MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

PORTARIA /INPI / Nº 30, DE 15 DE JUNHO DE 2021.

Institui a Política de Segurança da Informação (POSIN) no âmbito do Instituto Nacional da Propriedade Industrial.

O PRESIDENTE DO INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL – INPI, no exercício das suas atribuições que lhe conferem o Regimento Interno, aprovado pela Portaria do Ministério da Indústria, Comércio Exterior e Serviços (MDIC) nº 11 de 27 de janeiro de 2017, e tendo em vista o disposto no Decreto nº 9.637, de 26 de dezembro de 2018, e na Instrução Normativa nº 01, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República, assim como o constante nos autos do Processo INPI nº 52400.134534/2016-03,

R E S O L V E :

Art. 1º Fica instituída a Política de Segurança da Informação (POSIN) no âmbito do Instituto Nacional da Propriedade Industrial.

CAPÍTULO I

DO ESCOPO

Art. 2º Art. 2º A Política de Segurança da Informação provê as diretrizes, princípios, competências e responsabilidades necessárias a viabilizar a Gestão de Segurança da Informação (GSI) no INPI, visando assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas, transmitidas e custodiadas pelos sistemas de informação no âmbito do INPI.

Parágrafo único. A POSIN é aplicável a todo o Instituto, devendo ser observada por todos os servidores, colaboradores, fornecedores, prestadores de serviço e por aqueles que, de alguma forma, executem atividades vinculadas à atuação institucional do INPI

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 3º Para os efeitos desta Política são estabelecidos os seguintes conceitos e definições:

I - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para o INPI;

II - Atividades Críticas: atividades que devem ser executadas para garantir a prestação dos serviços fundamentais do INPI;

III - Ativo de Informação: recurso utilizado na produção, processamento, armazenamento, transmissão e recuperação da informação, incluindo a própria informação, sistemas de informação, locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

V - Celeridade: as ações relacionadas à segurança da informação deverão oferecer respostas ágeis para os incidentes e para as vulnerabilidades identificadas nos sistemas de informação do INPI;

VI - Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.Gov): O CTIR Gov é um "Computer Security Incident Response Team (CSIRT)", ou Grupo de Resposta a Incidentes de Segurança, que vem a ser uma organização responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores. O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) faz parte do Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

VII - Coordenação Geral de Tecnologia da Informação (CGTI): trata-se da Coordenação do INPI responsável pela área de Tecnologia da Informação;

VIII - Comitê de Segurança da Informação: grupo de pessoas, formalmente instituído pelo INPI, com a atribuição de assessorar a implementação das ações de segurança da informação e deliberar sobre assuntos relativos à POSIN e à Política Nacional de Segurança da Informação (PNSI);

IX - Computação em Nuvem: modelo computacional que permite o acesso por demanda, e independente da localização, a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, processamento, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

X - Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizados nem credenciados;

XI - Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XII - Dispositivos Móveis: equipamentos portáteis dotados de capacidade computacional, e dispositivos removíveis de memória para armazenamento, entre os quais se incluem, não se limitando a estes: notebooks, netbooks, smartphones, tablets, pendrives, USB drives, HDs externos e cartões de memória;

XIII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder às

notificações e atividades relacionadas a incidentes de segurança em rede de XIV - Gestão de Segurança da Informação (GSI): ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança computadores; cibernética, segurança lógica aos processos institucionais estratégicos, táticos e operacionais, não se limitando portanto à tecnologia da informação e comunicações;

XV - Gestor da Informação: indivíduo responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades institucionais;

XVI - Gestor de Segurança da Informação: responsável pelas ações de segurança da informação no âmbito do INPI;

XVII - Incidente de Segurança: qualquer evento adverso, confirmado ou sob suspeita, ou ocorrência que promova uma ou mais ações tendentes a comprometer ou ameaçar a disponibilidade, a integridade, confidencialidade ou a autenticidade de qualquer ativo de informação do INPI;

XVIII - Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIX - Quebra de Segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XX - Recursos Computacionais: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, estações de trabalho, notebooks, servidores de rede, equipamentos de conectividade e infraestrutura;

XXI - Redes Sociais: estruturas sociais digitais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns;

XXII - Segurança da Informação (SI): ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações em recursos de tecnologia da Informação;

XXIII - Tecnologia da Informação e Comunicações (TIC): ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas utilizados para obter, processar, armazenar, disseminar e fazer uso de informações;

XXIV - Usuário: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, habilitada pela administração para acessar os ativos de informação de um órgão ou entidade da APF, formalizada por meio da assinatura de Termo de Responsabilidade; e

XXV - Vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou por uma organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 4º A POSIN deve obedecer aos seguintes princípios:

I - o interesse público, a preservação e a defesa do patrimônio público;

II - a legalidade, a impessoalidade, a moralidade e a transparência;

III - a honestidade, a dignidade, o respeito e o decoro; e

IV - a integridade.

§ 1º Os bens de TIC cuja propriedade pertença ao INPI são de livre acesso à CGTI, sem necessidade de autorização ou ciência prévia do usuário.

§ 2º As políticas, as normas e os procedimentos deverão ser atualizados, sempre que ocorrerem mudanças legais, sociais ou tecnológicas que venham a interferir na sua aplicabilidade no âmbito do INPI.

§ 3º As atividades de SI levarão em consideração as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do INPI.

§ 4º O nível, a complexidade e os custos das ações de segurança da informação serão adequados ao entendimento administrativo e ao valor do ativo a se proteger.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 5º A Gestão de Segurança da Informação (GSI) compreende ações e métodos que visam à integração das atividades de SI aos processos institucionais estratégicos, táticos e operacionais.

§ 1º Todos os sistemas, serviços e recursos computacionais estão sujeitos a monitoramento, controle de acesso e auditoria.

§ 2º As informações e registros obtidos pelo desenvolvimento das atividades da GSI poderão ser utilizados para detecção de violações da POSIN e normas vigentes.

Art. 6º A presente POSIN apresenta diretrizes gerais sobre as seguintes disciplinas:

I - Tratamento da Informação;

II - Tratamento de Incidentes de Rede;

III - Gestão de Riscos de SI;

IV - Gestão de Continuidade de Negócios em SI;

V - Auditoria e Conformidade;

VI - Controles de Acesso;

VII - Uso do E-mail Institucional;

VIII - Acesso à Internet;

IX - Serviço de Cópia de Segurança;

X - Gestão de Recursos Computacionais e Uso de Dispositivos Móveis;

XI - Uso de Software; e

XII - Uso de Computação em Nuvem.

Parágrafo único. Serão fixados em norma complementar os procedimentos próprios e as diretrizes específicas para as disciplinas mencionadas neste artigo.

Seção I
Do Tratamento da Informação

Art. 7º Os ativos de informação serão protegidos contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Parágrafo único. É vedado ao usuário o acesso a ativos de informação e sistemas que não tenha sido expressamente autorizado pelo Gestor da Informação.

Art. 8º Os documentos eletrônicos considerados imprescindíveis para as atividades do Instituto deverão ser armazenados nos sistemas de informação ou nos servidores de arquivos disponibilizados pela Coordenação-Geral de Tecnologia da Informação.

Parágrafo único. A destruição de documentos eletrônicos deverá observar a sua classificação, adotando procedimentos de segurança que inviabilizem eventual recuperação e acesso não autorizado.

Art. 9º As informações criadas, armazenadas, manuseadas, transportadas ou descartadas no INPI deverão ser classificadas segundo o grau de sigilo, quando necessário, e protegidas segundo a sua criticidade e outros critérios, conforme as normas e a legislação em vigor.

§ 1º As informações públicas a que se refere este artigo serão adequadamente disponibilizadas à sociedade por mecanismos próprios de transparência previstos na Lei de Acesso à Informação e em suas regulamentações infralegais.

§ 2º As informações pessoais e sigilosas geradas ou mantidas pelo INPI serão objeto de tratamento e proteção que lhes garantam a inviolabilidade

Seção II
Do Tratamento de Incidentes de Rede

Art. 10. As ocorrências de incidentes de segurança em redes computacionais, no âmbito do INPI, deverão ser registradas, com a finalidade de assegurar a manutenção de histórico das atividades desenvolvidas.

Parágrafo único. As ocorrências citadas neste artigo deverão ser comunicadas pela ETIR-INPI ao Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR.Gov).

Seção III
Da Gestão de Riscos de Segurança da Informação

Art. 11. A Gestão de Riscos de SI deverá considerar, prioritariamente, a Política de Gestão de Riscos os objetivos estratégicos, os processos, os requisitos legais e a estrutura organizacional do INPI.

§ 1º A Gestão de Riscos de Segurança da Informação deverá identificar e implementar as medidas de proteção necessárias para o tratamento dos riscos.

§ 2º Deverá ser considerado o equilíbrio entre as medidas de proteção referidas no parágrafo precedente e os custos operacionais e financeiros envolvidos, evitando que ameaças, de origem natural ou humana, de forma acidental ou não, explorem as

vulnerabilidades dos ativos de informação e provoquem danos pela destruição não autorizada, revelação indevida, adulteração ou perda das informações do Instituto.

Seção IV
Da Gestão de Continuidade de Negócios em Segurança da Informação

Art. 12. A Gestão de Continuidade de Negócios em Segurança da Informação tem como finalidade evitar que os serviços institucionais, baseados em TIC, sejam interrompidos e, quando for o caso, assegurar o seu restabelecimento no tempo necessário.

Parágrafo único. O Instituto deverá definir quais são suas atividades críticas, com o objetivo de subsidiar a elaboração do Programa de Gestão de Continuidade de Negócios.

Seção V
Da Auditoria e Conformidade

Art. 13. A Coordenação-Geral de Tecnologia da Informação deverá manter registros, como trilhas de auditoria, que possibilitem a análise de conformidade através do rastreamento, monitoramento, controle e verificação de acessos aos sistemas e atividades críticas de TIC do Instituto.

Parágrafo único. A análise de conformidade será realizada de forma contínua – utilizando técnicas como análise forense, entrevistas ou testes de invasão –, identificando possíveis violações às legislações pertinentes.

Seção VI
Dos Controles de Acesso

Art. 14. Os controles de acesso deverão observar o princípio da proporcionalidade, restringindo o conjunto de privilégios ao mínimo necessário para o desempenho das atribuições profissionais do usuário.

Art. 15. O controle de acesso físico tem como finalidade proteger os equipamentos, documentos e suprimentos contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Art. 16. O controle de acesso lógico tem como finalidade proteger os sistemas de informação e demais ativos de informação contra ameaças e ações não autorizadas, acidentais ou não, com o objetivo de reduzir os riscos e de garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

Seção VII
Do Uso do E-mail Institucional

Art. 17. A criação de contas de e-mail institucional necessita de solicitação formal, com validação e autorização da chefia imediata, demonstrando a necessidade desse serviço para o desempenho das atribuições profissionais de cada usuário, devendo ser encaminhada à Coordenação-Geral de Tecnologia da Informação.

Art. 18. A Coordenação-Geral de Tecnologia da Informação deverá adotar mecanismos para reduzir o recebimento e o envio de mensagens indesejadas (SPAM ou Phishing) que representem risco ou estejam em desconformidade com os normativos vigentes.

Seção VIII
Do Acesso à Internet

Art. 19. O acesso à Internet concedido aos usuários deverá observar o princípio da proporcionalidade, restringindo o perfil de acesso ao mínimo necessário para o desempenho das atribuições profissionais do usuário. Parágrafo único. Situações excepcionais de acessos diferenciados deverão ser motivadas pelos gestores da informação, por tempo certo, na forma de regulamentação específica dessa disciplina.

Art. 20. Os perfis institucionais em propriedades digitais deverão ser administrados e gerenciados pela Coordenação de Comunicação Social, segundo as diretrizes previstas na Política de Comunicação do INPI e nas normas editadas pela Secretaria Especial de Comunicação Social da Secretaria de Governo da Presidência da República.

Seção IX
Do Serviço de Cópia de Segurança

Art. 21. Todo ativo de informação deverá ser considerado para inclusão na política de cópia de segurança, observando-se os requisitos legais e a criticidade das informações relacionadas às atividades do INPI.

Seção X
Da Gestão de Recursos Computacionais e Do Uso de Dispositivos Móveis

Art. 22. A gestão de recursos computacionais e o uso de dispositivos móveis, de propriedade do INPI, deverão ser pautados por comportamento ético e profissional, observando as determinações da POSIN e normativos vigentes.

Parágrafo único. O uso de dispositivos móveis, de propriedade do usuário, somente será permitido nos sistemas ou serviços homologados e autorizados pela Coordenação-Geral de Tecnologia da Informação.

Seção XI
Do Uso de Software

Art. 23. A instalação e a configuração, nos recursos computacionais e dispositivos móveis institucionais, dos softwares pertencentes ao INPI, ou de versões de testes ou gratuitas, deverão ser realizadas pela CGTI, que se responsabilizará pela guarda das mídias e sua eventual desinstalação.

Parágrafo único. Para garantir a SI, todo software deverá ser previamente homologado pela CGTI antes de sua utilização no ambiente do INPI.

Seção XII
Do Uso de Computação em Nuvem

Art. 24. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem possibilitar que todas as garantias legais atribuídas ao INPI sejam respeitadas

CAPÍTULO V

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 25. O Gestor de Segurança da Informação será o Diretor Executivo ou outro Diretor designado pelo Presidente do INPI e terá as seguintes competências:

I - promover a cultura de segurança da informação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de SI executadas pela ETIR;

III - propor à autoridade máxima do INPI os recursos necessários às ações de SI;

IV - coordenar o Comitê de Segurança da Informação ou estrutura equivalente;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SI;

VI - manter contato permanente e estreito com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República para o trato de assuntos relativos à SI; e

VII - propor normas e procedimentos relativos à SI.

§1º A promoção da cultura da SI a que se refere o inciso I será atendida mediante:

I - campanhas de conscientização dos usuários em relação à relevância da SI para o Instituto, inclusive por palestras e treinamentos; e

II - interlocução permanente com a Diretoria de Administração para garantir que os usuários tomem conhecimento da POSIN e assinem o Termo de Sigilo e Responsabilidade, constante do Anexo I, no ato da admissão.

§2º A ETIR, referida no inciso II, encontra-se instituída nos termos da Resolução INPI/PR nº 168, de 21 de junho de 2016.

Art. 26. A Gestão de Segurança da Informação do INPI será realizada pelo Gestor de Segurança da Informação e pelo Comitê de Segurança da Informação ou estrutura equivalente.

Art. 27. Aos usuários compete:

I - utilizar os recursos de TIC do INPI exclusivamente para atividades relacionadas com suas atribuições funcionais;

II - responsabilizar-se pelas informações armazenadas na estação de trabalho e nos demais dispositivos móveis que utilizar para desempenho de suas funções; e

III - armazenar informações estritamente corporativas no servidor de arquivos disponibilizado para sua unidade de lotação, respeitado o processo de controle de acesso regulamentado pela CGTI.

Parágrafo único. É obrigatória a assinatura por todo usuário do Termo de Sigilo e Responsabilidade, constante do Anexo I, sobretudo para as concessões de primeiro acesso.

CAPÍTULO VI

DAS PENALIDADES

Art. 28. O descumprimento de um ou mais itens da POSIN sujeita o infrator à aplicação de sanções administrativas, penais ou civis previstas na legislação vigente.

§ 1º Sempre que instado, o INPI deverá cooperar ativamente com as autoridades competentes na apuração de possível prática de atividade ilícita realizada através dos seus recursos computacionais ou por usuário do Instituto.

§ 2º O usuário que tomar ciência de qualquer violação desta POSIN deverá comunicá-la à CGTI, que será a responsável pela análise preliminar da infração, pelas medidas de restrição de acesso cabíveis e pelo eventual encaminhamento aos órgãos de apuração competentes, tanto internos quanto externos.

CAPÍTULO VII

DA ATUALIZAÇÃO

Art. 29. A Política de Segurança da Informação deve ser revisada sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

CAPÍTULO VIII

DAS DISPOSIÇÕES FINAIS

Art. 30. A elaboração da POSIN adotou por referência o disposto na legislação e normatização elencadas no Anexo II – Referências Legais e Normativas.

Art. 31. Os casos omissos e as dúvidas surgidas na aplicação desta Política serão dirimidos pelo Comitê de Segurança da Informação.

Art. 32. Revogam-se a Instrução Normativa n.º 24, de 29 de julho de 2013 e o Anexo I da Resolução INPI/PR nº 07/2013.

Art. 33. Esta Portaria entra em vigor em 01 de julho de 2021.

CLAUDIO VILAR FURTADO
Presidente

Documento assinado eletronicamente por **CLAUDIO VILAR FURTADO**, **Presidente**, em 15/06/2021, às 18:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.inpi.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **0439219** e o código CRC **915D0A6E**.

MINISTÉRIO DA ECONOMIA
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

ANEXO I

TERMO DE SIGILO E RESPONSABILIDADE

Nome:
Empresa:
Cargo / Função / Vínculo:
Matrícula SIAPE / CPF:
Data:

Cláusula 1ª – Declaro ter conhecimento da Política de Segurança da Informação (POSIN) adotada pelo INPI para utilização dos bens e recursos de tecnologia da informação e comunicação (TIC), e me comprometo ao seu fiel cumprimento e observância.

Cláusula 2ª – Responsabilizo-me pelo correto uso dos recursos de TIC do INPI, comprometendo-me a utilizá-los somente para fins institucionais, cumprindo as determinações e recomendações contidas na POSIN e normativos vigentes.

Cláusula 3ª – Comprometo-me a manter sigilo absoluto sobre os sistemas e informações a mim confiados, bem como aos que venha a ter conhecimento em função da execução de atividades desenvolvidas para atendimento dos objetivos do Instituto.

Cláusula 4ª – Estou ciente e concordo que a utilização do e-mail institucional, da internet e demais acessos devem ocorrer em consonância com o disposto na POSIN e normativos vigentes.

Cláusula 5ª – Estou ciente de que o INPI pode monitorar o uso das informações e recursos de TIC do INPI, conforme previsto na POSIN e em suas normas complementares, sem prejuízo das ações preventivas, corretivas ou disciplinares que possam ser tomadas.

Cláusula 6ª – Estou ciente de que as senhas de acesso aos sistemas e a ambientes físicos têm caráter confidencial, pessoal e intransferível, sendo minha responsabilidade zelar pelo seu sigilo.

Cláusula 7ª – Declaro, finalmente, que tenho pleno conhecimento de que todas as minhas ações no ambiente de TIC do Instituto podem ser registradas, ciente de que o uso indevido ou fraudulento das informações e dos recursos ensejará apuração de responsabilidade, nos termos da legislação vigente.

_____

Assinatura

ANEXO II

REFERÊNCIAS LEGAIS E NORMATIVAS

I - Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais.

II - Lei n° 9.983, de 14 de julho de 2000, que dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública.

III - Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da administração pública federal, por meio da Rede Mundial de Computadores (Internet).

IV - Norma ABNT NBR/ISO/IEC 27002:2005, que institui o código de melhores práticas para Gestão de Segurança da Informação e Comunicações.

V - Norma ABNT NBR/ISO/IEC 27001:2006, que estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações.

VI - Portaria Interministerial MCT/MPOG nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores (Internet) e dá outras providências.

VII - Norma ABNT NBR/ISO/IEC 15999:2007, que institui o código de melhores práticas para Gestão de continuidade de negócios.

VIII - Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências.

IX - Norma ABNT NBR ISO/IEC 27005:2008, que fornece as diretrizes para a Gestão de Riscos de Segurança da Informação e Comunicações.

X - Norma Complementar nº 04/IN01/DSIC/GSI/PR (Revisão 01), de 15 de fevereiro de 2013, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal, direta e indireta.

XI - Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) nos órgãos e entidades da Administração Pública Federal, direta e indireta.

XII - Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009, que 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.

XIII - Norma Complementar nº 07/IN01/DSIC/GSI/PR (Revisão 01), de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta.

XIV - Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 19 de agosto de 2010, que estabelece as Diretrizes para Gestão de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

XV - Norma Complementar nº 10/IN01/DSIC/GSIPR, que 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.

XVI - Norma Complementar nº 11/IN01/DSIC/GSIPR, que 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.

XVII - Norma Complementar nº 12/IN01/DSIC/GSIPR, que 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.

XVIII - Norma Complementar nº 13/IN01/DSIC/GSIPR, que 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).

XIX - Norma Complementar nº 14/IN01/DSIC/GSIPR, que 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.

XX - Norma Complementar nº 15/IN01/DSIC/GSIPR, que 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.

XXI - Norma Complementar nº 16/IN01/DSIC/GSIPR, que estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta.

XXII - Norma Complementar nº 17/IN01/DSIC/GSIPR, que 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).

XXIII - Norma Complementar nº 18/IN01/DSIC/GSIPR, que estabelece as Diretrizes para as Atividades de Ensino em Segurança da Informação e Comunicações (SIC) nos Órgãos e Entidades da Administração Pública Federal (APF).

XXIV - Norma Complementar nº 19/IN01/DSIC/GSIPR, que estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.

XXV - Norma Complementar nº 20/IN01/DSIC/GSIPR (Revisão 01),, que 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.

XXVI - Norma Complementar nº 21/IN01/DSIC/GSIPR, que 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.

XXVII - Instrução Normativa GSI nº 2, 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.

XXVIII - Instrução Normativa GSI nº 3, de 6 de março de 2013 - 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.

XXIX - Lei nº 12.527, de 18 de novembro de 2011 – Lei de acesso à informação.

XXX - Decreto nº 7.724, de 16 de maio de 2012 – Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

XXXI - Decreto nº 7.845, de 14 de novembro de 2012 – Dispõe sobre os 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 - Decreto nº 8.777, de 11 de maio de 2016 - Institui a Política de Dados Abertos do Poder Executivo federal.

XXXIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, e altera o Decreto n.º 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei n.º 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

XXXIV - Decreto nº 9,832, de 12 de junho de 2019, que altera o Decreto nº 9.637 para dispor sobre o Comitê Gestor de Segurança da Informação.

XXXV - Instrução Normativa nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

XXXVI - Instrução Normativa nº 2, de 24 de julho de 2020, que altera a Instrução Normativa nº 1, de 27 de maio de 2020.