Política de segurança da informação do Sistema RNP

CAIS | Rede Nacional de Ensino e Pesquisa

Código: SEG.P.002 | Versão: 1.0

SUMÁRIO

1. OBJETIVO

Estabelecer princípios, diretrizes e deveres no âmbito da segurança da informação para todos os componentes do Sistema RNP, que garantam:

I. A promoção do desenvolvimento científico e educacional e de inovação no Sistema RNP
II. A operacionalidade e a usabilidade do Sistema RNP
III. A conformidade legal do Sistema RNP
IV. O uso seguro dos recursos providos ao Sistema RNP.

2. ESCOPO

Esta política aplica-se a todos os componentes do Sistema RNP definidos pelo Programa RNP, que são:

I. Rede Ipê e seus Pontos de Presença (PoP) e Pontos de Agregação (PoA) nas Unidades da Federação;
II. Redes Metropolitanas Comunitárias (Redecomep), baseadas em modelos associativos de diversas instituições, incluindo as Organizações Usuárias;
III. Organizações Usuárias (OU), e
IV. Redes de Colaboração de Comunidades (RCC).

3. PRINCIPIOS DA SEGURANÇA DA INFORMAÇÃO NO SISTEMA RNP

São princípios fundamentais e balizadores sobre a segurança da informação para o Sistema RNP:

I. A funcionalidade, segurança e estabilidade da ciberinfraestrutura do Sistema RNP
II. O cumprimento às obrigações legais e regulatórias aplicáveis
III. A inovação para impulsionamento do ensino, pesquisa e inovação no país
IV. A inimputabilidade do Sistema RNP
V. O uso dos recursos tecnológicos respeitando a liberdade, universalidade, diversidade, privacidade e direitos humanos de todos os usuários

4. TERMOS E DEFINIÇÕES

4.1. **Organização Social RNP (RNP)**: Associação RNP qualificada como Organização Social pelo Decreto nº 4.077 de 09/01/2002, conforme definido na Lei nº 9.637 de 15/05/1998, responsável pela coordenação e consecução dos objetivos do Programa RNP e pelo desenvolvimento, qualificação e sustentação do Sistema RNP.

4.2. **Sistema RNP**: Sistema responsável pelo desenvolvimento, oferta e uso de serviços para atender às necessidades da pesquisa, educação e inovação. Explora tecnologias de informação e comunicação emergentes, disponibilizando uma Ciberinfraestrutura de recursos federados, seguros, de alta capacidade e desempenho, por meio de mecanismos de governança multiinstitucional, estabelecidos pelo Programa RNP conforme Portaria Interministerial nº 3.825, de 12 de dezembro de 2018.

4.3. **Componentes do Sistema RNP**: O Sistema RNP é composto por: (i) a rede nacional Ipê, seus Pontos de Presença e Pontos de Agregação nas Unidades da Federação; (ii) as Redes Metropolitanas Comunitárias; (iii) as Organizações Usuárias; e (iv) as Redes de Colaboração de Comunidades.

4.4. **Ciberinfraestrutura**: Plataforma digital distribuída integrada por redes de comunicação, sistemas de computação e armazenamento, componentes de hardware e software, e dispositivos de sensoriamento e aquisição de dados, que, em conjunto, habilitam e suportam a pesquisa, a educação e a inovação.

4.5. **Organização Usuária (OU)**: Instituição pública ou privada habilitada para compartilhar da Ciberinfraestrutura para Educação, Pesquisa e Inovação e, por adesão, compor o Sistema RNP, fruindo de seus serviços mediante compartilhamento de custos nos termos definidos por esta Política de Uso;

4.6. **Ponto de Presença (PoP)**: Componente do Sistema RNP hospedado em uma Organização Usuária, instituição de educação ou pesquisa (instituição-abrigo), integrado à sua estrutura e atuante em cada Unidade da Federação que realiza a representação e a articulação institucional e a oferta de serviços do Sistema RNP. Possui papel de liderança e promoção de ações estaduais em benefício das organizações usuárias, da comunidade acadêmica e de políticas públicas. Os 27 Pontos de Presença atuam de forma integrada entre si e com ao RNP e são corresponsáveis pela implementação dos procedimentos e tecnologias necessários ao cumprimento desta Política de Uso.

4.7. **Ponto de Agregação (PoA)**: Componente do Sistema RNP, hospedado em uma instituição ou empresa, normalmente distante do Ponto de Presença (PoP), que provê a agregação de serviços locais e regionais em apoio a este PoP, especialmente na interconexão em rede de Organizações Usuárias e de Redes Comunitárias.

4.8. **Rede Metropolitana Comunitária de Educação e Pesquisa (Redecomep)**: Iniciativa associativa de instituições públicas e privadas que mantém uma rede de comunicação multimídia de interesse público e coletivo, não comercial, restrita a uma região metropolitana. Uma Redecomep é formada por associação de instituições de educação, pesquisa, empresas e instituições de governos locais, responsável pelo planejamento, operação e sustentação de serviços de forma colaborativa e integrada ao Sistema RNP.

4.9. **Rede Ipê**: Infraestrutura nacional de serviços avançados de redes de comunicação de dados que interliga as organizações usuárias entre si e, internacionalmente, com o sistema global de redes de pesquisa nacionais e regionais. A Rede Ipê também oferece acesso de alta qualidade para a Internet, por meio de acordos de trânsito e troca de tráfego com outras redes privadas e públicas.

4.10. **Rede de Colaboração de Comunidade (RCC)**: grupo de indivíduos (pesquisadores, professores, técnicos, alunos e outros profissionais), artefatos de pesquisa e instituições, operando em rede, que constituem uma comunidade colaborativa, baseada em cooperação, comunicação e coordenação regulares associadas a um campo de conhecimento. Como rede, trabalha em torno

de objetivos comuns de educação, pesquisa, desenvolvimento, formação e disseminação de conhecimentos, modelos e práticas, apoiados no Sistema RNP.

4.11. **Incidente de segurança da informação**: Um evento único ou uma série de eventos de segurança da informação indesejados ou inesperados, que possam comprometer as operações do sistema RNP ou violar sua Política de uso.

5. DIRETRIZES

São diretrizes desta política, a serem cumpridas por todos os componentes do Sistema RNP:

Sobre o tratamento de incidentes de segurança

A RNP, através de seus recursos tecnológicos, humanos e processuais, deve garantir a realização de ações continuas para a identificação e tratamento de ameaças à segurança do Sistema RNP e dos incidentes de segurança em ambientes computacionais do mesmo. Tem a RNP o papel de coordenar as ações e dar os encaminhamentos necessários para a resolução de incidentes e/ou a mitigação dos impactos dos mesmos.

Os componentes do Sistema RNP devem:

5.1. Indicar formalmente à RNP o(s) responsável(eis) pelo tratamento de incidentes, riscos e ameaças à segurança da informação das TIC que se integrem ou impactem o Sistema RNP, indicando os meios de comunicação direta com o(s) mesmo(s). Devem manter a RNP atualizada sobre mudanças desse(s) responsável(eis). Devem também manter pública nos seus canais institucionais esses meios de comunicação.

5.2. Atuar para o tratamento e resposta em tempo hábil todos os incidentes de segurança da informação que forem descobertos ou reportados nas TIC que integrem ou impactem o Sistema RNP.

5.3. Informar a RNP, em tempo hábil, incidentes de segurança ocorridos em sua TIC que impactem o Sistema RNP, exceto quando os mesmos lhe forem reportados pela própria RNP.

Sobre a conformidade legal

Esta política e suas diretrizes não se sobrepõem à legislação brasileira vigente ou demais dispositivos legais aplicáveis a cada componente do Sistema RNP. Nenhuma diretriz de segurança da informação deve ser contrária a Lei, jurisprudência e aos bons costumes.

Os componentes do Sistema RNP devem:

5.4. Comprometer-se com o cumprimento de todas as leis, normas e regulamentos à instituição ou entidade aplicáveis e que impliquem ou estejam relacionadas à segurança das TIC que se integrem ou impactem o Sistema RNP.

5.5. Empenhar esforços na identificação dos responsáveis por crimes cibernéticos que tenham sido cometidos por meio ou no uso da ciberinfraestrutura do Sistema RNP. (ex.: violação de direitos autorais de recursos tecnológicos, pedofilia, racismo, etc)

5.6. Responder em tempo hábil a toda e qualquer ordem judicial ou dispositivo equivalente, provenientes do poder judiciário que estejam relacionadas à segurança das TIC que envolvam ou impactem o Sistema RNP.

Sobre a Segurança institucional

Os componentes do Sistema RNP devem:

5.7. Investir ações que inibam e mitiguem danos causados por vazamentos de dados sigilosos ou sensíveis que impactem o Sistema RNP.

5.8. Colaborar com as ações de segurança promovidas pela RNP, que visem o fortalecimento da segurança da informação no Sistema RNP.

5.9. Ter processos e recursos mínimos para a gestão e tratamento de ameaças e riscos de segurança que envolvam as TIC que impactem o Sistema RNP.

5.10. Ter processos para a execução de backups, que contemplem os ativos que armazenam informações do Sistema RNP, de forma a evitar ou minimizar os impactos por possíveis perdas de dados diante da ocorrência de incidentes.

6. PAPEIS E RESPONSABILIDADES

Da RNP:

6.1. Monitorar os recursos de TIC por ela providos ou gerenciados, para a identificação e coordenação de ações de tratamento de ameaças cibernéticas, riscos ou atividades maliciosas. O monitoramento deve respeitar os princípios de proteção de dados pessoais, de produção e propriedade intelectual e demais legislações vigentes e aplicáveis, além de não poder ser utilizado no estabelecimento de perfis de comportamento pessoais. Em casos específicos pode a RNP compartilhar informações provenientes desse monitoramento com parceiros para fins de investigação, pesquisa e casos com interesses legítimos.

6.2. Notificar os componentes do Sistema RNP quando forem identificados incidentes, vulnerabilidades e/ou outras atividades maliciosas, nos ativos de TIC do Sistema RNP.

6.3. Publicar, dar conhecimento a todos os componentes do Sistema RNP e manter atualizadas políticas e normas referentes à segurança da informação.

6.4. Prover aos componentes do Sistema RNP apoio para o cumprimento de demandas das entidades legais, jurídicas ou autoridades aplicáveis.

6.5. Promover ações de segurança da informação que apoiem e possibilitem aos componentes do Sistema RNP o cumprimento desta política, evitando danos e se antecipando às consequências de eventuais violações.

6.6. Gerir ações para a apuração do cumprimento desta política por parte dos componentes, registrando e tratando com as mesmas eventuais violações da mesma.

Dos Componentes do Sistema RNP

6.7. Zelar pelo cumprimento desta política, difundindo-a internamente e priorizando ações para aplicação da mesma.

6.8. Manter em seus procedimentos internos as orientações e informações dos canais de comunicação da RNP para casos envolvendo a segurança da informação.

6.9. Reportar à RNP eventuais dificuldades ou descumprimentos desta política, a fim de, com o apoio da mesma, planejar ações de remediação.

6.10. Responder à RNP por eventuais violações dessa política.

7. TRATAMENTO DE VIOLAÇÕES

Eventuais violações à esta política serão tratadas pela RNP junto ao componente. Prioritariamente buscar-se-á executar ações que possibilitem a adequação do componente à política.

Violações que, comprovadamente, exponham a ciberinfraestura do Sistema RNP a situações que o afete, com prejuízo a sua operacionalidade, usabilidade, imagem ou que afete outros componentes do sistema, estarão sujeitas a medidas de mitigação emergenciais para reestabelecer a normalidade do sistema. Tais medidas deverão ser aplicadas enquanto durar a violação, procurando ser minimamente disruptivas e serão sempre comunicadas ao componente diretamente afetado.

O descumprimento reincidente dessa política de segurança, após esforços para a adequação deverá ser apurada por um grupo interno, formado por representantes internos das áreas da RNP afetadas pelo ato, que apresentará seu parecer à Diretoria Executiva da RNP. Tal parecer poderá incluir a recomendação de sanções como a interrupção temporário ou descontinuidade de serviços.

Cabe a RNP conduzir todo o processo com transparência e idoneidade, mantendo os componentes diretamente envolvidos na violação informados e atualizados quanto ao andamento da apuração.

DISTRIBUIÇÃO E VIGÊNCIA

Este documento consiste na Política de segurança da informação para o Sistema RNP, que deve ser de ciência e observância de todas as instituições componentes do referido Sistema e partes externas, quando necessário.

Esta versão foi aprovada pela Diretoria Executiva da RNP e, juntamente com seus anexos, entra em vigor imediatamente após a sua aprovação e automaticamente revoga as versões anteriores.

Este documento, incluindo seus anexos, é válido até que nova versão seja aprovada e divulgada e suas revisões devem ser realizadas a cada dois anos, considerando sua data de aprovação, ou a qualquer tempo diante de mudanças nos requisitos legais e direcionadores ou objetivos estratégicos da RNP.

CICLO DE APROVAÇÃO

Elaboradores	Data
Christian Lyra Gomes, Claudia Santos Silva, Edilson Ferreira Lima, Rodrigo Facio de Paula e Yuri Alexandro Ferreira	03/02/2020

Revisores e aprovadores	Data
Comitê de Segurança da Informação da RNP, composto por Alex Moura, Christian Lyra Gomes, Claudia Santos Silva, Claudio Fabricio Silva, Edilson Ferreira Lima, Emilio Tissato Nakamura, Emmanuel Gomes Sanches, Fernanda Boquimpani de Oliveira, Francisco Adair dos Santos Junior, Janice Nogueira Ribeiro, Liliana Esther Velásquez Alegre Solha, Luciana Batista da Silva, Marcelino Nascentes Cunha, Marcello de Jesus Fernandes, Marcia Regina de Souza, Ricardo Tulio Gandelman, Suelaine Montanini	16/03/2020

Aprovadores Finais	Data
Diretoria Executiva da RNP, composta por Eduardo Cezar Grizendi, Iara Machado José Luiz Ribeiro Filho e Nelson Simões	02/07/2020

CONTROLE DE VERSÕES

Versão	Data	Responsável	Natureza das Modificações
1.0	02/07/2020	Edilson Ferreira Lima	1ª versão do documento

ANEXO A - LEGISLAÇÃO BÁSICA

Referência do arcabouço legal vigente composto por leis, regulamentações e normas aplicáveis à segurança da informação.

Legislação geral

- Constituição da República Federativa do Brasil, de 05 de outubro de 1988; http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
- Decreto-Lei nº 2.848, de 07 de dezembro de 1940 (Código Penal); http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm
- Decreto-Lei nº 3.689, de 03 de outubro de 1941 (Código de Processo Penal); http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm
- Decreto-Lei nº 4.657, de 04 de setembro de 1942 (Lei de Introdução às normas do Direito Brasileiro); http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657.htm
- Decreto-Lei nº 5.452, de 01 de outubro de 1943 (Consolidação das Leis do Trabalho); http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm
- Lei nº 8.112, de 11 de dezembro de 1990 (Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais); http://www.planalto.gov.br/ccivil_03/leis/l8112cons.htm
- Lei nº 8.159, de 08 de janeiro de 1991 (Política Nacional de Arquivos Públicos e Privados); http://www.planalto.gov.br/ccivil_03/LEIS/L8159.htm
- Lei nº 10.406, de 10 de janeiro de 2002 (Institui o Código Civil); http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm
- Lei nº 13.105, de 16 de março de 2015 (Código de Processo Civil); http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13105.htm
- Lei nº 13.964, de 24 de dezembro de 2019 (Aperfeiçoa a legislação penal e processual penal); http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13964.htm

Legislação Específica

- Lei nº 9.279, de 14 de maio de 1996 (Lei de Propriedade Industrial); http://www.planalto.gov.br/ccivil_03/leis/l9279.htm
- Lei nº 9.296, de 24 de julho de 1996 (Lei da Interceptação Telefônica); http://www.planalto.gov.br/ccivil_03/leis/l9296.htm
- Lei nº 9.609, de 19 de fevereiro de 1998 (Lei do Software); http://www.planalto.gov.br/ccivil_03/leis/l9609.htm
- Lei nº 9.610, de 19 de fevereiro de 1998 (Lei de Direitos Autorais); http://www.planalto.gov.br/CCivil_03/leis/L9610.htm
- Lei nº 9.983, de 14 de julho de 2000 (Altera o capítulo do Código Penal - Dos crimes praticados por funcionário público contra a Administração em geral); http://www.planalto.gov.br/ccivil_03/leis/L9983.htm

- Medida Provisória nº 2.200-2, de 24 de agosto de 2001 (Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil); http://www.planalto.gov.br/ccivil_03/mpv/Antigas_2001/2200-2.htm
- Decreto nº 4.073, de 03 de janeiro de 2002 (Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados); http://www.planalto.gov.br/ccivil_03/decreto/2002/d4073.htm
- Decreto nº 5.482, de 30 de junho de 2005 (Dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores – Internet); http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5482.htm
- Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso a Informação); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm
- Lei nº 12.551, de 15 de dezembro de 2011 (Equipara os efeitos jurídicos da subordinação exercida por meios telemáticos e informatizados à exercida por meios pessoais e diretos); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12551.htm
- Decreto nº 7.724, de 16 de maio de 2012 (Regulamenta a Lei de Acesso a Informação); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7724.htm
- Lei nº 12.682, de 09 de julho de 2012 (Dispõe sobre a elaboração e o arquivamento de documentos em meios eletromagnéticos); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12682.htm
- Decreto nº 7.845, de 14 de novembro de 2012 (Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7845.htm
- Lei nº 12.735, de 30 de novembro de 2012 (Tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares); http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm
- Lei nº 12.737, de 30 de novembro de 2012 (Dispõe sobre a tipificação criminal de delitos informáticos); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm
- Lei nº 12.846, de 01 de agosto de 2013 (Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm
- Lei nº 12.965, de 23 de abril de 2014 (Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil); http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
- Decreto nº 8.771, de 11 de maio de 2016 (Regulamenta o Marco Civil da Internet); http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm
- Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD); http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

- Decreto nº 9.637, de 26 de dezembro de 2018 (Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional); http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm
- Lei nº 13.853, de 8 de julho de 2019 (Altera a LGPD, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados); http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm

Normas Infralegais

- Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008 (Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta) – e respectivas Normas Complementares, a saber: https://dsic.planalto.gov.br/legislacao/in_01_gsidsic.pdf
- Norma Complementar nº 01/IN01/DSIC/GSIPR, Atividade de Normatização; https://dsic.planalto.gov.br/legislacao/nc_1_normatizacao.pdf
- Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações; https://dsic.planalto.gov.br/legislacao/nc_2_metodologia.pdf
- Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal; https://dsic.planalto.gov.br/legislacao/nc_3_psic.pdf
- 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 Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal; https://dsic.planalto.gov.br/legislacao/nc_04_grsic.pdf
- 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; https://dsic.planalto.gov.br/legislacao/nc_05_etir.pdf
- Norma Complementar nº 06/IN01/DSIC/GSIPR, 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; https://dsic.planalto.gov.br/legislacao/nc_6_gcn.pdf
- Norma Complementar nº 07/IN01/DSIC/GSIPR, (Revisão 01) 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; https://dsic.planalto.gov.br/legislacao/nc_07_revisao_01.pdf
- 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;

https://dsic.planalto.gov.br/legislacao/nc_8_gestao_etir.pdf

- Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 02) 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; https://dsic.planalto.gov.br/legislacao/nc_09_revisao_02.pdf
- 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 Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
  https://dsic.planalto.gov.br/legislacao/nc_10_ativos.pdf
- Norma Complementar nº 11/IN01/DSIC/GSIPR, 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; https://dsic.planalto.gov.br/legislacao/nc_11_conformidade.pdf
- 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 Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
  https://dsic.planalto.gov.br/legislacao/nc_12_dispositivos.pdf
- Norma Complementar nº 13/IN01/DSIC/GSIPR, 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); https://dsic.planalto.gov.br/legislacao/nc_13_mudancas.pdf
- 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 Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
  https://dsic.planalto.gov.br/legislacao/nc_14_nuvem.pdf
- Norma Complementar nº 15/IN01/DSIC/GSIPR, 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;
  https://dsic.planalto.gov.br/legislacao/nc_15_redes_sociais.pdf
- 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; https://dsic.planalto.gov.br/legislacao/nc_16_software_seguro.pdf
- Norma Complementar nº 17/IN01/DSIC/GSIPR, 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); https://dsic.planalto.gov.br/legislacao/nc_17_profissionais_sic.pdf
- Norma Complementar nº 18/IN01/DSIC/GSIPR, Estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da

Administração Pública Federal (APF); https://dsic.planalto.gov.br/legislacao/nc_18_atividades_ensino.pdf

- Norma Complementar nº 19/IN01/DSIC/GSIPR, Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta; https://dsic.planalto.gov.br/legislacao/nc_19_SISTEMAS_ESTRUTURANTES.pdf
- Norma Complementar nº 20/IN01/DSIC/GSIPR, 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; https://dsic.planalto.gov.br/legislacao/NC20_Revisao01.pdf
- 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; https://dsic.planalto.gov.br/legislacao/nc_21_preservacao_de_evidencias.pdf
- Portaria Interministerial MP/MC/MD nº 141, de 02 de maio de 2014 (Dispõe que as comunicações de dados da Administração Pública Federal direta, autárquica e fundacional deverão ser realizadas por redes de telecomunicações e serviços de tecnologia da informação fornecidos por órgãos ou entidades da Administração Pública Federal, incluindo empresas públicas e sociedades de economia mista da União e suas subsidiárias, observado o disposto nesta Portaria); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=82&data=05/05/2014
- Portaria nº 40 CDN/PR, de 08 de outubro de 2014 (Homologa a Norma Complementar nº 21/IN01/DSIC/GSIPR que estabelece 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); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/10/2014&jornal=1&pagina=5&totalArquivos=224
- Portaria nº 49 CDN/PR, de 12 de dezembro de 2014 (Homologa a Revisão 01 da Norma Complementar nº 20/IN01/DSIC/GSI - 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); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=4&data=15/12/2014
- Portaria nº 92 SLTI/MPOG, de 24 de dezembro de 2014 (Institui a arquitetura ePING - Padrões de Interoperabilidade de Governo Eletrônico, que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação – TIC na interoperabilidade de serviços de Governo Eletrônico); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=50&data=26/12/2014

- Portaria nº 14 CDN/PR, de 11 de maio de 2015 (Homologa a "Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal - 2015/2018, versão 1.0", desdobramento da Instrução Normativa GSI/PR nº 01/2008); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=4&data=12/05/2015
- Portaria nº 96 CDN/PR, de 4 de maio de 2016 (Homologa o dia 8 de maio como "Dia da Segurança da Informação e Comunicações (SIC) e da Segurança Cibernética (SegCiber) da Administração Pública Federal"); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=09/05/2016&jornal=1&pagina=13&totalArquivos=216
- Portaria nº 09 GSI/PR, de 15 de março de 2018 (Homologa a Revisão 01 da Norma Complementar nº 14/IN01/DSIC/GSIPR); http://dsic.planalto.gov.br/assuntos/editoria-c/documentos-pdf-1/portaria-09-gsi-de-9-de-marco-de-2018-nc-14-in01-computacao-em-nuvem.pdf
- Portaria nº 41 SEDGGD/ME, de 3 de setembro de 2019 (Declara a alteração e a revogação de atos normativos, para fins do disposto no art. 9º do Decreto nº 9.759, de 11 de abril de 2019); http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=25/09/2019&jornal=515&pagina=24&totalArquivos=86

- Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI). http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm
  Lei nº 12.965, de 23 de abril de 2014 **(**Marco Civil da Internet - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil). http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

- Lei nº 13.709, DE 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 - Marco Civil da Internet). http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm
- Decreto-Lei nº 4.657, de 26 de dezembro de 2018 (Política Nacional de Segurança da Informação - PNSI, dispõe sobre a governança da segurança da informação no âmbito da APF); http://www.planalto.gov.br/ccivil_03/decreto-lei/Del4657.htm

- Lei nº 13.853, de 08 de julho de 2019 (Dispõe sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências) http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm