



**Centro Universitário de Brasília
Instituto CEUB de Pesquisa e Desenvolvimento - ICPD**

LEANDRO LIMA RAINERI

**ANÁLISE DE ADEQUAÇÃO DA POLÍTICA DE SEGURANÇA DA
INFORMAÇÃO DOS MINISTÉRIOS FEDERAIS FRENTE AS NORMAS
DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E
COMUNICAÇÕES.**

Brasília
2016

LEANDRO LIMA RAINERI

**ANÁLISE DE ADEQUAÇÃO DA POLÍTICA DE SEGURANÇA DA
INFORMAÇÃO DOS MINISTÉRIOS FEDERAIS FRENTE AS NORMAS
DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E
COMUNICAÇÕES.**

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* em Governança em Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra

Brasília
2016

LEANDRO LIMA RAINERI

**ANÁLISE DE ADEQUAÇÃO DA POLÍTICA DE SEGURANÇA DA
INFORMAÇÃO DOS MINISTÉRIOS FEDERAIS FRENTE AS NORMAS
DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO E
COMUNICAÇÕES.**

Trabalho apresentado ao Centro
Universitário de Brasília (UniCEUB/ICPD)
como pré-requisito para a obtenção de
Certificado de Conclusão de Curso de Pós-
graduação *Lato Sensu* em Governança em
Tecnologia da Informação.

Orientador: Prof. Dr. Maurício Lyra

Brasília, ____ de _____ de 2016.

Banca Examinadora

Prof. Dr. Paulo R. Foina

Prof. Dr. Gilson Ciarallo

Dedico este singelo trabalho:

A meus pais, Paulo Raineri e Clélia M. da S. Lima Raineri, que sempre me apoiaram e me deram todo suporte para evoluir na caminhada acadêmica;

A minha companheira Ana Paula B. Carvalho, por estar sempre a meu lado em todos os momentos, aproveitando as alegrias e compartilhando as tristezas; e

A meu filho, Eduardo Papa Raineri, muito amado, cuja amizade, carinho e presença me incentivam a querer ser um homem melhor no futuro.

O preço da liberdade é a eterna vigilância.
John Philpot Curran (1750-1817)

RESUMO

O avanço da tecnologia da informação nesta última década aliado com o crescimento vertiginoso dos sistemas informatizados integrados por meio de redes é um fato determinante para a evolução do conhecimento. No entanto, esta nova sociedade digital fica sujeita a várias ameaças que comprometem seriamente a segurança do simples usuário até mesmo as grandes organizações. A tecnologia da informação pode auxiliar e, até mesmo, mitigar grande parte destas ameaças, porém não é capaz de resolvê-la na sua íntegra. Os sistemas de tecnologia da informação necessitam de uma política de segurança da informação e comunicação aliada e que contemple, de forma equilibrada, não somente aspectos tecnológicos, mas aspectos humanos e principalmente comportamentais a fim de mitigar possíveis ameaças e vulnerabilidades às organizações. Pensado nisso o Departamento de Segurança da Informação e Comunicações, ligado à Presidência da República, positivou algumas normas específicas que regulamentam a segurança da informação para a Administração Pública Federal. Assim sendo, este trabalho teve por finalidade apresentar uma análise qualitativa do grau de maturidade de cada Ministério Federal em relação às vinte e uma Instruções Normativas positivadas pelo Departamento de Segurança da Informação e Comunicações. Para tanto, procedeu-se a uma coleta de artigos e trabalhos na área de segurança da informação assim como das políticas de segurança da informação e comunicação de todos os vinte e quatro Ministérios Federais. Os resultados obtidos sugeriram, de forma geral, uma heterogeneidade no nível de maturidade das políticas de segurança da informação e comunicação destes órgãos analisados.

Palavras-chave: Segurança da Informação. Política de Segurança da Informação. Departamento de Segurança da Informação e Comunicações. Instrução Normativa.

ABSTRACT

The advancement of information technology in this last decade associate with the rapid growth of integrated computer systems through networks is a key factor in the evolution of knowledge. However, this new digital society is subject to various threats that seriously compromise the security of the simple user even large organizations. Information technology can assist and even largely mitigate these threats, but is not able to solve it in its entirety. The information technology systems require a security policy of information and communication together and including a balanced way, not only technological aspects but mainly human and behavioral aspects in order to mitigate potential threats and vulnerabilities for organizations. Having saying that, the Security Department of Information and Communications, attached to the Republic Presidency, made some specific rules governing information security for the Federal Public Administration. This paper aims to provide a qualitative analysis of the degree of maturity of each Federal Ministry over the twenty-one Normative Instructions made by the Security Department of Information and Communications. Therefore, we proceeded to a collection of articles and papers in the information security area as well as security policy of information and communication of all twenty-four Federal Ministry. The results suggest a general heterogeneity in the level of maturity of security policies of information and communication of these organs analyzed.

Key words: Information Security. Information Security Policy. Security Department of Information and Communication.

LISTA DE ABREVIATURAS E SIGRAS

APF	Administração Pública Federal.
CDN	Conselho de Defesa Nacional.
CGGSIC	Coordenação Geral de Gestão da Segurança da Informação e Comunicações.
CGSIC	Comitê Gestor da Segurança da Informação.
DSIC	Departamento de Segurança da Informação e Comunicações.
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
GRSICC	Gestão de Riscos de Segurança da Informação e Comunicações
GSI	Gabinete de Segurança Institucional.
MC	Ministério das Comunicações
MCTI	Ministério da Ciência, Tecnologia e Inovação
MD	Ministério da Defesa
MDA	Ministério do Desenvolvimento Agrário
MDIC	Ministério do Desenvolvimento, Indústria e Comercio Exterior
MDS	Ministério do Desenvolvimento Social e Combate a Fome
ME	Ministério dos Esportes
MEC	Ministério da Educação
MF	Ministério da Fazenda
MI	Ministério da Integração Social
MinC	Ministério da Cultura
MJ	Ministério da Justiça
MMA	Ministério do Meio Ambiente
MME	Ministério das Minas e Energia
MP	Ministério do Planejamento
MPA	Ministério da Pesca e Agricultura
MPS	Ministério da Previdência Social
MRE	Ministério da Relações Exteriores
MS	Ministério da Saúde
MT	Ministério dos Transportes
MTE	Ministério do Trabalho e Emprego
MTUR	Ministério do Turismo

NC	Norma Complementar
PCN	Plano de Continuidade de Negócios
POSIC	Política de Segurança da Informação e Comunicações.
PR	Presidência da República.
SGSI	Sistema de Gestão de Segurança da Informação.

SUMÁRIO

INTRODUÇÃO	9
1 SEGURANÇA DA INFORMAÇÃO	12
1.1 Definição	12
1.2 Princípios	12
1.2.1 Autenticidade.....	13
1.2.2 Confidencialidade	13
1.2.3 Disponibilidade	13
1.2.4 Integridade	14
1.2.4 Legalidade.....	14
1.3 Violação de Segurança da Informação	15
2 POLITICA DE SEGURANÇA DA INFORMAÇÃO	17
2.2 Tipos de Políticas	18
2.2.1 Regulatória	19
2.2.2 Consultiva.....	19
2.2.3 Informativa.....	19
3 ÓRGÃOS QUE REGULAMENTAM A SEGURANÇA DE TI PARA A APF	21
3.1 Gabinete de Segurança Institucional	21
3.2 Departamento de Segurança da Informação e Comunicações	22
3.3 Coordenação Geral de Gestão da Segurança da Informação e Comunicações	22
3.4 Organograma	23
3.5 Conselho de Defesa Nacional	24
3.6 Comitê Gestor de Segurança da Informação	25
3.7 Agência Brasileira de Inteligência	25
4 LEGISLAÇÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	26
4.1 Instrução Normativa	26
4.2 Normas Complementares	27
5 ANÁLISE DAS POSICS	30
5.1 Norma Complementar 01/IN01	31
5.2 Norma Complementar 02/IN01	32
5.3 Norma Complementar 03/IN01	33
5.4 Norma Complementar 04/IN01	34
5.5 Norma Complementar 05/IN01	35
5.6 Norma Complementar 06/IN01	36
5.7 Norma Complementar 07/IN01	37
5.8 Norma Complementar 08/IN01	38

5.9 Norma Complementar 09/IN01	39
5.10 Norma Complementar 10/IN01	40
5.11 Norma Complementar 11/IN01	41
5.12 Norma Complementar 12/IN01	42
5.13 Norma Complementar 13/IN01	43
5.14 Norma Complementar 14/IN01	44
5.15 Norma Complementar 15/IN01	45
5.16 Norma Complementar 16/IN01	46
5.17 Norma Complementar 17/IN01	47
5.18 Norma Complementar 18/IN01	48
5.19 Norma Complementar 19/IN01	49
5.20 Norma Complementar 20/IN01	50
5.21 Norma Complementar 21/IN01	51
5.22 Consolidado das Análises das POSICs	52
6 ANÁLISE DOS RESULTADOS	53
6.1 Agrupamento Visando as NCs Relacionadas	53
6.1.1 Normatização da POSIC	53
6.1.2 Normas Relacionadas ao Plano de Continuidade de Negócios	54
6.1.3 Normas Relacionadas a ETIR	55
6.1.4 Normas Relacionadas a Profissionais de SIC	55
6.2 Agrupamento Visando a Afinidade dos Ministérios	56
6.2.1 Ministérios Ligados a Meios de Produção Agrícola.....	56
6.2.2 Ministérios Ligados a Educação.....	57
6.2.4 Ministérios Ligados a Tecnologia	58
6.2.4 Ministérios Ligados ao Trabalho.....	59
6.3 Análise Levando em Conta as Datas de Publicação	59
6.4 Notas dos Ministérios	62
CONCLUSÃO	65
REFERÊNCIAS	67

INTRODUÇÃO

A evolução do conhecimento sofreu um grande avanço nos últimos dez anos, através do crescimento dos sistemas integrados informatizados de redes. Em contrapartida, a vulnerabilidade tem sido uma preocupação em relação à segurança da informação, pois o maior prejudicado é o usuário, o que não o isenta de culpa, devido à falta de conscientização de recusa ao acesso, que pode comprometer a segurança da rede na instituição.

A tecnologia da informação, oferece recursos que amenizam esta situação, isto se dá por meio de Política de Segurança da Informação e Comunicação (POSIC) a ser implantada pelas organizações, juntamente com uma divulgação explicativa dos riscos aos seus interessados.

Sabendo disso o Governo Federal, via Gabinete de Segurança Institucional da Presidência da República (GSI/PR) através do Departamento de Segurança da Informação e Comunicações (DSIC), publicou Instruções Normativas e Normas Complementares que orientam e regulamentam assuntos ligados a segurança da informação e comunicação a serem implementadas nos órgãos da Administração Pública Federal (APF).

A fim de pôr em prática estas instruções, buscou-se na elaboração desse trabalho, apresentar um estudo visando mensurar o nível de adequação das Políticas de Segurança da Informação e Comunicação às Normas Complementares publicadas pelo DSIC. As políticas de segurança da informação foram obtidas através da Lei de Acesso à Informação (LAI) submetida a todos os Ministérios Federais. Após análise, observou-se o balanço geral da realidade destas instituições, ao ponto de mensurar o grau de adequação da POSIC - elaborada por cada Ministério – em relação as normas estabelecidas pelo DSIC.

Os objetivos do presente trabalho são: avaliar o grau de aderência dos Ministérios Federais em relação a legislação publicada pelo DSIC; verificar quais itens da POSIC de cada Ministério correspondem as normas complementares do DSIC, e; apresentar uma análise das POSIC dos Ministérios mostrando o resultado com o grau de aderência destes documentos analisados em relação a legislação vigente.

Para alcançar esses objetivos, primeiro foi necessário utilizar a Lei de Acesso a Informação (LAI) para coletar as vinte e quatro (24) POSICs dos Ministérios Federais. Depois, elaboramos uma escala para medir o grau de adequação das POSICs em relação às normas positivadas pelo DISC, estudamos cada POSIC com a finalidade de entender seu grau de aderência às normas e, por fim, apresentamos os resultados desta comparação utilizando a escala elaborada.

A relevância deste trabalho está na apresentação de um insight da situação atual dos vinte e quatro Ministérios que fazem parte da Administração Pública Federal em relação à legislação que rege a segurança da informação e comunicações, coletar as POSICs e confrontá-las com as Normas Complementares elaboradas e publicadas pelo DSIC visando prover um estudo qualitativo do grau de maturidade dos órgãos elencados com a legislação vigente.

O presente trabalho foi então estruturado em oito capítulos. Inicia-se o trabalho pela Introdução, onde se faz referência ao tema, definição, objetivos gerais e específicos, a metodologia utilizada e por fim uma breve explicação da estrutura do trabalho.

O primeiro capítulo traz os conceitos relacionados à segurança da informação, tais como os princípios, atributos, vulnerabilidades, assim como normas e padrões relacionados ao tema.

O capítulo seguinte aborda aspectos de uma POSIC, apresentando informações sobre a estruturação de uma POSIC, suas topologias e requisitos necessários.

O quarto capítulo versa sobre as organizações que definem as normas de segurança da informação para a APF, sua construção e cronograma.

O próximo capítulo aborda a legislação positivada que regulamenta a segurança da informação para a APF, suas estruturas e hierarquia.

No sexto capítulo analisam-se as POSICs dos vinte e quatro ministérios federais, onde se apresenta uma matriz com o grau de aderência das POSICs referentes às NCs.

O capítulo seguinte discorre sobre a análise dos dados de forma gráfica apresentando diferentes visões sobre os dados colhidos na pesquisa.

Na última seção são apresentadas as conclusões do trabalho.

1 SEGURANÇA DA INFORMAÇÃO

1.1 Definição

Atualmente a informação é arma estratégica em qualquer empresa e também é um recurso de vital importância nas organizações. A segurança da informação tem por finalidade resguardar qualquer tipo de informação ou ativo de acessos indevidos.

A ISSO/IEC 27002 (2013) A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e conseqüentemente necessita ser adequadamente protegida. [...]

Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Sêmola (2003, p. 34) define segurança da informação como sendo “uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade”.

Segundo Fontes (2006, p. 19), Segurança da Informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e sua missão seja alcançada.

Para Beal (2005, p. 26), segurança da informação pode ser entendida como o processo de proteger informações das ameaças para garantir a sua integridade, disponibilidade e confidencialidade. Porém, segurança da informação não pode ser encarada como “guardar em um cofre todas as informações disponíveis”, mas sim elaborar uma boa política de proteção evitando riscos e vulnerabilidade.

1.2 Princípios

Os princípios da Segurança da Informação são os conceitos que norteiam todas as ações nesta área. Diversos autores, dentre eles a ISSO/IEC 27002, descrevem os princípios básicos para garantir a segurança da informação como sendo três: Confidencialidade; Disponibilidade e Integridade.

Outros autores, como Dias (2000) e Sêmola (2003) já reconhecem a existência de outros princípios que compõe a segurança da Informação.

1.2.1 Autenticidade

Spanceski (2004, p. 32) é um dos autores que defendem que a autenticidade também é um dos princípios da segurança da informação, segundo ele:

O controle de autenticidade está associado com identificação de um utilizador ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo. Normalmente, isso é implementado a partir de um mecanismo de senhas ou de assinatura digital. A verificação de autenticidade é necessária após todo processo de identificação seja de um usuário para um sistema ou de um sistema para outro sistema. A autenticidade é a medida de proteção de um serviço/informação contra a personificação por intrusos.

1.2.2 Confidencialidade

Este princípio visa manter informações sigilosas longe de pessoas não autorizadas. Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo. Conforme Spanceski (2004, p. 35):

Confidencialidade é proteger informações contra acesso por alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital. O objetivo da confidencialidade é proteger informação privada.

1.2.3 Disponibilidade

A Disponibilidade pretende garantir que toda informação gerada ou adquirida deve estar disponível aos seus usuários no momento em que eles necessitem dela. Segundo Dias (2000 apud SIEWERT, s/d):

A disponibilidade protege os serviços de informática de tal forma que não sejam degradados ou fiquem indisponíveis sem a devida autorização. Para um utilizador autorizado, um sistema não disponível quando se necessita dele, pode ser tão ruim quanto um sistema inexistente ou destruído.

As medidas relacionadas a esse objetivo, podem ser a duplicação de equipamentos ou backup, disponibilidade pode ser definida como a garantia de que os serviços prestados por um sistema são acessíveis, sob demanda, aos utilizadores autorizados.

1.2.4 Integridade

Este princípio tem por finalidade a proteção dos dados ou informações contra modificações intencionais ou acidentais não autorizadas. Conforme Dias (2000 apud SIEWERT, s/d).

A integridade consiste em evitar que os dados sejam apagados ou de alguma forma alterada, sem a permissão do proprietário da informação. O conceito de dados nesse objetivo é mais amplo, englobando dados, programas, documentação, registros, fitas magnéticas, etc.

1.2.4 Legalidade

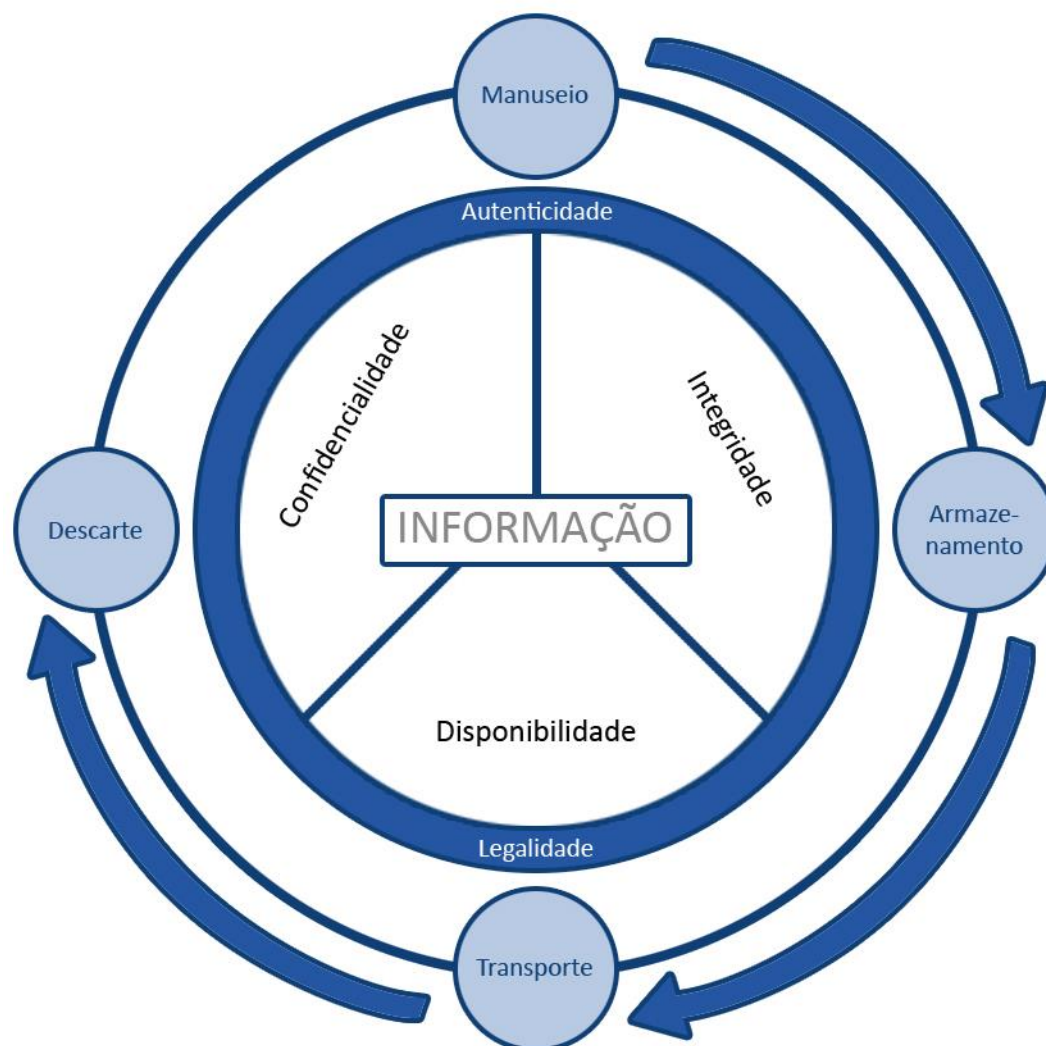
A Legalidade pretende garantir que as informações foram produzidas respeitando e obedecendo a legislação vigente. Segundo Bishop (2003, p. 41).

O princípio da Legalidade garante a legalidade (jurídica) da informação; Aderência de um sistema à legislação; Característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

Sêmola (2003) aleta a importância de estar atento aos princípios em todos os momentos do ciclo de vida da informação, como ilustra a figura 1, onde é estabelecida como cerne por onde decorrem os princípios.

A Autenticidade e Legalidade são formas de garantir a legitimidade da informação. No entorno, aparecem os estágios do ciclo (manuseio, armazenamento, transporte e descarte) da informação, pois, em todos esses momentos, pode haver falhas de segurança que prejudiquem a organização.

Figura 01 – Princípios básicos e aspectos complementares no ciclo de vida da informação.



Fonte – Sêmola (2003)

1.3 Violação de Segurança da Informação

Uma ameaça consiste em uma possível violação da segurança de um sistema. O termo ameaça é utilizado para identificar circunstâncias, condições ou eventos que forneçam algum potencial de violação de segurança. Resumidamente, ameaças são “os meios pelos quais a confidencialidade, integridade e disponibilidade da informação podem ser comprometidas.” (SÊMOLA, 2003, p. 54).

A vulnerabilidade se refere a falhas ou características que podem ser exploradas em determinados sistemas computacionais. Conforme Sêmola (2003, p. 54) “Vulnerabilidade são as circunstâncias que aumentam a possibilidade de uma

ameaça ser concretizada, aumentando sua frequência e seu impacto. Na análise do risco, vulnerabilidade é a falta de segurança para determinado ativo ou grupo de ativos”. Através destas vulnerabilidades os sistemas podem sofrer violações.

Conforme Bishop (2003, p. 22). A concretização das violações varia desde a observação de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema. Um ataque é identificado como um conjunto de ações conduzidas por uma entidade não autorizada, tendo como objetivo a violação de segurança.

Como forma de proteção, as organizações utilizam medidas visando aumentar a segurança que, segundo Sêmola (2003, p. 55), podem evitar o incidente antes que ele ocorra (as preventivas), identificar as condições ou indivíduos causadores de ameaças (detectáveis), corrigir uma estrutura tecnológica ou humana para que se adaptem ao ambiente seguro ou reduzir impactos causados por falta de segurança (as corretivas).

Um sistema de informação de uma empresa pode ser considerado seguro se não contém vulnerabilidades. Ainda que existam ameaças, a ausência de vulnerabilidades torna tais ameaças sem efeito, já que não há nenhuma fragilidade a ser explorada.

2 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A política de segurança é a base para todas as questões relacionadas à proteção da informação, desempenhando um papel importante em todas as organizações, sendo a elaboração de uma política de segurança da informação é essencial, pois definem normas, procedimentos, ferramentas e responsabilidades para garantir o controle e a segurança da informação na empresa.

Política de Segurança da Informação é basicamente um manual de procedimentos que descreve como os recursos de que manipulam as informações da empresa devem ser protegidos e utilizados e é o pilar da eficácia da Segurança da Informação, estabelecendo investimentos em recursos humanos e tecnológicos (CASTRO, 2002).

Esta política é apenas a formalização dos anseios da empresa quanto à proteção das informações. Para Abreu (2002, p. 33).

Em um país, temos a legislação que deve ser seguida para que tenhamos um padrão de conduta considerado adequado às necessidades da nação para garantia de seu progresso e harmonia. Não havia como ser diferente em uma empresa. Nesta precisamos definir padrões de conduta para garantir o sucesso do negócio.

Na definição acima, política de segurança é comparada com a legislação que todos devemos seguir, de modo que o cumprimento da legislação nos garante que o padrão de conduta está sendo seguido, a política de segurança também deve ser seguida por todos os funcionários de uma organização, garantindo assim a proteção das informações e o sucesso do negócio.

Conforme descrito por Marciano (2006, p. 62) uma política de segurança da informação é um conjunto de regras, normas e procedimentos que regulam como deve ser gerenciada e protegida a informação sensível, assim classificada pela organização ou pelo Estado, além dos recursos e utilizadores que com ela interagem. Todo o ciclo de vida da informação deve ser objeto da política.

Segundo Sousa (2006, p. 74) o desenvolvimento de uma política de segurança é a base de segurança de informação em uma empresa. Alguns padrões e normas internacionais de segurança foram desenvolvidos por organizações normatizadoras como ISO (*Internacional Standards Organization*) e a BS (*British Standard*), como ISO 17799 e a BS 7799.

Segundo Wadlow (2000, p. 49) uma política de segurança atende a vários propósitos:

- Descreve o que está sendo protegido e por quê;
- Define prioridades sobre o que precisa ser protegido em primeiro lugar e com qual custo;
- Permite estabelecer um acordo explícito com várias partes da empresa em relação ao valor da segurança;
- Fornece ao departamento de segurança um motivo válido para dizer “não” quando necessário;
- Proporciona ao departamento de segurança a autoridade necessária para sustentar o “não”;
- Impede que o departamento de segurança tenha um desempenho fútil.

Ferreira (2006, p. 61) expõe as características que uma POSIC deve ter, segundo ele uma política de segurança da informação não deve ser elaborada se não tiver as seguintes características:

- Simples;
- Compreensível, ou seja, escrita de maneira clara e objetiva;
- Homologada e assinada pela Alta Administração;
- Estruturada, estabelecendo padrões;
- Alinhada com a estratégia da missão da organização;
- Orientada aos riscos, ou seja, direcionar para os riscos da organização;
- Flexível, ou seja, moldáveis aos novos requerimentos de tecnologia;
- Protetora dos ativos de informação, priorizando os de maior valor e de maior importância;
- Positiva e não apenas concentradas em ações proibitivas ou punitivas;
- Deve conter atribuições de regras e responsabilidades;
- Deve conter a forma de educar os usuários;
- Deve ser dinâmica, ser atualizada sempre que necessário;
- Deve ser acessível a todos; e
- Deve ser exequível, ou seja, descreva regras de comportamentos que possam ser cumpridas, fáceis de executar, sejam na área tecnológica ou humana.

2.2 Tipos de Políticas

Existem três tipos de políticas: Regulatória; Consultiva e Informativa. Cada uma tem suas peculiaridades e são usadas a depender das necessidades da instituição.

2.2.1 Regulatória

Ferreira (2006, p. 35), afirma que políticas regulatórias são implementadas devido às necessidades legais que são impostas à organização. Normalmente são muito específicas para um tipo de ramo de atividade.

Uma política regulatória é definida como se fosse uma série de especificações legais. Descreve, com riqueza de detalhes, o que deve ser feito, quem deve fazer e fornecer algum tipo de parecer, relatando qual ação é importante.

Deve assegurar que a organização está seguindo os procedimentos e normas para seu ramo de atuação, provendo conforto para a organização na execução de suas atividades, pois estão seguindo os requisitos legais necessários para o seu ramo de atividade.

2.2.2 Consultiva

A política consultiva apenas sugere quais ações ou métodos devem ser utilizados para a realização de uma tarefa. A ideia principal é esclarecer as atividades cotidianas do dia a dia da empresa de maneira bastante direta.

Deve-se considerar que é importante que os usuários conheçam essas ações definidas para realização de suas tarefas diárias, com o intuito de ser evitados riscos do não cumprimento das mesmas estabelecidas.

2.2.3 Informativa

Este tipo de política é menos rigorosa que as outras e possui caráter apenas informativo, nenhuma ação é desejada e não existem riscos, caso não seja cumprida. Porém, também pode contemplar uma série de observações importantes, bem como advertências severas.

Por exemplo, a política pode ressaltar que o uso de um determinado sistema é restrito a pessoas autorizadas e qualquer funcionário que realizar algum tipo de violação será penalizado. Nesta sentença não são informados quais funcionários estão autorizados, mas está determinando severas consequências para quem desrespeitá-la.

3 ÓRGÃOS QUE REGULAMENTAM A SEGURANÇA DE TI PARA A APF

Conforme Carvalho (2011, p. 12) “de modo geral, todas as instâncias do Estado devem buscar garantir e melhorar o nível de segurança da informação a nível nacional”. De forma mais específica a segurança da informação para a APF encontra-se sob responsabilidade do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

3.1. Gabinete de Segurança Institucional

O Gabinete de Segurança Institucional (GSI) é o órgão da Presidência da República encarregado da coordenação, no âmbito da Administração Pública Federal (APF), de alguns assuntos estratégicos que afetam a segurança da sociedade e do Estado, tais como: segurança das infraestruturas críticas nacionais, Segurança da Informação e Comunicações (SIC), segurança cibernética e inteligência federal.

Pela Medida Provisória (MP) nº 1.911-10, de 24 de setembro de 1999, que altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, passou a Casa Militar a chamar-se Gabinete de Segurança Institucional. E, de acordo com o que dispõe a Lei nº 10.683/03, tem como área de competência os seguintes assuntos:

- I - assistência direta e imediata ao Presidente da República no desempenho de suas atribuições;
- II - prevenção da ocorrência e articulação do gerenciamento de crises, em caso de grave e iminente ameaça à estabilidade institucional;
- III - assessoramento pessoal ao Presidente da República em assuntos militares e de segurança;
- IV - coordenação das atividades de inteligência federal e de segurança da informação;
- V - segurança pessoal do Chefe de Estado, do Vice-Presidente da República e dos respectivos familiares, dos titulares dos órgãos essenciais da Presidência da República e de outras autoridades ou personalidades quando determinado pelo Presidente da República, assegurado o exercício do poder de polícia; e
- VI - segurança dos palácios presidenciais e das residências do Presidente da República e do Vice-Presidente da República, assegurado o exercício do poder de polícia.

Compete, ainda, ao Gabinete de Segurança Institucional, segundo Lei nº 8.183/91:

- I - executar as atividades permanentes, técnicas e de apoio administrativo, necessárias ao exercício da competência do Conselho de Defesa Nacional;
- II - exercer as atividades de Secretaria Executiva da Câmara de Relações Exteriores e Defesa Nacional, do Conselho de Governo, de conformidade com regulamentação específica; e
- III - exercer as atividades de Órgão Central do Sistema de Proteção ao Programa Nuclear Brasileiro - SIPRON.

3.2. Departamento de Segurança da Informação e Comunicações

O Departamento de Segurança da Informação e Comunicações (DSIC), tem como missão operacionalizar as atividades de segurança da informação e comunicações na Administração Pública Federal, regulamentando e capacitando os servidores públicos federais.

De acordo com o Art. 6º do Decreto nº 8.100, de 4 de setembro de 2013, ao Departamento de Segurança da Informação e Comunicações compete:

- I - coordenar a execução de ações de segurança da informação e comunicações na administração pública federal;
- II - definir requisitos metodológicos para implementação de ações de segurança da informação e comunicações pelos órgãos e entidades da administração pública federal;
- III - operacionalizar e manter centro de tratamento e resposta a incidentes ocorridos nas redes de computadores da administração pública federal;
- IV - avaliar tratados, acordos ou atos internacionais relacionados à segurança da informação e comunicações;
- V - coordenar as atividades relacionadas à segurança e ao credenciamento de pessoas e de empresas no trato de assuntos e documentos sigilosos; e
- VI - exercer outras atribuições que lhe forem delegadas pelo Secretário-Executivo.

3.3. Coordenação Geral de Gestão da Segurança da Informação e Comunicações

O CGSIC criado pelo Decreto nº 3.505, de 13 de junho de 2000, o Comitê Gestor da Segurança da Informação assessora a Secretaria Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como

na avaliação e análise de assuntos relativos aos objetivos estabelecidos nesse Decreto.

De acordo com o art. 38 da Portaria nº 56 - GSI, de 5 de novembro de 2009, a missão do CGGSIC é:

I - planejar e coordenar a gestão da segurança da informação e comunicações na administração pública federal;

II - orientar a implementação dos requisitos metodológicos da segurança da informação e comunicações nos órgãos e entidades da administração pública federal;

III - difundir e promover o cumprimento da Política de Segurança nos órgãos e entidades da administração pública federal;

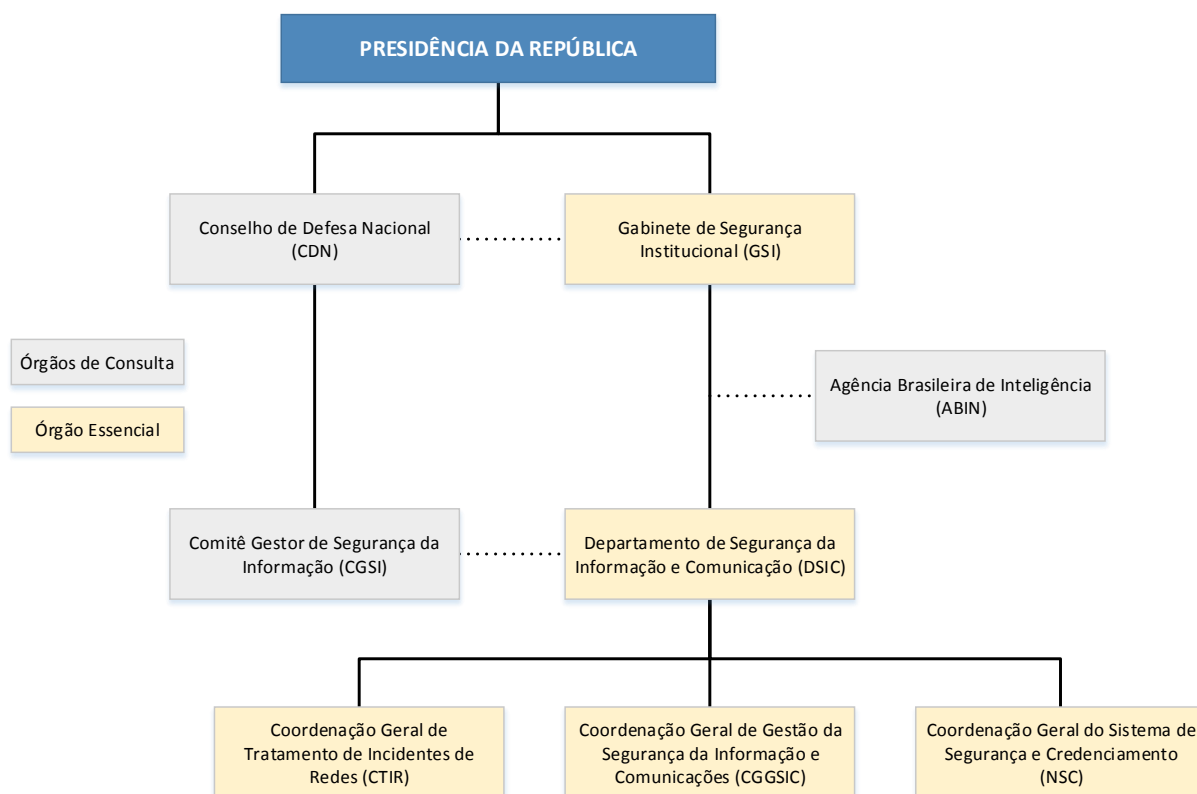
IV - coordenar no âmbito da administração pública federal, programas destinados à conscientização e à capacitação em segurança da informação e comunicações; e

V - executar outras atribuições relacionadas à gestão da segurança da informação e comunicações na administração pública federal.

3.4. Organograma

Para o cumprimento da atribuição de coordenar as atividades de segurança da informação, o GSI conta, em sua estrutura organizacional, com órgãos subordinados como demonstra o organograma seguir (FIGURA 2).

Figura 02 – Organograma.



Fonte – Departamento de Segurança da Informação e Comunicações.

3.5. Conselho de Defesa Nacional

O Conselho de Defesa Nacional (CDN) é órgão de consulta do Presidente da República nos assuntos relacionados à soberania nacional e à defesa do Estado democrático, e sua atuação tem amparo no art. 91 da Constituição Federal. Compete ao CDN propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo, bem como estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.

3.6. Comitê Gestor de Segurança da Informação

Criado pelo Decreto nº 3505 de 13 de junho de 2000, o Comitê Gestor da Segurança da Informação (CGSIC) assessora a Secretaria Executiva do Conselho de Defesa Nacional, na consecução das diretrizes da Política de Segurança da Informação, nos órgãos e nas entidades da Administração Pública Federal, bem como na avaliação e análise de assuntos relativos aos objetivos estabelecidos nesse Decreto.

3.7. Agência Brasileira de Inteligência

A ABIN, órgão central do Sistema Brasileiro de Inteligência (SISBIN), tem a seu cargo: planejar, executar, coordenar, supervisionar e controlar a atividade de Inteligência. Em consequência, cabe-lhe a atribuição de executar a Política Nacional de Inteligência no mais alto nível do governo, de forma a integrar os trabalhos dos demais órgãos setoriais de Inteligência do país.

De acordo com o site da ABIN. A ABIN tem como competência assessorar o Chefe de Estado no desempenho de suas elevadas funções, sobretudo em caráter preventivo, assegurando-lhe o conhecimento antecipado de fatos e situações relacionados ao bem-estar da sociedade e ao desenvolvimento e segurança do país.

A esse órgão, também, cabe a assessorar o GSI no que tange ajustar as políticas de segurança da informação para melhor atender aos níveis de segurança desejados.

4 LEGISLAÇÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES

Devido ao crescente número de ataques, principalmente os casos que tiveram como foco o governo federal, observou-se a necessidade de marcos legais que disciplinem e obriguem que as organizações da APF observem atentamente a segurança das informações sob custódia do governo, de forma a evitar potenciais conflitos e consequências danosas.

Através do DSIC o GSI vem, com efetiva colaboração de representantes de vários órgãos da APF e também com participação da sociedade civil, realizando um excelente trabalho de construção da normatização da segurança da informação além de conscientização dos gestores da APF com cursos, seminários e publicações.

Dentre outras publicações, em 2000 lançou O Livro Verde que apresenta que “No Brasil, governo e sociedade devem andar juntos para assegurar a perspectiva de que seus benefícios efetivamente alcancem a todos os brasileiros”. Outra publicação de destaque foi em 2010 com o Guia de Referência para a Segurança das Infraestruturas Críticas da Informação que traz uma série de orientações importantes para aplicações nas organizações da APF. Segundo Fernandes (2010).

Hoje já existem normas federais que disciplinam o desenvolvimento de políticas de segurança da informação e comunicações em órgãos da Administração Pública Federal, como a que confere direitos e deveres ao gestor público, no que concerne à proteção dos sistemas e da informação públicos.

4.1. Instrução Normativa

O GSI publicou três Instruções Normativas (IN), que são atos administrativos que definiram os conceitos, responsabilidades, papéis e normatizações para a segurança da informação na APF.

A IN GSI nº 01, de 13 de junho de 2008, disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

A IN GSI nº 02, de 5 de fevereiro de 2013, dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal.

E a IN GSI nº 03, de 6 de março de 2008, dispõe sobre os parâmetros e padrões mínimos dos recursos criptográficos baseados em algoritmos de Estado para criptografia da informação classificada no âmbito do Poder Executivo Federal.

4.2. Normas Complementares

As INs trazem definições de conceitos e planos genéricos de como se espera que a segurança funcione, para definir procedimentos e tecnologias é necessário complementar as INs com Normas Complementares (NC). Até o presente o DSIC publicou 22 NC, sendo que 21 para a IN 01 e 1 para a IN 02.

As 21 NCs da IN 01 são as seguintes.

NC nº 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, regulamenta a atividade de normatização.

NC nº 02/IN01/DSIC/GSIPR, de 14 de outubro de 2008, apresenta a metodologia de gestão de segurança da informação e comunicações.

NC nº 03/IN01/DSIC/GSIPR, de 03 de julho de 2009, traz as diretrizes para a elaboração de Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

NC nº 04/IN01/DSIC/GSIPR, de 25 de fevereiro de 2013, demonstra as diretrizes para o processo de gestão de riscos de segurança da Informação e comunicações - GRSIC - nos órgãos e entidades da Administração Pública Federal.

NC nº 05/IN01/DSIC/GSIPR, de 17 de agosto de 2009, disciplina a criação de equipes de tratamento e respostas a incidentes em redes computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

NC nº 06/IN01/DSIC/GSIPR, de 23 de novembro de 2009, estabelece diretrizes para gestão de continuidade de negócios, nos aspectos relacionados à

segurança da informação e comunicações, nos órgãos e entidades da administração Pública Federal, direta e indireta – APF.

NC nº 07/IN01/DSIC/GSIPR, de 16 de julho de 2014, estabelece as diretrizes para implementação de controles de acesso relativos à segurança da informação e comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

NC nº 08/IN01/DSIC/GSIPR, de 24 de agosto de 2010, estabelece as diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e entidades da Administração Pública Federal.

NC nº 09/IN01/DSIC/GSIPR, de 16 de julho de 2014, estabelece orientações específicas para o uso de recursos criptográficos em segurança da informação e comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.

NC nº 10/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, estabelece diretrizes para o processo de inventário e mapeamento de ativos de informação, para apoiar a segurança da informação e comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

NC nº 11/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, estabelece diretrizes para avaliação de conformidade nos aspectos relativos à segurança da informação e comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF.

NC nº 12/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à segurança da informação e comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

NC nº 13/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, estabelece diretrizes para a gestão de mudanças nos aspectos relativos à segurança da informação e comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF).

NC nº 14/IN01/DSIC/GSIPR, de 10 de fevereiro de 2012, estabelece diretrizes para a utilização de tecnologias de computação em nuvem, nos aspectos

relacionados à segurança da informação e comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

NC nº 15/IN01/DSIC/GSIPR, de 11 de junho de 2012, estabelece diretrizes de segurança da informação e comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

NC nº 16/IN01/DSIC/GSIPR, de 21 de novembro de 2012, estabelece as diretrizes para o desenvolvimento e obtenção de software seguro nos órgãos e entidades da Administração Pública Federal, direta e indireta.

NC nº 17/IN01/DSIC/GSIPR, de 10 de abril de 2013, estabelece diretrizes nos contextos de atuação e adequações para profissionais da área de segurança da informação e comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF).

NC nº 18/IN01/DSIC/GSIPR, de 10 de abril de 2013, estabelece as diretrizes para as atividades de ensino em segurança da informação e comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF).

NC nº 19/IN01/DSIC/GSIPR, de 16 de julho de 2014, estabelece padrões mínimos de segurança da informação e comunicações para os sistemas estruturantes da Administração Pública Federal (APF), direta e indireta.

NC nº 20/IN01/DSIC/GSIPR, de 15 de dezembro de 2014, estabelece as diretrizes de segurança da informação e comunicações para instituição do processo de tratamento da informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

NC nº 21/IN01/DSIC/GSIPR, de 10 de outubro de 2014, estabelece as diretrizes para o registro de eventos, coleta e preservação de evidências de incidentes de segurança em redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.

A única NC da IN 02 tem o nº 01/IN02/NSC/GSIPR, de 28 de julho de 2013, e disciplina o credenciamento de segurança de pessoas naturais, órgãos e entidades públicas e privadas para o tratamento de informações classificadas.

5 ANÁLISE DAS POSICS

Todas as POSICs, dos vinte e quatro ministérios, foram analisadas frente as vinte e uma Normas Complementares, publicadas pelo DESIC, que regulamentam a segurança da informação na APF, com a finalidade de realizar uma análise qualitativa observando o grau de observância de cada POSIC com a Norma em estudo.

Organizamos o estudo tendo como origem a Norma Complementar, onde criamos critérios para observar se a POSIC está de acordo com a Norma. Assim sendo, para verificar o grau de adequação da POSIC em relação a Norma utilizamos uma escala representada no quadro 1.

Quadro 01 – Fórmula para medir a adequação frente as N.C.

Legenda	Critério	Nota
Não Adere (N.A.)	Menor que 30%	0
Adere Parcialmente (A.P.)	Entre 30% e 50%	2
Adere (A.)	Entre 50% e 80%	4
Adere Completamente (A.C.)	Maior que 80%	8

Fonte – Próprio autor.

A nota é uma medida elaborada para, ao final do estudo, apresentar um estudo qualitativo entre o grau de adequação das POSICs dos ministérios de maneira a classificar quais POSICs estão mais próximo das Instruções Normativas do DSIC.

5.1. Norma Complementar 01/IN01

A NC 01 tem como objetivo estabelecer os critérios e procedimentos para a elaboração da POSIC na APF. Esta é uma norma bem genérica e indica algumas diretrizes que podem ser seguidas no momento da elaboração da POSIC.

Tabela 01 – Análise das POSICs frente a NC 01.

Ministério	Tem POSIC publicada	Segue o padrão formal
MAPA	A.C.	A.C.
MC	A.C.	A.C.
MCidades	A.C.	A.C.
MCTI	A.C.	A.C.
MD	A.C.	A.C.
MDA	A.C.	A.C.
MDIC	A.C.	A.C.
MDS	A.C.	A.C.
ME	A.C.	A.C.
MEC	A.C.	A.C.
MF	A.C.	A.C.
MI	A.C.	A.C.
MinC	A.C.	A.C.
MJ	A.C.	A.C.
MMA	A.C.	A.C.
MME	A.C.	A.C.
MPA	A.C.	A.C.
MPOG	A.C.	A.C.
MPS	A.C.	A.C.
MRE	A.C.	A.C.
MS	A.C.	A.C.
MT	A.C.	A.C.
MTE	A.C.	A.C.
MTUR	A.C.	A.C.

Fonte – Próprio autor.

5.2. Norma Complementar 02/IN01

A NC 02 tem por objetivo definir a metodologia de gestão de segurança da informação e comunicações utilizada pela APF.

Tabela 02 – Análise das POSICs frente a NC 02.

Ministério	Observa PDCA		Obteve apoio da alta direção	
	Qualificação	Item	Qualificação	Item
MAPA	A.C.	4.1.5 e 5.1	A.C.	5.2
MC	A.P.	Art. 28°	N.A.	
MCidades	A.P.	Art. 1° III § único	N.A.	
MCTI	A.P.	Art. 14°	A.P.	Art. 75°
MD	A.	5.7.2 e 9.1.1	A.P.	9.1.1
MDA	N.A.		N.A.	
MDIC	N.A.		N.A.	
MDS	A.P.	Art. 57°	A.P.	Art. 58° I
ME	A.	9.1, 9.2.1 e 9.2.2	A.P.	9.2.1
MEC	N.A.		A.P.	Art. 41°
MF	A.P.	Art. 39	N.A.	
MI	A.P.	1.11.1	N.A.	
MinC	N.A.		N.A.	
MJ	N.A.		N.A.	
MMA	N.A.		A.P.	Art. 14°
MME	A.P.	Art 10° I	N.A.	
MPA	A.P.	5	N.A.	
MPOG	A.P.	Art. 91°	N.A.	
MPS	N.A.		N.A.	
MRE	A.P.	25.2	A.P.	Art. 1°
MS	N.A.		N.A.	
MT	A.P.	Art. 8°	N.A.	
MTE	A.P.	Art. 38°	A.	Art. 32°
MTUR	A.P.	Art. 72°	A.C.	Art. 65°

Fonte – Próprio autor.

5.3. Norma Complementar 03/IN01

A NC 03 tem como objetivo estabelecer diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da POSIC dos órgãos da APF.

Tabela 03 – Análise das POSICs frente a NC 03.

Ministério	Tem escopo		Competências e responsabilidades	
	Qualificação	Item	Qualificação	Item
MAPA	A.C.	2	A.C.	6
MC	A.C.	Cap. I	A.C.	Cap. V
MCidades	A.C.	1	A.C.	6
MCTI	A.C.	Cap. I	A.C.	Cap. VIII
MD	A.C.	1	A.C.	7
MDA	A.P.	Art. 1º	A.C.	Cap. V
MDIC	N.A.		A.P.	Cap. III
MDS	A.P.	Art. 5º	A.C.	Cap. V
ME	A.C.	1	A.C.	7
MEC	A.C.	Cap. I	A.C.	Cap. VII
MF	A.C.	Cap. I	A.C.	Cap. VII
MI	A.C.	1.1 e 1.2	A.C.	1.8
MinC	N.A.		N.A.	
MJ	A.C.	Cap. II	A.	Cap. IV
MMA	N.A.		A.	Art. 9º, 10º e 11º
MME	A.P.	Cap. I	A.C.	Cap. V
MPA	A.	4	A.C.	6
MPOG	A.C.	Cap. I	A.C.	Cap. VII
MPS	A.P.	3	A.C.	6
MRE	A.P.	1	N.A.	
MS	N.A.		N.A.	
MT	N.A.		N.A.	
MTE	A.C.	Cap. I	A.C.	Cap. VI
MTUR	A.P.	Cap. II	A.C.	Cap. XXI

Fonte – Próprio autor.

5.4. Norma Complementar 04/IN01

A NC 04 tem por objetivo estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações (GRSICC) nos órgãos da APF.

Tabela 04 – Análise das POSICs frente a NC 04.

Ministérios	Possui gestão de riscos	
	Qualificação	Item
MAPA	N.A.	
MC	A.P.	Cap. II
MCidades	A.P.	4.2
MCTI	A.P.	XII
MD	A.P.	5.5, 5.5.1 e 5.5.2
MDA	A.P.	Cap. IX
MDIC	N.A.	
MDS	A.P.	Art. 22° e 23°
ME	A.	5.3.4
MEC	A.P.	Cap. V Seq. VI
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	A.P.	Art. 5° VII
MPA	N.A.	
MPOG	AP.	Art. 33° e 34°
MPS	N.A.	
MRE	A.P.	16
MS	N.A.	
MT	N.A.	
MTE	A.P.	Art. 15
MTUR	A.	Cap. VIII

Fonte – Próprio autor.

5.5. Norma Complementar 05/IN01

A NC 05 visa disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos da APF.

Tabela 05 – Análise das POSICs frente a NC 05.

Ministérios	Estabelece ETIR		Tem missão do ETIR	
	Qualificação	Item	Qualificação	Item
MAPA	A.	6.5	A.C.	6.5 a
MC	A.C.	Art. 9°	A.C.	Arts. 36° e 37°
MCidades	N.A.		N.A.	
MCTI	A.	Art. 22 II	N.A.	
MD	A.	5.4.1	A.P.	5.4.1
MDA	A.	Art. 15°	A.C.	Art. 15° e § único
MDIC	A.	Art. 13°	N.A.	
MDS	N.A.		A.C.	Art. 51
ME	A.	5.3.3.1	A.P.	5.3.3.1
MEC	A.	Art. 23°	A.P.	Art. 23°
MF	A.	Art. 22°	A.P.	Art. 22°
MI	N.A.		N.A.	
MinC	A.C.	Art. 8°	N.A.	
MJ	A.C.	Art. 9°	A.C.	Art. 9°
MMA	A.	Art. 4° II	A.P.	Art. 4° II
MME	N.A.		N.A.	
MPA	N.A.		N.A.	
MPOG	A.	Art. 15°	A.C.	Arts. 15° e 85°
MPS	N.A.		N.A.	
MRE	A.	3.1.9	A.P.	3.1.9 e 15.2
MS	N.A.		N.A.	
MT	A.	Art. 2° IV	A.P.	Art. 2° IV
MTE	A.	Art. 20°	A.P.	Art. 20°
MTUR	A.C.	Art. 9°	A.C.	Art. 9° e 68°

Fonte – Próprio autor.

5.6. Norma Complementar 06/IN01

A NC 06 visa estabelecer diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos da APF.

Tabela 06 – Análise das POSICs frente a NC 06.

Ministério	Estabelece GCN		Os planos são testados	
	Qualificação	Item	Qualificação	Item
MAPA	A.C.	5.13	A.C.	5.13 e
MC	A.	Cap. III Seç. X	N.A.	
MCidades	A.	4.5	A.	4.5
MCTI	A.	Art. 49°	N.A.	
MD	A.	5.6	N.A.	
MDA	A.C.	Cap. III Seç. X	N.A.	
MDIC	A.P.	Art. 12°	N.A.	
MDS	A.P.	Art. 43°	N.A.	
ME	A.C.	5.3.5	N.A.	
MEC	A.C.	Cap. V Seç. VII	N.A.	
MF	A.C.	Cap. V Seç. VII	N.A.	
MI	N.A.		N.A.	
MinC	N.A.		N.A.	
MJ	N.A.		N.A.	
MMA	N.A.		N.A.	
MME	N.A.		N.A.	
MPA	A.P.	7.10	A.	7.10
MPOG	A.P.	Cap. V Seç. X	N.A.	
MPS	A.P.	5 VIII	A.	5 VIII
MRE	A.	17	N.A.	
MS	A.C.	Cap. II Seç. IV	N.A.	
MT	N.A.		N.A.	
MTE	A.C.	Seç. IV Sub. VI	N.A.	
MTUR	A.	Cap. XIV	N.A.	

Fonte – Próprio autor.

5.7. Norma Complementar 07/IN01

A NC 07 tem por objetivo estabelecer diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da APF.

Tabela 07 – Análise das POSICs frente a NC 07.

Ministério	Possui controle de acesso virtual		Possui controle de acesso físico	
	Qualificação	Item	Qualificação	Item
MAPA	N.A.		N.A.	
MC	A.C.	Cap. III Seç. IV	A.P.	Cap. III Seç. III
MCidades	A.C.	4.3	N.A.	
MCTI	A.C.	Cap. VI Seç. III	A.	Cap. VI Seç. X
MD	A.P.	5.8.1	N.A.	
MDA	A.C.	Cap. III Seç. V	N.A.	
MDIC	N.A.		N.A.	
MDS	A.C.	Cap. III Seç. VII	N.A.	
ME	A.	5.3.7	A.P.	5.3.7.3
MEC	A.C.	Cap. V Seç. XI	A.P.	Art. 30º
MF	A.C.	Cap. V Seç. XI	A.P.	Art. 29º
MI	A.P.	1.7.7	N.A.	
MinC	N.A.		N.A.	
MJ	A.P.	Cap. II Seç. II II	A.P.	Cap. II Seç. II II
MMA	A.P.	Art. 7º VIII a IVX	N.A.	
MME	A.P.	Cap. IV V	N.A.	
MPA	A.P.	7.11 a 7.13	N.A.	
MPOG	A.C.	Cap. V Seç. VI	N.A.	
MPS	A.	Cap. V IX a XV	N.A.	
MRE	A.C.	4 e 14	A.C.	20
MS	A.C.	Cap. II III	N.A.	
MT	A.P.	Cap. III V	N.A.	
MTE	A.C.	Seç. IV Sub. X	N.A.	
MTUR	A.C.	Cap. X	A.P.	Cap. XI

Fonte – Próprio autor.

5.8. Norma Complementar 08/IN01

A NC 08 visa disciplinar o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais, nos órgãos e entidades da APF.

Tabela 08 – Análise das POSICs frente a NC 08.

Ministério	Tem catálogo se serviços do ETIR		Registro de incidentes de segurança	
	Qualificação	Item	Qualificação	Item
MAPA	N.A.		A.	6.5 a
MC	A.C.	Arts. 36° e 37°	A.C.	Arts. 36° I a e 37° II
MCidades	N.A.		N.A.	
MCTI	N.A.		N.A.	
MD	N.A.		A.P.	5.4.1
MDA	A.	Art. 15°	A.C.	Art. 15° e § único
MDIC	N.A.		N.A.	
MDS	A.P.	Art. 51	N.A.	
ME	A.P.	5.3.3.1	N.A.	
MEC	A.P.	Art. 23°	N.A.	
MF	A.P.	Art. 22°	N.A.	
MI	N.A.		N.A.	
MinC	N.A.		N.A.	
MJ	A.	Art. 9°	A.C.	Art. 9° I
MMA	A.P.	Art. 4° II	N.A.	
MME	N.A.		N.A.	
MPA	N.A.		N.A.	
MPOG	A.P.	Art. 15°	N.A.	
MPS	N.A.		N.A.	
MRE	N.A.		A.P.	3.1.9
MS	N.A.		N.A.	
MT	A.P.	Art. 2° IV	N.A.	
MTE	A.P.	Art. 20°	N.A.	
MTUR	A.P.	Art. 9°	A.P.	Art. 68 VIII

Fonte – Próprio autor.

5.9. Norma Complementar 09/IN01

A NC 09 visa normatizar o uso de recurso criptográfico para a segurança de informações produzidas nos órgãos e entidades da APF.

Tabela 09 – Análise das POSICs frente a NC 09.

Ministério	Impões utilização de criptografia		Utiliza algoritmo de estado	
	Qualificação	Item	Qualificação	Item
MAPA	N.A		N.A	
MC	A.C.	Cap. III Seç. VII	N.A	
MCidades	N.A		N.A	
MCTI	A.C.	Cap. VI Seç. XV	A.C.	Art. 43° § 2°
MD	A.P.	5.14	A.C.	5.14.1
MDA	N.A.		N.A.	
MDIC	N.A		N.A	
MDS	N.A		N.A	
ME	N.A		N.A	
MEC	N.A		N.A	
MF	N.A		N.A	
MI	N.A		N.A	
MinC	N.A		N.A	
MJ	N.A		N.A	
MMA	N.A		N.A	
MME	N.A		N.A	
MPA	N.A		N.A	
MPOG	A.P.	Cap. V. Seç. VII	N.A	
MPS	N.A		N.A	
MRE	N.A		N.A	
MS	N.A		N.A	
MT	N.A		N.A	
MTE	N.A		N.A	
MTUR	A.P.	Cap. XV	N.A	

Fonte – Próprio autor.

5.10. Norma Complementar 10/IN01

A NC 10 tem por objetivo estabelecer diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a SIC, nos órgãos e entidades da APF.

Tabela 10 – Análise das POSICs frente a NC 10.

Ministério	Possui inventário e mapeamento de ativos	
	Qualificação	Item
MAPA	N.A.	
MC	A.	Art. 13°
MCidades	N.A.	
MCTI	A.C.	Cap. VI Seç. IV
MD	A.C.	5.11°
MDA	N.A.	
MDIC	N.A.	
MDS	A.C.	Cap. III Seç. I
ME	A.C.	5.3.1.5
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	A.C.	Art. 27
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	A.C.	Art. 20°

Fonte – Próprio autor.

5.11. Norma Complementar 11/IN01

A NC 11 tem por objetivo estabelecer diretrizes para avaliação de conformidade nos aspectos relativos à SIC, nos órgãos e entidades da APF.

Tabela 11 – Análise das POSICs frente a NC 11.

Ministério	Possui avaliação de conformidade em SIC	
	Qualificação	Item
MAPA	A.P.	5.18°
MC	A.C.	Cap. III Seç. XI
MCidades	A.P.	4.10°
MCTI	A.C.	Cap. VI Seç. XVI
MD	A.C.	5.7°
MDA	A.	Cap. III Seç. VII
MDIC	A.P.	Art. 11°
MDS	A.	Art. 9°
ME	A.C.	5.3.6
MEC	A.	Cap. V Seç. X
MF	A.	Cap. V Seç. X
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	A.C.	Cap. V Seç. XI
MPS	N.A.	
MRE	A.P.	19
MS	N.A.	
MT	N.A.	
MTE	N.A.	Seç. IV Sub. IX
MTUR	A.	Cap. XVI

Fonte – Próprio autor.

5.12. Norma Complementar 12/IN01

A NC 12 tem por objetivo estabelecer diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à SIC, nos órgãos e entidades da APF.

Tabela 12 – Análise das POSICs frente a NC 12.

Ministério	Possui diretrizes para dispositivos móveis	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	A.	5.12
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	A.P.	8
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.13. Norma Complementar 13/IN01

A NC 13 tem por objetivo estabelecer diretrizes para a Gestão de Mudanças nos aspectos relativos à SIC, nos órgãos e entidades da APF.

Tabela 13 – Análise das POSICs frente a NC 13.

Ministério	Define processo de gestão de mudanças	
	Qualificação	Item
MAPA	N.A.	
MC	A.P.	Cap. III sec. XV
MCidades	N.A.	
MCTI	N.A.	
MD	N.A.	
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	A.	18
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.14. Norma Complementar 14/IN01

A NC 14 visa estabelecer diretrizes para a utilização de tecnologias de Computação em Nuvem nos aspectos relacionados à SIC, nos órgãos e entidades da APF.

Tabela 14 – Análise das POSICs frente a NC 14.

Ministério	Define processo de computação em nuvem	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	A.P.	5.13
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.15. Norma Complementar 15/IN01

A NC 15 visa estabelecer diretrizes SIC para o uso das redes sociais, nos órgãos e entidades da APF.

Tabela 15 – Análise das POSICs frente a NC 15.

Ministério	Diretrizes para utilização de redes sociais	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	A.P.	5.15
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	A.P.	7
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.16. Norma Complementar 16/IN01

A NC 16 visa estabelecer diretrizes de SIC para a obtenção de software seguro, nos órgãos e entidades da APF.

Tabela 16 – Análise das POSICs frente a NC 16.

Ministério	Possui diretrizes para software seguro	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	N.A.	
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.17. Norma Complementar 17/IN01

A NC 17 visa estabelecer diretrizes nos contextos de atuação e adequações para profissionais da área de SIC, nos órgãos e entidades da APF.

Tabela 17 – Análise das POSICs frente a NC 17.

Ministério	Adequação para os profissionais de segurança	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	N.A.	
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.18. Norma Complementar 18/IN01

A NC 18 tem por objetivo estabelecer diretrizes para as atividades de ensino em SIC nos órgãos e entidades da APF.

Tabela 18 – Análise das POSICs frente a NC 18.

Ministério	Possui ensino de SIC	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	A.P.	4.7
MCTI	N.A.	
MD	N.A.	
MDA	A.	Art. 6°
MDIC	A.	Art. 10°
MDS	A.P.	Art. 27°
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.19. Norma Complementar 19/IN01

A NC 19 visa estabelecer padrões mínimos para a Segurança da Informação e Comunicação dos sistemas estruturantes nos órgãos e entidades da APF.

Tabela 19 – Análise das POSICs frente a NC 19.

Ministério	Padrões mínimos SIC dos sistemas estruturantes	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	N.A.	
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.20. Norma Complementar 20/IN01

A NC 20 tem por objetivo estabelecer diretrizes de Segurança da Informação e Comunicações para instituição do processo de tratamento da informação, envolvendo todas as etapas do ciclo de vida da informação, nos órgãos e entidades da APF.

Tabela 20 – Análise das POSICs frente a NC 20.

Ministério	Instituição do processo de tratamento da informação	
	Qualificação	Item
MAPA	A.	5.4 a 5.4.4
MC	N.A.	
MCidades	A.	4.1 a 4.1.5
MCTI	A.	Art. 16°, 42° e 43°
MD	A.P.	5.3.1 e 5.3.4
MDA	A.P.	Art. 4°, 5 e 10°
MDIC	N.A.	
MDS	A.P.	Art. 18°
ME	A.C.	5.3.2
MEC	A.C.	Cap. V. Seç. II e IV
MF	A.C.	Cap. V. Seç. II e IV
MI	A.	1.7.15 a 1.7.19
MinC	A.P.	Art. 10° e 11°
MJ	A.P.	Art. 4° I
MMA	N.A.	
MME	N.A.	
MPA	A.C.	8
MPOG	A.P.	Art. 29°
MPS	N.A.	
MRE	A.	Art. 14°
MS	A.C.	Art. 4° I, II e III
MT	A.C.	Art. 5° I, II e III
MTE	A.	Seç. IV Sub. II
MTUR	N.A.	

Fonte – Próprio autor.

5.21. Norma Complementar 21/IN01

A NC 21 visa estabelecer diretrizes para o registro, coleta e preservação de evidências de incidentes de segurança em redes computacionais, nos órgãos e entidades da APF.

Tabela 21 – Análise das POSICs frente a NC 21.

Ministério	Registro, coleta e preservação de evidências	
	Qualificação	Item
MAPA	N.A.	
MC	N.A.	
MCidades	N.A.	
MCTI	N.A.	
MD	N.A.	
MDA	N.A.	
MDIC	N.A.	
MDS	N.A.	
ME	N.A.	
MEC	N.A.	
MF	N.A.	
MI	N.A.	
MinC	N.A.	
MJ	N.A.	
MMA	N.A.	
MME	N.A.	
MPA	N.A.	
MPOG	N.A.	
MPS	N.A.	
MRE	N.A.	
MS	N.A.	
MT	N.A.	
MTE	N.A.	
MTUR	N.A.	

Fonte – Próprio autor.

5.22. Consolidado das Análises das POSICs

Com o intuito de melhor compreender as diferenças entre cada Ministério, o quadro 2 apresenta a análise consolidada confrontando cada POSIC com cada Norma Complementar.

É importante informar que, para as tabelas que possuem mais de uma pergunta, foi levado em conta apenas a primeira pergunta na montagem do quadro 2, uma vez que esta é considerada a pergunta mais significativa.

Quadro 02 – Consolidado das análises das POSICs.

NC	MAPA	MC	MCidades	MCTI	MD	MDA	MDIC	MDS	ME	MEC	MF	MI	MinC	MJ	MMA	MME	MPA	MPOG	MPS	MRE	MS	MT	MTE	MTUR
01	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C	A.C
02	A.C	A.P	A.P	A.P	A.	N.A	N.A	A.P	A.	N.A	A.P.	A.P	N.A	N.A	N.A	A.P	A.P	A.P	N.A	A.P	N.A	A.P	A.P	A.P
03	A.C	A.C	A.C	A.C	A.C	A.P	N.A	A.P	A.C	A.C	A.C	A.C	N.A	A.C	N.A	A.P	A.	A.C	A.P	A.P	N.A	N.A	A.C	A.P.
04	N.A	A.P	A.P	A.P	A.P	A.P	N.A	A.P	A	A.P	N.A	N.A	N.A	N.A	N.A	A.P	N.A	A.P	N.A	A.P	N.A	N.A	A.P	A.
05	A.	A.C	N.A	A.	A.	A.	A.	N.A	A.	A.	A.	N.A	A.C	A.C	A.	N.A	N.A	A.	N.A	A.	N.A	A.	A.	A.C
06	A.C	A.	A.	A.	A.	A.C	A.P	A.P	A.C	A.C	A.C	N.A	N.A	N.A	N.A	N.A.	A.P	A.P	A.P	A.	A.C	N.A	A.C	A.
07	N.A	A.C	A.C	A.C	A.P	A.C	N.A	A.C	A.	A.C	A.C	A.P	N.A	A.P	A.P	A.P	A.P	A.C	A.	A.C	A.C	A.P	A.C	A.C
08	N.A	A.C	N.A	N.A	N.A	A.	N.A	A.P	A.P	A.P	A.P	N.A	N.A	A.	A.P	N.A	N.A	A.P	N.A	N.A	N.A	A.P	A.P	A.P
09	N.A	A.C	N.A	A.C	A.P	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	A.P	N.A	N.A	N.A	N.A	N.A	A.P
10	N.A	A.	N.A	A.C	A.C	N.A	N.A	A.C	A.C	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	A.C	N.A.	N.A	N.A	N.A	N.A	A.C
11	A.P	A.C	A.P	A.C	A.C	A.	A.P	A.	A.C	A.	A.	N.A	N.A	N.A	N.A	N.A	N.A	A.C	N.A	A.P	N.A	N.A	N.A	A.
12	N.A	N.A	N.A	N.A	A.	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	A.P	N.A	N.A	N.A	N.A
13	N.A	A.P	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	A.	N.A	N.A	N.A	N.A
14	N.A	N.A	N.A	N.A	A.P	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A
15	N.A	N.A	N.A	N.A	A.P	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	A.P	N.A	N.A	N.A	N.A
16	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A
17	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A
18	N.A	N.A	A.P	N.A	N.A	A.	A.	A.P	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A
19	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A
20	A.	N.A	A.	A.	A.P	A.P	N.A	A.P	A.C	A.C	A.C	A.	A.P	A.P	N.A	N.A	A.C	A.P	N.A	A.	A.C	A.C	A.	N.A
21	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A	N.A

Fonte – Próprio autor.

6 ANÁLISE DOS RESULTADOS

Visando o melhor entendimento da pesquisa realizada, dividimos esse capítulo em três sub tópicos para agrupar e analisar alguns resultados interessantes encontrados na pesquisa.

O primeiro sub tópico pretende organizar os resultados observando a afinidade de tema entre as NCs, o segundo agrupa os ministérios que tem afinidade na área de atuação e, por último, apresentamos um estudo correlacionando as datas de publicação das NCs e das POSICs.

6.1. Agrupamento Visando as NCs Relacionadas

Observando pela visão das Normas Complementares, algumas delas tem temas em comum, nesse sentido pretendemos fazer alguns agrupamentos por temas relacionados entre as INs.

6.1.1 Normatização da POSIC

As Normas Complementares números 1 e 3 dizem respeito a como a POSIC deve ser feita, trazendo critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da POSIC.

Com relação a primeira Norma Complementar (NC 01), observamos que todas as POSICs aderem completamente a essa norma, visto que ela é apenas uma norma que estabelece os critérios e organização de como uma POSIC deve ser redigida. Esse resultado era esperado uma vez que ter uma POSIC é obrigatória na APF nada mais normal do que redigir o documento seguindo os critérios normativos positivados.

O mesmo não se aplicou a NC 03, que apresenta mais detalhes referentes a divulgação e atualização das POSICs. Neste ponto a análise qualitativa desta norma revelou que, apesar de a maioria dos ministérios respeitarem essa norma, cinco

ministérios não a observaram e mais sete não contemplaram toda a norma em suas políticas.

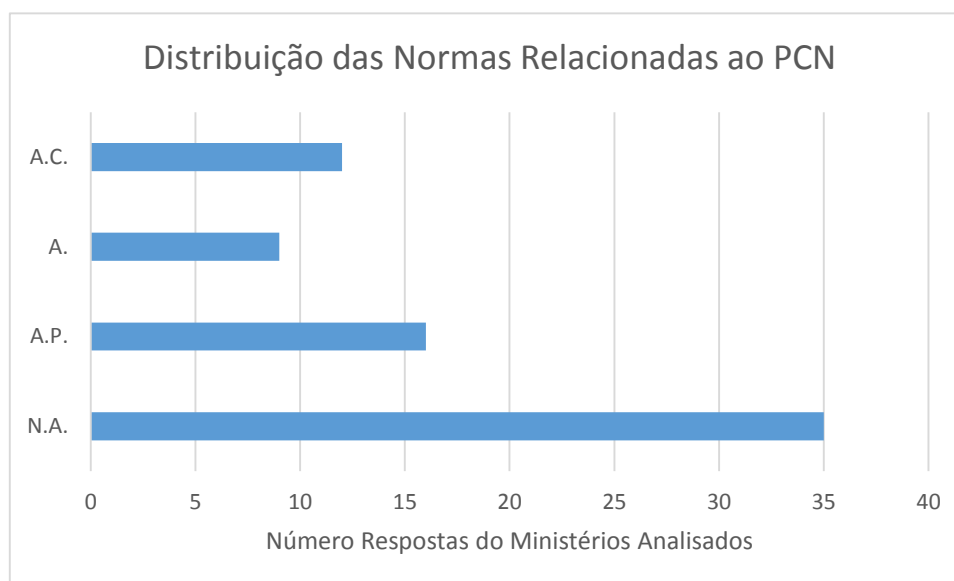
Assim sendo, metade dos ministérios não cumpriu completamente as NCs que normatizam como uma POSIC deve ser elaborada, institucionalizada, divulgada e atualizada.

6.1.2. Normas Relacionadas ao Plano de Continuidade de Negócios

O Plano de Continuidade de Negócios (PCN) é um plano formado por diversos outros planos que visam blindar os processos da organização contra desastres que eventualmente podem acontecer.

Identificamos três normas que atendem a essa função e pretendem estabelecer procedimentos que objetivam a continuidade do negócio, são elas as Normas Complementares 04, 06 e 10. Cabe lembrar que são vinte e quatro ministérios avaliados, assim sendo o número total de resposta é igual a setenta e duas. Nesse sentido a distribuição de ministério ficou conforme demonstra o gráfico 01.

Gráfico 01 – Distribuição das normas relacionadas ao PCN.



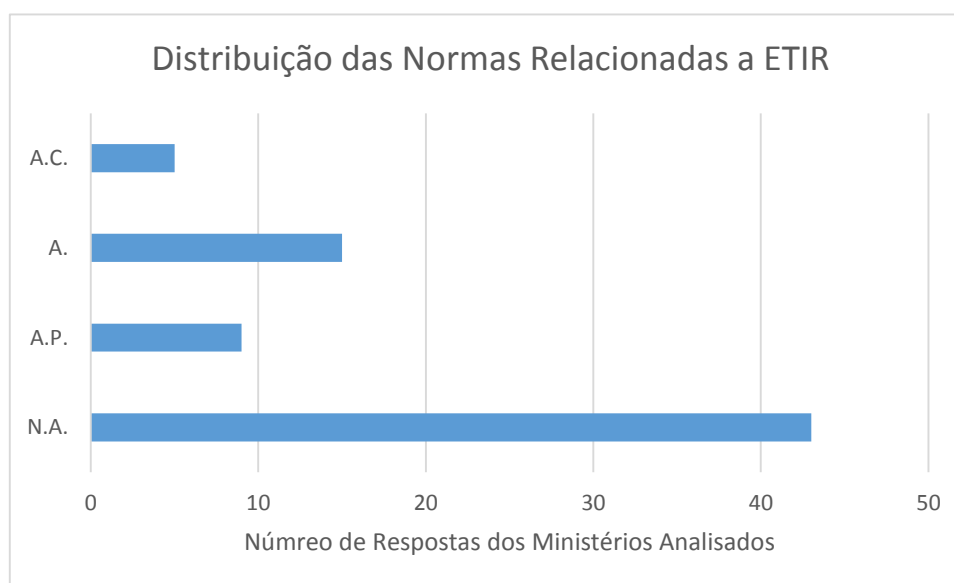
Fonte – Próprio autor.

6.1.3. Normas Relacionadas a ETIR

São três as Normas Complementares que fazem referência a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR). A NC 05 que normatiza a criação da ETIR nos órgãos da APF, a NC 08 que disciplina o gerenciamento de incidentes de segurança em redes de computadores e a NC 21 que pretende estabelecer diretrizes para o registro, coleta e preservação de evidências de incidentes de segurança.

Como é possível observar na distribuição do gráfico 02, é possível notar que a maioria das POSIC não contempla essas normas. Também ficou evidente que nenhuma POSIC observou a NC 21 que é fundamental para auditorias de segurança da informação.

Gráfico 02 – Distribuição das normas relacionadas a ETIR.



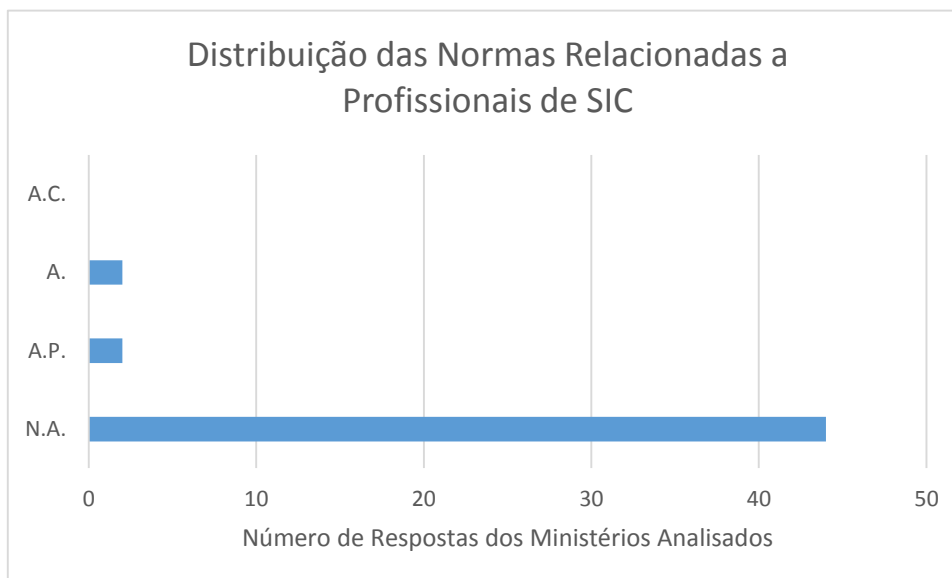
Fonte – Próprio autor.

6.1.4. Normas Relacionadas a Profissionais de SIC

As Normas Complementares dezessete e dezoito versam sobre os profissionais de segurança da informação. Mais especificamente a norma dezessete estabelecer diretrizes nos contextos de atuação e adequações para profissionais da área de SIC e a norma dezoito tem a atribuição ligada a ensino de segurança da informação na APF.

Ficou evidenciado pelo resultado exposto no gráfico 03 que a grande maioria das POSICs (mais de 91%) não faz qualquer menção sobre os profissionais de SIC. Com relação a NC 17, todas as POSIC foram silentes.

Gráfico 03 – Distribuição das normas relacionadas a profissionais de SIC.



Fonte – Próprio autor.

6.2. Agrupamento Visando a Afinidade dos Ministérios

Apesar da divisão clara entre os serviços prestados por cada ministério, é possível agrupar essas organizações independentes por área de atuação. Assim sendo, segue uma análise dos dados agrupando os ministérios por afinidade em suas áreas de atuação.

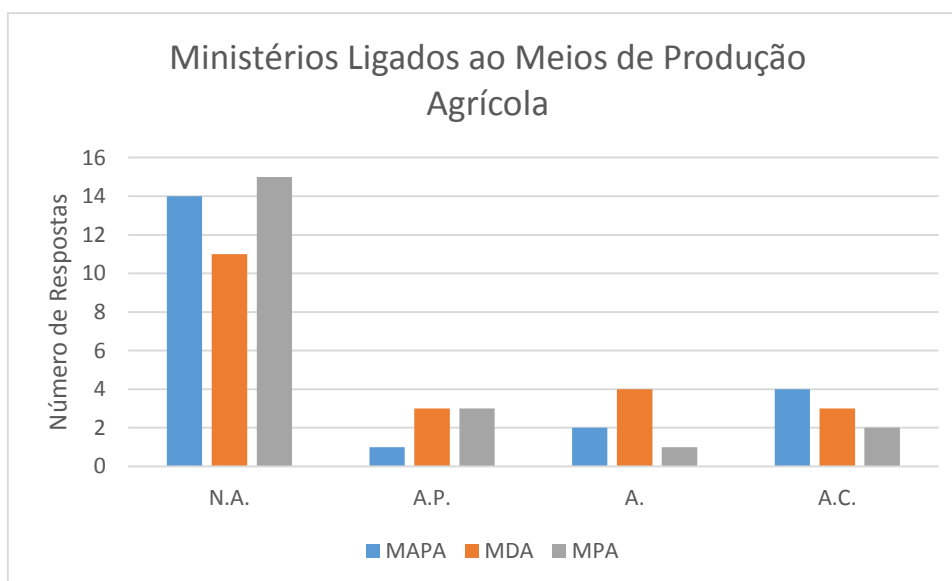
6.2.1. Ministérios Ligados a Meios de Produção Agrícola

Nessa categoria agrupamos os ministérios MPA (Ministério da Pesca e Aquicultura), MAPA (Ministério da Agricultura, Pecuária e Abastecimento), MDA (Ministério do Desenvolvimento Agrário).

A adequação das POSICs dos ministérios em reação as NCs foram homogêneas para esses ministérios. É possível observar que as POSICs não aderem a maioria das NCs.

O MDA é o ministério que se saiu melhor nesta comparação pois tem menos não aderências do que os outros ministérios ligados a meios de produção agrícola (GRÁFICO 04).

Gráfico 04 – Distribuição dos ministérios ligados a meios de produção agrícola.



Fonte – Próprio autor.

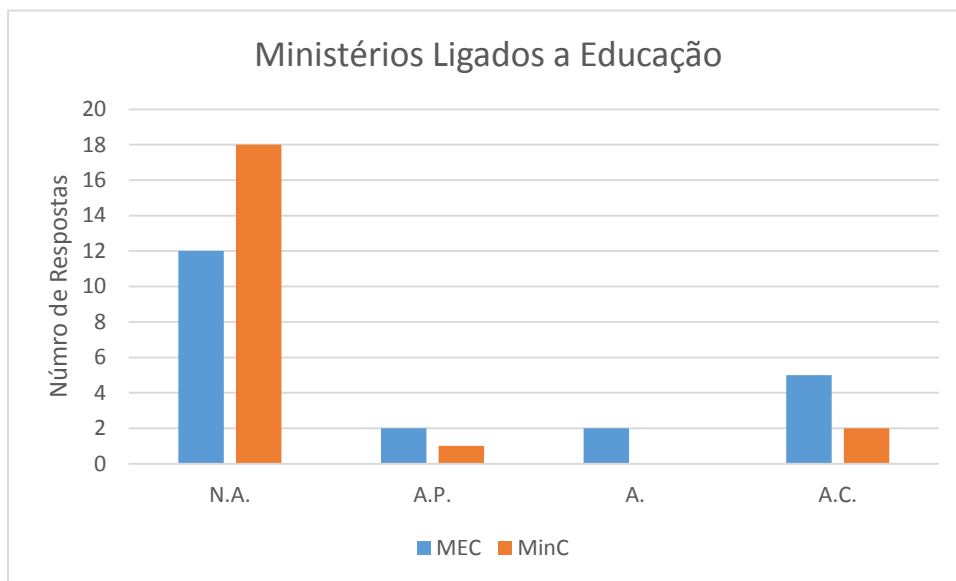
6.2.2. Ministérios Ligados a Educação

Nessa categoria agrupamos os ministérios MEC (Ministério da Educação) e MinC (Ministério da Cultura).

No caso dos ministérios ligados a educação a resposta apareceu mais dispare, o MinC apenas atende completamente a duas NCs (01 e 05), sedo que a NC 01 todos os ministérios atenderam completamente, também atendeu parcialmente a NC 20.

A POSIC do MEC teve mais conformidade com as NCs comparado com a do MinC, onde para cinco NCs (01, 05,06, 07, e 20) houve a aderência completa, conforme gráfico 05.

Gráfico 05 – Distribuição dos ministérios ligados a educação.

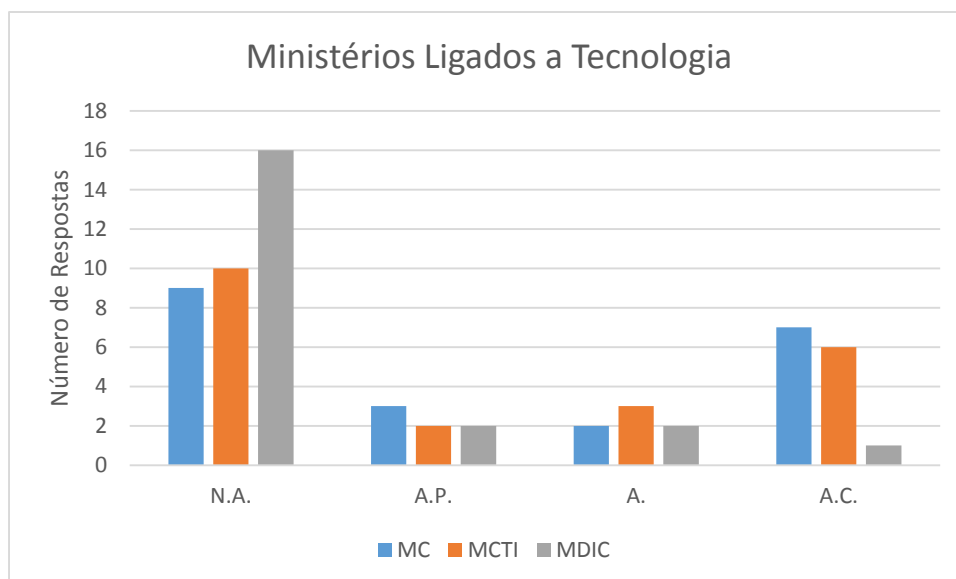


Fonte – Próprio autor.

6.2.4. Ministérios Ligados a Tecnologia

Nessa categoria agrupamos os ministérios MC (Ministério das Comunicações), MCTI (Ministério da Ciência, Tecnologia e Inovação) e MDIC (Ministério do Desenvolvimento, Indústria e Comercio Exterior) (GRAFICO 06).

Gráfico 06 – Distribuição dos ministérios ligados a tecnologia.



Fonte – Próprio autor.

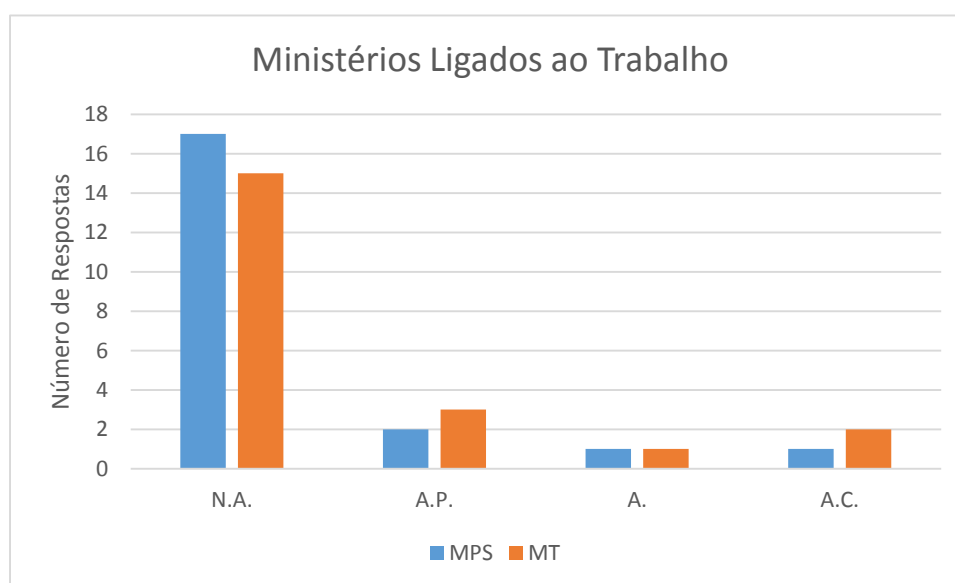
As POSICs do MC e MCTI são muito parecidas nos números de adequações as NCs. Contudo, a POSIC do MDIC não segue essa linha e possui um nível de não aderência muito maior que dos outros, destoando dos demais ministérios.

6.2.4. Ministérios Ligados ao Trabalho

Nessa categoria agrupamos os ministérios MPS (Ministério da Previdência Social) e MTE (Ministério do Trabalho e Emprego).

O gráfico 07 mostra que as POSICs dos ministérios ligados ao trabalho também têm um padrão parecido de adequação as NCs. A POSIC do MT está um pouco melhor visto que tem uma aderência parcial e uma aderência completa a mais que a do MPS.

Gráfico 07 – Distribuição dos ministérios ligados ao trabalho.



Fonte – Próprio autor.

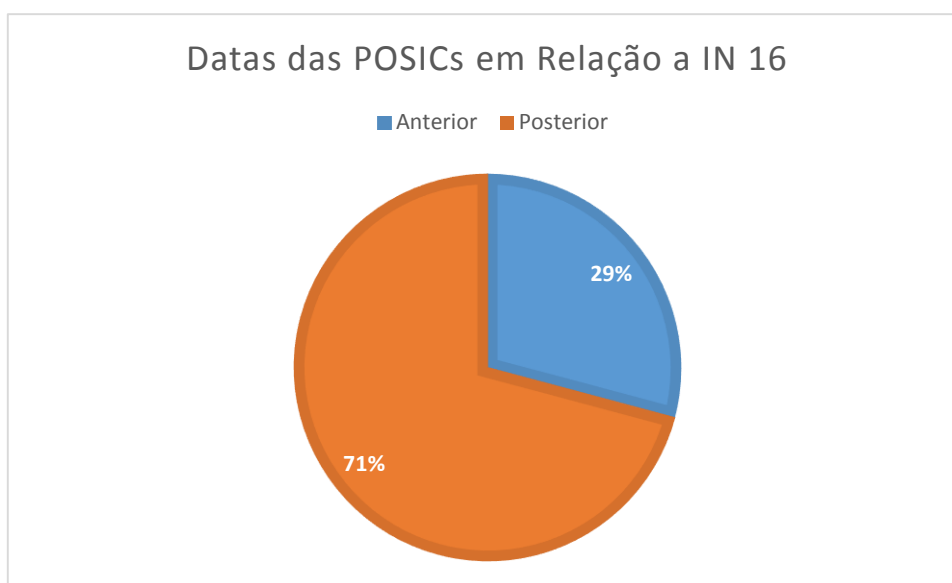
6.3. Análise Levando em Conta as Datas de Publicação

Um resultado que cabe destacar é que nenhum dos ministérios mencionada em suas POSICs sobre as NCs: 16 (versa sobre desenvolvimento seguro); 17 (diretrizes para atuação dos profissionais de SIC); 19 (diz respeito a padrões mínimos

de segurança para os sistemas estruturantes) e 21 (dispõe sobre a preservação de evidências de segurança da informação).

Essa unanimidade na não aderência a essas normas nos levou a questionar se as datas de publicação das POSICs pudessem ser anterior as datas de publicação das NCs, o que justificaria a não aderência total de todas as POSICs em relação as normas citadas, nesse sentido observou-se o que as porcentagens que seguem nos gráficos de 08 a 11 (GRÁFICO 08).

Gráfico 08 – Data de publicação das POSICs em relação a data de publicação da NC 16.



Fonte – Próprio autor.

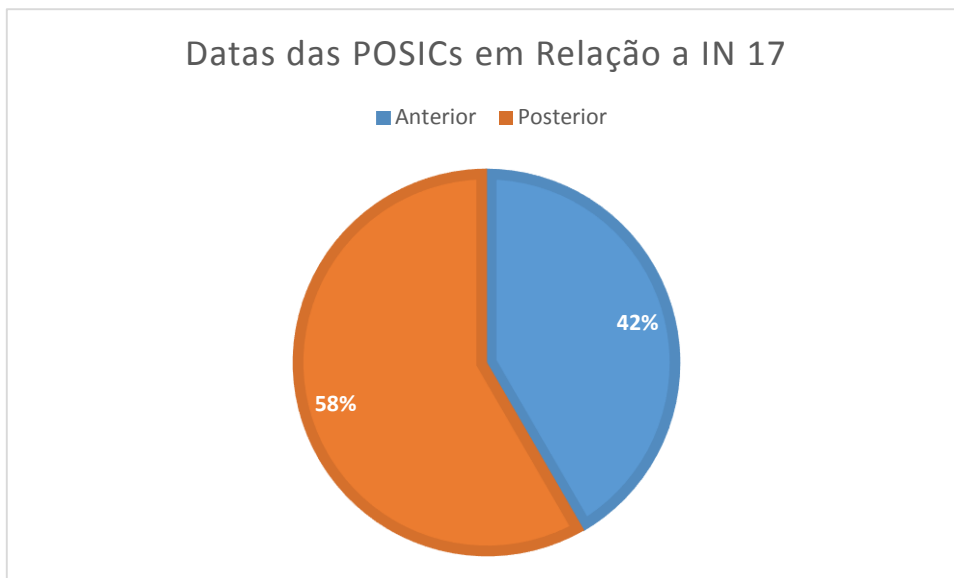
No que tange a NC 16 (publicada em novembro de 2012), apenas 29% das POSICs eram anteriores a publicação da NC, assim sendo essas POSICs não poderiam aderir a essa NC visto que foram elaboradas e publicadas antes da NC 16 entrar em vigor.

Toda via, mais de 70% das POSICs foram publicadas depois que a NC 16 entrou em vigor, essas POSICs deveriam contemplar algum nível de aderência a NC 16 visto que essa norma já estava positivada como uma exigência do DSIC antes da publicação das POSICs.

Conforme demonstra o gráfico 09, o número de POSICs feitas anteriores a NC 17 aumenta para perto da metade, pois a NC 17 foi publicada em março de 2013.

No entanto, 58% das POSICs foram publicadas depois que a NC 17 entrou em vigor, o que, novamente, deveria se traduzir em alguma conformidade com essa norma.

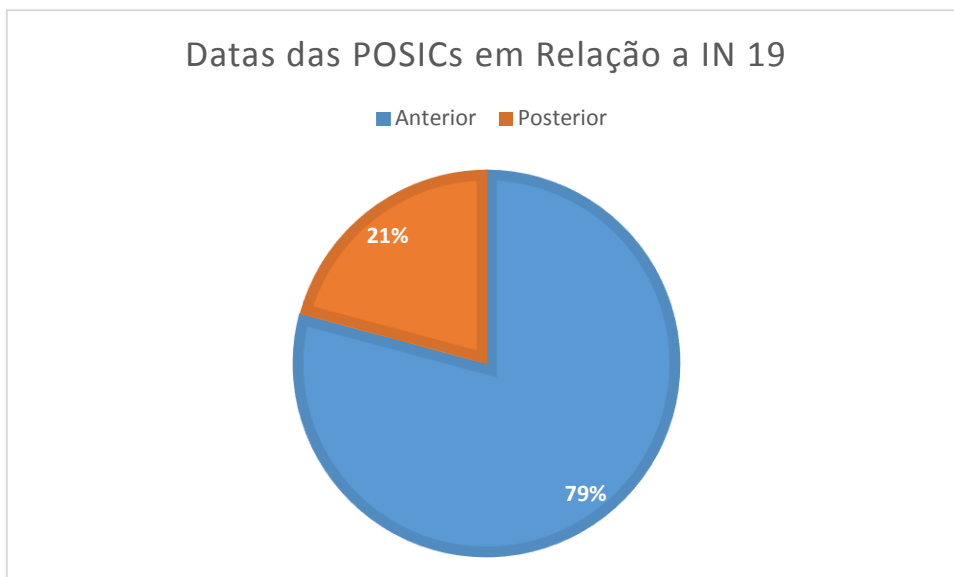
Gráfico 09 – Data de publicação das POSICs em relação a data de publicação da NC 17.



Fonte – Próprio autor.

Para a NC 19 temos que quase 80% das POSICs são anteriores a publicação da NC 19 (que ocorreu em julho de 2014). Assim sendo, poderíamos esperar um pequeno grau de aderência, ilustrada no gráfico 10.

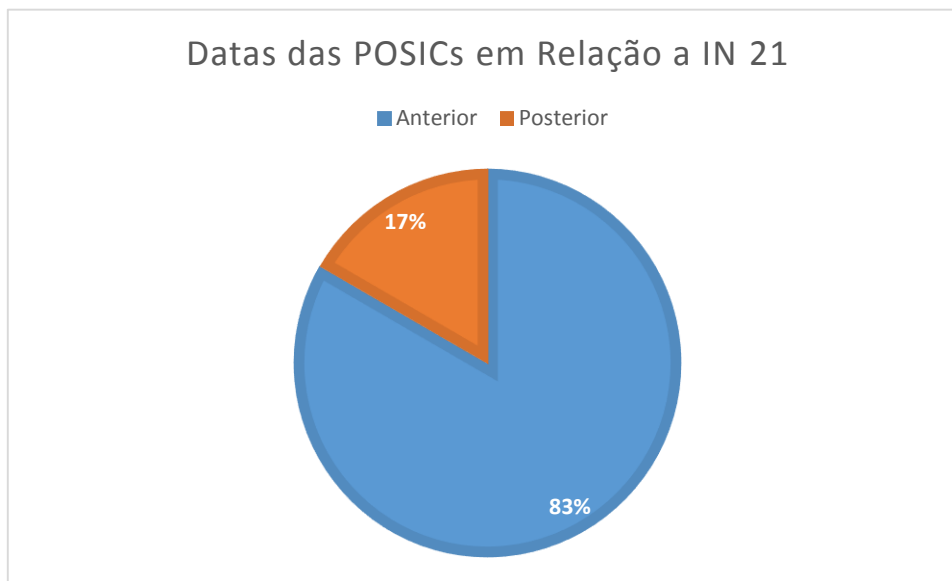
Gráfico 10 – Data de publicação das POSICs em relação a data de publicação da NC 19.



Fonte – Próprio autor.

O pior caso entre as NCs que não tiveram nenhum tipo de aderência em todas as POSICs é o da NC 21, que foi publicada em outubro de 2014. Apenas 17% das POSICs tiveram sua publicação posterior a essa data e com probabilidade de contemplar alguma aderência a essa NC (GRÁFICO 11).

Gráfico 11 – Data de publicação das POSICs em relação a data de publicação da NC 21.



Fonte – Próprio autor.

Em todo o caso, é necessário aguardar pela revisão que toda POSIC deveria passar depois de um determinado lapso temporal, ocasião em que a POSIC deveria ser revista objetivando, além de correções e adequações, também, a contemplar todas as novas e NCs atualmente em vigor.

6.4. Notas dos Ministérios

Conforme elaborado no capítulo 5, cada ministério recebeu uma nota para cada NC estudada, finalizando classificar o nível de conformidade dos ministérios as vinte e uma Instruções Normativas estudadas.

O número total - soma das notas de cada NC relacionado com a POSIC de cada ministério - foi utilizada para elencar quais POSICs dos ministérios estão mais e menos aderentes as NCs do DSIC.

É possível observar, no quadro 3, que nenhum ministério atingiu a nota máxima, que seria 168, isso indicaria de a POSIC teria aderência completa a todas as normas.

Quadro 03 – Consolidado das notas dos ministérios.

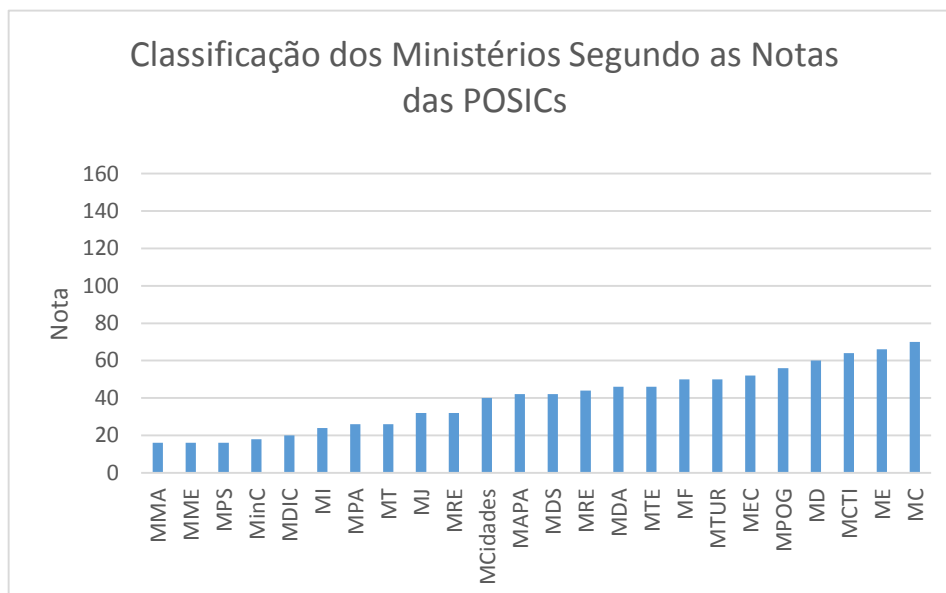
NC	MAPA	MC	MCidades	MCTI	MD	MDA	MDIC	MDS	ME	MEC	MF	MI	MinC	MJ	MMA	MME	MPA	MPOG	MPS	MRE	MS	MT	MTE	MTUR
01	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
02	8	2	2	2	4	0	0	2	4	0	2	2	0	0	0	2	2	2	0	2	0	2	2	2
03	8	8	8	8	8	2	0	2	8	8	8	8	0	8	0	2	4	8	2	2	0	0	8	2
04	0	2	2	2	2	2	0	2	4	2	0	0	0	0	0	2	0	2	0	2	0	0	2	4
05	4	8	0	4	4	4	4	0	4	4	4	0	8	8	4	0	0	4	0	4	0	4	4	8
06	8	4	4	4	4	8	2	2	8	8	8	0	0	0	0	0	2	2	2	4	8	0	8	4
07	0	8	8	8	2	8	0	8	4	8	8	2	0	2	2	2	2	8	4	8	8	2	8	8
08	0	8	0	0	0	4	0	2	2	2	2	0	0	4	2	0	0	2	0	0	0	2	2	2
09	0	8	0	8	2	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0	2
10	0	4	0	8	8	0	0	8	8	0	0	0	0	0	0	0	0	8	0	0	0	0	0	8
11	2	8	2	8	8	4	2	4	8	4	4	0	0	0	0	0	0	8	0	2	0	0	0	4
12	0	0	0	0	4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
13	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	4	0	0	0	0
14	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	2	0	0	4	4	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	4	0	4	4	2	2	0	2	8	8	8	4	2	2	0	0	8	2	0	4	8	8	4	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Total	42	70	40	64	60	46	20	42	66	52	50	24	18	32	16	16	26	56	16	44	32	26	46	50

Fonte – Próprio autor.

As maiores três notas ficaram com o Ministérios das Comunicações (70), Ministério da Educação (62) e Ministério da Ciência e Tecnologia (64). Esses têm as maiores médias de aderência as NCs estudadas.

Enquanto que as piores notas ficaram com o Ministério do Meio Ambiente, Ministério de Minas e Energia e Ministério da Previdência Social, todos esses obtiveram nota 16, conforme ilustra o gráfico 12.

Gráfico 12 – Classificação dos Ministérios Segundo as Notas das POSICs.



Fonte – Próprio autor.

Levando em conta que foram vinte e uma as normas analisadas e a nota máxima para cada uma, no caso de completa aderência, é oito, então a nota máxima que a POSIC do ministério poderia alcançar seria cento e sessenta e oito. Todavia, a POSIC com a maior nota foi setenta (Ministérios das Comunicações) atingindo, assim, 41.66% do total. Enquanto que a média de aderência dos ministérios ficou em torno de 39,75%.

CONCLUSÃO

No estudo realizado, é possível observar, por meio da análise das POSICs e NCs, que o Governo Federal está direcionando os seus esforços para que a implementação da segurança da informação seja realizada na APF de modo a atender suas necessidades de forma compatível com as melhores práticas e legislações específicas.

Verificamos que as Normas Complementares são normas muito bem redigidas, com objetivos claros, delegação de responsabilidades, observa o ciclo PDCA, é baseada nos frameworks e melhores práticas do mercado. Trazem uma visão atual e holística da segurança da informação. Entendemos que a total observância dessas normas atingiria seu objetivo que é aumentar a segurança da informação nos órgãos da APF.

No entanto, baseado nos dados levantados dos ministérios que foram objeto de estudo, pode-se verificar que as POSICs dos órgãos da administração pública federal direta estão num nível de aderência bem diversificada, necessitando de uma melhor orientação a fim de que haja uma maior homogeneidade e maturidade com intuito de que estas políticas não sejam uma mera formalização, mas um documento que agregue valor e seja uma diretriz a ser seguida pela organização.

Com relação às vinte e uma NCs positivadas pelo DSIC, que formam um arcabouço legislativo obrigatório para a APF, constatou-se que nenhuma das POSICs dos ministérios federais analisados contemplou todas elas, o que mostra uma deficiência e um risco aos órgãos públicos de forma geral, pois caso todas as NCs fossem bem implementadas poderia mitigar ou, ao mesmo, responsabilizar ações indesejadas numa organização.

Além disso, ficou evidenciado que nenhum dos ministérios contemplou em suas POSICs nada no que diz respeito às NCs 16, 17, 19 e 21. Esse é um fato surpreendente e preocupante do ponto de vista governamental, pois demonstra que, além das POSICs não estarem de acordo com a normativa vigente, é necessário uma revisão e atualização das POSICs de tal sorte que se adequem a normativa e, sob tudo, melhorem o nível de segurança da informação dos ministérios federais.

Quando observamos o estudo visando agrupar as NCs por afinidade no tema que normatizam, observamos que toda as POSICs atendem aos critérios formais de como escrever as POSICs. No entanto, temas muito importante para a segurança da informação foram pouco contemplados, como continuidade de negócio, uma quantidade menor de POSICs levaram em conta a equipe e procedimentos de ETIR e o tema ligado a profissionais de SIC quase não tiveram observância.

Analisando os dados coletados por outra dimensão e agrupando por área de atuação dos ministérios, é possível notar que os ministérios ligados a tecnologia obtiveram maior grau de maturidade em relação as NCs do que os ligados a meios de produção agrícola e ligados ao trabalho.

Por fim, conclui-se que as POSICs dos vinte e quatro ministérios da administração pública federal deveriam passar por uma revisão, de maneira que fossem atualizadas e que possam aderir completamente a todas as vinte e uma NCs atualmente publicadas. Essa medida elevaria o grau de segurança da informação dos ministérios da APF.

REFERÊNCIAS

ABNT. Tecnologia da informação - Técnicas de segurança - **Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2013**. 2a. ed. Rio de Janeiro, 2013.

ABREU, Dimitri. **Melhores práticas para classificar as informações**. Disponível em: www.modulo.com.br. Acesso em: 11 jul. 2015.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2005.

BISHOP, M. **Computer Security: Art and Science**. Addison Wesley, 2003.

BLUE PHOENIX. **Boas práticas de segurança**. Disponível em: www.bluephoenix.pt. Acesso em: 30 de maio 2015.

BRASIL. Agencia Brasileira de Inteligência. Finalidade e Subordinação. Disponível em <http://www.abin.gov.br/>. Acesso em: 10 jul. 2015.

BRASIL. Departamento de Segurança da Informação e Comunicações. Quem somos. Disponível em <http://dsic.planalto.gov.br>. Acesso em: 22 de jun. 2015.

BRASIL. Gabinete de Segurança Institucional. O que é. Disponível em <http://www.gsi.gov.br>. Acesso em: 02 jul. 2015.

BRASIL. LEI nº 8.183, de 11 de abril de 1991. Disponível em http://www.planalto.gov.br/ccivil_03/leis/L8183.htm. Acesso em: 05 jul. 2015.

BRASIL. LEI nº 10.683, de 28 de maio de 2003. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2003/L10.683.htm. Acesso em: 05 jul. 2015.

CARVALHO, P.S.M. **O Setor Cibernético nas Forças Armadas Brasileiras**. In: Desafios Estratégicos para a Segurança e Defesa Cibernética. 1a. Ed. Brasília: Presidência da República, 2011, p. 13-34.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2000.

FERNANDES, J.H.C. **Gestão da Segurança e Comunicações**. Série Segurança da Informação, 2010

FERREIRA, F. N. F. **Política de Segurança da Informação: Guia Prático para Implementação e Elaboração**. Rio de Janeiro: Editora Ciência Moderna Ltda, 2006

FONTES, Edson. **Segurança da Informação: o usuário faz a diferença**. Microsoft, São Paulo. Editora Saraiva, 2006.

MARCIANO, P.L. João. Segurança da Informação - uma abordagem social, monografia de doutor em Ciências da Informação, 2006, publicada Universidade de Brasília. Disponível em <<http://repositorio.unb.br/bitstream/10482/1943/1/Jo%C3%A3o%20Luiz%20Pereira%20Marciano.pdf>>. Acesso em: 18 jul. 2015.

SÊMOLA, M. **Gestão da Segurança da Informação – Uma visão executiva**. 3. Ed. Rio de Janeiro: Elsevier, 2003.

SIEWERT, C.Vanderson, (s/d), integração da política de segurança da informação com o firewall, [em linha] disponível em http://artigo cientifico.tebas.kinghost.net/uploads/artc_1202930234_72.pdf. Acesso em: 16 jun. 2015.

SOUSA, B. Lindeberg. **TCP/IP Básico Conectividade em Redes**, Dados. 3. Ed. São Paulo: Érica, 2006.

SPANCESKI, R. Francini. Política de segurança da informação – Desenvolvimento de um Modelo voltado para Instituições de ensino. Monografia (graduação). 2004. Disponível em http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf Acesso em: 04 de jun. 2015.

WADLOW, Tomas A. **Segurança de Redes: Projeto e gerenciamento de redes seguras**. Rio de Janeiro: Campus, 2000. Tradução: Fábio Freitas da Silva.