MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

RESOLUÇÃO Nº 070/2017-CONSAD, de 07 de dezembro de 2017.

Institui a Política de Segurança da Informação e Comunicação – POSIC, da Universidade Federal do Rio Grande do Norte – UFRN.

O REITOR EM EXERCÍCIO DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE faz saber que o Conselho de Administração, usando das atribuições que lhe confere o artigo 19, inciso XI, do Estatuto da UFRN,

CONSIDERANDO a Portaria nº 2605/15-R, 28 de dezembro de 2015, publicada no Boletim de Serviço nº 243/2015, de 30 de dezembro de 2015;

CONSIDERANDO o que consta no processo nº 23077.077931/2017-64,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação e Comunicação – POSIC, da Universidade Federal do Rio Grande do Norte – UFRN, de acordo com o texto em anexo que é parte integrante e inseparável da presente Resolução.

Art. 2º Esta Resolução entra em vigor na data da sua publicação, revogadas as disposições em contrário.

Reitoria, em Natal, 07 de dezembro de 2017.

José Daniel Diniz Melo
REITOR EM EXERCÍCIO

UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO – POSIC

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Seção I
Da Finalidade

Art.1º A Política de Segurança da Informação e Comunicação (POSIC) da UFRN é uma declaração formal da Instituição acerca do seu compromisso com a proteção dos ATIVOS DE INFORMAÇÃO, FÍSICOS E DE SOFTWARE de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos que tenham acesso a quaisquer desses ativos.

Art. 2º O objetivo desta Política de Segurança da Informação e Comunicação é estabelecer diretrizes e responsabilidades no que diz respeito ao manuseio, tratamento, controle e proteção dos ativos mencionados, servindo de apoio à alta direção na implementação da gestão de segurança da informação e comunicação na UFRN, buscando assegurar a confidencialidade, a integridade, a autenticidade, o não-repúdio e a disponibilidade dos dados e das informações tratadas, classificadas e sensíveis.

Seção II
Do Escopo

Art. 3º O escopo da Política de Segurança da Informação e Comunicação da UFRN envolve: aspectos estratégicos, estruturais, organizacionais e humanos, bem como elementos físicos e lógicos, preparando a base para elaboração dos demais documentos normativos.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES
Seção I
Da Terminologia

Art. 4º São termos e definições utilizados nesta Política de Segurança da Informação e Comunicação:

I – Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a Instituição;

II – Ativo: qualquer bem, tangível ou intangível, que tenha valor para a Instituição;

III – Ativos de informação: base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

IV – Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

V – Ativos físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;

VI – Auditoria: consiste na avaliação dos registros e procedimentos, como trilhas de auditoria e outros, que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet;

VII – Comunidade Acadêmica: entende-se por comunidade acadêmica o conjunto de docentes, técnico-administrativos e discentes da UFRN;

VIII – Comunicação: no contexto da Política de Segurança da Informação e

Comunicação, comunicação se refere a transmissão de dados;

IX – Incidente de segurança: qualquer evento adverso relacionado à segurança de sistemas de informação levando ao comprometimento de um ou mais princípios básicos de Segurança da Informação;

X – Recursos de Tecnologia da Informação e Comunicação (RTIC): os equipamentos, instalações e recursos de informação direta ou indiretamente administrados, mantidos ou operados nas Unidades, tais como:

a) equipamentos de informática e de telecomunicações de qualquer espécie;
b) infraestrutura e materiais de redes lógicas e de telecomunicações de qualquer espécie; e
c) recursos de informação eletrônicos, tais como: serviços de rede, sistemas de informação, programas de computador, arquivos de configuração que são armazenados, executados e/ou transmitidos por meio da infraestrutura computacional do UFRN, redes ou outros sistemas de informação;

XI – Serviço de rede: processo de software que estabelece conexões de rede para fornecer armazenamento, manipulação, apresentação e/ou transmissão de dados ou outra capacidade;

XII – Usuário da Informação: todos que tenham acesso a ativo físico, de informação e de software.-

Seção II
Das Instâncias Administrativas

Art. 5º Para os efeitos desta Política e das normas dela originadas, entende-se por:

I – Reitoria: é o órgão executivo superior, ao qual compete dirigir, administrar, planejar, coordenar, estabelecer parcerias e fiscalizar as atividades da universidade;

II – Unidade: qualquer instância administrativa da UFRN a exemplo dos campi, unidades ligadas aos campi, núcleos de pesquisa e centros com funcionalidades específicas;

III – Comitê Permanente de Segurança da Informação (CPSI): Comitê responsável por elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicação e normas relacionadas, submetendo à aprovação do Conselho Superior, entre outras competências;

IV – Superintendência de Informática (SINFO): instância administrativa/executiva responsável pelo desenvolvimento, implantação e manutenção dos recursos de tecnologia da informação e comunicação;

V – Comitê Gestor de Tecnologia da Informação (CGTI): tem entre suas atribuições principais: participar e orientar o planejamento dos investimentos em Tecnologia da Informação e Comunicação de acordo com as diretrizes do Plano Diretor Institucional da UFRN e do Plano de Gestão em execução; estabelecer as políticas, diretrizes e prioridades na área de Tecnologia da Informação e Comunicação (TIC); promover e estimular o desenvolvimento da Tecnologia da Informação e Comunicação no âmbito da UFRN; elaborar, acompanhar e avaliar um Plano Diretor de Tecnologia da Informação (PDTI) para a UFRN; elaborar, acompanhar e avaliar as Políticas de Segurança da Informação e Comunicação para a UFRN.

CAPÍTULO III
FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

Art. 6º As referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicação da UFRN são apresentadas no Anexo.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 7º A Política de Segurança da Informação e Comunicação da UFRN é guiada pelos princípios básicos da administração pública. Para o contexto dos serviços, recursos e informações gerenciadas na infraestrutura de Tecnologia da Informação e Comunicação da UFRN, considera-se ainda os preceitos básicos da segurança da informação: integridade, confidencialidade, disponibilidade, autenticidade e irretratabilidade.

Art. 8º A Política de Segurança da Informação e Comunicação da UFRN é regida também pelos seguintes princípios:

I – Criticidade: princípio de segurança que define a importância da informação para a continuidade da atividade-fim da Instituição;

II – Responsabilidade: as responsabilidades iniciais e finais pela proteção de cada ativo e pelo cumprimento de processos de segurança devem ser claramente definidas. Todos os usuários da informação são responsáveis pelo cumprimento das Normas de Segurança da Informação e Comunicação advindas desta política;

III – Ciência: todos os usuários da informação devem ter ciência das normas, procedimentos, orientações e outras informações que permitam a execução de suas atribuições sem comprometer a segurança;

IV – Ética: todos os direitos e interesses legítimos dos usuários da informação devem ser respeitados;

V – Proporcionalidade: o nível, a complexidade e os custos das ações de Segurança da Informação na UFRN serão adequados ao entendimento administrativo e ao valor do ativo a proteger.

CAPÍTULO V
DIRETRIZES GERAIS

Art. 9º São diretrizes gerais da Política de Segurança da Informação e Comunicação da UFRN:

I – estar alinhada aos objetivos estratégicos, processos, requisitos legais e estrutura da UFRN, bem como ao Plano Diretor de Tecnologia da Informação;

II – estabelecer medidas e procedimentos para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

III – observar as boas práticas e procedimentos de Segurança da Informação e Comunicação recomendados por órgãos e entidades responsáveis pelo estabelecimento de padrões.

Art. 10. As Diretrizes de Segurança da Informação definidas neste documento são aplicadas aos ATIVOS DE INFORMAÇÃO, FÍSICOS E DE SOFTWARE e devem servir de orientação para instrumentos táticos e operacionais a serem observados pelos usuários da informação.

Art. 11. É dever de todos os usuários da informação zelar pela Segurança da Informação e Comunicação.

Art. 12. A UFRN, como usuária dos serviços providos pela Rede Nacional de Pesquisa (RNP) é, por princípio, signatária de suas Políticas e Normas de Segurança.

Seção I
Das Diretrizes para o Tratamento de Ativos

Art. 13. Os ativos deverão ser inventariados, classificados, documentados e sua documentação mantida atualizada, devendo ser revista sempre que ocorrerem fatos que justifiquem sua atualização.

§1º A documentação dos ativos deverá fornecer subsídios para a sua recuperação após um desastre.

§2º As regras de documentação dos ativos serão definidas em normas específicas.

Art. 14. Os ativos de um setor deverão ser de responsabilidade do seu gestor, ou de alguém por ele designado, que ficará encarregado pela sua manutenção e documentação, bem como pela notificação de qualquer evento que aconteça a ele.

Art. 15. A instituição deverá adotar as medidas necessárias para que os responsáveis pelos ativos possam geri-los adequadamente, cabendo ao gestor do ativo solicitar os recursos necessários para tal.

Seção II
Dos Ativos de Informação

Art. 16. As informações existentes no âmbito da UFRN apresentam diferentes níveis de confidencialidade e devem ser classificadas de acordo com a legislação vigente.

Art. 17. Normas complementares estabelecerão procedimentos que visem garantir a integridade, a confidencialidade e a disponibilidade das informações, incluindo procedimentos para a criação, manutenção e verificação dos ativos de informação e de suas cópias de segurança.

Art. 18. Os ativos de informação armazenados nos equipamentos utilizados pelos usuários (computadores, dispositivos móveis, dispositivos de armazenamento externo, entre outros) são de sua responsabilidade, cabendo aos mesmos adotar as medidas necessárias para realizar as cópias de segurança desses ativos e proceder à sua recuperação em caso de perda.

Seção III
Dos Ativos de Software

Art. 19. A utilização de ativos de software em equipamentos da instituição deve ser previamente autorizada pelo seu responsável, conforme o artigo 14 desta Política de Segurança da Informação e Comunicação, cabendo ao mesmo providenciar os procedimentos necessários à sua utilização.

Art. 20. É vedada a utilização e/ou instalação de software que possa de qualquer forma ferir esta política de segurança, bem como direitos autorais, de propriedade intelectual ou quaisquer legislações vigentes.

Seção IV
Dos Ativos Físicos

Art. 21. Cabe ao responsável pelo ativo a elaboração de procedimentos para o seu uso e controle, devendo ainda zelar pelo cumprimento destes procedimentos.

Seção V
Dos Serviços de Rede

Art.22. Os serviços de rede no ambiente da UFRN também constituem ativos passíveis de inventário, documentação e auditoria, devendo estes procedimentos serem definidos através de normas específicas.

CAPÍTULO VI
DIRETRIZES ESPECÍFICAS
Seção I
Do Tratamento de Incidentes de Segurança da Informação e Comunicação

Art. 23. A UFRN manterá permanentemente um núcleo de tratamento e resposta a

incidentes de segurança da informação e comunicação com a responsabilidade de receber, filtrar, classificar e responder às solicitações e alertas, além de realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa.

Seção II
Da Gestão de Risco

Art. 24. Um Plano de Gestão de Riscos deve ser elaborado e mantido pela UFRN, com base na legislação vigente, contendo necessariamente uma lista das ameaças mais prováveis e suas ocorrências, uma classificação dos riscos e alternativas para mitigá-los.

Seção III
Da Gestão de Continuidade

Art. 25. Faz-se necessária a adoção de um conjunto de procedimentos emergenciais, através da definição de um Sistema de Gestão de Continuidade de Negócios (SGCN), para a eventualidade da ocorrência de algum incidente de segurança da informação que possa causar interrupção na continuidade de processos organizacionais para a UFRN, decorrentes de desastres ou falhas em recursos de Tecnologia da Informação e Comunicação.

Seção IV
Da Auditoria

Art. 26. Todos os ativos de informação, ativos de software, ativos físicos e serviços de rede no âmbito da UFRN são passíveis de auditoria técnica a cargo da Superintendência de Informática, segundo plano a ser estabelecido em norma específica.

Parágrafo único. Cabe ao Comitê Gestor de Tecnologia da Informação aprovar o plano de Auditoria e Conformidade que deverá incluir métodos, técnicas, procedimentos, normas e responsabilidades para o efetivo cumprimento do estabelecido por esta Política de Segurança da Informação e Comunicação no âmbito da UFRN.

Seção V
Dos Controles de Acesso

Art. 27. O objetivo do controle de acesso é limitar as ações que um usuário legítimo de um sistema pode efetuar, buscando prevenir a realização de atividades que venham ocasionar algum incidente de segurança.

Art. 28. Deve ser definido Plano de Controle de Acesso que estabeleça procedimentos para a identificação dos ATIVOS DE INFORMAÇÃO, FÍSICOS E DE SOFTWARE com acesso controlado, assim como dos usuários que devem ter privilégio de acesso, e as áreas físicas protegidas contra o acesso de pessoas não autorizadas.

Seção VI
Do Uso de Correio Eletrônico Institucional

Art. 29. Todos os membros da comunidade acadêmica da UFRN possuirão um endereço de correio eletrônico institucional.

Art. 30. O serviço de correio eletrônico institucional será usado para atividades acadêmicas e administrativas dos usuários da informação no âmbito da UFRN.

Art. 31. As responsabilidades, direitos e penalidades referentes ao uso de correio eletrônico institucional serão especificadas através de normas complementares.

Seção VII
Do Acesso e Publicação de Informações na Internet

Art. 32. O acesso à Internet no âmbito da UFRN é fornecido para fins diretos e complementares às atividades da instituição, sendo, portanto, passível de registro e auditoria.

Art. 33. Perfis de redes sociais, sites e portais específicos, pertencentes a alguma das unidades organizacionais da UFRN, devem ser criados, atualizados e descontinuados sob a anuência do gestor responsável pela unidade, devendo preferencialmente estar registrado em um domínio da UFRN.

Art. 34. O conteúdo acessado ou publicado não pode possuir elementos que possam ser considerados ofensivos, destrutivos, difamatórios ou pejorativos, incluindo, mas não limitado a comentários ou imagens sexuais, calúnias raciais, ou outros comentários/imagens que possam ofender alguém por sua raça, classe social, nacionalidade, gênero, orientação sexual, crença religiosa, orientação política ou condição de deficiência.

Art. 35. Não é permitida a utilização de conteúdos de terceiros, sujeitos às leis de direito autoral ou classificados como segredo, sem autorização escrita, em qualquer tipo de publicação on-line pertencente a alguma das unidades organizacionais da UFRN.

Seção VIII
Da Capacitação e Aperfeiçoamento

Art. 36. Os servidores deverão ser continuamente capacitados para o desenvolvimento de competências em Segurança da Informação e Comunicação.

Seção IX
Da Utilização de Equipamentos Particulares/Privados

Art. 37. Equipamentos particulares e/ou privados, como computadores ou quaisquer dispositivos que possam armazenar e/ou processar dados, não devem ser usados para armazenar e/ou processar informações que sejam classificadas como sensíveis para a atividade da UFRN, sem prévia autorização expressa do custodiante dos dados ou da Direção da Unidade.

Seção X
Dos Cuidados com o Posto de Trabalho

Art. 38. Nenhuma informação sensível deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

Seção XI
Das Conversas em Locais Públicos, Redes Sociais e outros meios

Art. 39. Não se deve discutir ou comentar assuntos confidenciais em locais públicos ou por meio de mensagens de qualquer tipo em redes sociais ou qualquer outro meio que não garanta sigilo.

Seção XII
Do Termo de Responsabilidade e Sigilo

Art. 40. O Termo de Responsabilidade e Sigilo é o documento oficial que

compromete e deve ser firmado por todos os usuários da informação na UFRN.

Art. 41. Como linhas gerais para a confecção do Termo de Responsabilidade e Sigilo, seus signatários devem assumir o compromisso de:

I – declarar o conhecimento e aceitação dos termos desta política de segurança e de suas políticas e normas complementares, não podendo a qualquer tempo alegar desconhecimento ou ignorância;

II – declarar estar ciente que os acessos realizados através da estrutura de Tecnologia da Informação e Comunicação da UFRN são passíveis de auditoria;

III – manter a confidencialidade de suas credenciais, notificando a UFRN sempre que existir qualquer indício de possível comprometimento, para que sejam tomadas as providências cabíveis.

Art. 42. A assinatura do Termo de Responsabilidade e Sigilo deve preceder do consentimento livre e esclarecido.

CAPÍTULO VII
COMPETÊNCIAS E RESPONSABILIDADES

Art. 43. Compete ao Comitê Permanente de Segurança da Informação:

I – propor, avaliar e revisar, regularmente, a Política de Segurança da Informação e Comunicação e seus planos de ação;

II – propor, avaliar e revisar normas complementares alinhadas à Política de Segurança da Informação e Comunicação em conformidade com as legislações vigentes;

III – apoiar o Comitê Gestor de Tecnologia da Informação nas ações de segurança da informação e comunicação;

IV – elaborar em conjunto com o Comitê Gestor de Tecnologia da Informação proposta anual de alocação de recursos orçamentários necessários às ações de segurança da informação e comunicação;

V – realizar e acompanhar estudos de novas tecnologias quanto a possíveis impactos na segurança da informação e comunicação;

VI – propor programas destinados à conscientização e à capacitação de recursos humanos em segurança da informação e comunicação.

Art. 44. Compete aos usuários da informação:

I – conhecer e cumprir os princípios, diretrizes e responsabilidades desta Política de Segurança da Informação e Comunicação, bem como suas demais normas e resoluções complementares;

II – zelar pela segurança da informação e comunicação;

III – comunicar os incidentes de segurança, por eles conhecidos;

IV – propor melhorias à segurança da informação e comunicação no âmbito da UFRN.

CAPÍTULO VIII
VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 45. A desobediência ou violação às regras da Política de Segurança da Informação e Comunicação da UFRN e suas normas complementares aprovadas pelo Comitê Gestor de Tecnologia da Informação implicará em sanções administrativas nos termos da lei e normas complementares, sem prejuízo de outras previstas nas esferas cível e penal.

CAPÍTULO IX
DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

Art. 46. A Política de Segurança da Informação e Comunicação e suas normas

complementares devem ser amplamente divulgadas a todos os usuários da informação da UFRN e dispostas de maneira que o seu conteúdo possa ser consultado a qualquer momento.

CAPÍTULO X
DISPOSIÇÕES FINAIS

Art. 47. Os casos omissos e as dúvidas surgidas na aplicação do disposto na Política de Segurança da Informação e Comunicação da UFRN deverão ser tratados pelo Comitê Permanente de Segurança da Informação.

Art. 48. A presente política passa a vigorar a partir da data de sua publicação.

FUNDAMENTAÇÕES LEGAIS E NORMATIVAS

I. Plano Diretor de Tecnologia da Informação (PDTI) 2016-2017 da Universidade Federal do Rio Grande do Norte (UFRN);

II. Resolução nº 056/2011-CONSAD, de 15 de dezembro de 2011 que normatiza a criação do Comitê Gestor de Tecnologia da Informação - CGTI da Universidade Federal do Rio Grande do Norte UFRN, atualizada pela Resolução nº 053/2016-CONSAD, de 29 de setembro de 2016;

III. Portaria nº 2.605/15-R, de 28 de dezembro de 2015, que institui a Comissão Permanente de Segurança da Informação da Universidade Federal do Rio Grande do Norte;

I. Portaria 016/2017, de 04 de Maio de 2017 que cria a Política de Gestão de Riscos da Universidade Federal do Rio Grande do Norte – UFRN e o Comitê de Governança, Riscos e Controles da Universidade Federal do Rio Grande do Norte;

II. ABNT NBR ISO/IEC 27001 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. ABNT, 2013;

III. ABNT NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão de segurança da informação. ABNT, 2013;

IV. ABNT NBR ISO/IEC 27005 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação. ABNT, 2011;

V. 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;

VI. Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicação na Administração Pública Federal, direta e indireta;

VII. Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização. Publicada no DOU Nº 200, de 15 Out 2008 - Seção 1;

VIII. Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicação. Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1;

IX. Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicação nos Órgãos e Entidades da Administração Pública Federal. Publicada no DOU Nº 125, de 03 Jul 2009 - Seção 1;

X. Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01) Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicação - GRSIC nos órgãos e entidades da Administração Pública Federal.

Publicada no DOU Nº 37, de 25 Fev 2013 - Seção 1;

XI. Norma Complementar nº 05/IN01/DSIC/GSIPR, e seu anexo, Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1;

XII. Norma Complementar nº 06/IN01/DSIC/GSIPR, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicação, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 223, de 23 Nov 2009 - Seção 1;

XIII. Norma Complementar nº 07/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicação, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1;

XIV. Norma Complementar nº 08/IN01/DSIC/GSIPR, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1;

XV. Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 02) Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicação, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1;

XVI. Norma Complementar nº 10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicação (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1;

XVII. Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicação (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1;

XVIII. Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicação (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1;

XIX. Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicação (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF). Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1;

XX. Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicação (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 30, de 10 Fev 2012 - Seção 1;

XXI. Norma Complementar nº 15/IN01/DSIC/GSIPR, Estabelece diretrizes de Segurança da Informação e Comunicação para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 119, de 21 Jun 2012 - Seção 1;

XXII. Norma Complementar nº 16/IN01/DSIC/GSIPR, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta. Publicada no DOU Nº 224, de

21 Nov 2012 - Seção 1;

XXIII. Norma Complementar nº 17/IN01/DSIC/GSIPR, Estabelece Diretrizes nos contextos de atuação e adequações para Profissionais da Área de Segurança da Informação e Comunicação (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Publicada no DOU Nº 68, de 10 Abr 2013 - Seção 1;

XXIV. Norma Complementar nº 18/IN01/DSIC/GSIPR, Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicação (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF). Publicada no DOU Nº 68, de 10 Abril 2013 - Seção 1;

XXV. Norma Complementar nº 19/IN01/DSIC/GSIPR, Estabelece Padrões Mínimos de Segurança da Informação e Comunicação para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 134, de 16 Jul 2014 - Seção 1;

XXVI. Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01)Estabelece as Diretrizes de Segurança da Informação e Comunicação para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta. Publicada no DOU Nº 242, de 15 Dez 2014 - Seção 1;

XXVII. Norma Complementar nº 21/IN01/DSIC/GSIPR, 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. Publicada no DOU Nº 196, de 10 Out 2014 - Seção 1;

XXVIII. Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação/MPOG, de 11 de setembro de 2014, que dispõe sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

XXIX. Lei de Acesso à Informação (LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011);

XXX. Decreto 3.505, DE 13 DE JUNHO DE 2000, que Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos;

XXXI. Decreto 7.845/2012, DE 14 DE NOVEMBRO DE 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

XXXII. LEI Nº 12.965, DE 23 DE ABRIL DE 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Marco Civil da Internet;

XXXIII. Lei nº 9.610/98 - Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências;

XXXIV. ePING – Padrões de Interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008;

XXXV. Política de Uso da Rede IPÊ, elaborada pelo Comitê Gestor da RNP, em outubro de 2007.