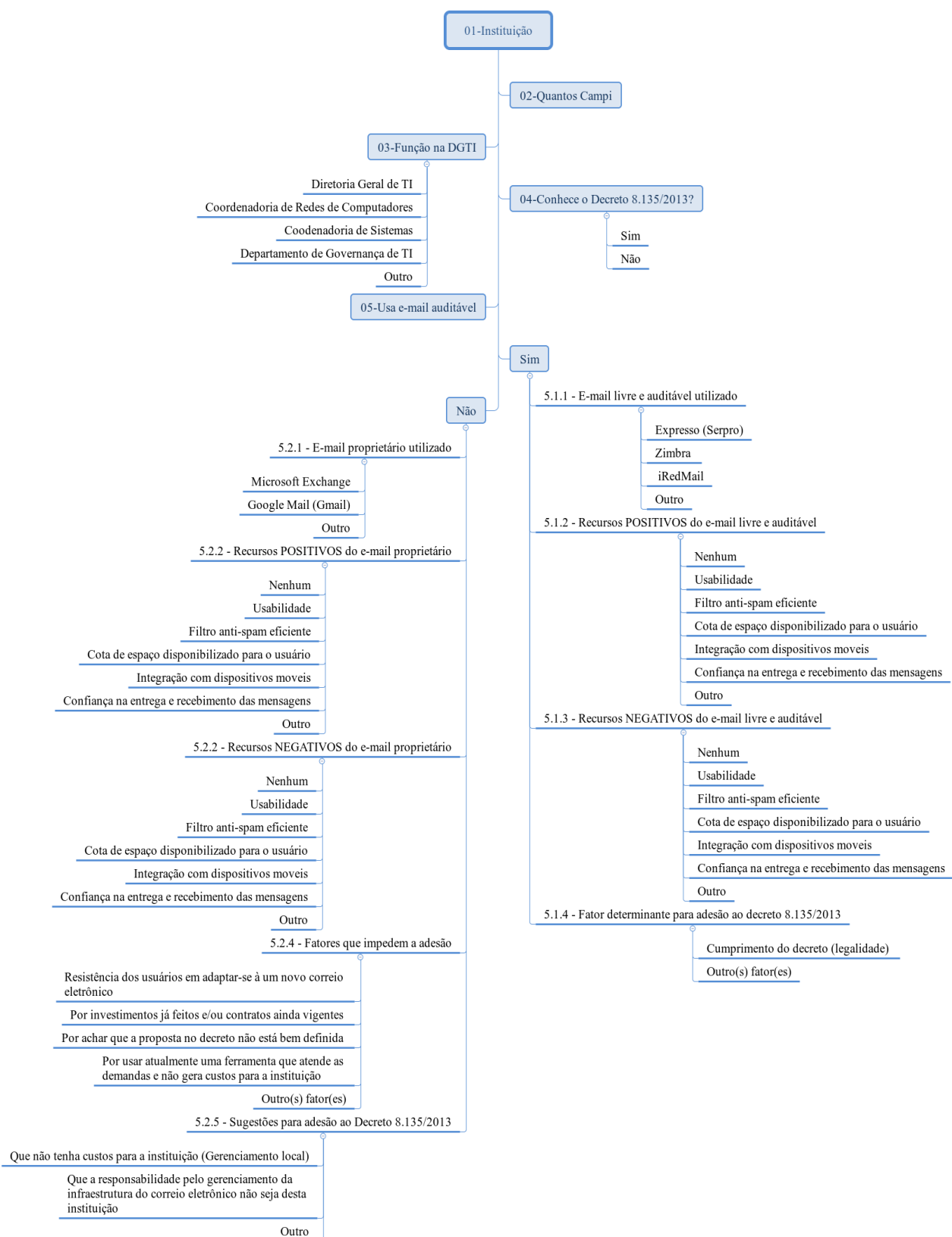
Dessa forma, 92,86% do total de instituições pesquisadas enviaram respostas válidas que em seguida, foram exportadas para uma planilha de cálculo, na qual foi possível efetuar a tabulação, análises e a geração de gráficos para uma melhor representação dos resultados.

O questionário eletrônico enviado para as instituições, inicialmente apresenta um resumo da proposta do decreto 8.135/2013 e da portaria 141/2014, além de disponibilizar os *links* eletrônicos para as referidas normativas, para que se possa tomar conhecimento na íntegra do que as mesmas propõem.

Visando atender os objetivos propostos por essa pesquisa, as quatro primeiras questões do questionário identificam a instituição, o cargo ocupado pelo respondente e se o mesmo conhece o teor do decreto 8.135/2013.

Na quinta questão, é perguntado se a instituição utiliza serviço de correio eletrônico livre e auditável e caso a resposta seja afirmativa, o respondente será direcionado para o grupo de questões iniciadas com 5.1, as quais são relacionadas às instituições que utilizam *e-mail* livre e auditável, de acordo com o organograma representado na Figura 3.1. Caso a resposta seja negativa, o respondente será direcionado para o grupo de questões iniciadas com 5.2, e que estão relacionadas às instituições que utilizam *e-mail* proprietário e, portanto, não auditável.

**Figura 3.1: Estrutura do questionário**



**Fonte:** Elaborada pelo autor (2017).

### 3.1 Análise dos dados

Para análise dos dados coletados nas instituições pesquisadas, foi aplicada a técnica de percentagem como forma de melhor quantificar e expressar os resultados obtidos, pois segundo Marconi e Lakatos (2011), as percentagens servem para dar forma numérica às características qualitativas além de reduzir suas distribuições por frequências a uma base comum simplificando muito a comparação. Gil (2010, p. 114) afirma que “esse procedimento estatístico está intimamente relacionado com os objetivos da pesquisa”. Dessa forma, justifica-se o uso dessa técnica para quantificar, analisar e permitir melhor base de interpretação.

A análise dos dados foi realizada baseando-se nas respostas obtidas com o questionário apresentado no APÊNDICE A, com o objetivo de coletar informações que permitissem traçar um perfil da instituição e a partir desse diagnóstico poder identificar os fatores determinantes para adesão ou não adesão por parte dessas instituições ao modelo de correio eletrônico que é proposto no decreto 8135/2013, além de, após analisar esses fatores, poder sugerir um conjunto de recomendações que venham favorecer a adesão por parte desses órgãos, ao que é proposto no referido decreto.

#### 3.1.1 Identificação da Instituição e a função do respondente

Esse grupo inicial de questões do formulário detalhadas nesse tópico visa fazer uma identificação prévia da instituição e do respondente e se a instituição utiliza sistema de correio eletrônico em conformidade com o decreto.

#### **Q01 – Instituição**

---

Selecione a instituição que você trabalha?

Nesta questão, foi disponibilizada ao respondente a possibilidade de escolher a sua instituição por meio de uma listagem com todas as 42 instituições participantes da pesquisa e que compõem a RFEPECT.

Após análise das respostas, foram identificadas como respondentes da pesquisa as seguintes instituições: Instituto Federal de Brasília, Instituto Federal de

Goiás, Instituto Federal Goiano, Instituto Federal do Mato Grosso do Sul, Instituto Federal de Mato Grosso, Instituto Federal de Alagoas, Instituto Federal da Bahia, Instituto Federal Baiano, Instituto Federal do Ceará, Instituto Federal do Maranhão, Instituto Federal da Paraíba, Instituto Federal de Pernambuco, Instituto Federal do Piauí, Instituto Federal do Rio Grande do Norte, Instituto Federal de Sergipe, Instituto Federal do Sertão Pernambucano, Instituto Federal do Acre, Instituto Federal do Amazonas, Instituto Federal do Amapá, Instituto Federal do Pará, Instituto Federal de Rondônia, Instituto Federal de Roraima, Centro Federal de Educação Tecnológica Celso Suckow da Fonseca, Centro Federal de Minas Gerais, Colégio Pedro II, Instituto Federal do Espírito Santo, Instituto Federal Fluminense, Instituto Federal de Minas Gerais, Instituto Federal do Norte de Minas Gerais, Instituto Federal do Rio de Janeiro, Instituto Federal de São Paulo, Instituto Federal do Sudeste de Minas, Instituto Federal do Sul de Minas, Instituto Federal do Triângulo Mineiro, Instituto Federal Catarinense, Instituto Federal de Farroupilha, Instituto Federal do Paraná, Instituto Federal do Rio Grande do Sul e Instituto Federal de Santa Catarina.

#### **Q02 - Quantos *campi***

---

Quantos *campi* possui a sua instituição?

Esta questão objetivou identificar o total de *campi* existente nas instituições participantes da pesquisa e que serão afetadas diretamente pela adesão ou não à proposta do decreto 8.135/2013.

Após consulta ao site do Conselho Nacional das Instituições da Rede Federal de Educação - CONIF<sup>34</sup> identificou-se um quantitativo total de 603 *campi* existentes nas 39 instituições que responderam a pesquisa e estão distribuídos nas seguintes regiões: 5 na região Centro-oeste com 66 *campi*; 11 na região Nordeste com 182 *campi*; 6 na região Norte com 70 *campi*; 12 na região Sudeste com 169 *campi* e 5 na região Sul com 116 *campi*, conforme Tabela 3.2.

---

<sup>34</sup> Conselho Nacional das Instituições da Rede Federal de Educação - <http://portal.conif.org.br>



**Tabela 3.2:** Quantitativo de *campi* por região

REGIÃO	SIGLA	INSTITUIÇÃO	CAMPI	TOTAL
CENTRO - OESTE	IFB	INSTITUTO FEDERAL – BRASÍLIA	11	66
	IFG	INSTITUTO FEDERAL – GOIÁS	14	
	IFGOIANO	INSTITUTO FEDERAL – GOIANO	12	
	IFMS	INSTITUTO FEDERAL - MATO GROSSO DO SUL	10	
	IFMT	INSTITUTO FEDERAL - MATO GROSSO	19	
NORDESTE	IFAL	INSTITUTO FEDERAL – ALAGOAS	16	182
	IFBA	INSTITUTO FEDERAL – BAHIA	24	
	IFBAIANO	INSTITUTO FEDERAL – BAIANO	14	
	IFCE	INSTITUTO FEDERAL – CEARÁ	31	
	IFMA	INSTITUTO FEDERAL – MARANHÃO	28	
	IFPB	INSTITUTO FEDERAL – PARAIBA	18	
	IFPE	INSTITUTO FEDERAL – PERNAMBUCO	15	
	IFPI	INSTITUTO FEDERAL – PIAUÍ	20	
	IFRN	INSTITUTO FEDERAL - RIO GRANDE DO NORTE	20	
	IFS	INSTITUTO FEDERAL – SERGIPE	9	
	IFSERTAO-PE	INSTITUTO FEDERAL - SERTÃO PERNAMBUCANO	7	
NORTE	IFAC	INSTITUTO FEDERAL – ACRE	6	70
	IFAM	INSTITUTO FEDERAL – AMAZONAS	15	
	IFAP	INSTITUTO FEDERAL – AMAPÁ	6	
	IFPA	INSTITUTO FEDERAL - DO PARÁ	18	
	IFRO	INSTITUTO FEDERAL – RONDÔNIA	9	
	IFRR	INSTITUTO FEDERAL – RORAIMA	5	
SUDESTE	CEFET RJ	CENTRO FEDERAL DE EDUC. CELSO SUCKOW DA FONSECA	7	169
	CEFET MG	CENTRO FEDERAL DE EDUC. MINAS GERAIS	9	
	CPII	COLÉGIO PEDRO II	14	
	IFES	INSTITUTO FEDERAL - ESPÍRITO SANTO	21	
	IFF	INSTITUTO FEDERAL – FLUMINENSE	12	
	IFMG	INSTITUTO FEDERAL - MINAS GERAIS	17	
	IFNMG	INSTITUTO FEDERAL - NORTE DE MINAS GERAIS	11	
	IFRJ	INSTITUTO FEDERAL - RIO DE JANEIRO	12	
	IFSP	INSTITUTO FEDERAL - SÃO PAULO	38	
	IFSUDESTEMG	INSTITUTO FEDERAL - SUDESTE DE MINAS	10	
	IFSULDEMINAS	INSTITUTO FEDERAL - SUL DE MINAS	9	
SUL	IFTM	INSTITUTO FEDERAL - TRIÂNGULO MINEIRO	9	116
	IFC	INSTITUTO FEDERAL – CATARINENSE	15	
	IFFARROUPILHA	INSTITUTO FEDERAL – FARROUPILHA	10	
	IFPR	INSTITUTO FEDERAL – PARANÁ	25	
	IFRS	INSTITUTO FEDERAL - RIO GRANDE DO SUL	17	
	IFSC	INSTITUTO FEDERAL - SANTA CATARINA	22	
<b>TOTAL GERAL DE CAMPI</b>				<b>603</b>

Fonte: Elaborada pelo autor (2017)

**Q03 - Função na DGTI**

---

Qual a sua função na Diretoria Geral de Tecnologia da Informação da sua instituição?

- Diretoria Geral de TI
- Coordenadoria de Redes de Computadores
- Coordenadoria de Sistemas
- Departamento de Governança de TI
- Outro:

Considerando o questionário ter sido enviado somente para os membros da Diretoria Geral de Tecnologia da Informação de cada instituição, esta questão permite que os 39 respondentes identifiquem qual a função que os mesmos exercem na DGTI, e caso a função não esteja relacionada, os mesmos poderão digitá-la no campo Outro. O resultado da análise pode ser visualizado no Gráfico 3.1.

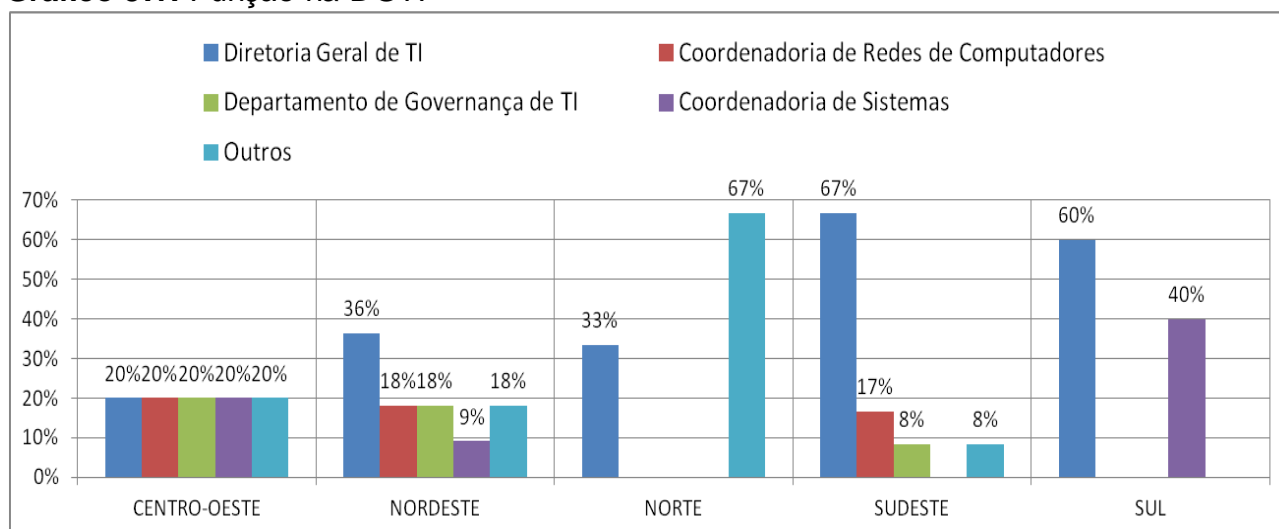
A análise mostra que na região Centro-oeste o percentual de 20% foi representado nas funções de Diretores Gerais de Tecnologia da Informação, Coordenadoria de redes de computadores, Departamento de Governança de TI, Coordenadoria de sistemas e Gerente de TI que foi representado no campo Outros.

Na região Nordeste 36% dos respondentes são Diretores Geral de TI, 18% ocupam as funções de Coordenadoria de redes de computadores, Departamento de Governança de TI, Analista de TI e Diretor de Tecnologias Educacionais, sendo esses dois últimos representados no campo Outros, e 9% ocupam a função de Coordenadoria de sistemas.

Na região Norte 33% são Diretores de TI e 67% pertencem as funções de Analista de TI, Coordenador Geral de TI e Soluções de TI, representados no campo Outros.

Na região Sudeste 67% são Diretores Gerais de TI, 17% são Coordenadores de redes de computadores, e, 8% são do Departamento de Governança de TI e Tecnólogo em Segurança da Informação, representados no campo Outro.

E na região Sul 60% são Diretores de TI e 40% pertencem a Coordenadoria de Sistemas.

**Gráfico 3.1: Função na DGTI**

Fonte: Elaborado pelo autor (2017)

#### Q04 - Conhece o decreto?

Você tem conhecimento do decreto 8.135/2013 e de que é proposto nele a utilização de um correio eletrônico utilizando *Software* livre e auditável?

- Sim
- Não

A referida questão aborda não somente sobre o conhecimento do respondente quanto ao decreto 8.135/2013, mas também se o mesmo tem conhecimento de que o decreto sugere que as instituições do governo devam utilizar um correio eletrônico que seja livre e auditável.

Das 39 respostas obtidas, vê-se que a maioria das instituições tem conhecimento do Decreto 8.135/2013 e da obrigatoriedade que o mesmo impõe com relação ao uso do *e-mail* institucional livre e auditável, e essa constatação pode ser visualizada na representação feita por região, no Gráfico 3.2.

Na região Centro-oeste, 100% dos respondentes afirmaram terem conhecimento do decreto.

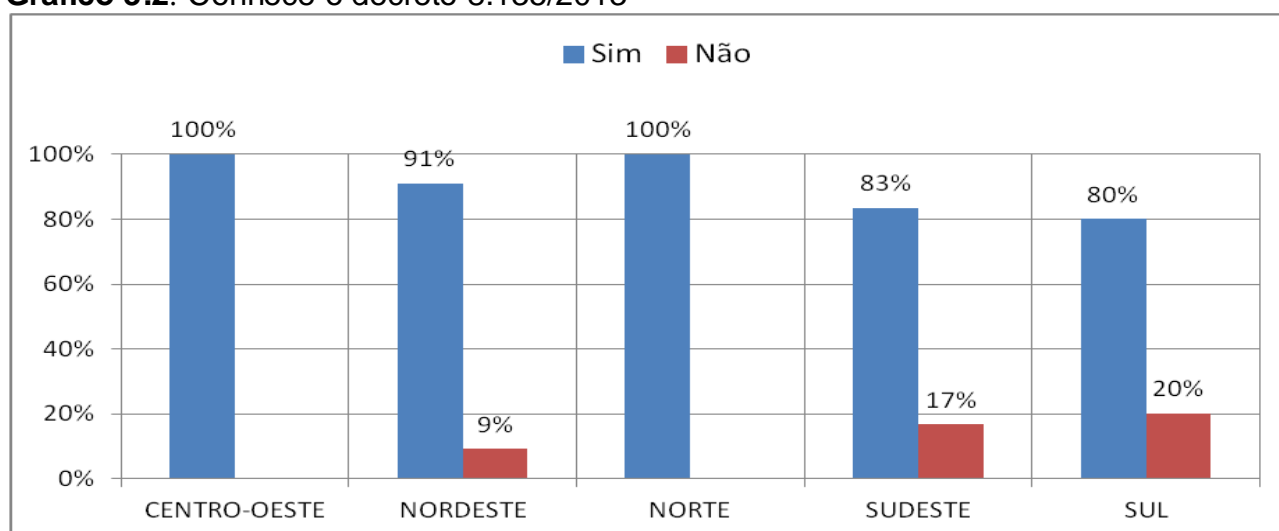
Na região Nordeste, 91% afirmaram conhecer a normativa e somente 9% mostraram não ter conhecimento da mesma.

Na região Norte também 100% dos respondentes tem conhecimento da existência do referido decreto.

Na região Sudeste 83% conhecem a normativa e 17% afirmaram não conhecerem a mesma.

E na região Sul, 80% possuem conhecimento do Decreto 8.135 e somente 20% afirmaram não o conhecerem.

**Gráfico 3.2:** Conhece o decreto 8.135/2013



Fonte: Elaborado pelo autor (2017)

#### **Q05 - Usa e-mail auditável?**

A sua instituição usa correio eletrônico, utilizando *Software* livre e auditável, de acordo com os moldes do decreto?

- Sim
- Não

Nesta questão, é perguntado se a instituição utiliza um correio eletrônico que seja livre e auditável, de acordo com os moldes do decreto e os resultados da análise que se segue, podem ser visualizados no Gráfico 3.3.

Como resposta a esta questão, na região Centro-oeste 100% afirmam utilizarem um e-mail livre e auditável.

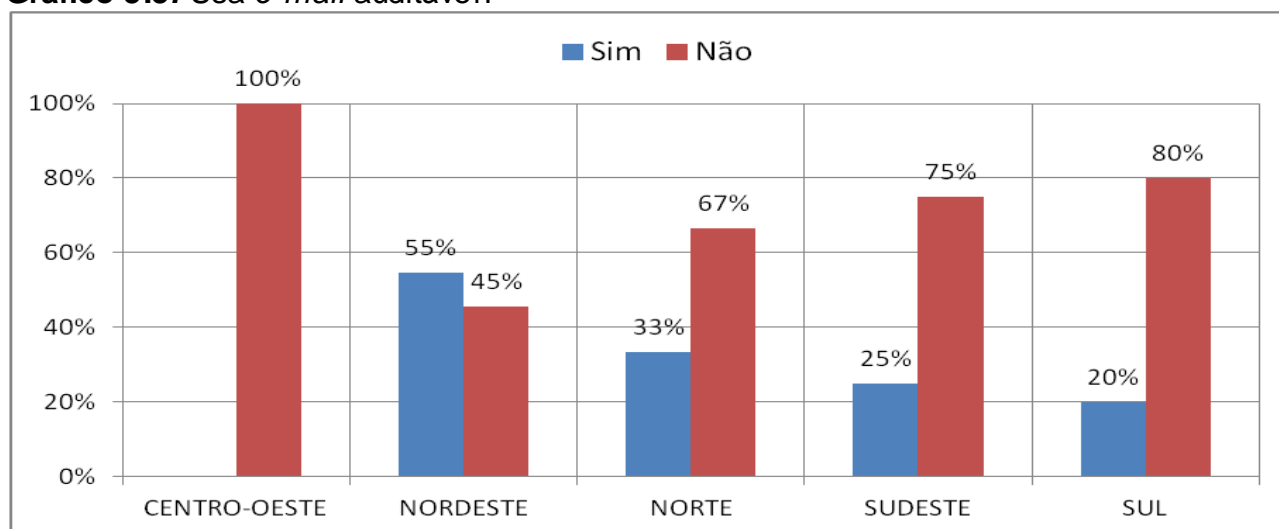
Na região Nordeste 55% responderam positivamente a esta questão, contra 45% que disseram não utilizar um correio eletrônico livre e auditável.

O cenário da região Norte mostra que 33% das instituições utilizam e-mail auditável, contra 67% que afirmam o oposto.

Na região Sudeste, 25% apontam positivamente quanto a utilização de um correio eletrônico auditável contra 75% que dizem não utilizarem.

E na região Sul, 20% das instituições usam e-mail auditável contra 80% que afirmam não utilizarem.

**Gráfico 3.3:** Usa *e-mail* auditável?



Fonte: Elaborado pelo autor (2017)

Dessa forma, mesmo com o Decreto 8.135 vigorando desde 2013 e a grande maioria das instituições afirmarem terem conhecimento sobre o mesmo, pode-se observar que muitas dessas instituições ainda não aderiram à proposta do decreto.

Quanto ao prazo de adesão ao *e-mail* livre e auditável, de acordo com as normativas do governo, no Art. 18º da Portaria Interministerial MP/MC/MD Nº 141, foi definido um prazo de cinco anos, a contar da data de publicação desta portaria, que é de 02/05/2014, tendo, portanto as instituições até 2019 para efetuarem a adesão. (BRASIL, 2014a).

### 3.1.2 O correio eletrônico livre e auditável utilizado

As questões do formulário detalhadas neste tópico são direcionadas para instituições que utilizam correio eletrônico livre e auditável e que estão em conformidade com a proposta do decreto 8.135/2013.

#### **Q5.1.1 - *E-mail* livre utilizado**

Escolha a ferramenta de correio eletrônico livre, utilizada na instituição (Se utilizar mais de uma ferramenta, preencha outro formulário para cada ferramenta utilizada)

- Expresso (Serpro)
- Zimbra
- iRedMail
- Outro:

Nesta questão é solicitado que seja feito o apontamento da ferramenta de correio eletrônico livre e auditável que é utilizada na instituição. Foram sugeridas ao respondente as três ferramentas livres e auditáveis mais utilizadas nos Institutos Federais de Educação, Ciência e Tecnologia, resultantes de uma pesquisa realizada junto a essas instituições, por intermédio do Grupo de Servidores de TI dos Institutos Federais, GSTI-IF (2016), e caso a ferramenta utilizada não esteja na relação apresentada, é disponibilizado o campo Outro para que o respondente possa apontá-la.

De acordo com os dados analisados das 12 instituições que responderam a esta questão, pôde-se identificar as ferramentas livres e auditáveis utilizadas e resultado dessa análise pode ser visualizado no Gráfico 3.4.

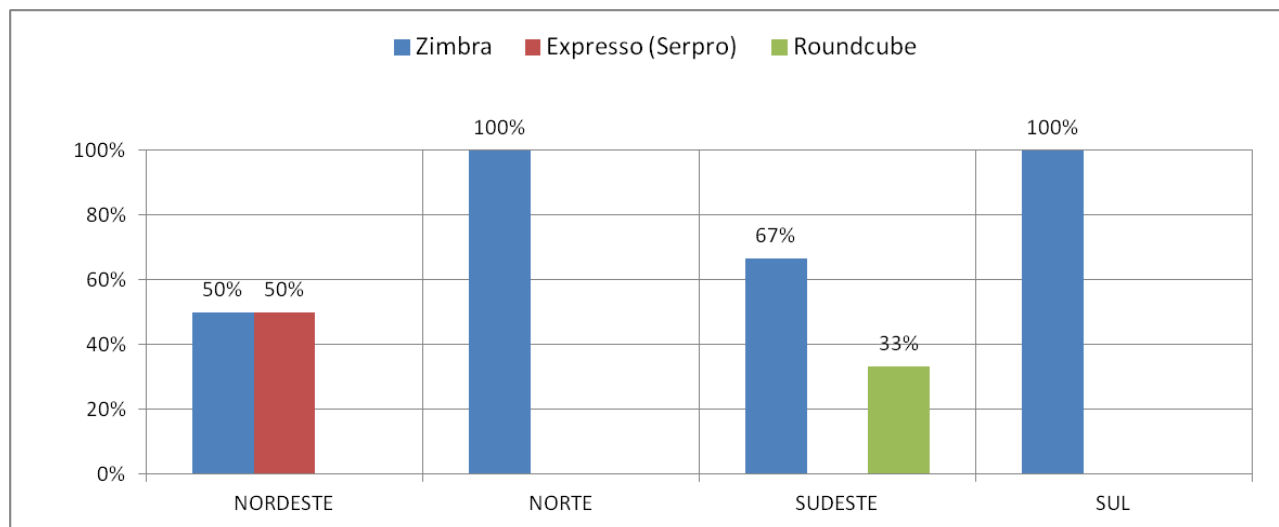
A região Nordeste mostra um empate entre as ferramentas de correio eletrônico Zimbra e Expresso, ambas com 50%.

A região Norte teve o Zimbra, com 100% como única ferramenta de correio eletrônico auditável utilizada.

A região Sudeste mostrou a utilização do Zimbra em 67% das instituições, seguida da ferramenta Roundcube, com 33%.

E na região Sul, com uma representatividade de 100%, a única ferramenta utilizada foi o Zimbra.

**Gráfico 3.4:** *E-mail* livre utilizado



Fonte: Elaborado pelo autor (2017)

Mesmo que Veloso (2014), baseando-se no Artigo 1º, §2º do decreto 8.135/2014, afirme que a Administração Pública Federal terá uma contratação restrita a um único fornecedor, no caso, o Serviço Federal de Processamento de Dados – Serpro, com a sua ferramenta Expresso, os dados analisados mostram que a utilização desta ferramenta ainda é pequena, mesmo entre o grupo de instituições que utilizam *Software* livre no seu sistema de correio eletrônico.

#### Q5.1.2 - Recursos POSITIVOS do *e-mail* livre

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como POSITIVO e/ou acrescente mais algum no campo OUTRO?

- Nenhum
- Usabilidade
- Filtro anti-spam
- Cota de espaço disponibilizado para o usuário
- Integração com dispositivos móveis
- Confiança na entrega e recebimento das mensagens
- Outro:

Considerando que a instituição utiliza *e-mail* livre e auditável, nesta questão é solicitado que sejam apontados os recursos considerados positivos na ferramenta

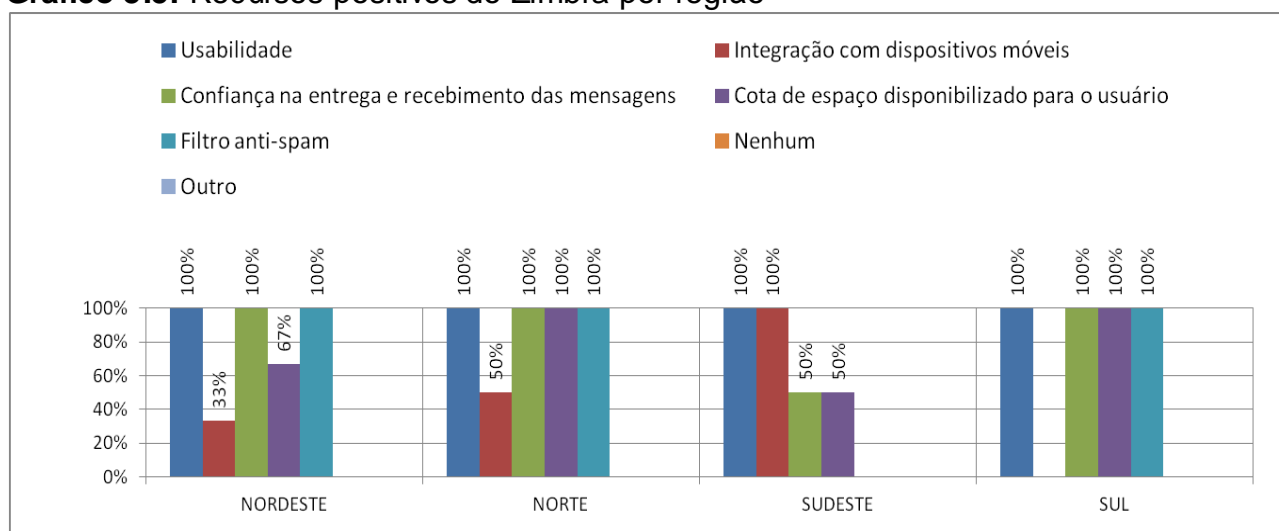
utilizada, ou escolher Nenhum, caso considere não existir nenhum recurso positivo na referida ferramenta, e mais uma vez é disponibilizado o campo Outro para que seja apontado algum recurso positivo extra que não tenha sido disponibilizado na listagem.

Para as 12 instituições que responderam a essa questão e afirmaram utilizar um correio eletrônico livre e auditável, foi disponibilizada a possibilidade de selecionar mais de um recurso que seja considerado positivo na ferramenta utilizada.

### 3.1.2.1 Recursos positivos da ferramenta Zimbra

A análise dos fatores considerados positivos para a ferramenta Zimbra e representados por região podem ser visualizados no Gráfico 3.5.

**Gráfico 3.5:** Recursos positivos do Zimbra por região



Fonte: Elaborado pelo autor (2017)

Conforme representação do Gráfico 3.5, na região Nordeste, 100% das instituições apontaram como recursos positivos para a ferramenta Zimbra, a Usabilidade, Confiança na entrega e recebimento das mensagens e Filtro *anti-spam*. Na sequência, 67% indicaram a Cota de espaço disponibilizado para o usuário e, 33% apontaram o recurso de Integração com dispositivos móveis.

Na região Norte, 100% das instituições apontaram os recursos de Usabilidade, Confiança na entrega e recebimento das mensagens, Cota de espaço disponibilizado



para o usuário e Filtro *anti-spam*, e, 50% apontaram a Integração com dispositivos móveis como recurso positivo do Zimbra.

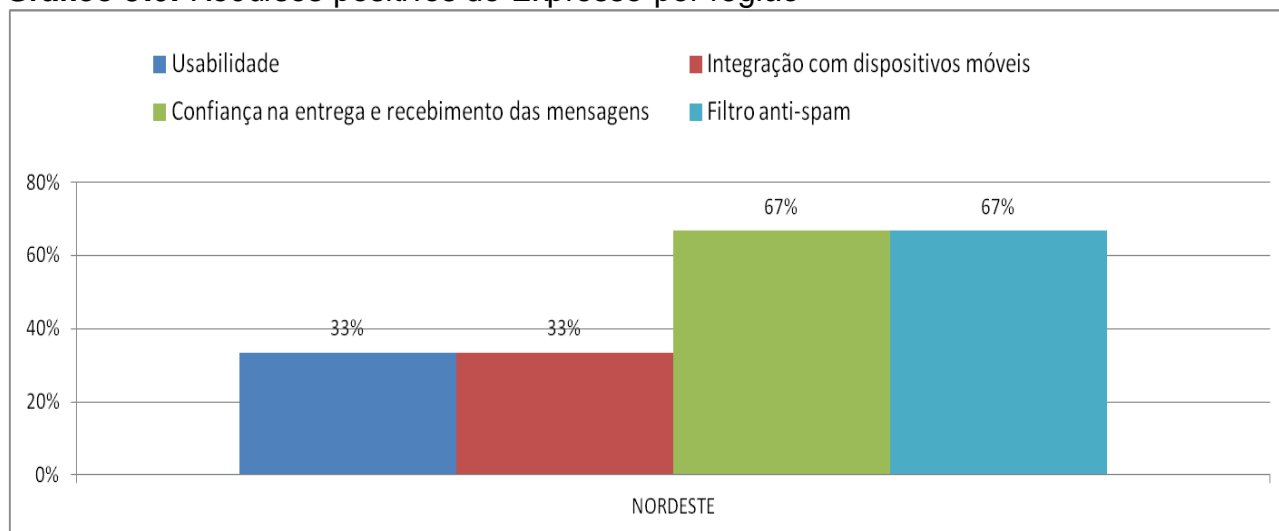
A região Sudeste, 100% das instituições indicaram a Usabilidade e Integração com dispositivos móveis, seguido de outro empate entre Confiança na entrega e recebimento das mensagens e Cota de espaço disponibilizado para o usuário, ambos indicados por 50% dos respondentes.

Por sua vez, 100% das instituições da região Sul apontaram os recursos positivos de Usabilidade, Confiança na entrega e recebimento das mensagens, Cota de espaço disponibilizado para o usuário, e Filtro *anti-spam*.

### 3.1.2.2 Recursos positivos da ferramenta Expresso

A análise dos fatores considerados positivos para a ferramenta Expresso e representados por região podem ser visualizados no Gráfico 3.6.

**Gráfico 3.6:** Recursos positivos do Expresso por região



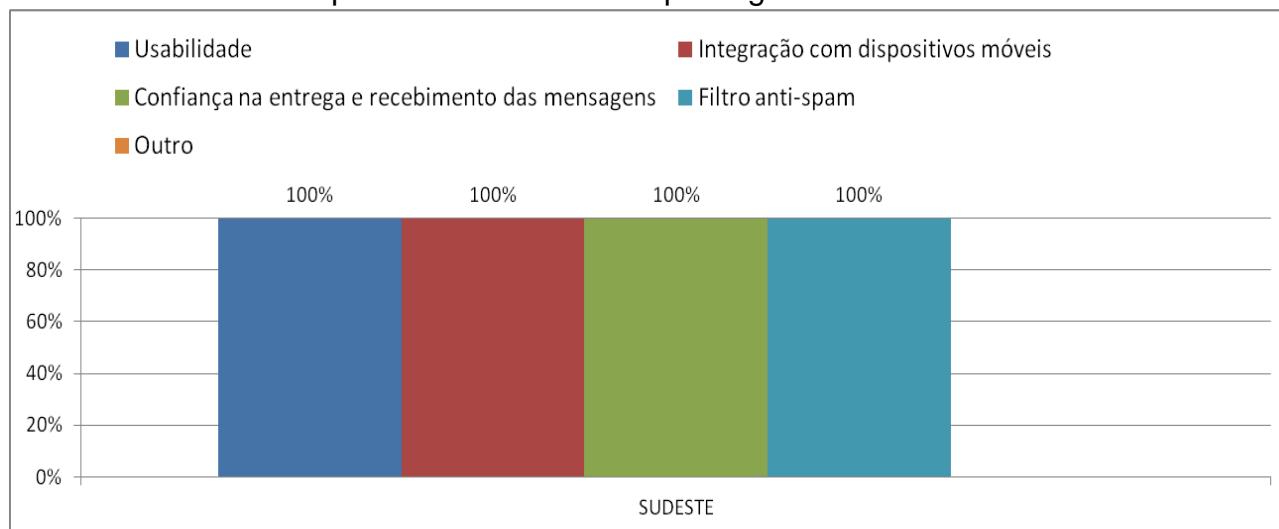
**Fonte:** Elaborado pelo autor (2017)

Para a Ferramenta Expresso do Serpro, somente a região Nordeste apontou recursos positivos, sendo que 33% das instituições apontaram a Usabilidade e Integração com dispositivos móveis, e 67% dos respondentes apontaram Confiança na entrega e recebimento das mensagens e Filtro anti-spam como recursos positivos da ferramenta.

### 3.1.2.3 Recursos positivos da ferramenta Roundcube

A análise dos fatores considerados positivos para a ferramenta Roundcube e representados por região podem ser visualizados no Gráfico 3.7.

**Gráfico 3.7:** Recursos positivos do Roundcube por região



Fonte: Elaborado pelo autor (2017)

Para a ferramenta de correio eletrônico Roundcube, utilizada somente na região Sudeste, 100% das instituições escolheram como recursos positivos, a Usabilidade, Integração com dispositivos móveis, Confiança na entrega e recebimento das mensagens, e Filtro anti-spam.

De acordo com a ISO 9241-11 (1998) e Nielsen (2003), citados por MARTINS (2013), a usabilidade pode ser encarada como uma medida de como um produto pode ser usado por utilizadores específicos para alcançar objetivos específicos com eficácia, eficiência e satisfação, num contexto de utilização específico. MARTINS (2013) ainda cita que, dentro da Interação Humano-Computador (IHC), o conceito de usabilidade foi sendo reconstruído continuamente e tornou-se cada vez mais rico e problemático, e o autor ainda diz que a usabilidade integra, agora, qualidades como diversão, bem-estar, eficácia coletiva, estética, criatividade, suporte para o desenvolvimento humano, entre outras.

Com relação a Confiança na entrega e recebimento das mensagens, a escolha dessa opção demonstra por parte do respondente a confiança que a ferramenta oferece na manipulação das informações do usuário, e essa confiança vai ao encontro das propriedades essenciais para a segurança das informações, como a Disponibilidade, Integridade, Confidencialidade e a Autenticidade (DICA), que recebem as seguintes definições na portaria 141/2014:

**VIII - disponibilidade:** propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

**XIV - integridade:** propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

**VII - confidencialidade:** propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

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

A portaria 141/2014 ainda reforça no seu Art. 3º, inciso IV, a necessidade de implementação de ações e procedimentos que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, incluindo a adoção de programas e equipamentos que possam ser auditados.

#### **Q5.1.3 - Recursos negativos do e-mail auditável**

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como NEGATIVO e/ou acrescente mais algum no campo OUTRO?

- Nenhum
- Usabilidade
- Filtro anti-spam
- Cota de espaço disponibilizado para o usuário
- Integração com dispositivos móveis
- Confiança na entrega e recebimento das mensagens
- Outro:

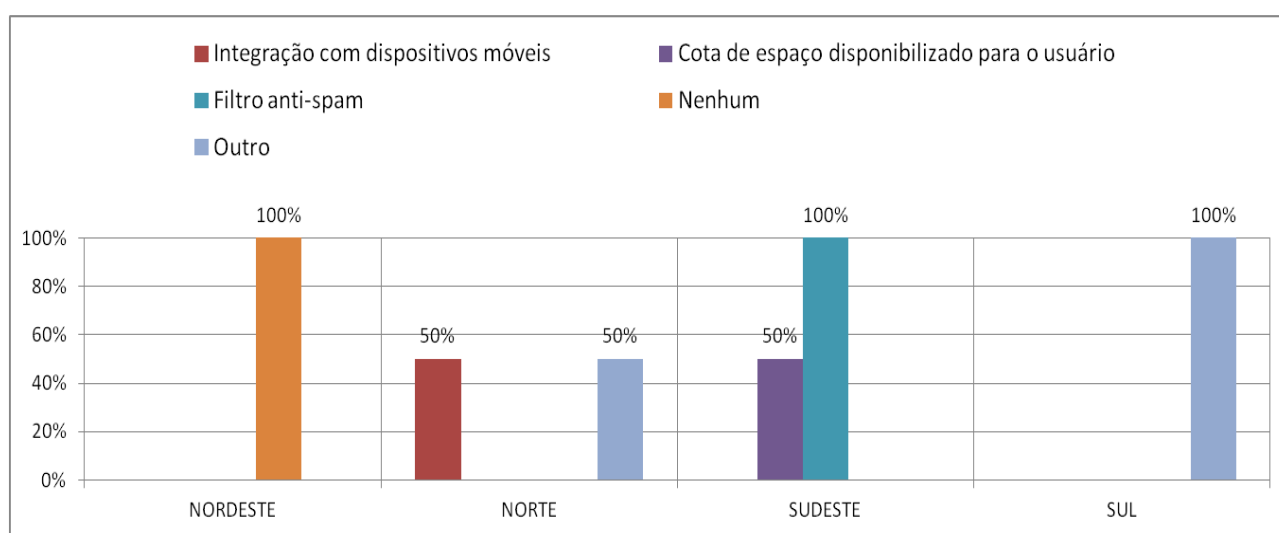
Nesta questão é solicitado que seja feito o apontamento dos recursos considerados negativos na ferramenta de correio eletrônico utilizada, que selecione Nenhum em caso de não identificar nenhum recurso negativo, ou que seja apontado no campo Outro algum recurso extra negativo que não foi listado.

Para as 12 instituições que responderam a essa questão e afirmaram utilizar um correio eletrônico livre e auditável, foi disponibilizada a possibilidade de selecionar mais de um recurso que seja considerado negativo na ferramenta utilizada.

#### 3.1.2.4 Recursos negativos da ferramenta Zimbra

A análise dos fatores considerados negativos para a ferramenta Zimbra e representados por região pode ser visualizada no Gráfico 3.8.

**Gráfico 3.8:** Recursos negativos do Zimbra por região



**Fonte:** Elaborado pelo autor (2017)

Como recursos negativos identificados na ferramenta Zimbra, 100% das instituições da região Nordeste disseram não existir Nenhum considerado negativo.

Na região Norte, 50% das instituições indicaram como recursos considerados negativos para a ferramenta Zimbra, a Integração com dispositivos móveis e Interface, sendo este ultimo apontado no campo Outro.

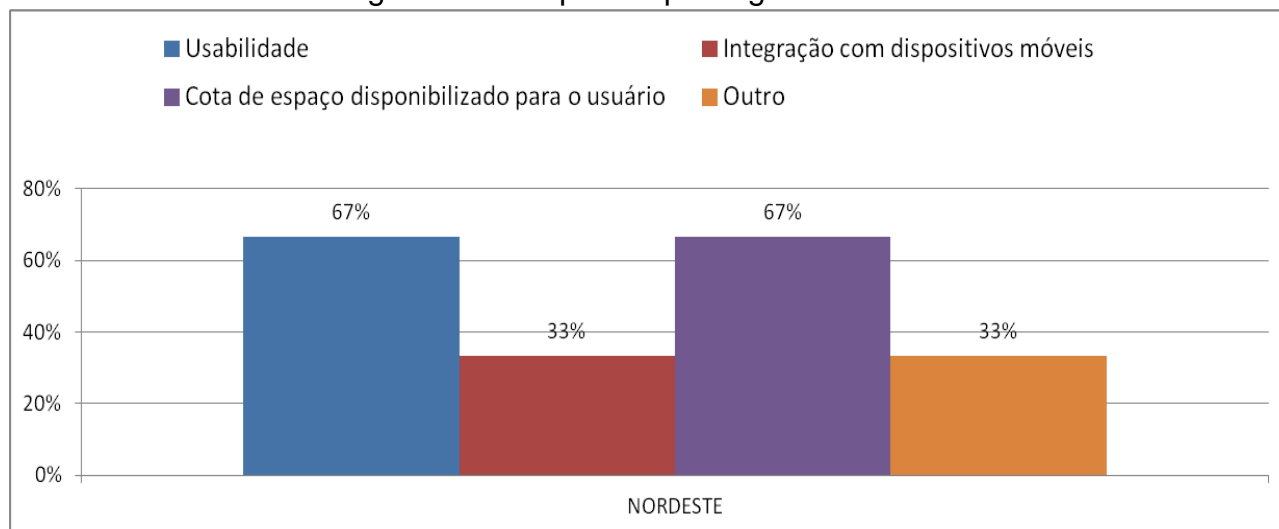
Na região Sudeste, 50% dos respondentes indicaram a Cota de espaço disponibilizado para o usuário e 100% apontaram o Filtro anti-spam.

E, na região Sul, 100% das instituições consideram Não ter as funcionalidades que a versão paga tem, como recurso negativo para a ferramenta Zimbra e que foi especificado no campo Outro.

### 3.1.2.5 Recursos negativos da ferramenta Expresso

A análise dos fatores considerados negativos para a ferramenta Expresso e representados por região pode ser visualizada no Gráfico 3.9.

**Gráfico 3.9:** Recursos negativos do Expresso por região

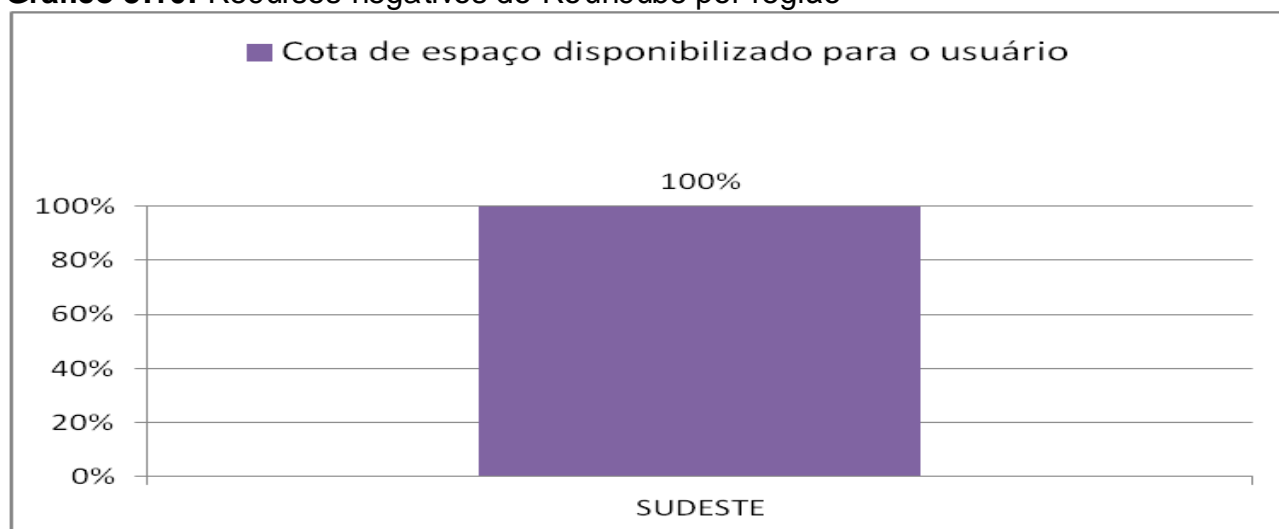


Fonte: Elaborado pelo autor (2017)

Para a ferramenta Expresso do Serpro, somente a região Nordeste apontou os recursos considerados negativos e, 67% indicaram a Usabilidade e Cota de espaço disponibilizado para o usuário, seguida da indicação de 33% dos respondentes para Integração com dispositivos móveis, e ainda Não dispor de ferramenta de gerencia de contas automatizadas, que foi indicada no campo Outro.

### 3.1.2.6 Recursos negativos da ferramenta Roundcube

A análise dos fatores considerados negativos para a ferramenta Roundcube e representados por região pode ser visualizada no Gráfico 3.10.

**Gráfico 3.10:** Recursos negativos do Roundcube por região

Fonte: Elaborado pelo autor (2017)

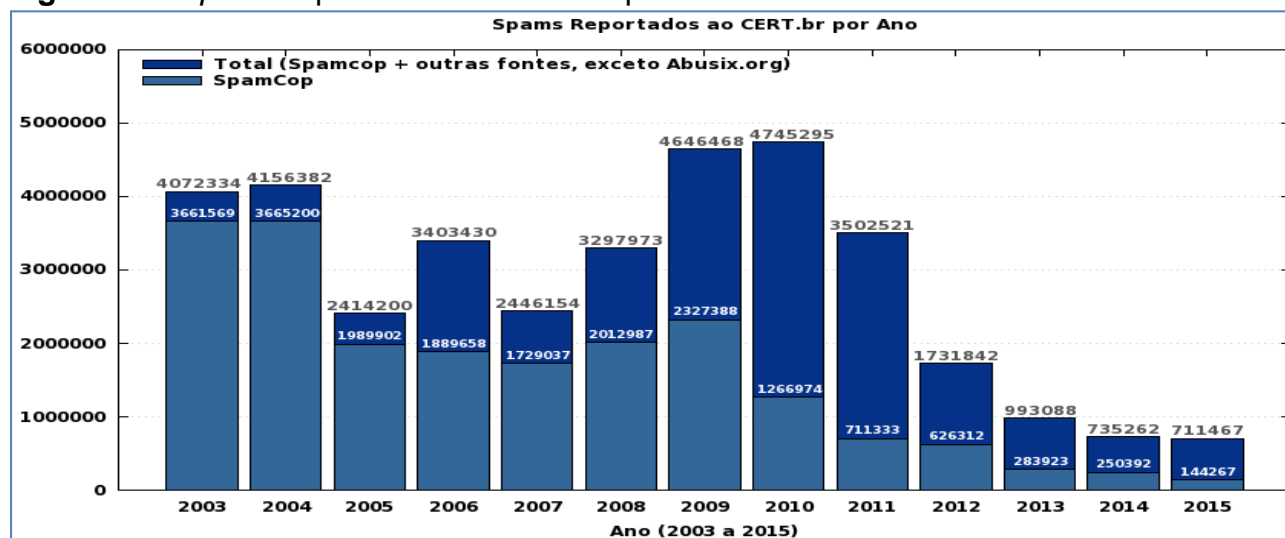
Para a ferramenta Roundcube, a única indicação partiu da região Sudeste onde 100% apontaram a Cota de espaço disponibilizada para o usuário, como recurso considerado negativo na ferramenta.

Entre os recursos negativos destacados, temos a insatisfação com a cota de espaço que é disponibilizada para o usuário do correio eletrônico e essa insatisfação também pode ser justificada pela crescente utilização das mídias digitais, as quais são anexadas às mensagens eletrônicas, e que tem sido causa de grande demanda de espaço para que o usuário de *e-mail* possa armazenar as suas mensagens, causando o uso total da cota disponibilizada e forçando o usuário a ter que apagar mensagens do seu *e-mail* institucional.

Outro ponto que merece destaque é a insatisfação por parte dos usuários com o filtro *anti-spam*, e esse motivo realmente merece uma atenção especial, pois a ineficiência do mesmo pode comprometer seriamente a segurança da informação na instituição, e em virtude nas inúmeras ameaças virtuais existentes, os incidentes de segurança relacionados aos *Spams* são constantes e de grande representatividade ao

longo dos anos, conforme apresenta a estatística do - CERT.br<sup>35</sup> que pode ser visualizada na Figura 3.7.

**Figura 3.7:** *Spams* reportados ao CERT.br por ano



Fonte: <https://www.cert.br/stats/spam/>

#### Q5.1.4 - Fator determinante para adesão

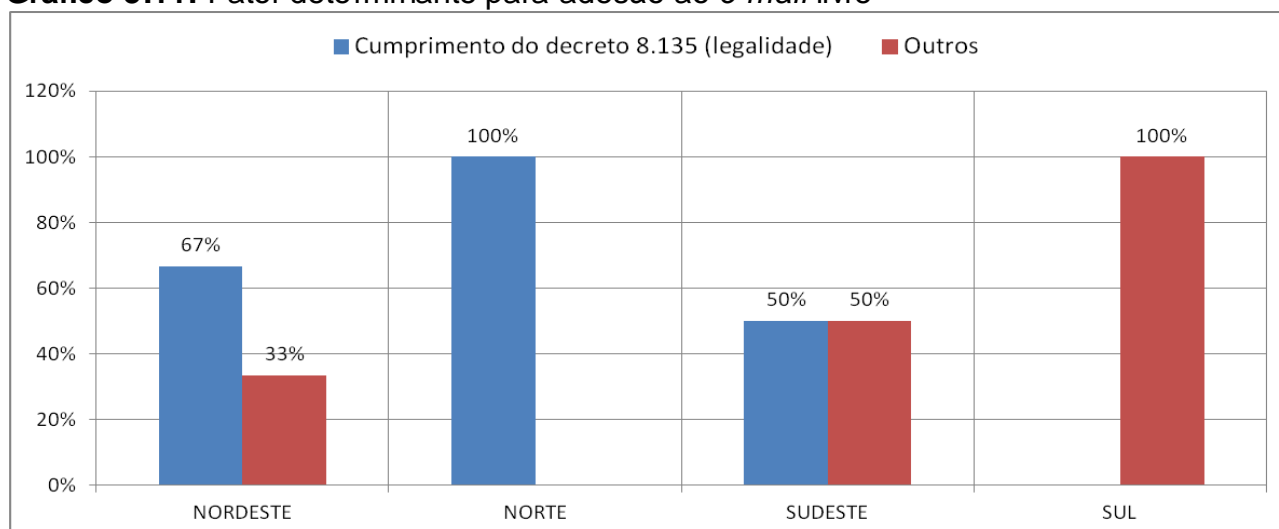
Fator(es) determinante(s) para adesão à ferramenta

- Cumprimento do decreto 8.135/2013 (legalidade)
- Outro:

Considerando que a instituição usa um correio eletrônico de acordo com o decreto, solicitou-se que fosse apontado o fator determinante para adesão à ferramenta de correio eletrônico livre e auditável.

Foram ofertadas duas opções para que o respondente aponte o motivo da utilização da ferramenta. Na primeira opção fica estabelecido que a utilização da ferramenta seja por questão de legalidade e em cumprimento ao decreto 8.135/2013 ou, na existência de outro motivo, é disponibilizado o campo Outro para que seja especificado o motivo para a utilização da ferramenta que atende as exigências do decreto e a análise dos dados coletados das 12 instituições que responderam a essa questão é representada no Gráfico 3.11.

<sup>35</sup> CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

**Gráfico 3.11:** Fator determinante para adesão ao *e-mail* livre

**Fonte:** Elaborado pelo autor (2017)

Na região Nordeste, 67% afirmam que utilizam um correio eletrônico auditável em cumprimento ao decreto, enquanto outros 33% apontaram no campo Outros que já utilizavam uma ferramenta livre e auditável.

A análise da região Norte mostra que 100% das instituições utilizam correio eletrônico auditável em cumprimento ao decreto.

Na região Sudeste, a análise mostrou que o fator determinante para 67% tem a ver com o cumprimento da normativa enquanto outros 33% apontaram no campo Outros que já utilizavam um ferramenta auditável.

Na região Sul, 100% das instituições apontaram no campo Outros que já utilizavam uma ferramenta livre e auditável.

### 3.1.3 O correio eletrônico proprietário e não auditável utilizado

As próximas cinco questões serão respondidas considerando que na questão 5 (cinco), o respondente selecionou NÃO, quando perguntado se a sua instituição utiliza um correio eletrônico livre e auditável.



### Q5.2.1 - E-mail proprietário utilizado

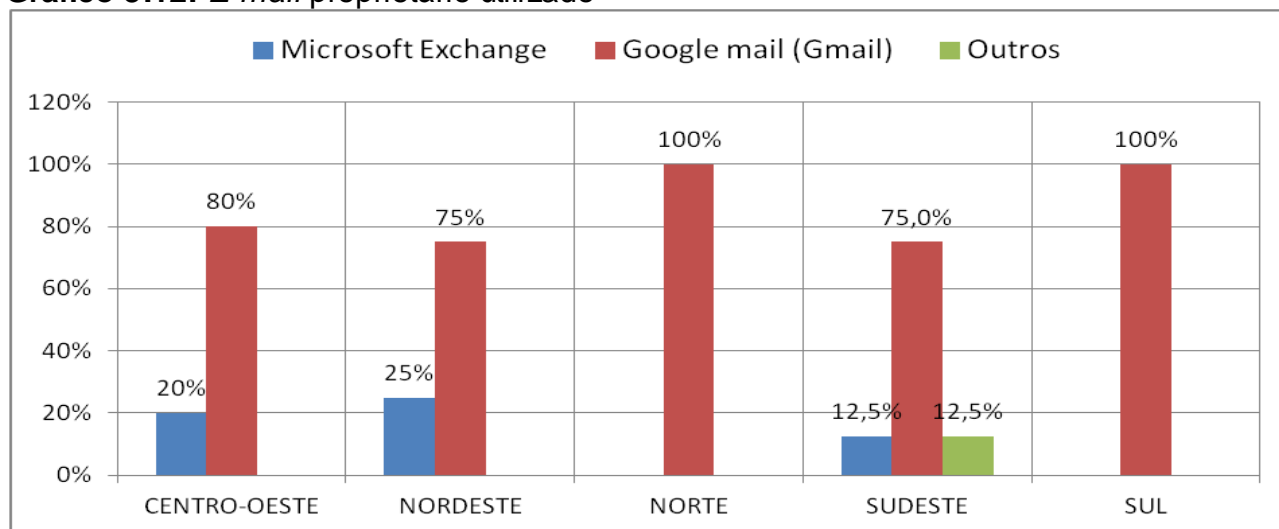
Escolha a ferramenta de correio eletrônico proprietária utilizada na instituição (Se utilizar mais de uma ferramenta, preencha outro formulário para cada ferramenta utilizada)

- Microsoft Exchange
- Google mail (Gmail)
- Outro:

Nesta questão é solicitado que seja feito o apontamento da ferramenta de correio eletrônico proprietária e não auditável que é utilizada na instituição. Foram sugeridas ao respondente as duas ferramentas mais utilizadas nos Institutos Federais de Educação, Ciência e Tecnologia, resultantes de uma pesquisa realizada junto a essas instituições, por intermédio do fórum GSTI-IF, além do campo Outro para que o mesmo possa descrever alguma ferramenta diferente das listadas.

A análise dos dados das 27 instituições que responderam a esta questão e o percentual dos clientes de *e-mails* proprietários utilizados na RFEPCT, obtidos por meio do questionário enviado podem ser visualizados no Gráfico 3.12.

**Gráfico 3.12: E-mail proprietário utilizado**



Fonte: Elaborado pelo autor (2017)

A análise dos dados da região Centro-oeste mostra que 20% das instituições utilizam como correio eletrônico proprietário a ferramenta Microsoft Exchange, enquanto 80% fazem uso do Gmail.

Na região Nordeste 25% das instituições utilizam o Microsoft Exchange, enquanto 75% tem preferência pela ferramenta da Google.

Na região Norte, 100% da preferência é pela ferramenta de correio eletrônico Gmail da Google.

Na região Sudeste, 12,5% das instituições utilizam o Microsoft Exchange, 75% usam o Gmail e outros 12,5% apontaram no campo Outros a utilização da ferramenta de correio eletrônico Office 365.

As instituições da região Sul mostraram 100% de preferência pela ferramenta Gmail.

Na análise desta questão, ainda foram apontadas por algumas instituições as ferramentas *Horde*<sup>36</sup> (1) e *Zimbra* (1), como sendo ferramentas de *e-mail* proprietárias, no entanto, essas duas ferramentas são livres e auditáveis, e, por estarem em desacordo com o que foi perguntado nesta questão, também serão desconsideradas na análise das questões Q5.2.2 e Q5.2.3.

Atualmente, as duas grandes empresas de tecnologia apontadas nas pesquisas, oferecem serviços online de comunicação e colaboração, de forma gratuita e voltada para instituições de ensino.

A Microsoft oferece o Office 365 com recursos gratuitos e também com a possibilidade de contratação de recursos extras, com preços acessíveis, conforme descrição apresentada no site do produto:

[...] Trata-se de um pacote baseado na nuvem que inclui as versões online das soluções Microsoft Office, Microsoft Exchange, Microsoft SharePoint e Microsoft Lync, permitindo acesso seguro e de qualquer lugar a *e-mails*, calendário, conferências, além de edição e compartilhamento de documentos em Word, Excel e PowerPoint.

---

<sup>36</sup>Web Mail Horde: <https://www.horde.org/apps/webmail>

Por sua vez, a Google oferece o G Suite for Education<sup>37</sup>, que também possui recursos gratuitos para instituições de ensino e a possibilidade de contratação de recursos extras, mediante pagamento. O site do produto apresenta a seguinte descrição para a sua ferramenta:

[...] é uma solução hospedada para *e-mail*, agenda e bate-papo com comunicação e colaboração integradas que o Google oferece às escolas. Além disso, você pode complementar o pacote básico para atender às necessidades dos seus usuários, com acesso a diversos outros serviços do Google.

Embora as duas empresas relacionadas na pesquisa ofereçam serviços voltados para a educação de forma gratuita, a pesquisa mostrou que a preferência das instituições pesquisadas é pela ferramenta Gmail da Google, conforme pode ser visualizado no Gráfico 3.8.

#### **Q5.2.2 - Recursos POSITIVOS do *e-mail* proprietário**

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como POSITIVOS e/ou acrescente mais algum no campo OUTRO?

- Nenhum
- Usabilidade
- Filtro anti-spam
- Cota de espaço disponibilizado para o usuário
- Integração com dispositivos móveis
- Confiança na entrega e recebimento das mensagens
- Outro:

Considerando que a instituição utiliza um *e-mail* proprietário e não auditável, nesta questão é solicitado que sejam apontados os recursos considerados positivos na ferramenta utilizada, ou escolher Nenhum, caso considere não existir algum recurso positivo na referida ferramenta. Mais uma vez é disponibilizado o campo Outro para que seja apontado algum recurso positivo extra que não tenha sido listado no questionário.

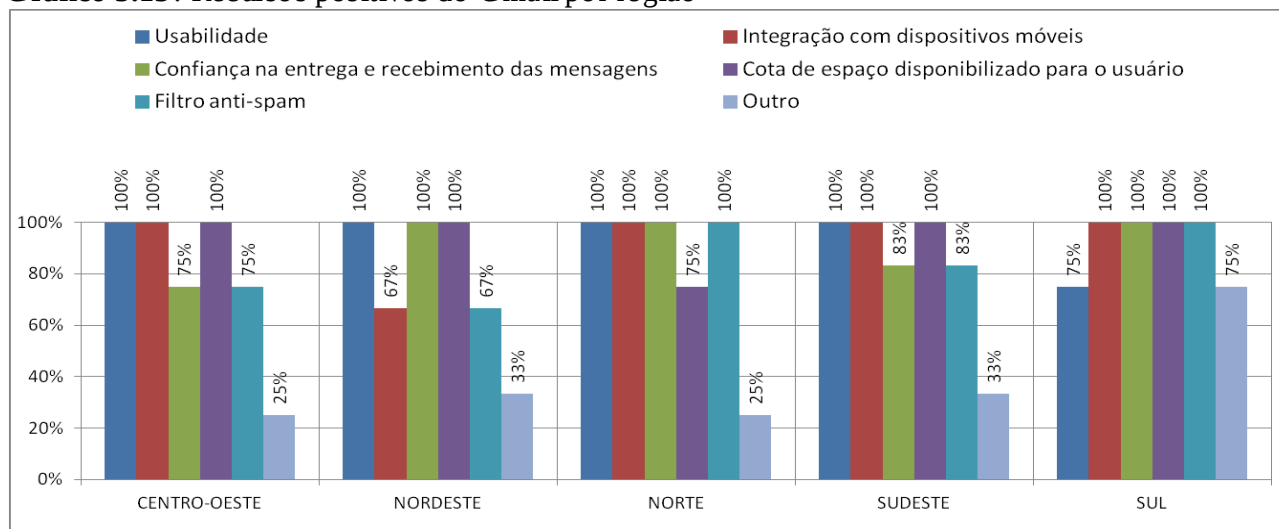
Para as 25 instituições que responderam a essa questão e afirmaram utilizar um correio eletrônico proprietário e não auditável, foi disponibilizada a possibilidade de selecionar mais de um recurso que seja considerado positivo na ferramenta utilizada.

<sup>37</sup> G Suite for Education: [https://support.google.com/a/answer/139019?hl=pt-BR&ref\\_topic=6047382](https://support.google.com/a/answer/139019?hl=pt-BR&ref_topic=6047382)

### 3.1.3.1 Recursos positivos da ferramenta Gmail

A análise dos fatores considerados positivos para a ferramenta Gmail e representados por região pode ser visualizada no Gráfico 3.13.

**Gráfico 3.13:** Recursos positivos do Gmail por região



Fonte: Elaborado pelo autor (2017)

A análise dos recursos positivos da ferramenta do Gmail, mostra na região Centro-Oeste a escolha de 100% das instituições que responderam a pesquisa pelos recursos Usabilidade, Integração com dispositivos móveis e Cota de espaço disponibilizado para o usuário, seguido de 75% que optaram por Confiança na entrega e recebimento das mensagens e Filtro Anti-spam, e, 25% que apontaram no campo Outro o fator Custo como recurso positivo da ferramenta.

Na região Nordeste, 100% das instituições escolheram os fatores Usabilidade, Confiança na entrega e recebimento das mensagens e Cota de espaço disponibilizado para o usuário. 67% escolheram Integração com dispositivos móveis e Filtro anti-spam, e, 33% apontaram no campo Outro, Ferramentas agregadas como recurso positivo.

Na região Norte, 100% apontaram os recursos Usabilidade, Integração com dispositivos móveis, Confiança na entrega e recebimento das mensagens, e Filtro Anti-spam. 75% apontaram a Cota de espaço disponibilidade para o usuário e 25%

apontaram no campo Outro, a Ausência de necessidade de investimento em infraestrutura e pessoal.

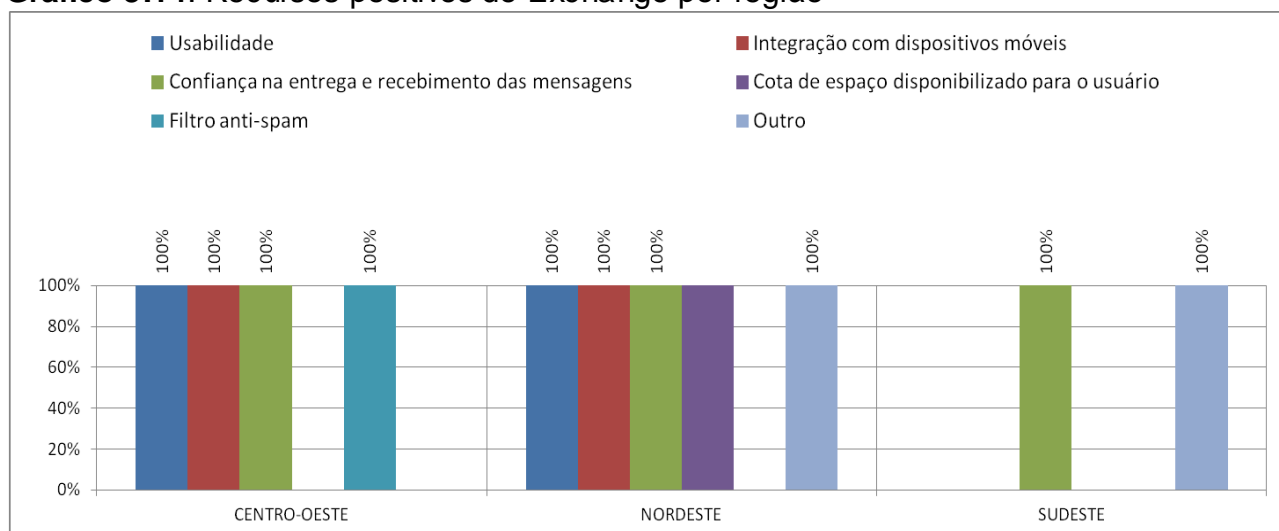
Na região Sudeste, 100% das instituições apontaram os recursos Usabilidade, Integração com dispositivos móveis e Cota de espaço disponibilidade para o usuário. 83% apontaram os recursos Confiança na entrega e recebimento das mensagens e Filtro anti-spam, e, 33% apontaram no campo Outro o recurso de Ferramentas agregadas.

O cenário da região Sul mostra a escolha de 100% das instituições pelos recursos de Integração com dispositivos móveis, Confiança na entrega e recebimento das mensagens, Cota de espaço disponibilidade para o usuário e Filtro anti-spam. O recurso Usabilidade foi apontado por 75% dos respondentes e também 75 das instituições apontaram no campo Outro os recursos de Ausência de necessidade de investimento em infraestrutura e pessoal, Disponibilidade e Backup.

### 3.1.3.2 Recursos positivos da ferramenta Exchange

A análise dos fatores considerados positivos para a ferramenta Exchange e representados por região pode ser visualizada no Gráfico 3.14.

**Gráfico 3.14:** Recursos positivos do Exchange por região



Fonte: Elaborado pelo autor (2017)

Para a ferramenta Exchange, a análise mostrou que na região Centro-oeste, 100% das instituições apontaram como recursos positivos, Usabilidade, Integração com

dispositivos móveis, Confiança na entrega e recebimento de mensagens e Filtro anti-spam.

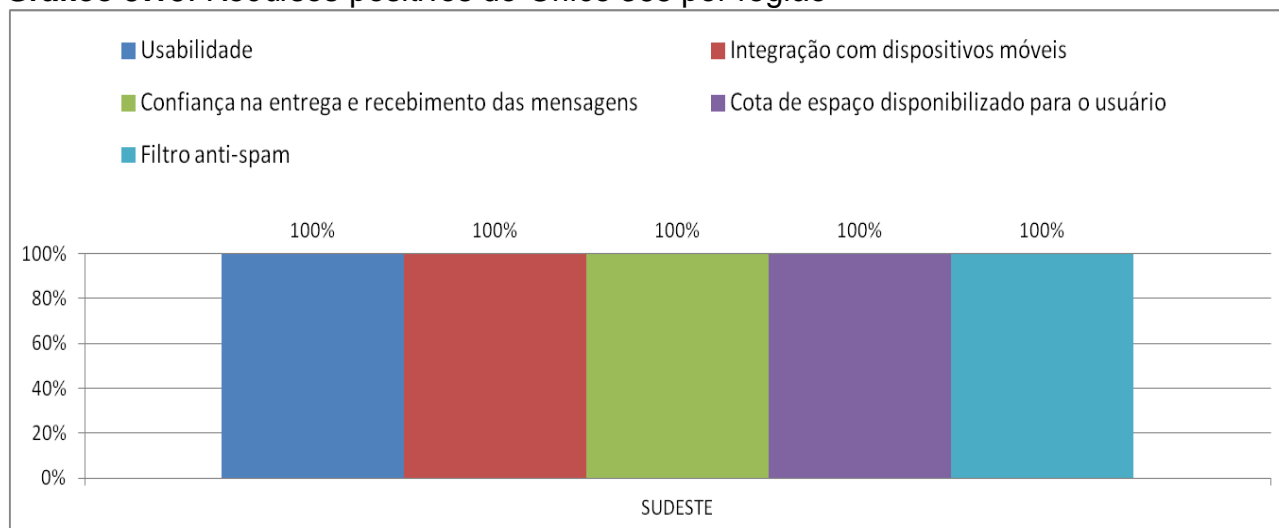
Na região Nordeste, 100% das instituições escolheram os recursos de Usabilidade, Integração com dispositivos móveis, Confiança na entrega e recebimento de mensagens, Cota de espaço disponibilizado para o usuário e Facilidade de administração, que foi apontado no campo Outro.

Na região Sudeste, 100% escolheram os recursos de Confiança na entrega e recebimento de mensagens e Integração com arquitetura tecnológica, que foi especificado no campo Outro.

### 3.1.3.3 Recursos positivos da ferramenta Office 365

A análise dos fatores considerados positivos para a ferramenta Office 365 e representados por região pode ser visualizada no Gráfico 3.15.

**Gráfico 3.15:** Recursos positivos do Office 365 por região



**Fonte:** Elaborado pelo autor (2017)

A análise mostra que na região Sudeste, os recursos Usabilidade, Integração com dispositivos móveis, Confiança na entrega e recebimento das mensagens, Cota de espaço disponibilizado para o usuário e Filtro anti-spam, foram apontados por 100% dos respondentes.

### Q5.2.3 - Recursos NEGATIVOS do e-mail proprietário

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como NEGATIVO e/ou acrescente mais algum no campo OUTRO?

- Nenhum
- Usabilidade
- Filtro anti-spam
- Cota de espaço disponibilizado para o usuário
- Integração com dispositivos móveis
- Confiança na entrega e recebimento das mensagens
- Outro:

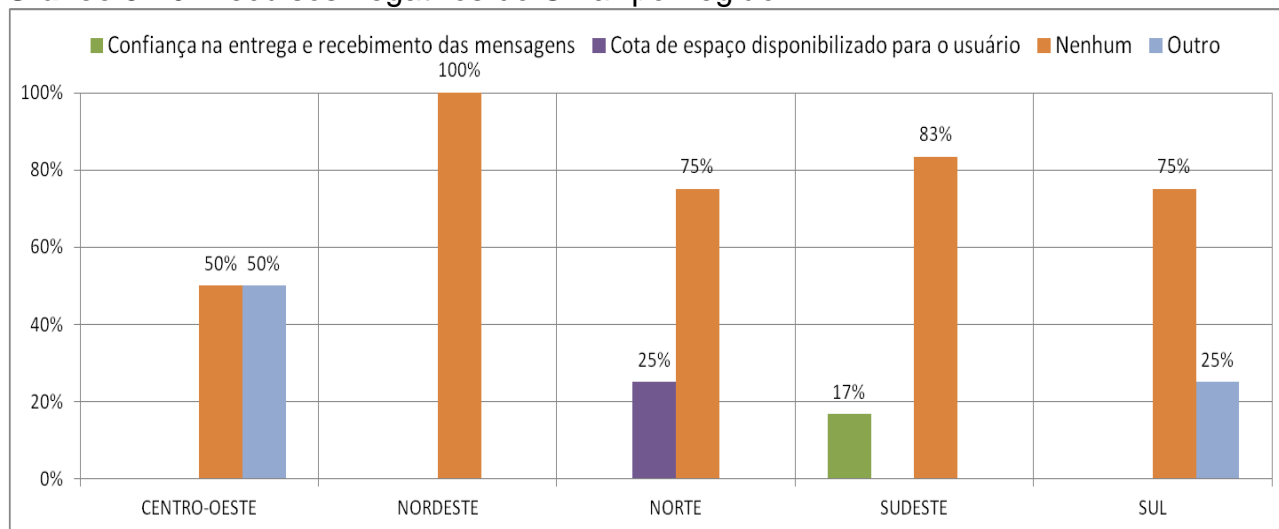
Nesta questão é solicitado que sejam apontados os recursos considerados negativos no e-mail proprietário e não auditável que é utilizado na instituição, que selecione nenhum em caso de não identificar algum recurso negativo, ou que seja apontado no campo Outro algum recurso extra negativo que não tenha sido listado.

Para as 25 instituições que responderam a essa questão e afirmaram utilizar um correio eletrônico proprietário e não auditável, foi disponibilizada a possibilidade de selecionar mais de um recurso que seja considerado negativo na ferramenta utilizada.

#### 3.1.3.4 Recursos negativos da ferramenta Gmail

A análise dos fatores considerados negativos para a ferramenta Gmail e representados por região pode ser visualizada no Gráfico 3.16.

**Gráfico 3.16:** Recursos negativos do Gmail por região



Fonte: Elaborado pelo autor (2017)

Na região Centro-oeste, 50% das instituições não identificam Nenhum recursos que possa ser considerado negativo na ferramenta e outros 50% apontaram a ausência de backup local.

Na região Nordeste, 100% das instituições afirmaram não existir Nenhum recurso que possa ser considerado negativo na ferramenta Gmail.

Na região Norte, 75% das instituições não identificaram Nenhum recurso negativo e 25% delas, apontaram a Cota de espaço disponibilizado para o usuário.

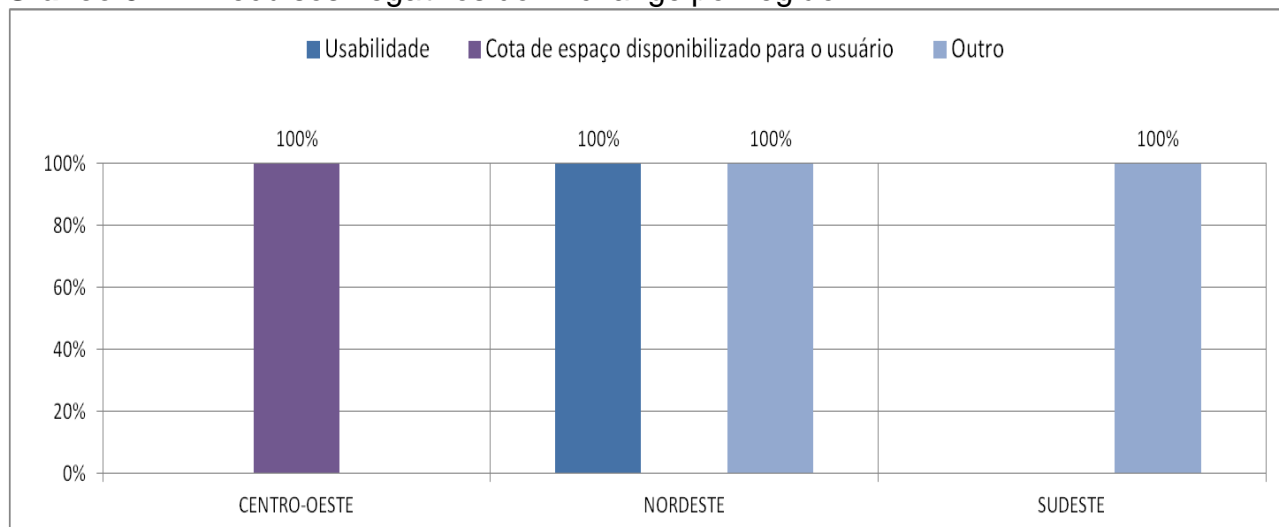
Na região Sudeste, 83% disseram não existir Nenhum recurso que possa ser considerado negativo na ferramenta, e 17% apontaram a Confiança na entrega e recebimento das mensagens.

E, 75% dos respondentes da região Sul disseram não existir nenhum recurso que possa ser considerado negativo na ferramenta, contra os 25% que apontaram no campo Outro o fato de não terem a Acesso às caixas postais no caso de ações judiciais.

### 3.1.3.5 Recursos negativos da ferramenta Exchange

A análise dos fatores considerados negativos para a ferramenta Exchange e representados por região pode ser visualizada no Gráfico 3.17.

**Gráfico 3.17:** Recursos negativos do Exchange por região



Fonte: Elaborado pelo autor (2017)



Na região Centro-oeste, 100% dos respondentes apontaram a Cota de espaço disponibilizada para o usuário como recurso negativo da ferramenta.

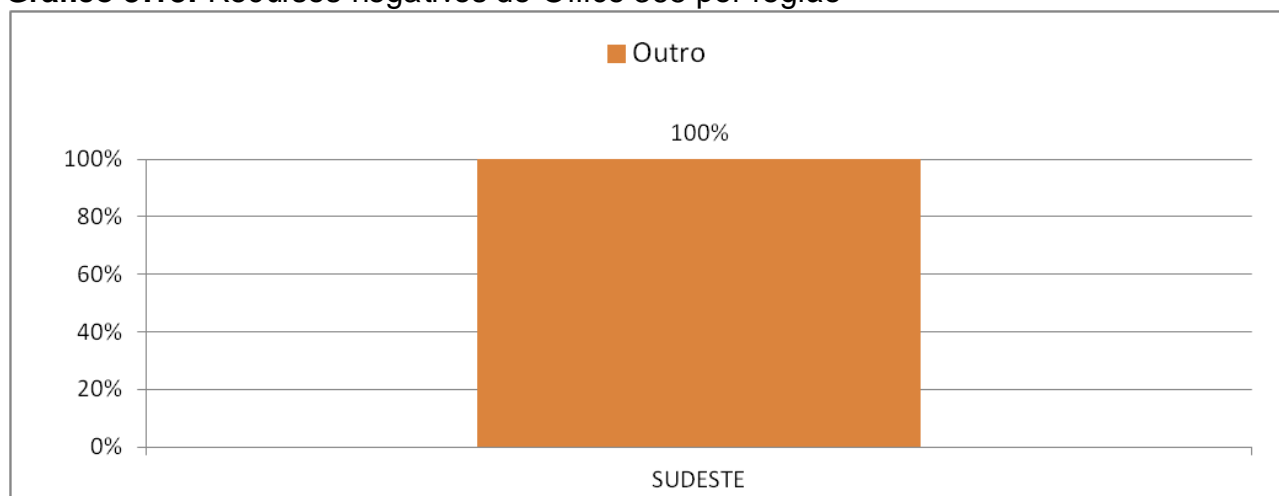
Na região Nordeste, 100% das instituições apontaram os recursos de Usabilidade e Custos, sendo esse ultimo apontado no campo Outro.

Para a região Sudeste, a análise mostrou como recurso negativo o Licenciamento que foi apontado no campo Outro, por 100% das instituições.

### 3.1.3.6 Recursos negativos da ferramenta Office 365

A análise dos fatores considerados negativos para a ferramenta Office 365 e representados por região pode ser visualizada no Gráfico 3.18.

**Gráfico 3.18:** Recursos negativos do Office 365 por região



Fonte: Elaborado pelo autor (2017)

A ferramenta Office 365, foi citada unicamente na região Sudeste e 100% das instituições que responderam o questionário, apontaram no campo Outro, como recurso negativo, a Segurança.

### 3.1.4 Fatores impeditivos para adesão ao decreto 8.135/2013

Considerando que muitas instituições não aderiram ao correio eletrônico nos padrões do decreto 8.135/2013, nesta seção serão identificados os fatores considerados impeditivos para que ocorresse essa adesão por parte dessas instituições.

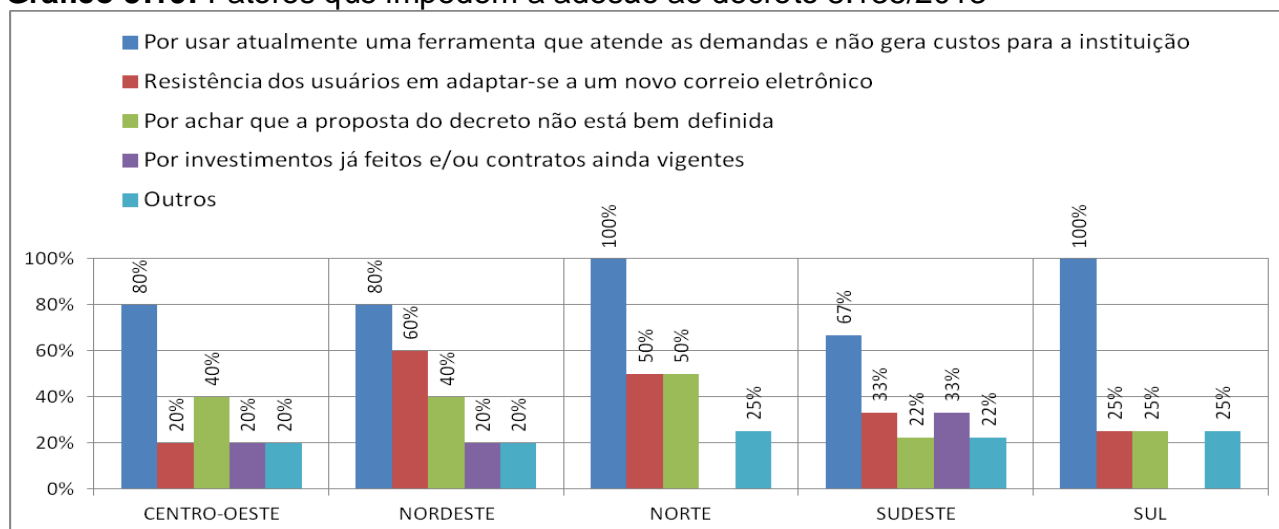
#### Q5.2.4 - Fatores que impedem a adesão

Tendo em vista que o decreto 8.135 e a portaria 141/2014 estabelecem diretrizes e prazo para adesão ao sistema de correio eletrônico livre e auditável, quais fatores impedem a adesão da sua instituição a essas normativas?

- Resistência dos usuários em adaptar-se a um novo correio eletrônico
- Por investimentos já feitos e/ou contratos ainda vigentes
- Por achar que a proposta do decreto não está bem definida
- Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição
- Outro

Esta questão alerta sobre as diretrizes e prazos que são estabelecidos no decreto 8.135/2013 e na portaria 141/2014 para adesão ao modelo de ferramenta livre e auditável e questiona quais são os fatores considerados impeditivos para a instituição aderir ao correio eletrônico nos moldes da normativa e a análise das respostas obtidas com as 25 instituições que responderam corretamente a essa questão pode ser visualizada no Gráfico 3.19.

**Gráfico 3.19:** Fatores que impedem a adesão ao decreto 8.135/2013



Fonte: Elaborado pelo autor (2017)

A análise mostrou que na região Centro-oeste, 80% das instituições disseram que o fator impeditivo de adesão à normativa é Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição; 40% alegaram que é Por achar que a proposta do decreto não está bem definida e 20% selecionaram os recursos de Resistência dos usuários em adaptarem-se a um novo correio eletrônico, Por

investimentos já feitos e/ou contratos ainda vigentes e também Pelos altos custos envolvidos na implantação de uma plataforma de correio eletrônica própria, incluindo nela: aquisição de infraestrutura, pessoal capacitado para implantação e manutenção, manutenção das contas, sendo esse ultimo apontado no campo Outro.

Para a região Nordeste, a análise mostrou que 80% definiram como fator impeditivo, Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição. 60% destacaram a Resistência dos usuários em adaptarem-se a um novo correio eletrônico; 40% acreditam que é Por achar que a proposta do decreto não está bem definida 20% disseram que é Por investimentos já feitos e/ou contratos ainda vigentes e também 20% apontaram como fator impeditivo à adesão, a Dificuldade em manter esse serviço com a infraestrutura atual.

Na região Norte, 100% dos respondentes disseram que Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição, isso seria um fator impeditivo. 50% disseram que a Resistência dos usuários em adaptarem-se a um novo correio eletrônico e Por achar que a proposta do decreto não está bem definida, são motivos que impedem a adesão ao decreto, e, 25% disseram no campo Outro que não possuem uma Infraestrutura como link e estabilidade elétrica suficiente para manter o serviço com alta disponibilidade.

Na região Sudeste, 67% disseram que o fator impeditivo é Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição; 33% apontaram os fatores Resistência dos usuários em adaptarem-se a um novo correio eletrônico e Por investimentos já feitos e/ou contratos ainda vigentes. 22% disseram que é Por achar que a proposta do decreto não está bem definida e no campo Outro, também com 22%, foi declarado que A implementação de uma estrutura própria geraria custos com pessoal, tecnológicos e necessidade de treinamento além de aumentar o nível de indisponibilidade do e-mail em relação ao serviço do Google.

Na região Sul, 100% dos respondentes disseram que Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição isso se torna um fator impeditivo para haver a adesão à normativa. Na sequencia, 25% das

instituições disseram que a Resistência dos usuários em adaptarem-se a um novo correio eletrônico, Por achar que a proposta do decreto não está bem definida e a Falta de recursos financeiros para adoção de outra ferramenta, que foi apontado no campo Outro, são fatores que impedem a adesão.

Também opinaram nas questões Q5.2.4 - Fatores que impedem a adesão e Q5.2.5 - Sugestões para adesão, as 4 (quatro) instituições representadas nas regiões Nordeste, Sudeste e Sul do Gráfico 3.2, e que responderam na Questão 04 não ter conhecimento sobre o decreto, pois todas elas afirmaram utilizarem um correio eletrônico proprietário e, dessa forma, considerou-se que o não conhecimento da normativa não seja fator impeditivo para que essas instituições pudessem opinar nas questões relacionadas acima.

A análise dos dados mostrou que uma grande quantidade de instituições não aderiu ao correio eletrônico sugerido no decreto 8.135/2013, por estarem satisfeitas com a ferramenta proprietária que utilizam atualmente e pela mesma não gerar custos. No entanto, essa decisão vai contra as prerrogativas existentes no decreto e o que o mesmo propõe para as instituições que fazem parte da Administração Pública Federal.

Outro ponto citado foi o fato de acharem que a proposta do decreto não está bem definida e com relação a esse posicionamento, na 7ª Reunião da Comissão de Coordenação do SISP/2016, já constou na pauta alguns pontos relevantes a serem futuramente revisados no decreto 8.135 e na portaria 141/2014, visando que essas normativas sejam mais bem definidas e possam melhor satisfazer os anseios dos fornecedores de serviços e produtos do governo federal, bem como das instituições que serão afetadas diretamente ao aderirem à proposta dessas normativas BRASIL (2016g).

### 3.1.5 Sugestões apresentadas para facilitar a adesão ao decreto 8.135/2013

#### **Q5.2.5 - Sugestões para adesão**

---

O que você sugere para que haja a adesão ao correio eletrônico utilizando *Software* livre e auditável, nos moldes do decreto 8.135/2013?

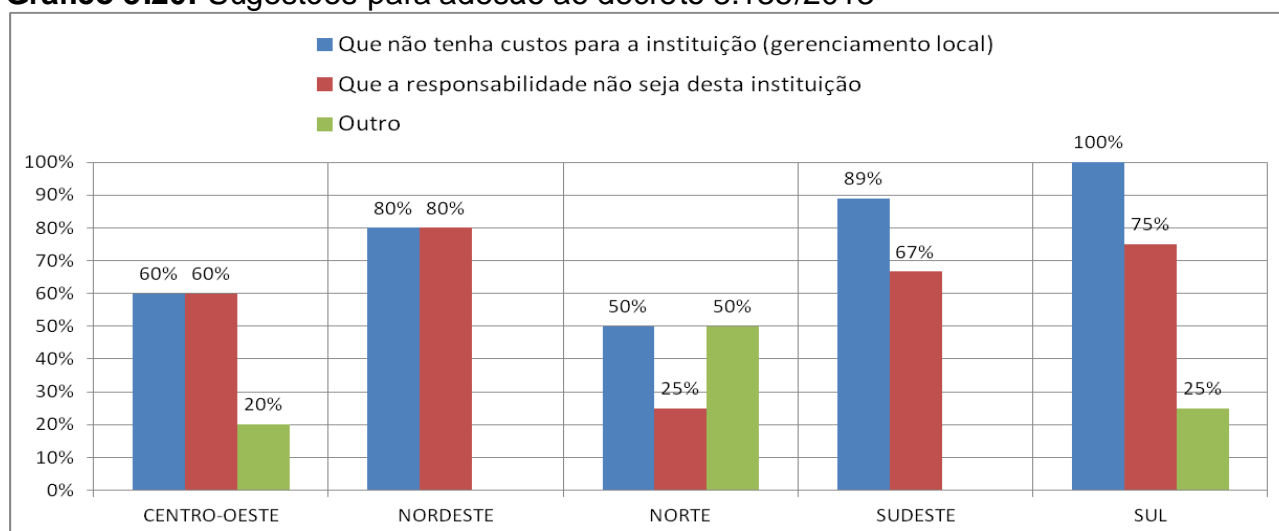
- Que não tenha custos para a instituição (Gerenciamento local)

- Que a responsabilidade pelo gerenciamento da infraestrutura do correio eletrônico não seja desta instituição
- Outro

Considerando que na questão anterior foram apontados os fatores considerados impeditivos para adesão ao modelo de ferramenta livre e auditável citado nas normativas, nesta questão é pedido que sejam apontadas sugestões para que aconteça a adesão por parte da instituição ao correio eletrônico auditável e os resultados analisados das 25 instituições participantes da pesquisa são mostrados no Gráfico 3.20.

Foi disponibilizado para as 25 instituições que responderam a essa questão, a possibilidade de selecionar ou especificar mais de uma sugestão considerada importante para que possa haver a adesão à normativa. Neste caso, a somatória dos percentuais pode ultrapassar os 100%.

**Gráfico 3.20:** Sugestões para adesão ao decreto 8.135/2013



Fonte: Elaborado pelo autor (2017)

As sugestões apresentadas na região Centro-oeste, revelam que 60% aceitam que o correio eletrônico seja instalado e gerenciado localmente, mas 60% querem que a responsabilidade não seja da instituição e se isentam de qualquer obrigação e no campo Outro, 20% desejam que os custos sejam os mínimos possíveis e que haja uma adesão massiva de todas a autarquia do governo federal.

Na região Nordeste 80% aceitam a instalação e gerenciamento local da ferramenta de correio eletrônico, mas querem Que não tenha custos para a instituição, enquanto outros 80% sugerem que para haver a adesão, é necessário Que a responsabilidade não seja da instituição e também se isentam de qualquer obrigação com a mesma.

Na região Norte, 50% aceitam o gerenciamento local da ferramenta, mas querem Que não tenha custos para a instituição; e outros 50% apresentaram no campo Outro, a Necessidade de recursos orçamentários para melhorar a infraestrutura e para manter a alta disponibilidade do serviço que é o mais utilizado pela instituição, além de Investimento em recursos humanos e infraestrutura suficiente. 25% das instituições se isentam de qualquer compromisso com a ferramenta e desejam Que a responsabilidade não seja da instituição.

Quanto a região Sudeste, 89% das instituições, referindo-se a implantação do correio eletrônico auditável, querem Que não tenha custos para a instituição, enquanto outros 67%, se isentam de qualquer compromisso com a implantação da ferramenta e querem Que a responsabilidade não seja da instituição.

Na região Sul, 100% querem Que não tenha custos para a instituição, 75% repassam para o governo a responsabilidade sobre o correio eletrônico auditável e pedem Que a responsabilidade não seja da instituição, enquanto 25% apontaram no campo Outro, como sugestão para haver a adesão ao decreto, Que o serviço seja provido por órgão público (rnp, mpog, etc)

Com seleção da opção que não tenha custos para a instituição, que foi feita por todas as instituições, mais uma vez fica evidenciada a questão orçamentária, pois aceita-se que a estrutura de correio eletrônico nos moldes do decreto seja instalada e gerenciada na instituição, mas que a responsabilidade orçamentária não seja uma obrigação da instituição.

Na opção seguinte, quando sugerem que a responsabilidade pelo gerenciamento da infraestrutura do correio eletrônico não seja da instituição, os

respondentes se isentam totalmente dessa responsabilidade e repassam para o governo federal a responsabilidade por implantar e gerenciar o correio eletrônico de acordo com o modelo proposto nas normativas.

### **3.2 Considerações finais do capítulo**

Neste capítulo foi apresentada a análise dos dados por região, referente à pesquisa feita com as instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica, com objetivo de identificar a estrutura de correio eletrônico dessas instituições e avaliar a aderências das mesmas ao modelo de correio eletrônico proposto no decreto 8.135/2013.

A pesquisa também solicitou às instituições que não aderiram ao correio eletrônico auditável e de acordo com a proposta da normativa, que apontassem os motivos para a não adesão, como também, sugestões para que essa adesão possa ocorrer, e esses dados ajudarão na construção de um conjunto de recomendações que será proposto no capítulo seguinte, visando uma melhor aceitação por parte das instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica, a proposta apresentada no decreto.

## **4. CONJUNTO DE RECOMENDAÇÕES**

Considerando a existência do decreto 8.135 desde 2013 e do mesmo propor a utilização de um correio eletrônico livre e auditável para a Administração Pública Federal, a preferência da maioria das instituições pesquisadas neste trabalho é pela utilização de correio eletrônico proprietário, com o Gmail liderando essa preferência, conforme mostrado no gráficos 3.12, no capítulo anterior.

Por existir essa preferência pelo correio eletrônico proprietário da Google, buscou-se identificar também as características relevantes existentes na ferramenta do Gmail que tanto agradam às instituições que o utilizam, a ponto de irem contra uma determinação do governo e fez-se um comparativo com as características existentes nas ferramentas livres e auditáveis analisadas.

Como forma de avaliar os motivos da não aderência por parte das instituições pesquisadas a proposta do decreto, foi perguntado, a quem não aderiu, os fatores impeditivos e sugestões para que pudesse ocorrer a aceitação e adesão ao correio eletrônico nos moldes das normativas.

A partir dessas informações coletadas e analisadas, será construído um conjunto de recomendações que possa viabilizar a aceitação e adesão ao correio eletrônico proposto nas normativas federais.

### **4.1 Fatores impeditivos para adesão ao correio eletrônico nos moldes do decreto e sugestões apresentadas na pesquisa**

Na análise dos resultados obtidos, foram apresentados pelas instituições pesquisadas diversos fatores considerados impeditivos para adesão ao correio eletrônico nos moldes do decreto, como também sugestões para que sejam resolvidos tais impedimentos.

Dessa forma, baseando-se nos fatores e sugestões apresentados, serão construídas as recomendações que possam servir como contribuição para facilitar uma



melhor adesão por parte das instituições que compõem a Rede Federal de Educação, ao correio eletrônico auditável que é proposto na normativa federal.

#### 4.1.1 Uso de uma ferramenta que atende às demandas e não gera custos

Este fator, que foi escolha da maioria dos respondentes desta questão, mostra a satisfação das instituições com a ferramenta que está atualmente sendo utilizada. No entanto, cabe observar que essa ferramenta mesmo não gerando custos para a instituição, é proprietária e não auditável, e está em desacordo com as normativas federais (decreto 8.135/2013 e Portaria 141/2014) que apresentam como medida para a segurança das informações na APF, um correio eletrônico que possibilite a auditoria.

Quando as instituições apontaram os recursos de Usabilidade, Integração com dispositivos móveis, Confiança na entrega e recebimento das mensagens, Cota de espaço disponibilizado para o usuário, Filtro anti-spam, Ausência de necessidade de investimento em infraestrutura e pessoal (custos), Integração com arquitetura tecnológica, Ferramentas agregadas de colaboração (drive, formulários) e Facilidade de administração como recursos positivos e determinantes para utilização da ferramenta de correio eletrônico proprietário, cabe observar, que quase todos esses recursos são oferecidos na ferramenta Expresso do Serpro, conforme especificações apresentadas no site da comunidade Expresso<sup>38</sup>.

Considerando que o Expresso do Serpro possui quase todos os recursos considerados relevantes nas ferramentas proprietárias, acredita-se que a resistência apresentada pelas instituições da Rede Federal de Educação em utilizar o correio eletrônico que é sugerido na normativa federal, se dê pela falta de conhecimento sobre o que tal ferramenta pode oferecer para o usuário, e tal fator impeditivo poderia ser amenizado com capacitação do usuário final da ferramenta a ser utilizada.

---

<sup>38</sup> Comunidade ExpressoBR - <http://comunidadeexpresso.serpro.gov.br>

#### 4.1.2 Resistência dos usuários em adaptar-se a um novo correio eletrônico

Este fator reflete a resistência apresentada pelos usuários do e-mail em ter que se adaptarem a uma ferramenta diferente da que é atualmente utilizada pelos mesmos.

Joshi (2005 apud Oliveira et al., 2009, p. 05) referindo-se à implantação de novos sistemas de informação, afirma que nessas situações, os usuários podem assumir postura de adoção ou de resistência ao uso, baseados em suas avaliações de ganhos e perdas associadas ao sistema.

Ainda com relação à resistência dos usuários em adaptar-se a novos sistemas, Lapointe (2005 apud Oliveira et al., 2009, p. 05) classifica a resistência em quatro níveis:

- a) apatia, relacionada à distância e à falta de interesse;
- b) resistência passiva, relacionada a táticas de demora, abandono, desculpas e persistência em comportamentos antigos;
- c) resistência ativa, relacionada a comportamento forte, não destrutivo e formação de coalizões; e;
- d) resistência agressiva, que abrange ameaças, lutas, greves, boicotes ou sabotagem, procurando acabar com a ordem ou destruir.

Como forma de resolução dos problemas apresentados nos itens 4.1.1 e 4.1.2, sugere-se que haja treinamento com os usuários do sistema de correio eletrônico, de forma que os mesmos possam conhecer a nova ferramenta e o que a mesma pode oferecer; mostrar os recursos considerados relevantes na ferramenta atual, e como os usuários poderão utilizá-los na nova ferramenta a ser implantada. Cabe também apresentar para os usuários, a proposta das normativas federais com relação ao correio eletrônico auditável e os benefícios que o mesmo oferece para a segurança das informações das instituições.

Acredita-se que essas medidas amenizarão a resistência existente por parte dos usuários, bem como farão com que os mesmos se sintam como participantes de um processo de mudança institucional e não somente cumpridores de decisões verticalizadas.

#### 4.1.3 Por achar que a proposta do decreto não está bem definida

Esse fator representa a insatisfação das instituições que consideraram que o decreto não está bem definido e, portanto, necessita de mudanças na sua estrutura para que possa atingir os objetivos que propõe para a APF.

Em sua avaliação da segurança das informações do governo brasileiro, Veloso (2014) apresenta uma avaliação do Decreto 8.135/2013 e suas consequências na APF e na segurança das informações:

Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

Veloso (2014) diz que tais serviços estarão restritos apenas ao SERPRO e TELEBRAS, e que por impedir a ampla concorrência com outras empresas, não se conseguirá produtos e serviços com bons preços e qualidade.

Quanto ao fato da comunicação de dados ser realizada por redes de comunicações e serviços de TI, Veloso (2014) diz que nesse caso subentende-se que esse seja o único meio permitido para a troca de informações. No entanto, o governo ainda utiliza os serviços tradicionais dos Correios, o que leva a crer que nesse caso, também esse serviço deverá ser substituído, o que embora seja possível em tese, na prática ainda é uma questão que demandará muito tempo e esforço para se concretizar.

§ 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

Para Veloso (2014), tal exigência apresenta-se como utópica e o seu cumprimento é praticamente impossível, pois na atualidade, as tecnologias por trás de redes, sistemas e serviços de TI são sempre providas a partir de “ecossistemas” complexos, compostos por equipamentos e sistemas provenientes, na maioria das vezes, de diferentes fabricantes e de diversos países. O autor afirma ainda que em muitos desses componentes seria impossível a realização de qualquer tipo de auditoria,

acrescentando não ser possível a utilização de um correio eletrônico com 100% de tecnologia nacional.

Também no documento de respostas da consulta pública nº 144/2014 da ePING<sup>39</sup>, referindo-se aos Critérios de Auditoria de Segurança presentes no decreto, foram citadas as seguintes observações:

A Cisco<sup>40</sup> acredita que a implementação de políticas industriais restritivas pode afastar os investimentos estrangeiros no desenvolvimento e produção nacional de equipamentos e de produtos de rede no Brasil, podendo trazer consequências negativas não previstas para todo o ecossistema de contratações. [...]

Já para a empresa The Software Alliance e Information Technology Industry Council (ITI)<sup>41</sup>, referindo-se à possibilidade de auditoria que o decreto exige nas contratações a serem feitas, diz o seguinte:

[...] Muitos fornecedores globais, muitos dos quais produzem as tecnologias de ponta em segurança que o governo brasileiro busca, provavelmente não participarão de licitações que exijam que se entregue ou disponibilize propriedade intelectual, como código-fonte ou outras informações de projeto. Isto privaria o governo brasileiro de algumas das tecnologias de ponta das quais poderia precisar para proteger seus sistemas [...]

Referindo-se ao armazenamento e a recuperação dos dados derivados das comunicações da administração pública federal direta, autárquica e fundacional, o § 4º do decreto 8.135/2013, diz o seguinte:

O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.

Para Veloso (2014), o resultado disso é que fica vedada a contratação de serviços tais como hospedagem, *collocation* ou computação em nuvem, e essa decisão vai contra uma tendência do mercado mundial.

O autor conclui dizendo que mesmo que o decreto possa ser considerado como uma iniciativa louvável, o mesmo ainda levanta muitas críticas da comunidade

---

<sup>39</sup> <https://www.governoeletronico.gov.br/documentos-e-arquivos/>

<sup>40</sup> <http://www.cisco.com/>

<sup>41</sup> <https://www.itic.org/>

especializada em segurança da informação, a qual questiona a eficácia de tais medidas e ainda alerta da necessidade de haver uma discussão mais ampla sobre o seu teor com a comunidade especializada e a sociedade.

Quando as instituições apontam a necessidade de reestruturação do decreto, fica clara a insatisfação por parte das mesmas com o modelo de correio eletrônico que é proposto e vê-se a necessidade de uma maior discussão sobre a normativa e os impactos que a mesma causará nos órgãos que utilizarão o sistema. Destaca-se também a necessidade de um maior envolvimento por parte das instituições envolvidas no processo na construção de uma melhor proposta.

#### 4.1.4 Fatores apresentados no campo *Outro*

Os fatores listados a seguir considerados impeditivos para que ocorra a adesão do correio eletrônico sugerido no decreto, foram adicionados pelos respondentes no campo *Outro*.

- Falta de recursos orçamentários para investir em infraestrutura e capacitação;
- A implementação de uma estrutura própria geraria custos com pessoal, tecnológicos e necessidade de treinamento além de aumentar o nível de indisponibilidade do *e-mail* em relação ao serviço do Google;
- Infraestrutura como link e estabilidade elétrica insuficiente para manter o serviço com alta disponibilidade;
- Pelos altos custos envolvidos na implantação de uma plataforma de correio eletrônica própria, incluindo nela: aquisição de infraestrutura, pessoal capacitado para implantação e manutenção, das contas (backup, etc);
- Dificuldade em manter esse serviço com a infraestrutura atual; e
- Falta de recursos financeiros para adoção de outra ferramenta.

Após análise dos fatores impeditivos listados, vê-se que na sua totalidade há relação com o fator financeiro, pois foram citados problemas relacionados à carência de infraestrutura adequada ou capacitação de pessoal para que se pudesse manter o

correio eletrônico na própria instituição, como também para contratação de um que atenda à proposta do decreto.

Essa questão financeira também foi citada na Questão 5.2.5 – Sugestões para adesão, como recomendação para que ocorra a adesão ao decreto, e muitas instituições selecionaram a opção que não tenha custos para a instituição (Gerenciamento local), mostrando dessa forma, que as mesmas aceitam que a instalação e o gerenciamento do correio eletrônico sejam realizados pela instituição, mas que os custos não saiam do já precário orçamento repassado às mesmas.

Outras instituições preferem que a responsabilidade pelo gerenciamento da infraestrutura do correio eletrônico não seja da instituição na qual trabalham, mas que seja totalmente assumido pelo governo federal.

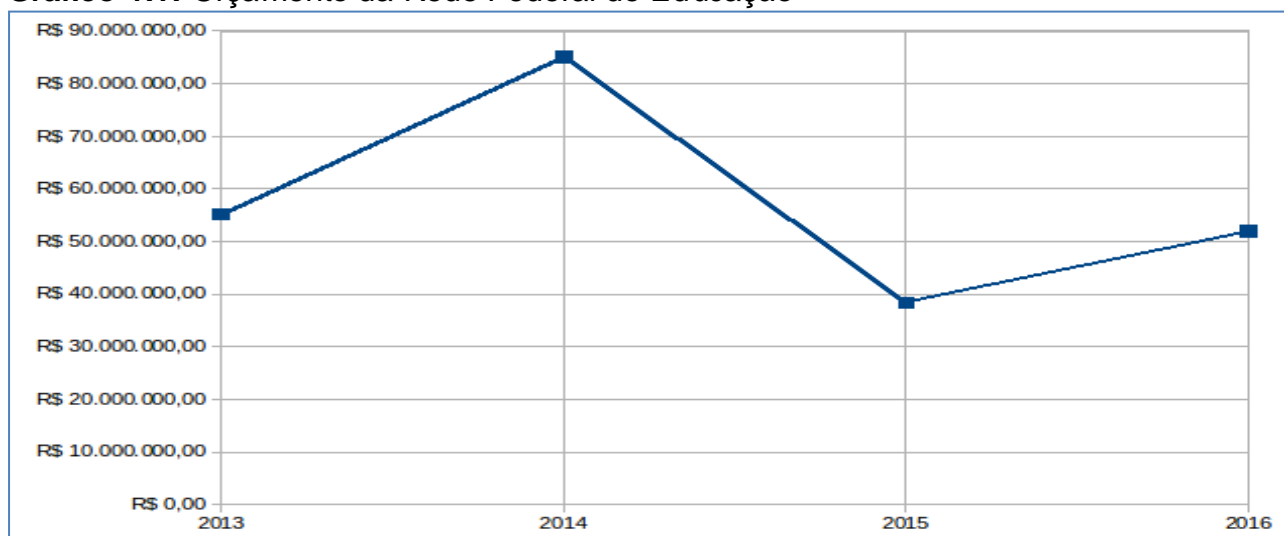
Foram apontados também no campo Outro, a necessidade de recursos orçamentários para melhorar a infraestrutura para manter a alta disponibilidade do serviço que é o mais utilizado pela instituição e que haja investimento em recursos humanos e infraestrutura suficiente.

Nessa mesma linha de pensamento, também sugeriram no campo Outro, que o serviço seja provido por órgãos públicos como RNP e MPOG; que os custos sejam os mínimos possíveis e que haja uma adesão massiva de todas as autarquias do governo federal.

Em consulta ao relatório de despesas de TI no painel do orçamento do site SIOP – Sistema Integrado de Planejamento e Orçamento do Governo Federal<sup>42</sup>, foi possível fazer um filtro do orçamento liberado para as 42 instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica, ao longo de quatro (04) anos conforme pode ser visto no Gráfico 4.1.

---

<sup>42</sup> SIOP - [www1.siop.planejamento.gov.br](http://www1.siop.planejamento.gov.br)

**Gráfico 4.1:** Orçamento da Rede Federal de Educação

Fonte: Elaborado pelo Autor (2017)

O Gráfico 4.1 apresenta em 2013, um orçamento inicial de R\$ 55.203.268,00, com uma ascensão em 2014 para o valor de R\$ 85.016.552,00, seguido de uma queda em 2015 para R\$ 38.389.457,00, e finalizando em 2016 com uma leve elevação para 51.906.465,00 comparado ao ano anterior, mas com uma grande diferença, se comparado a 2013.

Essa diminuição no orçamento investido em TI vai na contramão da expansão da Rede Federal de Educação, pois conforme pode ser visualizado na Figura 2.1 que mostra a expansão da Rede ao longo dos anos, e fazendo um comparativo com o Gráfico 4.1 que mostra o orçamento de TI entre 2013 e 2016, enquanto a Rede aumentou, o orçamento diminuiu.

Mediante tais problemas apresentados, fica clara a necessidade de um maior investimento financeiro por parte do governo federal, voltado para os setores de TI existentes nas instituições, de modo que esses tenham condições de melhor atender às exigências das normativas federais no que se refere à contratação de bens e serviços, bem como, poder atender de forma satisfatória às demandas da comunidade que irá utilizar as soluções a serem contratadas.

#### 4.1.5 Investimentos já feitos e/ou contratos ainda vigentes

Esse fator impeditivo mostra a realidade das instituições que já investiram na contratação de algum correio eletrônico, no entanto, tais instituições, caso sejam obrigadas a fazerem a adesão ao correio eletrônico sugerido no decreto, terão que abdicar da ferramenta contratada para utilizarem a sugerida pelo governo. No artigo 18 da Portaria 141/2014 é estabelecido o prazo máximo de cinco anos para que os órgãos possam efetuar essa migração.

Art. 18. A migração dos serviços de redes de telecomunicações e de tecnologia da informação em operação ou ativos deve ocorrer no prazo máximo de sessenta meses a partir da vigência desta Portaria.

Para essa situação, na qual será obrigatória a migração do sistema em uso para um novo sistema de acordo com o que determina a normativa, sugere-se a adoção das soluções já apresentadas anteriormente que vão desde a liberação orçamentária para contratação de uma nova ferramenta nos padrões da normativa federal, até as medidas voltadas para a conscientização e capacitação dos colaboradores como forma de amenizar a resistência dos mesmos e favorecer uma maior aceitação da nova ferramenta institucional.

#### 4.1.6 Alternativa ao correio eletrônico do decreto

Como forma de sugerir uma solução alternativa à utilização de um correio eletrônico institucional, além do Expresso do Serpro que é citado no Decreto 8.135/2013, propõe-se um consórcio entre as instituições que compõem a Rede Federal de Educação para implementação de um correio eletrônico de acordo com as exigências do decreto e que possa ser utilizado pela rede.

Serão eleitas as duas instituições da Rede Federal de Educação que sediarão o correio eletrônico institucional, utilizando software livre e auditável, conforme exigência do decreto, e que tenham condições de atender aos critérios de melhor infraestrutura de TI, localização geográfica, melhores links de internet, energia elétrica estável e equipe de TI capacitada.



O serviço de correio eletrônico funcionará hospedado em uma das instituições eleitas para sediar o equipamento, mas com redundância em outra como forma de garantir o armazenamento das informações de forma descentralizada, além de aumentar a disponibilidade do serviço em caso de falhas.

Como forma de garantia orçamentária para implantação e manutenção da infraestrutura de TI, bem como a capacitação da equipe responsável por manter tal estrutura, será feito um repasse orçamentário das demais instituições da Rede Federal que irão usufruir do e-mail institucional, permitindo dessa forma que a ferramenta venha a ter em longo prazo um baixo custo de manutenção.

Considerando o fato de que o serviço funcionará em uma estrutura pertencente à Rede Federal de Educação, fica evidente a concordância com o Art. 1º do Decreto 8.135/2013 e seus parágrafos:

Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias.

Considerando que o correio eletrônico deva ser fornecido por órgãos da administração pública federal, o § 2º reforça essa exigência:

§ 2º Os órgãos e entidades da União a que se refere o caput deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da administração pública federal.

Pelo fato da utilização de *software* livre e auditável na estrutura lógica do equipamento, vê-se que tais medidas estarão em concordância com o § 3º do decreto:

§ 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

Ainda considerando o fato da redundância entre os órgãos da Rede Federal que ficarão responsáveis pelo armazenamento e backup dos dados, esse fato vai ao encontro do § 4º:

§ 4º O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.

Desta forma, acredita-se com essa solução estar atendendo às exigências do decreto e oferecendo um correio eletrônico de qualidade, construído com a participação e envolvimento da comunidade que será usuária da solução como também dando autonomia à Rede Federal de Educação de poder implementar ou modificar alguns recursos que considerem ser necessários na solução utilizada, sem a dependência de terceiros.

## **4.2 Considerações finais do capítulo**

Esse capítulo apresentou os fatores apresentados como impeditivos para que possa ocorrer a adesão ao correio eletrônico, por parte das instituições que compõem a Rede Federal de Educação que o decreto governamental sugere, bem como as sugestões apresentadas pelas instituições participantes para superar tais impedimentos. A partir dessas informações coletadas e analisadas, e como forma de dar relevância ao trabalho efetuado, foram apresentadas recomendações que visam superar tais impedimentos e favorecer à adesão por parte das instituições da APF ao e-mail auditável, proposto no decreto 8.135/2013, como forma de proteção dos dados e de aumentar a segurança das informações na Administração Pública Federal do governo brasileiro.·.

## **5. CONSIDERAÇÕES FINAIS DO TRABALHO**

Este trabalho objetivou efetuar um estudo junto às instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnologia acerca dos fatores que influenciam a aderência ou não aderência por parte dessas instituições às referidas normativas federais e ao modelo de correio eletrônico proposto no Decreto 8.135/2013.

Por meio da análise dos dados coletados foi possível concluir que a preferência da maioria das instituições pesquisadas é pela utilização de ferramentas de correio eletrônico proprietário e apesar de o decreto ser de 2013 e apresentar um prazo de cinco (05) anos para adesão ao novo correio eletrônico auditável, a pesquisa mostrou uma baixa adesão à ferramenta Expresso do Serpro, sugerida no decreto como forma de garantir a segurança da informação da Administração Pública Federal.

Visando uma maior aceitação à proposta do decreto, foram apresentados alguns fatores considerados impeditivos, como também sugestões para que possa ocorrer a adesão ao correio eletrônico do decreto.

A partir da análise dos fatores considerados impeditivos e das sugestões para haver a adesão ao mesmo, concluiu-se que a grande maioria dos problemas está relacionada a questões financeiras, conscientização e capacitação dos usuários e também à reestruturação do decreto, de forma que possa haver um maior envolvimento das instituições que utilizarão o correio eletrônico nos moldes do decreto.

Foi apresentada ainda a proposta de um correio eletrônico financiado e gerenciado pela Rede Federal de Educação, como forma de oferecer uma ferramenta que atenda à demanda das instituições com relação à comunicação de dados e que possa também atender às exigências do decreto.

### **5.1 Limitações do trabalho**

Na sequência são citadas algumas limitações que foram detectadas ao longo da construção deste estudo:

- Limitações relacionadas a pouca bibliografia e estudos correlatos ao decreto 8.135/2013 e a sua aplicabilidade na Rede Federal de Educação;
- Retardo na obtenção dos dados a serem analisados que foram causados por interpretações errôneas do questionário enviado às instituições e que ocasionaram invalidação de algumas respostas, obrigando o entrevistador a intervir junto aos respondentes para que refizessem o questionário.
- Não ter ciência se é viável financeiramente para a RFEPECT, a solução apresentada na Seção 4.1.6 como alternativa ao correio eletrônico do decreto;
- Em virtude de a pesquisa ter sido feita somente com os membros da DGTI, ela não reflete a visão dos demais usuários do sistema.

## **5.2 Sugestões de trabalhos futuros**

Como forma de dar continuidade a esse trabalho, sugere-se que sejam efetuados estudos junto às instituições da RFEPECT, visando identificar quais delas atendem os critérios de melhor infraestrutura de TI, localização geográfica, melhores links de internet, energia elétrica estável e equipe de TI capacitada, e que foram sugeridos no item 4.1.6 como alternativa ao correio eletrônico do decreto.

Considerando que a metodologia deste trabalho ficou restrita a um questionário do tipo *survey* e aplicado somente com os membros das Diretorias Gerais de Tecnologia da Informação, considera-se de extrema relevância uma consulta ampla à comunidade usuária do sistema, como forma de engajá-la na construção do projeto do consorcio do correio eletrônico a ser utilizado pela Rede Federal de Educação.

## **5.3 Validação da proposta apresentada neste trabalho**

Depois de efetuada a pesquisa junto as instituições pertencentes a Rede Federal de Educação visando avaliar a aderência das mesmas ao modelo de correio eletrônico auditável proposto no decreto 8.135/20, foram geradas algumas recomendações visando apresentar uma solução alternativa à utilização de um correio eletrônico institucional que venha atender ao decreto.

Como forma de validar as recomendações resultantes deste trabalho, foi encaminhado para as instituições que participaram da pesquisa, um formulário eletrônico composto por questões objetivas e subjetivas que visando obter a identificação da instituição e do respondente, como também avaliar o grau de concordância ou discordância do respondente às recomendações apresentadas e permitir que o mesmo possa apresentar sugestões.

Para efetuar uma avaliação do nível de concordância ou discordância dos respondentes, foi utilizada na questão 3 (três) a escala de Likert, que foi criada pelo educador e psicólogo Rensis Likert em 1932, e que Appolinário (2007, p. 81), define como um “tipo de escala de atitude na qual o respondente indica seu grau de concordância ou discordância em relação a determinado objeto”.

Para Silva Junior e Costa (2014), a outra vantagem apresentada pela escala Likert é a simplicidade de aplicação, pois o respondente tem a possibilidade de concordar ou não com uma determinada afirmação de forma simplificada. No entanto, os autores alertam da necessidade do respondente fazer previamente uma análise do conteúdo e posteriormente da amplitude, para que se possa conhecer o grau de intensidade da afirmação.

O formulário que foi enviado para os membros das DGTI das 39 instituições da RFEPCCT que participaram da pesquisa, ficou disponível do dia 20/06/2017 a 19/07/2017 e foram coletadas 18 (dezoito) respostas, o que mostrou participação de mais de 46% das instituições.

A análise das validações apresentadas foi feita baseando-se nas respostas obtidas por meio do questionário disponibilizado no APÊNDICE B e também foi aplicada a técnica de porcentagem, visando melhor quantificar e expressar os resultados obtidos.

### 5.3.1 Identificação da instituição e do respondente da validação

Na sequência, é apresentada a estrutura do questionário eletrônico que foi enviado às instituições como forma de obter a validação das recomendações surgidas a partir deste trabalho.

#### **Q01 - Selecione a sua instituição**

---

Esta questão objetivou identificar as instituições que participaram da validação da pesquisa e o resultado, classificado por região, é apresentado abaixo.

**Centro-oeste:** Instituto Federal de Goiás, Instituto Federal Goiano e Instituto Federal do Mato Grosso;

**Nordeste:** Instituto Federal de Alagoas, Instituto Federal da Bahia, Instituto Federal do Ceará, Instituto Federal do Maranhão, Instituto Federal de Pernambuco, Instituto Federal do Piauí, Instituto Federal do Rio Grande do Norte e o Instituto Federal do Sertão Pernambucano.

**Norte:** Instituto Federal do Acre, Instituto Federal do Amazonas, Instituto Federal de Rondônia e o Instituto Federal de Roraima;

**Sudeste:** Instituto Federal do Espírito Santo, Instituto Federal Fluminense e o Instituto Federal do Rio de Janeiro.

#### **Q02 – Função na DGTI**

---

Considerando que o questionário foi enviado para os membros que compõem as DGTI das instituições, esta questão visa identificar o perfil profissional desses respondentes, e abaixo são relacionados os resultados obtidos por região.

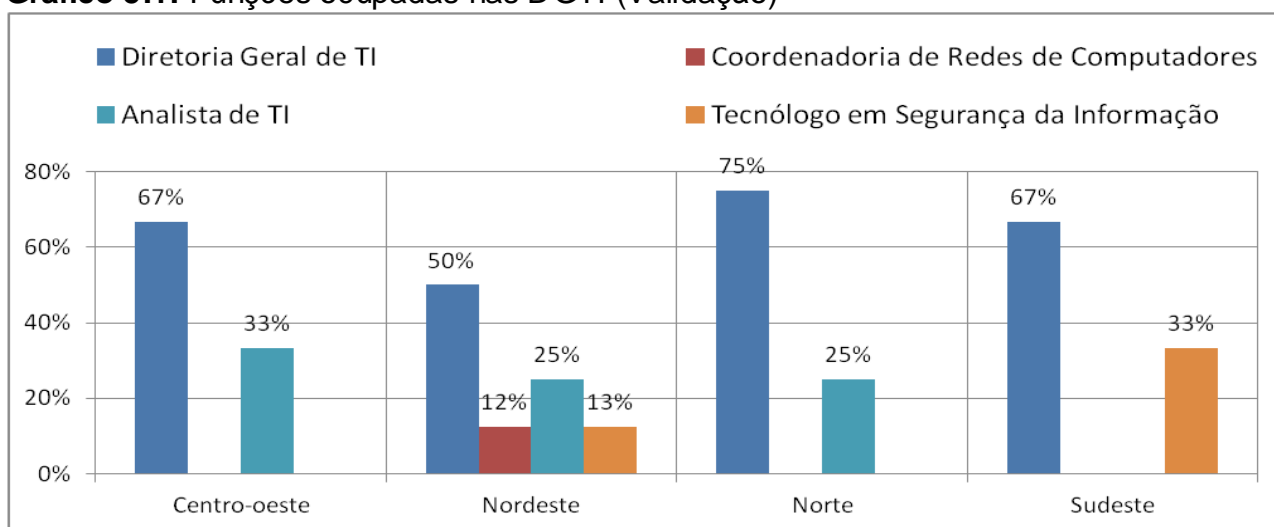
A análise dos dados que pode ser visualizado no Gráfico 5.1 mostra que na região Centro-oeste, 67% dos respondentes são Diretores Gerais de TI e 33%, são Analista de TI.

Na região Nordeste, 50% dos que responderam são Diretores de TI, 25% são Analistas de TI, 13% são Tecnólogos em Segurança da informação e 12% pertencem a Coordenadoria de redes de computadores.

Na região Norte, 50% são Diretores gerais de TI e 25% são Analistas de TI.

Na região Sudeste 67% representam os Diretores gerais de TI e 33% são Tecnólogos em segurança da informação.

**Gráfico 5.1:** Funções ocupadas nas DGTI (Validação)



**Fonte:** Elaborado pelo autor (2017)

### 5.3.2 Avaliação da proposta apresentada e sugestões do respondente

#### Q03 - Avaliação do nível de aceitação à proposta apresentada

Esta questão visa avaliar o nível de concordância ou discordância dos respondentes às recomendações apresentadas como solução alternativa à utilização de um correio eletrônico institucional que venha atender ao decreto.

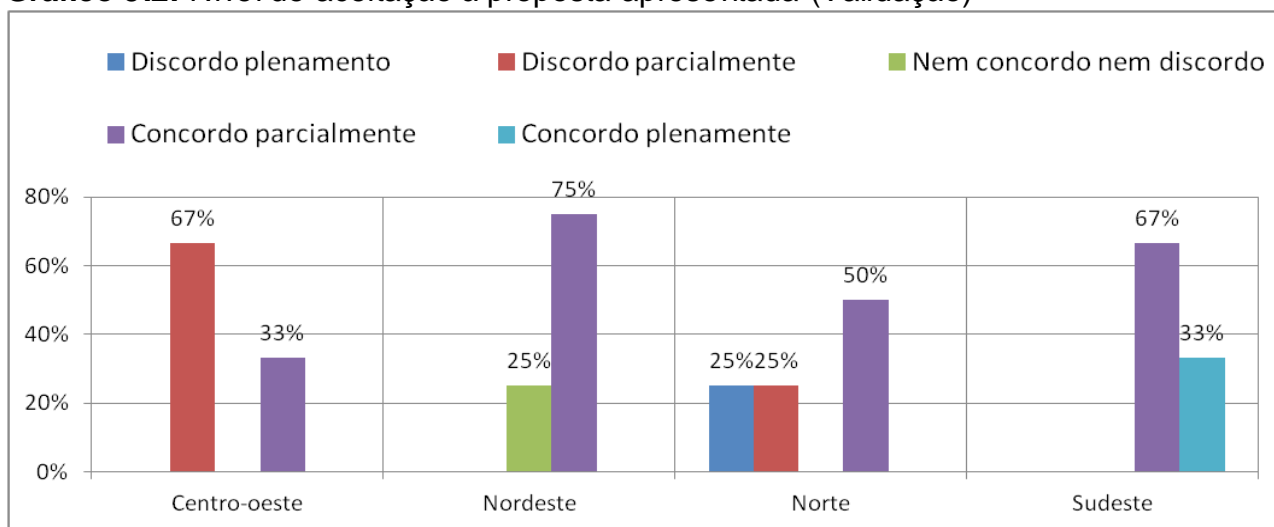
A análise dos dados obtidos, que pode ser visualizada no Gráfico 5.2, mostra que na região Centro-oeste, 67% discordaram parcialmente, contra 33% que concordaram parcialmente com a proposta apresentada.

Na região Nordeste, 75% disseram concordar parcialmente e 25% permaneceram neutro, preferindo não opinar.

Na região Norte, 50% concordaram parcialmente, 25% discordaram parcialmente e outros 25% discordaram plenamente com a proposta apresentada.

Na região Sudeste, 67% concordaram parcialmente e 33% afirmaram concordar plenamente com a proposta do correio eletrônico alternativo para a Rede Federal.

**Gráfico 5.2:** Nível de aceitação à proposta apresentada (Validação)



Fonte: Elaborado pelo autor (2017)

#### Q04 – Sugestões apresentadas

Nesta questão é perguntado se o respondente gostaria de fazer alguma sugestão ou observação como forma de complementar a resposta apresentada na questão anterior, e, por padrão, é selecionado a opção Não, mas também é disponibilizado o campo Outro para que o mesmo possa descrever o que deseja sugerir.

A análise das sugestões apresentadas pode ser visualizada no Gráfico 5.3, e mostrou que na região Centro-oeste, 67% dos respondentes (2) apresentaram no campo Outro as observações de que além do repasse de aporte financeiro, seria necessário definir uma equipe para manter a solução, e também o questionamento de onde viria a



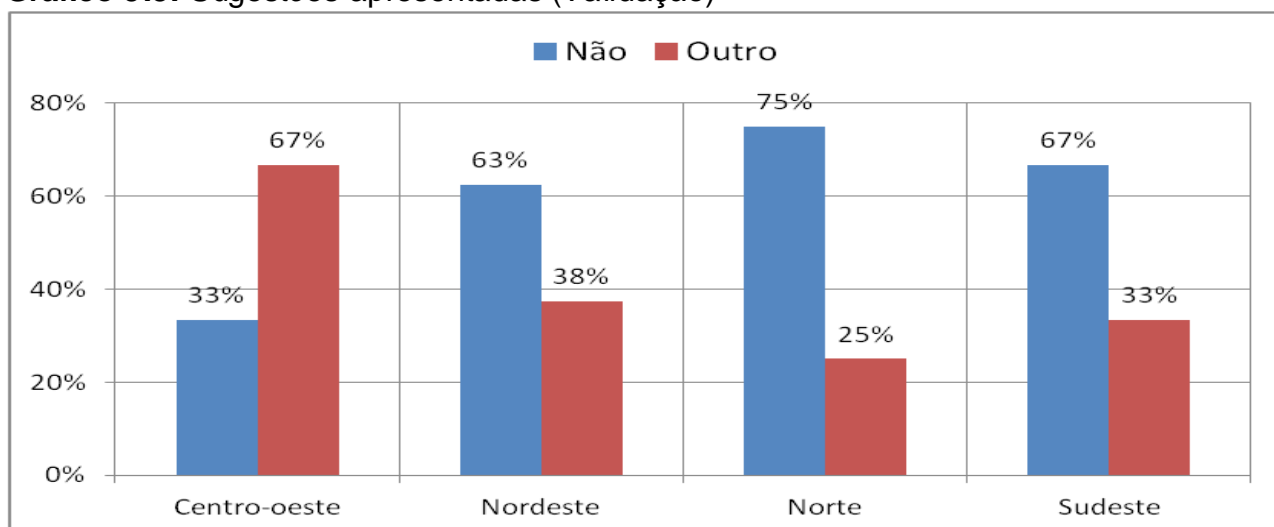
equipe que manteria em funcionamento a solução, uma vez que todos os IF já possuem um quadro reduzido.

Em outra avaliação foi questionado sobre a inviabilidade da Rede Federal sediar o e-mail de todas as instituições da Rede Federal de Educação, em virtude dos cortes financeiros existentes. As demais instituições, 33% (1), selecionaram a opção Não, preferindo não opinar.

Na região Nordeste, 63% (5) dos respondentes, selecionaram a opção Não e não opinaram e as demais instituições dessa região que representam 33% (3) apresentaram as seguintes observações: A primeira instituição não concorda com repasse de recursos, pois isso poderia afetar a aderência ao serviço. Uma segunda instituição alerta sobre a possibilidade de haver a replicação local do banco de dados das mensagens, para propiciar melhor disponibilidade do serviço, no caso de falha na instituição que hospeda o serviço; e outra instituição questiona quem manteria a infraestrutura do *datacenter* onde funcionaria o correio eletrônico da Rede Federal.

Na região Norte, 75% (3) dos respondentes preferiram não opinar, selecionando a opção Não. No entanto, houve o questionamento por parte de 33% (1) dos respondentes, sobre como seria feito o repasse financeiro entre as instituições que compõem a rede para manter o funcionamento da estrutura de correio eletrônico.

Na região Sudeste, 67% (2) dos respondentes, escolheram a opção de não opinar e 33% (1), apesar de na questão anterior ter concordado plenamente com a solução apresentada, disseram não acreditar que essa seja a melhor alternativa, por acreditar que o investimento feito em qualquer infraestrutura de TI que fique sob responsabilidade da Rede Federal, tende a ser uma solução ruim, e ainda sugere que seja feito investimento em serviços de nuvem já consolidados e flexibilizar o decreto à realidade das instituições que compõem a Rede Federal de Educação.

**Gráfico 5.3:** Sugestões apresentadas (Validação)

**Fonte:** Elaborado pelo autor (2017)

Com relação às sugestões/recomendações apresentadas na região Centro-oeste, com relação a definição da equipe para manter a solução em funcionamento, cabe salientar que a solução para esses impedimentos surgirão através de outros estudos que deverão ser feitos entre as instituições da Rede Federal, conforme sugerido no item 5.2 como Sugestões para trabalhos futuros.

Na região Nordeste, uma ouve questionamento sobre a possibilidade de haver a replicação local do banco de dados das mensagens, e sobre quem sediará a infraestrutura do *datacenter* onde funcionaria o correio eletrônico da Rede Federal. Esses questionamentos já foram previstos na proposta inicial do correio eletrônico alternativo, que foi apresentado no item 4.1.6 Alternativa ao correio eletrônico do decreto, quando falou-se da escolha de duas instituições que sediarão a solução, e da necessidade de redundância entre elas, como forma de garantir a segurança das informações.

Desta forma, após analisar os dados apresentados na avaliação, foi possível identificar um nível aceitação à proposta do correio eletrônico alternativo pela grande maioria das instituições.

## REFERÊNCIAS

---

BRASIL. Araújo, A. S. Ministério do Planejamento, Orçamento e Gestão. **Forum RNP 2015 - Mobilidade**: Brasília: RNP, 2015a. Disponível em: <[https://2015.forum.rnp.br/sites/forum2015/files/1\\_-\\_auditoria\\_de\\_programas\\_e\\_equipamentos\\_de\\_tic\\_anderson.pdf](https://2015.forum.rnp.br/sites/forum2015/files/1_-_auditoria_de_programas_e_equipamentos_de_tic_anderson.pdf)>. Acesso em: 29 nov. 2016.

BRASIL. Congresso. Senado Federal. Comissão Parlamentar de Inquérito. **CPI da Espionagem - Relatório Final**. Brasília, DF, 2014b. Disponível em: <<https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>>. Acesso em: 20 dez. 2016.

BRASIL. **Conjunto de Características, Critérios, Condições Mínimas e Medidas para Auditoria de Segurança da Informação em Programas e Equipamentos - Versão 1.3**, Agosto de 2015e. Disponível em: <<http://www.governoeletronico.gov.br/eixos-de-atuacao/governo/interoperabilidade/auditoria-em-programas-e-equipamentos>>. Acesso em: 8 out. 2016.

BRASIL. **Cronograma para Implantação dos Critérios; e Modelo de Governança e Gestão de Auditoria de Segurança da Informação em Programas e Equipamentos - Versão 1.2**, Agosto de 2015d. Disponível em: <<http://www.governoeletronico.gov.br/eixos-de-atuacao/governo/interoperabilidade/auditoria-em-programas-e-equipamentos>>. Acesso em: 7 out. 2016.

BRASIL. Decreto no 8.638, de 15, de janeiro de 2016. **Institui a Política de Governança Digital no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional**. Diário Oficial da República Federativa do Brasil, Poder Executivo, Brasília, DF, 18 jan. 2016f. Seção 1. p.2.

BRASIL. DSIC – Departamento de Segurança de Informação e Comunicação: **Missão do DSIC**. 2009. Disponível em: <<http://dsic.planalto.gov.br/missao-do-dsic>>. Acesso em: 13 dez. 2016.

BRASIL. Ministério da Ciência, Tecnologia, Inovação e Comunicações. **Ata da 7ª Reunião da Comissão de Coordenação do SISP/2016**. Brasília, DF, 19 jul. 2016g. Disponível em: <[http://sisp.gov.br/ccsisp/wiki/download/file/ata\\_CCSISP\\_jul%2f2016](http://sisp.gov.br/ccsisp/wiki/download/file/ata_CCSISP_jul%2f2016)>. Acesso em: 27 mar. 2016.

BRASIL. Ministério da Educação. **LEI 11.892** de 29 de dezembro de 2008. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2007-2010/2008/lei/l11892.htm](http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11892.htm)>. Acesso em: 21 set. 2016.

BRASIL. Ministério da Educação. **LEI 12.677** de 25 de junho de 2012. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/L12677.htm](http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/L12677.htm)>. Acesso em: 21 set. 2016.

BRASIL. Ministério da Educação. **NOTA TÉCNICA 50/2016** de 06 de maio de 2016b. Disponível em: <<http://portal.mec.gov.br/component/content/article?id=32151>>. Acesso em: 21 set. 2016.

BRASIL. Ministério do Planejamento, Orçamento e Gestão. **Estratégia de Governança Digital da Administração Pública Federal 2016-19 (EGD)** / Ministério do Planejamento, Orçamento e Gestão, Secretaria de Tecnologia da Informação. -- Brasília: MP, 2016e. Disponível em: <<http://planejamento.gov.br/EGD>>. Acesso em: 07 nov. 2016.

BRASIL. **Modelo de Governança e Gestão de Auditoria de Segurança da Informação em Programas e Equipamentos - Versão 1.2**, Agosto de 2015f. Disponível em: <<http://www.governoeletronico.gov.br/eixos-de-atuacao/governo/interoperabilidade/auditoria-em-programas-e-equipamentos>>. Acesso em: 7 out. 2016.

BRASIL. **Portal RedeFederal - Rede Federal de Educação Profissional, Científica e Tecnológica**. 2016a. Disponível em: <<http://redefederal.mec.gov.br/expansao-da-rede-federal>>. Acesso em: 30 jan. 2016.

BRASIL. **Portaria Interministerial MP/MC/MD nº 141**, de 2 de maio de 2014a. Disponível em: <<https://www.legisweb.com.br/legislacao/?id=269793>>. Acesso em: 30 jan. 2016.

BRASIL. **Portaria nº 2**, de 24 de fevereiro de 2015b. Disponível em: <[http://www.lex.com.br/legis\\_26523840\\_PORTARIA\\_N\\_2\\_DE\\_24\\_DE\\_FEVEREIRO\\_DE\\_2015.aspx](http://www.lex.com.br/legis_26523840_PORTARIA_N_2_DE_24_DE_FEVEREIRO_DE_2015.aspx)>. Acesso em: 29 nov. 2016.

BRASIL. Presidência da República. Casa Militar. Departamento de Segurança da Informação e Comunicações. **Guia básico de orientações ao gestor em segurança da informação e comunicações : versão 2.0** / Casa Militar, Departamento de Segurança da Informação e Comunicações; organizadores Danielle Rocha da Costa, José Ney de Oliveira Lima. – Brasília: Presidência da República, 2016c. Disponível em: <<http://dsic.planalto.gov.br/publicacoes-2>>. Acesso em: 03 nov. 2016.

BRASIL. Presidência da República. **Decreto 8.135** de 4 de novembro de 2013. Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_Ato2011-2014/2013/Decreto/D8135.htm](http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D8135.htm)>. Acesso em: 01 dez. 2014.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro verde: segurança cibernética no Brasil**, organização Claudia Canongia e Raphael Mandarin Junior. Brasília, DF, GSIPR/SE/DSIC, 2010a. Disponível em: <<http://dsic.planalto.gov.br/publicacoes-2>>. Acesso em: 02 nov. 2016.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018: versão 1.0** / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. – Brasília: Presidência da República, 2015c. Disponível em: <<http://dsic.planalto.gov.br/publicacoes-2>>. Acesso em: 04 nov. 2016.

BRASIL. Secretário de Tecnologia da Informação do Ministério do Planejamento. **Portaria nº 46, de 28 de setembro de 2016d. Dispõe sobre a disponibilização de Software Público Brasileiro e dá outras providências.** Disponível em: <[https://Softwarepublico.gov.br/social/articles/0004/5932/PORTARIA\\_N\\_\\_46\\_\\_DE\\_28\\_D\\_E\\_SETEMBRO\\_DE\\_2016.pdf](https://Softwarepublico.gov.br/social/articles/0004/5932/PORTARIA_N__46__DE_28_D_E_SETEMBRO_DE_2016.pdf)>. Acesso em: 05 jan. 2016.

APPOLINÁRIO, F.; ATLAS, (Ed.) Dicionário de Metodologia Científica. São Paulo: Atlas, 2007.

COELHO, F. E. S.; ARAÚJO, L. G. S.; BEZERRA, E. K. **Gestão da Segurança da Informação NBR 27001 e NBR 27002.** Rio de Janeiro-RJ, RNP/ESR, 2014.

DESLAURIERS, J. ; KÉRISIT, M. O delineamento de pesquisa qualitativa. In: POUPART, Jean et al. **A pesquisa qualitativa:** Enfoques epistemológicos e metodológicos. Petrópolis, RJ: Vozes, 2008, p. 127-153.

DIAS, T. **Por que o software livre vai perder espaço no governo federal.** 03 nov. 2016. Disponível em: <<https://www.nexojornal.com.br/expresso/2016/11/03/Por-que-o-software-livre-vai-perder-espaco-no-governo-federal>>. Acesso em: 05 jan. 2017.

FONSECA, J. J. S. **Metodologia da pesquisa científica.** Fortaleza: UECE, 2002.

G1. (2014). **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA.** Disponível em: <<http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>>. Acesso em: 17 fev. 2016.

GERMANI, L. **Um passo a frente, um passo atrás.** 10 mar. 2016. Disponível em: <<https://leogermani.com.br/2016/03/10/um-passo-a-frente-um-passo-atras/>>. Acesso em: 05 jan. 2017.

GIL, A. C. **Como Elaborar Projetos de Pesquisa** / Antônio Carlos Gil. – 5. Ed. – São Paulo: Atlas, 2010.

GROSSMANN, L. O. (2013). **“E-mail seguro” em todos os ministérios custará R\$ 300 milhões.** Disponível em: <<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=35394&sid=11#.Uv9ZHvldWzY>>. Acesso em: 15 fev. 2016

GROSSMANN, L. O. (2016). **Governo ainda discute conformidade de e-mail ‘seguro’.** Disponível em:

<<http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infol=42223&sid=18>>. Acesso em: 25 abr. 2016.

**GSTI - Grupo de Servidores de Ti dos Institutos Federais - Planilha da pesquisa sobre ferramentas utilizadas nos IFET do grupo GSTI-IF:**  
<[https://docs.google.com/spreadsheets/d/1kWSNF2gk0e-570HuOAWy9N1fVUwOcRi2rSolf1vNCFM/edit?usp=docslist\\_api](https://docs.google.com/spreadsheets/d/1kWSNF2gk0e-570HuOAWy9N1fVUwOcRi2rSolf1vNCFM/edit?usp=docslist_api)>. Recuperado em 20 mai. 2016.

HARDING, L. **Os arquivos Snowden: a história secreta do homem mais procurado do mundo** / Luke Harding; tradução de Alice Klesck, Bruno Correia. – Rio de Janeiro: LeYa, 2014.

KUHN, D. L. **O Software Livre no Governo Federal, desafios e disputas**. Disponível em: <<https://www.youtube.com/watch?v=n1c7Pin4t64>>. Acesso em: 12 out. 2016.

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Técnicas de Pesquisa: planejamento e execução de pesquisas, amostragens e técnicas de pesquisa, elaboração, análise e interpretação de dados**. – 7. Ed. – 4. Reimp. – São Paulo : Atlas, 2011.

MARTINS, Ana Isabel et al . **Avaliação de Usabilidade: Uma Revisão Sistemática da Literatura**. RISTI, Porto, n. 11, p. 31-43, jun. 2013. Disponível em <[http://www.scielo.mec.pt/scielo.php?script=sci\\_arttext&pid=S1646-98952013000100004&lng=pt&nrm=iso](http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952013000100004&lng=pt&nrm=iso)>. Acesso em 13 mar. 2017.

MINAYO, M. C. de S. **O desafio do conhecimento**. 10. ed. São Paulo: HUCITEC, 2007.

MORAES, Henrique Viana Bandeira. **Aplicabilidade do decreto presidencial nº. 8.135, de 04 de novembro de 2013**. Conteúdo Jurídico, Brasília-DF: 18 mar. 2014. Disponível em: <<http://www.conteudojuridico.com.br/?artigos&ver=2.47468&seo=1>>. Acesso em: 04 out. 2016.

NASCIMENTO, J. E. A política de expansão da Rede Federal de Educação Profissional, Científica e Tecnológica: O papel do IFMA no processo de modernização do noroeste maranhense. In: **Anais do VII CONEPI – Congresso Norte Nordeste de Pesquisa e Inovação**. Tocantins, Palmas, out. 2012.

OLIVEIRA, M. M. et al. **Análise dos fatores de resistência na implantação de sistemas de informação na manufatura de eletrônicos**. Journal of Information Systems and echnology Management, São Paulo, 2009, v.6, n.3, p.507-524, Jan. 2009. Disponível em: <<http://www.redalyc.org/pdf/2032/203219575006.pdf>>. Acesso em: 04 abr. 2016.

PEREIRA, L. A. C. **A Rede Federal de Educação Profissional e o desenvolvimento local**. 2003. Dissertação de Mestrado (Anexo 29).

PINSONNEAULT, A. e KRAEMER, K. L. **Survey research in management information systems: an assesement. Journal of Management Information System**, 1993.

SANTOS, A. R. **Metodologia científica: a construção do conhecimento**. Rio de Janeiro: DP&A, 1999.

SILVA JUNIOR, S.D.; COSTA, F. J. Mensuração e Escalas de Verificação: uma Análise Comparativa das Escalas de Likert e PhraseCompletion. PMKT – Revista Brasileira de Pesquisas de Marketing, Opinião e Mídia, São Paulo, Brasil, v. 15, p. 1-16, out. 2014.

VELOSO, M. A. **Ciberspionagem global e o Decreto 8.135: segurança das informações no governo brasileiro**. Revista Jus Navigandi, Teresina, ano 19, n. 3936, 11 abr. 2014. Disponível em: <<https://jus.com.br/artigos/27383>>. Acesso em: 30 jan. 2016.

## APÊNDICE A – Questionário utilizado na coleta de dados

---

# Um estudo sobre a Aderência das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica ao decreto 8.135/2013

Meu nome é Vicente de Paulo Batista, sou aluno de mestrado em Ciência da Computação pelo Cin/UFPE, sob a orientação do professor Fernando da Fonseca de Souza, PhD.

O governo federal, por meio do decreto nº 8.135 de 04/11/2013, conhecido como o decreto do "e-mail seguro", da presidência da república, e, posteriormente, por meio da portaria ministerial MP/MC/MD nº 141 de 02/05/2014, definiu normas de comunicação para a rede federal, visando obter uma infraestrutura de comunicação e informação confiável e mais segura.

Entre as propostas apresentadas, está a de implantação de um correio eletrônico com características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações e o prazo apresentado para adesão a essas normativas é de 5 anos, portanto, os órgãos terão até 2018 para adesão as orientações do decreto.

Essa pesquisa, parte do meu trabalho de dissertação do Mestrado, visa aferir o nível de conhecimento e adesão das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica, ao decreto 8.135/2013, identificar dados que possam permitir conhecer a estrutura de correio eletrônico existente e os motivos da aderência ou não aderência ao referido decreto.

Para atingir o objetivo dessa pesquisa você só precisará responder na máximo a 10 questões.

Dados de contato:

Aluno: Vicente de Paulo Batista - [vpb@cin.ufpe.br](mailto:vpb@cin.ufpe.br)

Orientador: Prof. Fernando da Fonseca de Souza, PhD - [fdfd@cin.ufpe.br](mailto:fdfd@cin.ufpe.br)

Link para o decreto 8.135/2013: <http://goo.gl/DWAtUe>

Link para a portaria 141/2014: <https://goo.gl/kzLijV>

Conto com a sua colaboração e agradeço antecipadamente.



## Dados da instituição

### 01 - Instituição

Selecione a instituição que você trabalha?

Escolher

### 02 - Quantos campi

Quantos campi possui a sua instituição?

Sua resposta

### 03 - Função na DGTI

Qual a sua função na Diretoria Geral de Tecnologia da Informação da sua instituição?

- ☐ Diretoria Geral de TI
- ☐ Coordenadoria de Redes de Computadores
- ☐ Coordenadoria de Sistemas
- ☐ Departamento de Governança de TI
- ☐ Opção 5
- ☐ Outro: \_\_\_\_\_

### 04 - Conhece o decreto?

Você tem conhecimento do decreto 8.135/2013 e de que é proposto nele a utilização de um correio eletrônico utilizando software livre e auditável?

- ☐ Sim
- ☐ Não

### 05 - Usa e-mail auditável?

A sua instituição usa correio eletrônico, utilizando software livre e auditável, de acordo com os moldes do decreto?

- ☐ Sim
- ☒ Não

VOLTAR

PRÓXIMA

Página 2 de 4

## Correio eletrônico utilizado (software livre e auditável)

Utilize o campo OUTRO para descrever uma alternativa diferente das apresentadas

### 5.1.1 - E-mail livre utilizado

Escolha a ferramenta de correio eletrônico livre utilizada na instituição (Se utilizar mais de uma ferramenta na instituição, preencha um outro formulário para cada ferramenta utilizada)

- ☐ Expresso (Serpro)
- ☐ Zimbra
- ☐ iRedMail
- ☐ Outro:

### 5.1.2 - Recursos POSITIVOS do e-mail livre

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como POSITIVO e/ou acrescente mais algum no campo OUTRO?

- ☐ Nenhum
- ☐ Usabilidade
- ☐ Filtro anti-spam
- ☐ Cota de espaço disponibilizado para o usuário
- ☐ Integração com dispositivos moveis
- ☐ Confiança na entrega e recebimento das mensagens
- ☐ Outro: \_\_\_\_\_

### 5.1.3 - Recursos NEGATIVOS do e-mail livre

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como NEGATIVO e/ou acrescente mais algum no campo OUTRO?

- ☐ Nenhum
- ☐ Usabilidade
- ☐ Filtro anti-spam
- ☐ Cota de espaço disponibilizado para o usuário
- ☐ Integração com dispositivos moveis
- ☐ Confiança na entrega e recebimento das mensagens)
- ☐ Outro: \_\_\_\_\_

### 5.1.4 - Fator determinante para adesão

Fator(es) determinante(s) para adesão à ferramenta

- ☐ Cumprimento do decreto 8.135 (legalidade)
- ☐ Outro: \_\_\_\_\_

## Correio eletrônico utilizado (Proprietário e não auditável)

Utilize o campo OUTRO para descrever uma alternativa diferente das apresentadas

### 5.2.1 - E-mail proprietário utilizado

Escolha a ferramenta de correio eletrônico proprietária utilizada na instituição (Se utilizar mais de uma ferramenta na instituição, preencha um outro formulário para cada ferramenta utilizada)

- ☐ Microsoft Exchange
- ☐ Google mail (Gmail)
- ☐ Outro: \_\_\_\_\_

### 5.2.2 - Recursos POSITIVOS do e-mail proprietário

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como POSITIVOS e/ou acrescente mais algum no campo OUTRO?

- ☐ Nenhum
- ☐ Usabilidade
- ☐ Filtro anti-spam
- ☐ Cota de espaço disponibilizado para o usuário
- ☐ Integração com dispositivos moveis
- ☐ Confiança na entrega e recebimento das mensagens)
- ☐ Outro: \_\_\_\_\_

### 5.2.3 - Recursos NEGATIVOS do e-mail proprietário

Identifique os recursos da ferramenta de correio eletrônico em uso que você considera como NEGATIVO e/ou acrescente mais algum no campo OUTRO?

- ☐ Nenhum
- ☐ Usabilidade
- ☐ Filtro anti-spam
- ☐ Cota de espaço disponibilizado para o usuário
- ☐ Integração com dispositivos moveis
- ☐ Confiança na entrega e recebimento das mensagens)
- ☐ Outro: \_\_\_\_\_

### 5.2.4 - Fatores que impedem a adesão

Tendo em vista que o decreto 8.135 e a portaria 141 estabelecem diretrizes e prazo para adesão ao sistema de correio eletrônico livre e auditável, quais fatores impedem a adesão da sua instituição a essas normativas?

- ☐ Resistência dos usuários em adaptar-se a um novo correio eletrônico
- ☐ Por investimentos já feitos e/ou contratos ainda vigentes
- ☐ Por achar que a proposta do decreto não está bem definida
- ☐ Por usar atualmente uma ferramenta que atende as demandas e não gera custos para a instituição
- ☐ Outro:

### 5.2.5 - Sugestões para adesão

O que você sugere para que haja a adesão ao correio eletrônico utilizando software livre e auditável, nos moldes do decreto 8.135?

- ☐ Que não tenha custos para a instituição
- ☐ Que a responsabilidade pelo gerenciamento da infraestrutura do correio eletrônico não seja desta instituição
- ☐ Outro: \_\_\_\_\_

[VOLTAR](#)[ENVIAR](#) Página 4 de 4

## APÊNDICE B – Questionário utilizado na validação

---

### Validação das recomendações

Meu nome é Vicente de Paulo Batista, sou aluno de mestrado em Ciência da Computação pelo Cin/UFPE, sob a orientação do professor Fernando da Fonseca de Souza, PhD.

Agradeço a sua instituição por ter respondido ao questionário eletrônico visando avaliar a aderência da Rede Federal de Educação ao modelo de correio eletrônico auditável proposto no decreto 8.135/20. A partir da análise das respostas foram propostas recomendações no meu trabalho. Portanto, solicito mais uma vez sua valiosa colaboração para avaliar as referidas recomendações.

#### Alternativa ao correio eletrônico do decreto

Como solução alternativa à utilização de um correio eletrônico institucional, além do Expresso do Serpro, que é sugerido no Decreto 8.135/2013, é apresentada a proposta a seguir:

Que seja realizado um consórcio entre as instituições que compõem a Rede Federal de Educação para implementação de um correio eletrônico de acordo com as exigências do decreto e que possa ser utilizado pela rede.

Serão eleitas duas instituições da Rede Federal de Educação que sediarão o correio eletrônico institucional, utilizando software livre e auditável, conforme exigência do decreto, e que tenham condições de atender aos critérios de melhor infraestrutura de TI, localização geográfica, melhores links de internet, energia elétrica estável, e, equipe de TI capacitada.

O serviço de correio eletrônico funcionará hospedado em uma das instituições eleitas para sediar o equipamento, mas com redundância em outra como forma de garantir o armazenamento das informações de forma descentralizada, além de aumentar a disponibilidade do serviço em caso de falhas.

Como forma de garantia orçamentária para implantação e manutenção da infraestrutura de TI, bem como a capacitação da equipe responsável por manter tal estrutura, será feito um repasse orçamentário das demais instituições da Rede Federal que usufruirão do e-mail institucional, permitindo dessa forma que a ferramenta venha a ter em longo prazo um baixo custo de manutenção.

## 1-Selecione a sua instituição \*

Escolher



## 2-Função na DGTI \*

Função ocupada na Diretoria Geral de TI

- ☐ Diretoria Geral de TI
- ☐ Coordenadoria de Redes de Computadores
- ☐ Coordenadoria de Sistemas
- ☐ Departamento de Governança de TI
- ☐ Analista de TI
- ☐ Tecnólogo em Segurança da Informação
- ☐ Outro: \_\_\_\_\_

## 3-A proposta apresentada serve como alternativa ao correio eletrônico do decreto?

	Discordo plenamente	Discordo parcialmente	Nem concordo nem discordo	Concordo parcialmente	Concordo plenamente
Concorda ou discorda?	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

## 4-Você gostaria de fazer alguma observação/sugestão?

Caso tenha alguma observação/sugestão a fazer, por favor descreva no campo Outro

- ☐ Não
- ☐ Outro: \_\_\_\_\_

## **ANEXO A – Lei nº 11.892/2008 – Lei de instituição dos IFET**

---

**Presidência da República  
Casa Civil  
Subchefia para Assuntos Jurídicos**

LEI Nº 11.892, DE 29 DE DEZEMBRO DE 2008.  
(Vide Decreto nº 7.022, de 2009) .

Institui a Rede Federal de Educação Profissional, Científica e Tecnológica, cria os Institutos Federais de Educação, Ciência e Tecnologia, e dá outras providências.

**O PRESIDENTE DA REPÚBLICA** Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

**CAPÍTULO I**  
**DA REDE FEDERAL DE EDUCAÇÃO PROFISSIONAL, CIENTÍFICA E TECNOLÓGICA**

Art. 1º Fica instituída, no âmbito do sistema federal de ensino, a Rede Federal de Educação Profissional, Científica e Tecnológica, vinculada ao Ministério da Educação e constituída pelas seguintes instituições:

I - Institutos Federais de Educação, Ciência e Tecnologia - Institutos Federais;

II - Universidade Tecnológica Federal do Paraná - UTFPR;

III - Centros Federais de Educação Tecnológica Celso Suckow da Fonseca - CEFET-RJ e de Minas Gerais - CEFET-MG;

~~IV - Escolas Técnicas Vinculadas às Universidades Federais.~~

IV - Escolas Técnicas Vinculadas às Universidades Federais; e (Redação dada pela Lei nº 12.677, de 2012)

V - Colégio Pedro II. (Incluído pela Lei nº 12.677, de 2012)

~~Parágrafo único. As instituições mencionadas nos incisos I, II e III do caput deste artigo possuem natureza jurídica de autarquia, detentoras de autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar.~~

Parágrafo único. As instituições mencionadas nos incisos I, II, III e V do caput possuem natureza jurídica de autarquia, detentoras de autonomia administrativa, patrimonial, financeira, didático-pedagógica e disciplinar. (Redação dada pela Lei nº 12.677, de 2012)

Art. 2º Os Institutos Federais são instituições de educação superior, básica e profissional, pluricurriculares e multicampi, especializados na oferta de educação profissional e

tecnológica nas diferentes modalidades de ensino, com base na conjugação de conhecimentos técnicos e tecnológicos com as suas práticas pedagógicas, nos termos desta Lei.

§ 1º Para efeito da incidência das disposições que regem a regulação, avaliação e supervisão das instituições e dos cursos de educação superior, os Institutos Federais são equiparados às universidades federais.

§ 2º No âmbito de sua atuação, os Institutos Federais exercerão o papel de instituições acreditadoras e certificadoras de competências profissionais.

§ 3º Os Institutos Federais terão autonomia para criar e extinguir cursos, nos limites de sua área de atuação territorial, bem como para registrar diplomas dos cursos por eles oferecidos, mediante autorização do seu Conselho Superior, aplicando-se, no caso da oferta de cursos a distância, a legislação específica.

Art. 3º A UTFPR configura-se como universidade especializada, nos termos do parágrafo único do art. 52 da Lei no 9.394, de 20 de dezembro de 1996, regendo-se pelos princípios, finalidades e objetivos constantes da Lei no 11.184, de 7 de outubro de 2005.

~~Art. 4º As Escolas Técnicas Vinculadas às Universidades Federais são estabelecimentos de ensino pertencentes à estrutura organizacional das universidades federais, dedicando-se, precipuamente, à oferta de formação profissional técnica de nível médio, em suas respectivas áreas de atuação.~~

Art. 4º-A. O Colégio Pedro II é instituição federal de ensino, pluricurricular e multicampi, vinculada ao Ministério da Educação e especializada na oferta de educação básica e de licenciaturas. (Incluído pela Lei nº 12.677, de 2012)

Parágrafo único. O Colégio Pedro II é equiparado aos institutos federais para efeito de incidência das disposições que regem a autonomia e a utilização dos instrumentos de gestão do quadro de pessoal e de ações de regulação, avaliação e supervisão das instituições e dos cursos de educação profissional e superior. (Incluído pela Lei nº 12.677, de 2012)

## CAPÍTULO II DOS INSTITUTOS FEDERAIS DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA

### Seção I Da Criação dos Institutos Federais

Art. 5º Ficam criados os seguintes Institutos Federais de Educação, Ciência e Tecnologia:

I - Instituto Federal do Acre, mediante transformação da Escola Técnica Federal do Acre;



II - Instituto Federal de Alagoas, mediante integração do Centro Federal de Educação Tecnológica de Alagoas e da Escola Agrotécnica Federal de Satuba;

III - Instituto Federal do Amapá, mediante transformação da Escola Técnica Federal do Amapá;

IV - Instituto Federal do Amazonas, mediante integração do Centro Federal de Educação Tecnológica do Amazonas e das Escolas Agrotécnicas Federais de Manaus e de São Gabriel da Cachoeira;

V - Instituto Federal da Bahia, mediante transformação do Centro Federal de Educação Tecnológica da Bahia;

VI - Instituto Federal Baiano, mediante integração das Escolas Agrotécnicas Federais de Catu, de Guanambi (Antonio José Teixeira), de Santa Inês e de Senhor do Bonfim;

VII - Instituto Federal de Brasília, mediante transformação da Escola Técnica Federal de Brasília;

VIII - Instituto Federal do Ceará, mediante integração do Centro Federal de Educação Tecnológica do Ceará e das Escolas Agrotécnicas Federais de Crato e de Iguatu;

IX - Instituto Federal do Espírito Santo, mediante integração do Centro Federal de Educação Tecnológica do Espírito Santo e das Escolas Agrotécnicas Federais de Alegre, de Colatina e de Santa Teresa;

X - Instituto Federal de Goiás, mediante transformação do Centro Federal de Educação Tecnológica de Goiás;

XI - Instituto Federal Goiano, mediante integração dos Centros Federais de Educação Tecnológica de Rio Verde e de Urutaí, e da Escola Agrotécnica Federal de Ceres;

XII - Instituto Federal do Maranhão, mediante integração do Centro Federal de Educação Tecnológica do Maranhão e das Escolas Agrotécnicas Federais de Codó, de São Luís e de São Raimundo das Mangabeiras;

XIII - Instituto Federal de Minas Gerais, mediante integração dos Centros Federais de Educação Tecnológica de Ouro Preto e de Bambuí, e da Escola Agrotécnica Federal de São João Evangelista;

XIV - Instituto Federal do Norte de Minas Gerais, mediante integração do Centro Federal de Educação Tecnológica de Januária e da Escola Agrotécnica Federal de Salinas;

XV - Instituto Federal do Sudeste de Minas Gerais, mediante integração do Centro Federal de Educação Tecnológica de Rio Pomba e da Escola Agrotécnica Federal de Barbacena;

XVI - Instituto Federal do Sul de Minas Gerais, mediante integração das Escolas Agrotécnicas Federais de Inconfidentes, de Machado e de Muzambinho;

XVII - Instituto Federal do Triângulo Mineiro, mediante integração do Centro Federal de Educação Tecnológica de Uberaba e da Escola Agrotécnica Federal de Uberlândia;

XVIII - Instituto Federal de Mato Grosso, mediante integração dos Centros Federais de Educação Tecnológica de Mato Grosso e de Cuiabá, e da Escola Agrotécnica Federal de Cáceres;

XIX - Instituto Federal de Mato Grosso do Sul, mediante integração da Escola Técnica Federal de Mato Grosso do Sul e da Escola Agrotécnica Federal de Nova Andradina;

XX - Instituto Federal do Pará, mediante integração do Centro Federal de Educação Tecnológica do Pará e das Escolas Agrotécnicas Federais de Castanhal e de Marabá;

XXI - Instituto Federal da Paraíba, mediante integração do Centro Federal de Educação Tecnológica da Paraíba e da Escola Agrotécnica Federal de Sousa;

XXII - Instituto Federal de Pernambuco, mediante integração do Centro Federal de Educação Tecnológica de Pernambuco e das Escolas Agrotécnicas Federais de Barreiros, de Belo Jardim e de Vitória de Santo Antão;

XXIII - Instituto Federal do Sertão Pernambucano, mediante transformação do Centro Federal de Educação Tecnológica de Petrolina;

XXIV - Instituto Federal do Piauí, mediante transformação do Centro Federal de Educação Tecnológica do Piauí;

XXV - Instituto Federal do Paraná, mediante transformação da Escola Técnica da Universidade Federal do Paraná;

XXVI - Instituto Federal do Rio de Janeiro, mediante transformação do Centro Federal de Educação Tecnológica de Química de Nilópolis;

XXVII - Instituto Federal Fluminense, mediante transformação do Centro Federal de Educação Tecnológica de Campos;

XXVIII - Instituto Federal do Rio Grande do Norte, mediante transformação do Centro Federal de Educação Tecnológica do Rio Grande do Norte;

XXIX - Instituto Federal do Rio Grande do Sul, mediante integração do Centro Federal de Educação Tecnológica de Bento Gonçalves, da Escola Técnica Federal de Canoas e da Escola Agrotécnica Federal de Sertão;

XXX - Instituto Federal Farroupilha, mediante integração do Centro Federal de Educação Tecnológica de São Vicente do Sul e da Escola Agrotécnica Federal de Alegrete;

XXXI - Instituto Federal Sul-rio-grandense, mediante transformação do Centro Federal de Educação Tecnológica de Pelotas;

XXXII - Instituto Federal de Rondônia, mediante integração da Escola Técnica Federal de Rondônia e da Escola Agrotécnica Federal de Colorado do Oeste;

XXXIII - Instituto Federal de Roraima, mediante transformação do Centro Federal de Educação Tecnológica de Roraima;

XXXIV - Instituto Federal de Santa Catarina, mediante transformação do Centro Federal de Educação Tecnológica de Santa Catarina;

XXXV - Instituto Federal Catarinense, mediante integração das Escolas Agrotécnicas Federais de Concórdia, de Rio do Sul e de Sombrio;

XXXVI - Instituto Federal de São Paulo, mediante transformação do Centro Federal de Educação Tecnológica de São Paulo;

XXXVII - Instituto Federal de Sergipe, mediante integração do Centro Federal de Educação Tecnológica de Sergipe e da Escola Agrotécnica Federal de São Cristóvão; e

XXXVIII - Instituto Federal do Tocantins, mediante integração da Escola Técnica Federal de Palmas e da Escola Agrotécnica Federal de Araguatins.

§ 1º As localidades onde serão constituídas as reitorias dos Institutos Federais constam do Anexo I desta Lei.

§ 2º A unidade de ensino que compõe a estrutura organizacional de instituição transformada ou integrada em Instituto Federal passa de forma automática, independentemente de qualquer formalidade, à condição de campus da nova instituição.

§ 3º A relação de Escolas Técnicas Vinculadas a Universidades Federais que passam a integrar os Institutos Federais consta do Anexo II desta Lei.

§ 4º As Escolas Técnicas Vinculadas às Universidades Federais não mencionadas na composição dos Institutos Federais, conforme relação constante do Anexo III desta Lei, poderão, mediante aprovação do Conselho Superior de sua respectiva universidade federal, propor ao Ministério da Educação a adesão ao Instituto Federal que esteja constituído na mesma base territorial.

§ 5º A relação dos campi que integrarão cada um dos Institutos Federais criados nos termos desta Lei será estabelecida em ato do Ministro de Estado da Educação.

§ 6º Os Institutos Federais poderão conceder bolsas de pesquisa, desenvolvimento, inovação e intercâmbio a alunos, docentes e pesquisadores externos ou de empresas, a

serem regulamentadas por órgão técnico competente do Ministério da Educação. (Incluído pela Lei nº 12.863, de 2013)

## Seção II

### Das Finalidades e Características dos Institutos Federais

Art. 6º Os Institutos Federais têm por finalidades e características:

I - ofertar educação profissional e tecnológica, em todos os seus níveis e modalidades, formando e qualificando cidadãos com vistas na atuação profissional nos diversos setores da economia, com ênfase no desenvolvimento socioeconômico local, regional e nacional;

II - desenvolver a educação profissional e tecnológica como processo educativo e investigativo de geração e adaptação de soluções técnicas e tecnológicas às demandas sociais e peculiaridades regionais;

III - promover a integração e a verticalização da educação básica à educação profissional e educação superior, otimizando a infra-estrutura física, os quadros de pessoal e os recursos de gestão;

IV - orientar sua oferta formativa em benefício da consolidação e fortalecimento dos arranjos produtivos, sociais e culturais locais, identificados com base no mapeamento das potencialidades de desenvolvimento socioeconômico e cultural no âmbito de atuação do Instituto Federal;

V - constituir-se em centro de excelência na oferta do ensino de ciências, em geral, e de ciências aplicadas, em particular, estimulando o desenvolvimento de espírito crítico, voltado à investigação empírica;

VI - qualificar-se como centro de referência no apoio à oferta do ensino de ciências nas instituições públicas de ensino, oferecendo capacitação técnica e atualização pedagógica aos docentes das redes públicas de ensino;

VII - desenvolver programas de extensão e de divulgação científica e tecnológica;

VIII - realizar e estimular a pesquisa aplicada, a produção cultural, o empreendedorismo, o cooperativismo e o desenvolvimento científico e tecnológico;

IX - promover a produção, o desenvolvimento e a transferência de tecnologias sociais, notadamente as voltadas à preservação do meio ambiente.

## Seção III

### Dos Objetivos dos Institutos Federais

Art. 7º Observadas as finalidades e características definidas no art. 6º desta Lei, são objetivos dos Institutos Federais:

I - ministrar educação profissional técnica de nível médio, prioritariamente na forma de cursos integrados, para os concluintes do ensino fundamental e para o público da educação de jovens e adultos;

II - ministrar cursos de formação inicial e continuada de trabalhadores, objetivando a capacitação, o aperfeiçoamento, a especialização e a atualização de profissionais, em todos os níveis de escolaridade, nas áreas da educação profissional e tecnológica;

III - realizar pesquisas aplicadas, estimulando o desenvolvimento de soluções técnicas e tecnológicas, estendendo seus benefícios à comunidade;

IV - desenvolver atividades de extensão de acordo com os princípios e finalidades da educação profissional e tecnológica, em articulação com o mundo do trabalho e os segmentos sociais, e com ênfase na produção, desenvolvimento e difusão de conhecimentos científicos e tecnológicos;

V - estimular e apoiar processos educativos que levem à geração de trabalho e renda e à emancipação do cidadão na perspectiva do desenvolvimento socioeconômico local e regional; e

VI - ministrar em nível de educação superior:

a) cursos superiores de tecnologia visando à formação de profissionais para os diferentes setores da economia;

b) cursos de licenciatura, bem como programas especiais de formação pedagógica, com vistas na formação de professores para a educação básica, sobretudo nas áreas de ciências e matemática, e para a educação profissional;

c) cursos de bacharelado e engenharia, visando à formação de profissionais para os diferentes setores da economia e áreas do conhecimento;

d) cursos de pós-graduação lato sensu de aperfeiçoamento e especialização, visando à formação de especialistas nas diferentes áreas do conhecimento; e

e) cursos de pós-graduação stricto sensu de mestrado e doutorado, que contribuam para promover o estabelecimento de bases sólidas em educação, ciência e tecnologia, com vistas no processo de geração e inovação tecnológica.

Art. 8º No desenvolvimento da sua ação acadêmica, o Instituto Federal, em cada exercício, deverá garantir o mínimo de 50% (cinquenta por cento) de suas vagas para atender aos objetivos definidos no inciso I do caput do art. 7º desta Lei, e o mínimo de 20% (vinte por cento) de suas vagas para atender ao previsto na alínea b do inciso VI do caput do citado art. 7º.

§ 1º O cumprimento dos percentuais referidos no caput deverá observar o conceito de aluno-equivalente, conforme regulamentação a ser expedida pelo Ministério da Educação.

§ 2º Nas regiões em que as demandas sociais pela formação em nível superior justificarem, o Conselho Superior do Instituto Federal poderá, com anuência do Ministério da Educação, autorizar o ajuste da oferta desse nível de ensino, sem prejuízo do índice definido no caput deste artigo, para atender aos objetivos definidos no inciso I do caput do art. 7º desta Lei.

#### Seção IV

#### Da Estrutura Organizacional dos Institutos Federais

Art. 9º Cada Instituto Federal é organizado em estrutura multicampi, com proposta orçamentária anual identificada para cada campus e a reitoria, exceto no que diz respeito a pessoal, encargos sociais e benefícios aos servidores.

Art. 10. A administração dos Institutos Federais terá como órgãos superiores o Colégio de Dirigentes e o Conselho Superior.

§ 1º As presidências do Colégio de Dirigentes e do Conselho Superior serão exercidas pelo Reitor do Instituto Federal.

§ 2º O Colégio de Dirigentes, de caráter consultivo, será composto pelo Reitor, pelos Pró-Reitores e pelo Diretor-Geral de cada um dos campi que integram o Instituto Federal.

§ 3º O Conselho Superior, de caráter consultivo e deliberativo, será composto por representantes dos docentes, dos estudantes, dos servidores técnico-administrativos, dos egressos da instituição, da sociedade civil, do Ministério da Educação e do Colégio de Dirigentes do Instituto Federal, assegurando-se a representação paritária dos segmentos que compõem a comunidade acadêmica.

§ 4º O estatuto do Instituto Federal disporá sobre a estruturação, as competências e as normas de funcionamento do Colégio de Dirigentes e do Conselho Superior.

Art. 11. Os Institutos Federais terão como órgão executivo a reitoria, composta por 1 (um) Reitor e 5 (cinco) Pró-Reitores. (Regulamento)

~~§ 1º Poderão ser nomeados Pró-Reitores os servidores ocupantes de cargo efetivo da carreira docente ou de cargo efetivo de nível superior da carreira dos técnico-administrativos do Plano de Carreira dos Cargos Técnico-Administrativos em Educação, desde que possuam o mínimo de 5 (cinco) anos de efetivo exercício em instituição federal de educação profissional e tecnológica.~~

§ 1º Poderão ser nomeados Pró-Reitores os servidores ocupantes de cargo efetivo da Carreira docente ou de cargo efetivo com nível superior da Carreira dos técnico-administrativos do Plano de Carreira dos Cargos Técnico-Administrativos em Educação,

desde que possuam o mínimo de 5 (cinco) anos de efetivo exercício em instituição federal de educação profissional e tecnológica. (Redação dada pela Lei nº 12.772, de 2012)

§ 2º A reitoria, como órgão de administração central, poderá ser instalada em espaço físico distinto de qualquer dos campi que integram o Instituto Federal, desde que previsto em seu estatuto e aprovado pelo Ministério da Educação.

Art. 12. Os Reitores serão nomeados pelo Presidente da República, para mandato de 4 (quatro) anos, permitida uma recondução, após processo de consulta à comunidade escolar do respectivo Instituto Federal, atribuindo-se o peso de 1/3 (um terço) para a manifestação do corpo docente, de 1/3 (um terço) para a manifestação dos servidores técnico-administrativos e de 1/3 (um terço) para a manifestação do corpo discente. (Regulamento)

§ 1º Poderão candidatar-se ao cargo de Reitor os docentes pertencentes ao Quadro de Pessoal Ativo Permanente de qualquer dos campi que integram o Instituto Federal, desde que possuam o mínimo de 5 (cinco) anos de efetivo exercício em instituição federal de educação profissional e tecnológica e que atendam a, pelo menos, um dos seguintes requisitos:

I - possuir o título de doutor; ou

II - estar posicionado nas Classes DIV ou DV da Carreira do Magistério do Ensino Básico, Técnico e Tecnológico, ou na Classe de Professor Associado da Carreira do Magistério Superior.

§ 2º O mandato de Reitor extingue-se pelo decurso do prazo ou, antes desse prazo, pela aposentadoria, voluntária ou compulsória, pela renúncia e pela destituição ou vacância do cargo.

§ 3º Os Pró-Reitores são nomeados pelo Reitor do Instituto Federal, nos termos da legislação aplicável à nomeação de cargos de direção.

Art. 13. Os campi serão dirigidos por Diretores-Gerais, nomeados pelo Reitor para mandato de 4 (quatro) anos, permitida uma recondução, após processo de consulta à comunidade do respectivo campus, atribuindo-se o peso de 1/3 (um terço) para a manifestação do corpo docente, de 1/3 (um terço) para a manifestação dos servidores técnico-administrativos e de 1/3 (um terço) para a manifestação do corpo discente. (Regulamento)

§ 1º Poderão candidatar-se ao cargo de Diretor-Geral do campus os servidores ocupantes de cargo efetivo da carreira docente ou de cargo efetivo de nível superior da carreira dos técnico-administrativos do Plano de Carreira dos Cargos Técnico-Administrativos em Educação, desde que possuam o mínimo de 5 (cinco) anos de efetivo exercício em instituição federal de educação profissional e tecnológica e que se enquadrem em pelo menos uma das seguintes situações:

I - preencher os requisitos exigidos para a candidatura ao cargo de Reitor do Instituto Federal;

II - possuir o mínimo de 2 (dois) anos de exercício em cargo ou função de gestão na instituição; ou

III - ter concluído, com aproveitamento, curso de formação para o exercício de cargo ou função de gestão em instituições da administração pública.

§ 2º O Ministério da Educação expedirá normas complementares dispondo sobre o reconhecimento, a validação e a oferta regular dos cursos de que trata o inciso III do § 1º deste artigo.

#### CAPÍTULO II-A (Incluído pela Lei nº 12.677, de 2012) DO COLÉGIO PEDRO II

Art. 13-A. O Colégio Pedro II terá a mesma estrutura e organização dos Institutos Federais de Educação, Ciência e Tecnologia. (Incluído pela Lei nº 12.677, de 2012)

Art. 13-B. As unidades escolares que atualmente compõem a estrutura organizacional do Colégio Pedro II passam de forma automática, independentemente de qualquer formalidade, à condição de campi da instituição. (Incluído pela Lei nº 12.677, de 2012)

Parágrafo único. A criação de novos campi fica condicionada à expedição de autorização específica do Ministério da Educação. (Incluído pela Lei nº 12.677, de 2012)

#### CAPÍTULO III DISPOSIÇÕES GERAIS E TRANSITÓRIAS

Art. 14. O Diretor-Geral de instituição transformada ou integrada em Instituto Federal nomeado para o cargo de Reitor da nova instituição exercerá esse cargo até o final de seu mandato em curso e em caráter pro tempore, com a incumbência de promover, no prazo máximo de 180 (cento e oitenta) dias, a elaboração e encaminhamento ao Ministério da Educação da proposta de estatuto e de plano de desenvolvimento institucional do Instituto Federal, assegurada a participação da comunidade acadêmica na construção dos referidos instrumentos.

§ 1º Os Diretores-Gerais das instituições transformadas em campus de Instituto Federal exercerão, até o final de seu mandato e em caráter pro tempore, o cargo de Diretor-Geral do respectivo campus.

§ 2º Nos campi em processo de implantação, os cargos de Diretor-Geral serão providos em caráter pro tempore, por nomeação do Reitor do Instituto Federal, até que seja possível identificar candidatos que atendam aos requisitos previstos no § 1º do art. 13 desta Lei.



§ 3º O Diretor-Geral nomeado para o cargo de Reitor Pro-Tempore do Instituto Federal, ou de Diretor-Geral Pro-Tempore do Campus, não poderá candidatar-se a um novo mandato, desde que já se encontre no exercício do segundo mandato, em observância ao limite máximo de investidura permitida, que são de 2 (dois) mandatos consecutivos.

Art. 15. A criação de novas instituições federais de educação profissional e tecnológica, bem como a expansão das instituições já existentes, levará em conta o modelo de Instituto Federal, observando ainda os parâmetros e as normas definidas pelo Ministério da Educação.

Art. 16. Ficam redistribuídos para os Institutos Federais criados nos termos desta Lei todos os cargos e funções, ocupados e vagos, pertencentes aos quadros de pessoal das respectivas instituições que os integram.

§ 1º Todos os servidores e funcionários serão mantidos em sua lotação atual, exceto aqueles que forem designados pela administração superior de cada Instituto Federal para integrar o quadro de pessoal da Reitoria.

§ 2º A mudança de lotação de servidores entre diferentes campi de um mesmo Instituto Federal deverá observar o instituto da remoção, nos termos do art. 36 da Lei no 8.112, de 11 de dezembro de 1990.

Art. 17. O patrimônio de cada um dos novos Institutos Federais será constituído:

I - pelos bens e direitos que compõem o patrimônio de cada uma das instituições que o integram, os quais ficam automaticamente transferidos, sem reservas ou condições, ao novo ente;

II - pelos bens e direitos que vier a adquirir;

III - pelas doações ou legados que receber; e

IV - por incorporações que resultem de serviços por ele realizado.

Parágrafo único. Os bens e direitos do Instituto Federal serão utilizados ou aplicados, exclusivamente, para a consecução de seus objetivos, não podendo ser alienados a não ser nos casos e condições permitidos em lei.

Art. 18. Os Centros Federais de Educação Tecnológica Celso Suckow da Fonseca CEFET-RJ e de Minas Gerais - CEFET-MG, não inseridos no reordenamento de que trata o art. 5º desta Lei, permanecem como entidades autárquicas vinculadas ao Ministério da Educação, configurando-se como instituições de ensino superior pluricurriculares, especializadas na oferta de educação tecnológica nos diferentes níveis e modalidades de ensino, caracterizando-se pela atuação prioritária na área tecnológica, na forma da legislação.

Art. 19. Os arts. 1o, 2o, 4o e 5o da Lei no 11.740, de 16 de julho de 2008, passam a vigorar com as seguintes alterações:

“Art. 1º Ficam criados, no âmbito do Ministério da Educação, para redistribuição a instituições federais de educação profissional e tecnológica:  
.....” (NR)

“Art. 2º Ficam criados, no âmbito do Ministério da Educação, para alocação a instituições federais de educação profissional e tecnológica, os seguintes cargos em comissão e as seguintes funções gratificadas:

I - 38 (trinta e oito) cargos de direção - CD-1;  
.....

IV - 508 (quinhentos e oito) cargos de direção - CD-4;  
.....

VI - 2.139 (duas mil, cento e trinta e nove) Funções Gratificadas - FG-2.  
.....” (NR)

“Art. 4º Ficam criados, no âmbito do Ministério da Educação, para redistribuição a instituições federais de ensino superior, nos termos de ato do Ministro de Estado da Educação, os seguintes cargos:  
.....” (NR)

“Art. 5º Ficam criados, no âmbito do Ministério da Educação, para alocação a instituições federais de ensino superior, nos termos de ato do Ministro de Estado da Educação, os seguintes Cargos de Direção - CD e Funções Gratificadas - FG:  
.....” (NR)

Art. 20. Esta Lei entra em vigor na data de sua publicação.

Brasília, 29 de dezembro de 2008; 187o da Independência e 120o da República.

LUIZ INÁCIO LULA DA SILVA  
Fernando Haddad  
Paulo Bernardo Silva

Este texto não substitui o publicado no DOU de 30.12.2008

## ANEXO I

Localidades onde serão constituídas as Reitorias dos novos Institutos Federais

<b>Instituição</b>	<b>Sede da Reitoria</b>
Instituto Federal do Acre	Rio Branco
Instituto Federal de Alagoas	Maceió
Instituto Federal do Amapá	Macapá
Instituto Federal do Amazonas	Manaus
Instituto Federal da Bahia	Salvador
Instituto Federal Baiano	Salvador
Instituto Federal de Brasília	Brasília
Instituto Federal do Ceará	Fortaleza
Instituto Federal do Espírito Santo	Vitória
Instituto Federal de Goiás	Goiânia
Instituto Federal Goiano	Goiânia
Instituto Federal do Maranhão	São Luís
Instituto Federal de Minas Gerais	Belo Horizonte
Instituto Federal do Norte de Minas Gerais	Montes Claros
Instituto Federal do Sudeste de Minas Gerais	Juiz de Fora
Instituto Federal do Sul de Minas Gerais	Pouso Alegre
Instituto Federal do Triângulo Mineiro	Uberaba
Instituto Federal de Mato Grosso	Cuiabá
Instituto Federal de Mato Grosso do Sul	Campo Grande
Instituto Federal do Pará	Belém
Instituto Federal da Paraíba	João Pessoa
Instituto Federal de Pernambuco	Recife
Instituto Federal do Sertão Pernambucano	Petrolina
Instituto Federal do Piauí	Teresina
Instituto Federal do Paraná	Curitiba
Instituto Federal do Rio de Janeiro	Rio de Janeiro
Instituto Federal Fluminense	Campos dos Goytacazes
Instituto Federal do Rio Grande do Norte	Natal
Instituto Federal do Rio Grande do Sul	Bento Gonçalves
Instituto Federal Farroupilha	Santa Maria
Instituto Federal Sul-rio-grandense	Pelotas
Instituto Federal de Rondônia	Porto Velho
Instituto Federal de Roraima	Boa Vista
Instituto Federal de Santa Catarina	Florianópolis
Instituto Federal Catarinense	Blumenau
Instituto Federal de São Paulo	São Paulo
Instituto Federal de Sergipe	Aracaju
Instituto Federal do Tocantins	Palmas

ANEXO II  
Escolas Técnicas Vinculadas que passam a integrar os Institutos Federais

Escola Técnica Vinculada	Instituto Federal
Colégio Técnico Universitário – UFJF	Instituto Federal do Sudeste de Minas Gerais
Colégio Agrícola Nilo Peçanha – UFF	Instituto Federal do Rio de Janeiro
Colégio Técnico Agrícola Ildefonso Bastos Borges - UFF	Instituto Federal Fluminense
Escola Técnica – UFPR	Instituto Federal do Paraná
Escola Técnica – UFRGS	Instituto Federal do Rio Grande do Sul
Colégio Técnico Industrial Prof. Mário Alquati – FURG	Instituto Federal do Rio Grande do Sul
Colégio Agrícola de Camboriú – UFSC	Instituto Federal Catarinense
Colégio Agrícola Senador Carlos Gomes – UFSC	Instituto Federal Catarinense

ANEXO III  
Escolas Técnicas Vinculadas às Universidades Federais

Escola Técnica Vinculada	Universidade Federal
Escola Agrotécnica da Universidade Federal de Roraima - UFRR	Universidade Federal de Roraima
Colégio Universitário da UFMA	Universidade Federal do Maranhão
Escola Técnica de Artes da UFAL	Universidade Federal de Alagoas

## **ANEXO B – Decreto nº 8.135/2013**

---

Presidência da República  
Casa Civil  
Subchefia para Assuntos Jurídicos

DECRETO Nº 8.135, DE 4 DE NOVEMBRO DE 2013

### **Vigência**

Dispõe sobre as comunicações de dados da administração pública federal direta, autárquica e fundacional, e sobre a dispensa de licitação nas contratações que possam comprometer a segurança nacional.

A PRESIDENTA DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, caput, inciso IV, da Constituição, e tendo em vista o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, ouvido o Conselho de Defesa Nacional,

### **DECRETA:**

Art. 1º As comunicações de dados da administração pública federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias. (Vigência)

§ 1º O disposto no caput não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.

§ 2º Os órgãos e entidades da União a que se refere o caput deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da administração pública federal.

§ 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão ter características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma da regulamentação de que trata o § 5º.

§ 4º O armazenamento e a recuperação de dados a que se refere o caput deverá ser realizada em centro de processamento de dados fornecido por órgãos e entidades da administração pública federal.

§ 5º Ato conjunto dos Ministros de Estado da Defesa, do Planejamento, Orçamento e Gestão e das Comunicações disciplinará o disposto neste artigo e estabelecerá procedimentos, abrangência e prazos de implementação, considerando:

I - as peculiaridades das comunicações dos órgãos e entidades da administração pública federal; e

II - a capacidade dos órgãos e entidades da administração pública federal de ofertar satisfatoriamente as redes e os serviços a que se refere o caput.

Art. 2º Com vistas à preservação da segurança nacional, fica dispensada a licitação para a contratação de órgãos ou entidades da administração pública federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, para atendimento ao disposto no art. 1º.

§ 1º Enquadra-se no caput a implementação e a operação de redes de telecomunicações e de serviços de tecnologia da informação, em especial à garantia da inviolabilidade das comunicações de dados da administração pública federal direta e indireta.

§ 2º Os fornecimentos referidos no § 1º para a administração pública federal consistirão em:

I - rede de telecomunicações - provimento de serviços de telecomunicações, de tecnologia da informação, de valor adicionado e de infraestrutura para redes de comunicação de dados; e

II - serviços de tecnologia da informação - provimento de serviços de desenvolvimento, implantação, manutenção, armazenamento e recuperação de dados e operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico, necessários à gestão da segurança da informação e das comunicações.

§ 3º A dispensa de licitação será justificada quanto ao preço pelo órgão ou entidade competente pela contratação.

Art. 3º Este Decreto entra em vigor:

I - na data de sua publicação, em relação ao art. 2º; e

II - em cento e vinte dias após a data de sua publicação, em relação ao art. 1º.

Brasília, 4 de novembro de 2013; 192º da Independência e 125º da República.

DILMA ROUSSEFF  
Celso Luiz Nunes Amorim  
Miriam Belchior  
Paulo Bernardo Silva

Este texto não substitui o publicado no DOU de 5.11.2013

## **ANEXO C – Portaria 141/2014**

---

### **Portaria Interministerial MP/MC/MD Nº 141 DE 02/05/2014 Publicado no DO em 5 mai 2014**

Dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria.

Os Ministros de Estado do Planejamento, Orçamento e Gestão, das Comunicações e da Defesa, no uso das atribuições que lhes confere o art. 87, parágrafo único, inciso II, da Constituição Federal, e tendo em vista o disposto no art. 1º, § 5º, do Decreto nº 8.135, de 4 de novembro de 2013,

Resolvem:

#### **CAPÍTULO I DAS DISPOSIÇÕES GERAIS**

Art. 1º As comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria.

§ 1º O disposto no caput não se aplica às comunicações realizadas através de serviço móvel pessoal e serviço telefônico fixo comutado.

§ 2º Os órgãos e entidades da União a que se refere o caput deverão adotar os serviços de correio eletrônico e suas funcionalidades complementares oferecidos por órgãos e entidades da Administração Pública Federal.

§ 3º Os programas e equipamentos destinados às atividades de que trata o caput deverão possuir características que permitam auditoria para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações, na forma definida nesta Portaria.

§ 4º O armazenamento e a recuperação de dados a que se refere o caput serão realizados em centro de processamento de dados fornecido por órgãos e entidades da Administração Pública Federal.

Art. 2º Para o disposto nesta Portaria, consideram-se as seguintes definições:

I - armazenamento de dados: serviço de depósito e arquivamento de informações em formato digital que utiliza componentes de computadores ou mídias de gravação capazes de manter os dados por um intervalo de tempo;

II - auditoria: processos e procedimentos sistemáticos de levantamento de evidências que tem como objetivo verificar se os serviços de redes de telecomunicações e de tecnologia da informação atendem aos requisitos especificados previamente em termo de referência ou projeto básico para fins de garantia da disponibilidade, integridade, confidencialidade, autenticidade das informações;

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

IV - centro de processamento de dados: ambiente que concentra e gerencia recursos computacionais para armazenamento e tratamento sistemático de dados;

V - comunicação de dados: é a transmissão, emissão ou recepção de dados ou informações de qualquer natureza por meios confinados, radiofrequência ou qualquer outro processo eletrônico ou eletromagnético ou ótico;

VI - comunicação de dados militares operacionais: comunicação de dados realizada em proveito de operações militares, executadas no âmbito do Sistema Militar de Comando e Controle - (SISMC<sup>2</sup>), conforme disciplinado pelo Ministério da Defesa para o preparo e o emprego das Forças Armadas, em especial os sistemas de controle de tráfego aéreo, de controle de tráfego marítimo, de defesa aeroespacial, de monitoramento de fronteiras e de proteção de infraestruturas críticas;

VII - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;

VIII - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;

IX - fornecedor privado: pessoa jurídica de direito privado que presta serviços de rede de telecomunicações ou de tecnologia da informação e que não integra a Administração Pública Federal direta ou indireta;

X - órgão ou entidade fornecedor: órgão ou entidade da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, que forneça serviços de redes de telecomunicações e de tecnologia da informação para órgãos ou entidades contratantes;

XI - órgão ou entidade contratante: órgão ou entidade da Administração Pública Federal, que contrate serviços de redes de telecomunicações e de tecnologia da informação;



XII - órgão gerenciador: órgão responsável pelo estabelecimento, por meio de regulamentação específica, das regras, condições, parâmetros, preços e modelos de instrumentos de contratação que serão obrigatórios para os órgãos e entidades contratantes;

XIII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XIV - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XV - recuperação de dados: processo de restauração, em sistemas computacionais, de dados digitais perdidos, excluídos, corrompidos ou inacessíveis por qualquer motivo;

XVI - rede própria: conjunto de meios físicos, sistemas de telecomunicações e equipamentos de transmissão de dados, cuja posse, gestão, administração e responsabilidade pela operação sejam exclusivas do próprio órgão ou entidade da Administração Pública Federal;

XVII - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XVIII - serviços de redes de telecomunicações: provimento de serviços de telecomunicações, de tecnologia da informação, de valor adicionado e de infraestrutura para redes de comunicação de dados;

XIX - serviços de tecnologia da informação: provimento de serviços de desenvolvimento, implantação, manutenção, armazenamento e recuperação de dados e operação de sistemas de informação, projeto de infraestrutura de redes de comunicação de dados, modelagem de processos e assessoramento técnico, necessários à gestão da segurança da informação e comunicações;

XX - serviços de tecnologia da informação militares operacionais: recursos de Tecnologia da Informação e Comunicações que integram o SISMC2 proporcionando ferramentas por intermédio das quais as informações são coletadas, monitoradas, armazenadas, processadas, fundidas, disseminadas, apresentadas e protegidas;

XXI - serviços de tecnologia da informação próprios: conjunto de serviços de tecnologia da informação prestados por meio de plataformas desenvolvidas pelo próprio órgão ou entidade, cuja posse, gestão, administração e responsabilidade pela operação sejam exclusivas do próprio órgão ou entidade da Administração Pública Federal;

XXII - software livre: software cujo modelo de licença livre atende a liberdade para executar o programa, estudar como o programa funciona e adaptá-lo para as suas necessidades, redistribuir cópias do programa e aperfeiçoar o programa e liberar os seus aperfeiçoamentos sem restrição;

XXIII - software público brasileiro: software que adota um modelo de licença livre para o código-fonte, a proteção da identidade original entre o seu nome, marca, código-fonte, documentação e outros artefatos relacionados por meio do modelo de Licença Pública de Marca - LPM e é disponibilizado na Internet em ambiente virtual público, sendo tratado como um benefício para a sociedade, o mercado e o cidadão;

XXIV - Sistema Militar de Comando e Controle (SISMC<sup>2</sup>): conjunto de instalações, equipamentos, sistemas de informação, comunicações, doutrinas, procedimentos e pessoal essenciais para o comando e controle, visando atender ao preparo e ao emprego das Forças Armadas; e

XXV - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação e comunicações.

Art. 3º As comunicações de dados da Administração Pública Federal direta, autárquica e fundacional serão estruturadas e efetuadas em conformidade com as seguintes diretrizes:

I - criação, desenvolvimento e manutenção de ações de segurança da informação e comunicações;

II - planejamento, articulação e gestão integrada das políticas de segurança da informação e comunicações;

III - redução de pontos de vulnerabilidade por meio da padronização, integração e interoperabilidade das redes de telecomunicações e dos serviços de tecnologia da informação contratados; e

IV - implementação de ações e procedimentos que assegurem a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, incluindo a adoção de programas e equipamentos que possam ser auditados.

## CAPÍTULO II DO ÓRGÃO GERENCIADOR

Art. 4º O Ministério do Planejamento, Orçamento e Gestão será o órgão gerenciador em relação à contratação dos serviços previstos nesta Portaria, competindo-lhe:

I - regulamentar as contratações previstas nesta Portaria, estabelecendo:

a) prioridades de contratação, a partir da análise do plano de disponibilidade de prestação de serviços apresentado pelo órgão ou entidade fornecedor;

b) especificação técnica e níveis dos serviços padronizados a serem contratados pelos órgãos e entidades;

- c) as unidades de medida que permitam a quantificação das tarefas e dos serviços que serão contratados;
- d) regras, condições, parâmetros e preços para a execução dos serviços;
- e) modelos de instrumentos de contratação;
- f) descrição dos padrões de interoperabilidade;
- g) sanções a serem previstas em modelos de instrumentos de contratação;
- h) formas de implementação e monitoramento das atividades dos órgãos ou entidades fornecedores;
- i) indicadores de desempenho das contratações; e
- j) processos padronizados de contratação.

II - consolidar informações relativas às solicitações dos órgãos ou entidades para verificação do atendimento da regulamentação específica do serviço; e

III - revisar periodicamente os preços estabelecidos, a partir da avaliação da composição de preços dos serviços encaminhada pelo órgão ou entidade fornecedor.

### CAPÍTULO III

### DO PROCEDIMENTO DE CONTRATAÇÃO DOS SERVIÇOS

#### Seção I

#### Dos Procedimentos Gerais

Art. 5º Para atendimento ao disposto no art. 1º, a contratação de serviços de redes de telecomunicações e de tecnologia da informação prestados por órgãos ou entidades fornecedores deverá ser efetuada por dispensa de licitação.

§ 1º A contratação dos serviços de que trata o caput será efetuada em conformidade com as normas e os procedimentos estabelecidos pelo órgão gerenciador, observada as disposições relativas à segurança da informação e comunicações fixadas pelo Gabinete de Segurança Institucional da Presidência da República.

§ 2º Quando o órgão ou entidade contratante necessitar de serviços com parâmetros não previstos em regulamentação específica estabelecida pelo órgão gerenciador, a dispensa poderá ser feita a partir de critérios e especificações próprias.

§ 3º Nas hipóteses dos §§ 1º e 2º, até o término da fase de planejamento da contratação, o órgão ou entidade contratante deverá consultar a regulamentação do órgão

gerenciador ou os órgãos ou entidades fornecedores que prestem serviços compatíveis com o objeto da contratação sobre a disponibilidade para atendimento das especificações técnicas e níveis de serviço do objeto do contrato, conforme o caso.

Art. 6º A contratação de órgãos e entidades fornecedores a que se refere o caput do art. 5º não será obrigatória para:

I - os casos em que não houver oferta da prestação de serviços por órgãos ou entidades fornecedores, observado o disposto no art. 7º;

II - as comunicações de dados militares operacionais e os sistemas de tecnologia da informação militares operacionais, bem como às comunicações de caráter administrativo, assim entendidas como aquelas realizadas para execução da administração do Ministério da Defesa e órgãos subordinados, que trafegarem pelos mesmos canais das comunicações de dados militares operacionais, até a adequação de suas infraestruturas, de acordo com o planejamento a ser fixado por ato do Ministro de Estado da Defesa;

III - as comunicações de dados efetuadas por meio de redes próprias e serviços de tecnologia da informação próprios;

IV - a prestação de serviços de redes de telecomunicações fora do território nacional; e

V - os serviços objetos da presente regulamentação prestados pela Rede Nacional de Ensino e Pesquisa (RNP), desde que compatíveis com o contrato de gestão da instituição.

Parágrafo único. No prazo estabelecido pelo órgão gerenciador, as contratações previstas nos incisos I, III e V deverão observar o disposto nos Capítulos IV e V desta Portaria.

## Seção II

### Da Contratação com Fornecedores Privados

Art. 7º Nos casos em que não houver oferta da prestação de serviços por órgãos ou entidades fornecedores, é permitida a contratação de serviços de redes de telecomunicações ou de tecnologia da informação junto a fornecedores privados.

§ 1º Para fins desta Portaria, o serviço será considerado não ofertado quando o órgão ou entidade fornecedor:

I - não atender à localidade da prestação do serviço;

II - não atender aos requisitos técnicos relativos à infraestrutura ou aos serviços, conforme demandado pelo órgão ou entidade contratante, observada a regulamentação estabelecida pelo órgão gerenciador, quando houver;

III - não responder a consulta formal sobre o atendimento dos serviços no prazo de trinta dias; e

IV - não puder enquadrar a demanda do órgão ou entidade contratante nas prioridades de contratação de que trata o art. 4º, inciso I, alínea "a".

§ 2º A contratação com fornecedores privados será precedida de licitação, excetuadas as hipóteses de dispensa ou de inexigibilidade previstas na legislação.

§ 3º A não oferta de que trata o § 1º deverá ser demonstrada no processo de contratação mediante a juntada de documentos que atestem a realização da consulta referida no § 3º do art. 5º e o enquadramento em uma das hipóteses do § 1º.

§ 4º Nos casos em que o atendimento aos serviços for apenas parcial, o órgão ou entidade contratante deverá motivar a não contratação do órgão ou entidade fornecedor, mediante justificativa de que a cisão do objeto da contratação:

I - é inviável do ponto de vista técnico ou jurídico; ou

II - é desvantajosa tecnicamente para o órgão ou entidade contratante.

§ 5º O prazo referido no inciso III do § 1º poderá ser prorrogado, a critério do órgão ou entidade contratante, mediante justificativa.

## CAPÍTULO IV DOS REQUISITOS DE IMPLEMENTAÇÃO DOS SERVIÇOS

### Seção I

#### Dos Requisitos Comuns

Art. 8º Os serviços de redes de telecomunicações e de tecnologia da informação prestados por fornecedores privados ou por órgãos e entidades fornecedores devem adotar os padrões definidos, em capítulo específico, da arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico.

Art. 9º O termo de referência ou projeto básico e o contrato, observadas as especificidades técnicas de cada órgão ou entidade contratante e a regulamentação estabelecida pelo órgão gerenciador, quando houver, deverão conter obrigações de:

I - comprovação da disponibilidade, integridade, confidencialidade e autenticidade das informações trafegadas por meio de programas ou equipamentos para comunicação de dados;

II - apresentação da política de segurança de dados e o detalhamento das ações de segurança da informação e comunicações a serem implementadas nos serviços contratados;

III - fornecimento à Administração, ou a terceiro por ela indicado, de informações de monitoramento e acesso a instrumentos e procedimentos de prevenção e reação a incidentes de segurança;

IV - atendimento às normas e padrões de segurança estabelecidos pela Administração para acesso e uso das instalações e equipamentos;

V - manutenção de confidencialidade das informações e documentos aos quais venha a ter acesso em decorrência da prestação dos serviços contratados, sendo esta obrigação extensiva a seus sócios, diretores, mandatários, assim como todos os empregados envolvidos na contratação, não dispensando a assinatura de termo específico;

VI - comunicação à Administração da ocorrência de incidentes de segurança e a existência de vulnerabilidades relativas ao objeto da contratação, em periodicidade definida, em capítulo específico, da arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico, assim como tomar as ações imediatas de contenção;

VII - fornecimento de informações gerenciais sobre o desempenho dos serviços objeto do contrato, de maneira agregada e individualizada;

VIII - possibilidade de realização de auditoria em programas e equipamentos por órgão ou entidade contratante ou por instituição credenciada pelo Governo Federal; e

IX - aplicação de sanções em caso de incidente de segurança, intencionalmente ou por omissão.

## Seção II

### Dos Requisitos Específicos

Art. 10. Sem prejuízo do disposto nos arts. 8º e 9º, os serviços de redes de telecomunicações deverão atender aos seguintes requisitos mínimos:

I - utilização de ferramenta de monitoramento do tráfego; e

II - utilização de ferramentas de prevenção à intrusão no acesso do serviço de Internet.

Art. 11. Para fins desta Portaria, serviços de tecnologia da informação abrangem os serviços de:

I - correio eletrônico;

II - compartilhamento e sincronização de arquivos;

III - mensageria instantânea;

IV - conferência (teleconferência, telepresença e webconferência); e

V - comunicação de voz sobre protocolo de internet (VoIP).

Art. 12. Sem prejuízo dos requisitos previstos nos arts. 8º e 9º, os serviços de tecnologia da informação de que trata esta Portaria devem adotar os seguintes critérios mínimos de segurança da informação e comunicações:

I - uso de criptografia para informações sigilosas; e

II - uso de ferramenta de controle de acesso e de gerenciamento de identidades.

§ 1º Além dos critérios previstos no caput, para o fornecimento de serviços de correio eletrônico e mensageria instantânea devem ser exigidas as seguintes condições mínimas:

I - utilização de ferramenta de prevenção do envio de mensagens em massa; e

II - utilização de ferramenta de detecção de códigos maliciosos.

§ 2º Para o fornecimento de serviços de compartilhamento e sincronização de arquivos, além dos requisitos previstos no caput, será exigida no mínimo a utilização de ferramenta de detecção de códigos maliciosos.

## CAPÍTULO V DA AUDITORIA DE PROGRAMAS E EQUIPAMENTOS

Art. 13. Os programas e equipamentos destinados às atividades de que trata o art. 1º deverão ter características que permitam auditoria, pelo órgão ou entidade contratante ou por instituição credenciada pelo Governo Federal, para fins de garantia da disponibilidade, integridade, confidencialidade e autenticidade das informações.

Art. 14. O termo de referência ou projeto básico e o respectivo contrato celebrado com fornecedor privado ou com órgão ou entidade fornecedor deverá prever, entre outras disposições:

I - a possibilidade de realização de auditoria em programas e equipamentos; e

II - o detalhamento dos critérios e condições mínimas de segurança, bem como das respectivas obrigações a serem exigidas dos fornecedores, observado o disposto nos arts. 8º a 12 desta Portaria.

§ 1º Para fins do disposto no inciso I do caput, o órgão ou entidade contratante exigirá a adesão às diretrizes e especificações técnicas estabelecidas, em capítulo específico, da arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico.

§ 2º As diretrizes e especificações técnicas da e-PING referidas no § 1º deverão exigir, no mínimo, a possibilidade de abertura do código fonte no caso de programas para

comunicação de dados e de firmware e sistemas operacionais no caso de equipamentos para comunicação de dados.

§ 3º Para efeito dessa Portaria, são considerados auditáveis os software livres ou públicos brasileiros.

## CAPÍTULO VI DA GESTÃO E DO ACOMPANHAMENTO

Art. 15. A gestão e o acompanhamento do disposto nesta Portaria serão realizados pelo Ministério do Planejamento, Orçamento e Gestão, com o objetivo de:

I - monitorar as contratações dos serviços de redes de telecomunicações e de tecnologia da informação pelos órgãos e entidades contratantes;

II - solicitar aos órgãos e entidades fornecedores informações relativas à oferta dos serviços de que trata esta Portaria, inclusive quanto à ampliação da capacidade disponível e à observância dos prazos de atendimento, conforme previsto nas disposições finais desta Portaria;

III - em conjunto com o respectivo Ministério supervisor dos órgãos e entidades fornecedores, estabelecer diretrizes e definir prioridades a serem contempladas nos respectivos planos de expansão de oferta; e

IV - acompanhar as diretrizes e especificações técnicas estabelecidas pela arquitetura e-PING;

Parágrafo único. Para fins de auxiliar o desempenho das atividades previstas no caput, poderão ser convidados representantes de outros órgãos ou entidades, públicas ou privadas.

## CAPÍTULO VII DAS DISPOSIÇÕES FINAIS

Art. 16. As diretrizes definidas no § 1º do art. 14º serão estabelecidas no prazo máximo de sessenta dias a partir da publicação desta Portaria.

Art. 17. As novas implementações de serviços de redes de telecomunicações e de tecnologia da informação de que trata o art. 1º devem seguir as determinações desta Portaria.

§ 1º Não se aplica o disposto no caput para licitações em andamento, desde que já tenham sido publicados os respectivos editais.

§ 2º Na hipótese do § 1º, o contrato de prestação de serviço poderá ser prorrogado pelo prazo máximo de doze meses.



Art. 18. A migração dos serviços de redes de telecomunicações e de tecnologia da informação em operação ou ativos deve ocorrer no prazo máximo de sessenta meses a partir da vigência desta Portaria.

Parágrafo único. Havendo oferta dos serviços nos termos do § 1º do art. 5º, o contrato de prestação de serviço poderá ser prorrogado pelo prazo máximo de doze meses, respeitado o disposto no art. 57 da Lei nº 8.666, de 21 de junho de 1993.

Art. 19. O prazo máximo para oferta dos serviços a serem executados pelos órgãos ou entidades fornecedoras será:

I - para os serviços de tecnologia da informação, de vinte e quatro meses; e

II - para os serviços de redes de telecomunicações:

a) de vinte e quatro meses nas capitais e regiões metropolitanas; e

b) de sessenta meses nas demais localidades.

Art. 20. Aplicam-se subsidiariamente às contratações de que trata esta norma o disposto nas instruções normativas que disciplinam as contratações de serviços continuados ou não e as contratações de Soluções de Tecnologia da Informação pelos órgãos e entidades integrantes do Sistema de Serviços Gerais (SISG) e do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal.

Art. 21. Esta Portaria entra em vigor na data de sua publicação.

MIRIAM BELCHIOR

Ministra de Estado do Planejamento, Orçamento e Gestão

PAULO BERNARDO SILVA

Ministro de Estado das Comunicações

CELSO LUIZ NUNES AMORIM

Ministro de Estado da Defesa