Boletim Pessoal XI do mês de abril de 2025 expedido em 16/04/2025

MINISTÉRIO DO DESENVOLVIMENTO, INDÚSTRIA, COMÉRCIO E SERVIÇOS
INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL

PORTARIA/INPI/PR Nº 09, DE 15 DE ABRIL DE 2025

Institui a Política de Segurança da Informação (POSIN), a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e o Comitê de Segurança da Informação (CSI), no âmbito do Instituto Nacional da Propriedade Industrial – INPI, assim como regulamenta o funcionamento da ETIR e do CSI.

O PRESIDENTE DO INSTITUTO NACIONAL DA PROPRIEDADE INDUSTRIAL - INPI, no uso das atribuições que lhe conferem o Regimento Interno, aprovado, por meio da PORTARIA/INPI/PR Nº 09, de 06 de março de 2024, tendo em vista o disposto na Norma Complementar nº 05/IN01/DSIC/GSIPR, na Norma Complementar nº 08/IN01/DSIC/GSIPR, no Decreto nº 9.637, de 26 de dezembro de 2018, na Portaria SGD/MGI nº 852/2023, na Instrução Normativa nº 1, 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 52402.004313/2022-21,

RESOLVE:

Art. 1º Ficam instituídas a Política de Segurança da Informação (POSIN), a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) e o Comitê de Segurança da Informação (CSI) no âmbito do INPI, assim como regulamentado o funcionamento da ETIR e do CSI.

Art. 2º Para os efeitos desta norma são estabelecidos os seguintes conceitos e definições:

I - Agente responsável: Servidor Público ocupante de cargo efetivo do INPI incumbido de chefiar e gerenciar a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

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

III - Artefato malicioso: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

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

V - 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;

VI - 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;

VII - 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;

VIII - Comunidade ou Público Alvo: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (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 CTIR Gov faz parte do Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR);

X - 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);

XI - 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;

XII - 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;

XIII - Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

XIV - Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

XV - Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XVI - 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;

XVII - 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;

XVIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

XIX - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas à incidentes de segurança em redes de computadores;

XX - 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;

XXI - 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;

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

XXIII - 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;

XXIV - Informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

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

XXVI - Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

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

XXVIII - 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;

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

XXX - 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;

XXXI - Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

XXXII - 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;

XXXIII - Titular do Dado: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

XXXIV - Tratamento e Resposta a Incidentes Cibernéticos: é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XXXV - 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

XXXVI - 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 I
DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Seção I

Do escopo

Art. 3º 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, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.

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.

Seção II

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;

IV - a integridade; e

V - disponibilidade, integridade, confidencialidade e autenticidade das informações.

§ 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.

Seção III

Das diretrizes gerais

Art. 5º. As ações de segurança da informação do INPI são norteadas pelas seguintes diretrizes:

I - continuidade dos processos e serviços essenciais para o funcionamento do INPI;

II - economicidade da proteção dos ativos de informação;

III - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

IV - observância da publicidade como preceito geral e do sigilo como exceção;

V - responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VI - alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do INPI, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

VII - conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

VIII - educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º 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. 7º 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 IV

Do tratamento da informação

Art. 8º 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. 9º 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. 10 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 V

Do tratamento e resposta a incidentes cibernéticos

Art. 11. As ocorrências de incidentes cibernéticos, 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 Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

Seção VI

Da gestão de riscos de segurança da informação

Art. 12. 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 VII

Da gestão de continuidade de negócios em segurança da informação

Art. 13. 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 VIII

Da auditoria e conformidade

Art. 14. 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 IX

Dos controles de acesso

Art. 15. 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. 16. 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. 17. 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 X

Do uso do e-mail institucional

Art. 18. 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. 19. 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 XI

Do acesso à internet

Art. 20. 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. 21. 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 XII

Do serviço de cópia de segurança

Art. 22. 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 XIII

Da gestão de recursos computacionais e do uso de dispositivos móveis

Art. 23. 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 XIV

Do uso de software

Art. 24. 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 XV

Do uso de computação em nuvem

Art. 25. O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem possibilitar que todas as garantias legais atribuídas ao INPI sejam respeitadas.

Seção XVI

Das competências e responsabilidades

Art. 26. O Gestor de Segurança da Informação será designado dentre os servidores públicos ocupantes de cargo efetivo com formação ou capacitação técnica compatível com as normas estabelecidas pelo Decreto nº 9.637, de 26 de dezembro de 2018, e terá as seguintes competências:

I - promover a cultura de segurança da informação;

II - acompanhar as investigações e as avaliações dos danos apontados pela ETIR, bem como a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

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.

Parágrafo único. 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.

Art. 27. 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. 28. 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.

Art. 29. Ao Encarregado pelo Tratamento dos Dados Pessoais compete, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Seção XVII

Das penalidades

Art. 30. 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.

Seção XVIII

Da atualização

Art. 31. A Política de Segurança da Informação deve ser revisada sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

CAPÍTULO II
DA EQUIPE DE PREVENÇÃO, TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS

Seção I

Do escopo

Art. 32 A Equipe De Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do INPI, ETIR-INPI, tem como missão facilitar e coordenar as atividades de tratamento e resposta a incidentes cibernéticos, atuando também de forma proativa com o objetivo de minimizar vulnerabilidades e ameaças que possam comprometer o Instituto.

Art. 33 O público alvo das atividades pertinentes à ETIR-INPI incluem:

I - Todos os servidores e colaboradores que exercem suas atividades no âmbito do INPI;

II - Demais equipes de resposta a incidentes de segurança da informação e comunicações da Administração Pública Federal;

III - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR GOV;

IV - Órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos ou convênios com o INPI para o intercâmbio de informações;

V - Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República.

Seção II

Das responsabilidades e da formação da ETIR

Art. 34 A ETIR-INPI adota o Modelo 4 – combinado ou misto, descrito na Norma Complementar nº 05/IN01/DSIC/GSIPR, para o qual será utilizada uma Equipe Central de tratamento e respostas a incidentes e equipes de apoio distribuídas pela organização.

§ 1º A Equipe Central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes Distribuídas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV.

§ 2º As Equipes Distribuídas serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.

Art. 35 A ETIR-INPI ficará subordinada ao Gestor de Segurança da Informação que também será o agente responsável.

§ 1º A Equipe Central será formada pelos servidores públicos da Divisão de Segurança da Informação e Gestão de Riscos – DISEG.

§ 2º As Equipes Distribuídas serão formadas por servidores da Coordenação-Geral de Tecnologia da Informação - CGTI com o conhecimento e o perfil necessário para atuação nas respectivas áreas de responsabilidade: sistemas de informação; banco de dados; infraestrutura e suporte de TIC.

§ 4º A investigação da causa raiz de incidentes de segurança em redes computacionais, bem como a contenção e erradicação são coordenadas pela Equipe Central, e esta deverá ser subsidiada pela equipe distribuída, independente da subordinação ou hierarquia, objetivando clareza, inviolabilidade e veracidade para registro.

§ 5º A ETIR-INPI poderá ser estendida com o apoio consultivo de representantes legais de áreas especificas do Instituto, advogados, estatísticos, recursos humanos, controle interno, consultores técnicos, grupo de investigação ou qualquer outro que a equipe entenda ser adequado para o desenvolvimento de suas atividades.

§ 6º A omissão, subtração, destruição, desfiguração, ocultação, modificação de informações ou a não preservação de evidências de incidentes que impeçam a execução das atividades da ETIR-INPI serão informadas ao Comitê de Segurança da Informação, para as providências cabíveis.

Seção III

Das competências

Art. 36 Ao agente responsável da ETIR-INPI compete:

I - Coordenar a instituição, implementação e manutenção da infraestrutura necessária a ETIR-INPI;

II - Coordenar e orientar os membros da ETIR-INPI na gestão de incidentes em redes computacionais;

III - Gerenciar as atividades, os procedimentos internos e distribuir as tarefas para os integrantes da ETIR-INPI; e

IV - Coordenar o processo de capacitação e treinamento dos membros da ETIR-INPI.

Art. 37 À Equipe Central da ETIR-INPI compete:

I - Registrar, analisar, investigar e tratar incidentes de segurança em redes computacionais;

II - Emitir relatórios de notificações sobre novas ameaças e atualizações de softwares;

III - Recomendar controles aperfeiçoados ou adicionais para limitar a frequência, os danos e os impactos de futuras ocorrências de incidentes em rede computacionais; e

IV - Estabelecer canais de comunicação com atores externos tais como o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov – da Administração Pública Federal - APF, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT Br, Centro de Atendimento a Incidentes de Segurança - CAIS - da Rede Nacional de Ensino e Pesquisa - RNP, Autoridades Legais (Ministério Público, Polícia Federal, entre outros), outras ETIRs de órgãos da APF;

V - recuperar sistemas de informação.

Art. 38 Às Equipes Distribuídas da ETIR-INPI compete:

I - Analisar, investigar e auxiliar no tratamento de incidentes de segurança em suas respectivas áreas de responsabilidade;

II - Executar procedimentos de contenção, tratamento e erradicação de incidentes de segurança em suas respectivas áreas de responsabilidade;

III - Identificar e reportar à Equipe Central a causa raiz de incidentes de segurança em suas respectivas áreas de responsabilidade; e

IV - Recomendar controles aperfeiçoados ou adicionais para limitar a frequência, os danos e os impactos de futuras ocorrências de incidentes de segurança em suas respectivas áreas de responsabilidade.

Art. 39 A autonomia da ETIR-INPI é fundamentada nas recomendações da Norma Complementar nº 05 do DSIC/GSI/PR, sendo definida como compartilhada, tendo suas decisões submetidas ao Comitê de Segurança da Informação – CSI-INPI.

§ 1º A ETIR-INPI participará, através do seu agente responsável, no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório.

§ 2º Uma vez tomada a decisão, a ETIR-INPI tem plenas condições e autonomia de adotar as medidas necessárias para a recuperação e tratamento do incidente de segurança.

§ 3º Durante um incidente de segurança em redes de computadores, se houver comprovado prejuízo à imagem institucional ou ameaça efetiva que resulte no comprometimento da segurança das informações e comunicações, a ETIR-INPI poderá tomar a decisão de executar as medidas necessárias para conter/erradicar o incidente, sem esperar pelo processo de tomada de decisão. Tão logo sejam disparadas as ações emergenciais, as instâncias superiores deverão ser informadas.

Seção IV

Dos serviços

Art. 40 A ETIR-INPI proverá, a partir de sua instituição, os seguintes serviços:

I - Prevenção, tratamento e resposta a incidentes cibernéticos – Este serviço prevê receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail abuse@inpi.gov.br;

II - Tratamento de artefatos maliciosos - Este serviço prevê o recebimento de informações ou cópia do artefato malicioso que foi utilizado no ataque ou em qualquer outra atividade maliciosa. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail abuse@inpi.gov.br;

III - Tratamento de vulnerabilidades - Este serviço prevê o recebimento de informações sobre vulnerabilidades, quer sejam em hardware ou software, objetivando analisar sua natureza, mecanismo e suas consequências e desenvolver estratégias para detecção e correção dessas

vulnerabilidades. Será prestado durante o horário de expediente normal do órgão, recebendo as notificações e solicitações através do e-mail abuse@inpi.gov.br;

IV - Detecção de intrusão - Este serviço prevê a análise do histórico de dispositivos que detectam as tentativas de intrusões em redes de computadores, com vistas a identificar e iniciar os procedimentos de resposta à incidente de segurança em redes de computadores, com base em eventos com características pré-definidas, que possam levar a uma possível intrusão e, ainda, possibilitar o envio de alerta em consonância com padrão de comunicação previamente definido entre a ETIR-INPI e o CTIR Gov;

V - Anúncios - Este serviço consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças. Será prestado durante o horário de expediente, conforme necessidade, mas sem periodicidade definida e sempre através dos mecanismos formais de comunicação da Coordenação de Comunicação Social – CCOM;

VI - Emissão de alertas e advertências - Este serviço consiste em divulgar alertas ou advertências imediatas como uma reação diante de um incidente de segurança em redes de computadores ocorrido, com o objetivo de advertir a comunidade ou dar orientações sobre como a comunidade deve agir diante do problema. Será prestado durante o horário de expediente, conforme necessidade, mas sem periodicidade definida e sempre através dos mecanismos formais de comunicação da Coordenação de Comunicação Social – CCOM;

VII - Prospecção ou monitoração de novas tecnologias - Este serviço prospecta e/ou monitora o uso de novas técnicas das atividades de intrusão e tendências relacionadas, as quais ajudarão a identificar futuras ameaças. Este serviço inclui a participação em listas de discussão sobre incidentes de segurança em redes de computadores e o acompanhamento de notícias na mídia em geral sobre o tema; e

VIII - Avaliação de segurança - Este serviço consiste em efetuar uma análise detalhada da infraestrutura de segurança em redes de computadores e de sistemas de informação do INPI, com base em requisitos da própria organização ou em melhores práticas de mercado.

CAPÍTULO III
DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO – CSI-INPI

Seção I

Da natureza

Art. 41 O Comitê de Segurança da Informação do Instituto Nacional da Propriedade Industrial (CSI-INPI), órgão colegiado permanente, de natureza consultiva e deliberativa, será regulamentado pelo presente normativo.

Seção II

Das competências

Art. 42 São competências do CSI-INPI:

I – Exercer a Governança da Segurança da Informação no âmbito do INPI;

II – Apoiar a Alta Administração e o Comitê de Governança Digital do INPI (CGD-INPI), na qualidade de órgão consultivo e deliberativo, no direcionamento dos assuntos relacionados à segurança da informação;

III – Propor normas internas relativas à segurança da informação;

IV – Propor alterações na Política de Segurança da Informação (POSIN) do INPI;

V – Assessorar na implementação das ações de segurança da informação;

VI – Constituir grupos de trabalho, em caráter temporário, para tratar de temas e propor soluções específicas sobre segurança da informação, conforme especificado no Art. 52 desta Portaria;

VII – Assessorar o INPI, na qualidade de órgão consultivo, nos assuntos relativos à segurança da informação;

VIII – Promover a incorporação de padrões elevados de conduta para a garantia da segurança da informação;

IX – Estabelecer diretrizes para o processo de Gestão de Riscos de Segurança da Informação;

X – Implementar controles internos fundamentados na Gestão de Riscos de Segurança da Informação;

XI – Avaliar as ações propostas pelo gestor de segurança da informação;

XII – Implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança da informação que impactem ou possam impactar os serviços prestados ou contratados pelo INPI; e

XIII – Assegurar a conformidade do INPI às exigências legais relacionadas à segurança da informação e promover o aprimoramento da maturidade da instituição em relação à adoção das melhores práticas de Governança de Segurança da Informação e Gestão de Segurança da Informação.

Seção III

Da composição

Art. 43 O CSI-INPI será composto pelos membros a seguir elencados:

I – Gestor de Segurança da Informação do INPI, que o coordenará;

II – Diretor Executivo;

III – Diretor de Patentes, Programas de Computador e Topografia de Circuitos Integrados;

IV – Diretor de Marcas, Desenhos Industriais e Indicações Geográficas;

V – Diretor de Administração;

VI – Coordenador-Geral de Tecnologia da Informação; e

VII – Encarregado pelo Tratamento de Dados Pessoais.

§ 1º O Gestor de Segurança da Informação será designado pela autoridade máxima do INPI por meio de ato normativo próprio, observando-se o disposto na Política de Segurança da Informação do INPI.

§ 2º A Secretaria do CSI-INPI será exercida pela Coordenação-Geral de Tecnologia da Informação – CGTI.

§ 3º Nas eventuais hipóteses de ausência, impedimento ou afastamento, os membros titulares arrolados no caput serão substituídos pelos servidores ocupantes dos cargos de substitutos nas respectivas diretorias ou coordenações-gerais, na qualidade de suplentes.

§ 4º Uma vez participando das reuniões e atividades do CSI-INPI, os suplentes gozarão dos mesmos direitos, deveres e prerrogativas dos membros substituídos.

Seção IV

Das atribuições dos membros

Art. 44 São atribuições exclusivas da Coordenação do CSI-INPI:

I – Coordenar, orientar e supervisionar as atividades do CSI-INPI;

II – Definir datas e pautas para as reuniões do CSI-INPI;

III - Convocar, presidir, suspender, prorrogar e encerrar as reuniões ordinárias e extraordinárias do CSI-INPI;

IV – Submeter ao debate e à votação as matérias a serem deliberadas, apurando os votos e proclamando os resultados;

V – Decidir em caso de empate, utilizando o voto de desempate;

VI – Assinar documentos, atas das reuniões e proposições do CSI-INPI;

VII – Indicar membros para Grupos de Trabalho, visando à realização de estudos, levantamentos, investigações e emissão de pareceres necessários à consecução da finalidade do CSI-INPI, bem como relatores das matérias a serem apreciadas;

VIII – Indicar técnicos ou representantes de unidades administrativas do INPI, e também agentes externos, que possam contribuir com esclarecimentos e prover subsídios sobre as matérias constantes da pauta ou desenvolvimento das atividades do CSI-INPI, sem direito a voto;

IX - Requisitar informações e diligências necessárias à execução das atividades;

X – Expedir, *ad referendum* do Comitê, normas complementares relativas ao seu funcionamento e à ordem dos trabalhos, bem como atos administrativos, em vista de circunstâncias de urgência, ficando o tema obrigatoriamente inscrito na pauta da próxima reunião;

XI – Designar servidores responsáveis pelos trabalhos de apoio operacional e administrativo às reuniões do CSI-INPI; e

XII – Decidir questões de ordem.

Art. 45 São atribuições da Secretaria do CSI-INPI:

I – Auxiliar o Coordenador do CSI-INPI na coordenação, orientação e supervisão das atividades;

II – Propor calendário de reuniões;

III – Elaborar e apresentar a pauta de reunião;

IV – Organizar e distribuir documentos correlatos à pauta da reunião;

V – Encaminhar minutas de resoluções do CSI-INPI à Consultoria Jurídica;

VI – Lavrar as resoluções e as atas das reuniões e encaminhá-las aos demais membros; e

VII – Organizar, manter e disponibilizar os documentos correlatos ao CSI-INPI.

Art. 46 São atribuições de todos os membros do CSI-INPI:

I – Representar sua área nas reuniões ordinárias e extraordinárias do CSI-INPI;

II – Aprovar o calendário de reuniões;

III – Analisar, debater e votar as matérias em deliberação;

IV – Revisar as minutas de documentos apresentadas ao CSI-INPI;

V – Cumprir e fazer cumprir as decisões do CSI-INPI;

VI – Propor inclusão de matérias de interesse da área na pauta de reunião;

VII – Realizar estudos e pesquisas, apresentar proposições, apreciar, emitir pareceres e relatar as matérias que lhes forem submetidas pela Coordenação do CSI-INPI;

VIII – Sugerir normas e procedimentos necessários ao bom funcionamento das atividades;

IX – Propor e requerer esclarecimentos que lhes forem úteis à melhor apreciação das matérias em pauta;

X – Indicar técnicos ou representantes de unidades administrativas do INPI, e também agentes externos, que possam contribuir com esclarecimentos e prover subsídios sobre as matérias constantes da pauta ou desenvolvimento das atividades do CSI-INPI, sem direito a voto;

XI – Solicitar à Secretaria do CSI-INPI informações e documentos necessários ao desempenho das atividades;

XII – Comunicar à Coordenação do CSI-INPI, com antecedência, a impossibilidade do seu comparecimento à reunião;

XIII – Apreciar as decisões da Coordenação do CSI-INPI tomadas *ad referendum* em questões de urgência;

XIV – Assinar as resoluções e as atas das reuniões; e

XV – Propor a realização de reuniões extraordinárias.

Seção V

Do funcionamento

Art. 47 As reuniões do CSI-INPI serão realizadas com a seguinte periodicidade:

I – Ordinariamente, 4 (quatro) vezes ao ano, mediante convocação da Coordenação do CSI-INPI a ser feita 1 (uma) vez a cada trimestre, com antecedência mínima de 14 (quatorze) dias; e

II – Extraordinariamente, mediante convocação da Coordenação do CSI-INPI ou proposição formulada por quaisquer de seus membros, com antecedência mínima de 7 (sete) dias.

Art. 48 A convocação das reuniões deverá ser feita pela Coordenação do CSI-INPI, via e-mail institucional, que indicará:

I – Pauta;

II – Data;

III – Modalidade:

a) Presencial, na sede do INPI, na cidade do Rio de Janeiro;

b) Remota, mediante a indicação das informações para acesso à plataforma de videoconferência; ou

c) Híbrida, com a possibilidade de participação dos membros por meio de quaisquer das modalidades;

IV – Horário com previsão de início e término; e

V – Documentos complementares e modo de acesso ao conteúdo (se aplicável).

§ 1º A convocação para as reuniões deverá ser encaminhada pela Coordenação do CSI-INPI aos membros titulares e aos seus respectivos suplentes.

§ 2º Os membros do CSI-INPI poderão encaminhar à Secretaria, com antecedência mínima de 1 (um) dia útil, solicitações de inclusão de matérias na pauta, as quais serão reportadas aos demais membros quando da abertura da reunião pela Coordenação.

Art. 49 O quórum mínimo necessário para abertura e realização das reuniões do CSI-INPI, sejam ordinárias ou extraordinárias, é o correspondente à totalidade dos membros, independentemente se titulares ou suplentes, exceto nas hipóteses de vacância total do cargo.

Art. 50 O CSI-INPI emitirá pareceres e deliberará sobre todo e qualquer assunto relacionado à segurança da informação nos âmbitos estratégico, tático e operacional.

§ 1º Caso haja subcomitê constituído a respeito da matéria submetida à consulta ou deliberação, a votação deverá ser suspensa para que os membros do respectivo subcomitê integrem o quórum do CSI-INPI para votação.

§ 2º As votações no âmbito do CSI-INPI serão sempre nominais, abertas e iniciadas pelo Gestor de Segurança da Informação, que deverá fazer a relatoria do tema proposto e, em seguida, declarar seu voto.

§ 3º Todas as deliberações do CSI-INPI se darão por maioria simples, cabendo à Coordenação o exercício do voto adicional de desempate, quando necessário.

§ 4º Não será permitida a abstenção ao voto em relação às matérias em deliberação por nenhum dos membros do CSI-INPI.

Art. 51 Os pareceres e deliberações do CSI-INPI, acompanhados dos encaminhamentos correspondentes, deverão ser registrados em atas com lista de participantes, a serem publicadas pela Secretaria em repositório do CSI-INPI e disponibilizadas para consulta pública, exceto quando o conteúdo contemplar informações classificadas como não públicas pela legislação aplicável ou pelas diretrizes de segurança da informação do INPI.

Parágrafo único. As atas do CSI-INPI serão disponibilizadas aos membros do CSI, no prazo máximo de 5 dias úteis após a reunião, para solicitação de eventuais complementos e correções à Secretaria, que deverá providenciá-las em igual período, para posterior assinatura.

Seção VI

Dos grupos de trabalho

Art. 52 O CSI-INPI poderá determinar a criação de Grupos de Trabalho para endereçar assuntos específicos de segurança da informação de interesse do INPI, tanto com natureza de apoio administrativo, quanto de apoio técnico em relação a questões que demandem estudos e análises especializadas.

§ 1º Os Grupos de Trabalho de que trata o *caput* terão caráter temporário e duração não superior a um ano, sendo compostos por, no máximo, sete membros.

§ 2º Caberá à Coordenação do CSI-INPI determinar qual dos membros será responsável por exercer a coordenação dos Grupos de Trabalho com natureza de apoio técnico (relatoria), bem como por definir seus integrantes.

§ 3º O quórum mínimo necessário para abertura e realização das reuniões dos Grupos de Trabalho é o correspondente à totalidade de seus membros.

§ 4º Todas as deliberações dos Grupos de Trabalho se darão por maioria simples, cabendo à coordenação de cada Grupo de Trabalho o exercício do voto adicional de desempate, quando necessário.

§ 5º A criação e a disciplina dos Grupos de Trabalho, especialmente no que diz respeito ao escopo, prazo de conclusão e abrangência das atividades, serão publicadas pelo INPI, em normativo próprio, conforme as definições do CSI-INPI.

§ 6º É vedado o funcionamento simultâneo de mais de dois Grupos de Trabalho.

CAPÍTULO IV
DAS DISPOSIÇÕES FINAIS

Art. 53 Os casos omissos e as dúvidas surgidas na aplicação da POSIN e da ETIR serão dirimidos pelo Comitê de Segurança da Informação.

Art. 54 O Coordenador do CSI-INPI poderá convidar representantes de outros órgãos e entidades, externos ao INPI, para participar das reuniões sem direito a voto.

Art. 55 Em havendo convidados externos ao INPI nas reuniões do CSI-INPI, a permanência dos mesmos deverá ser limitada ao tempo necessário à apresentação dos esclarecimentos solicitados por ocasião da formulação do convite, sendo vedada a participação ou acompanhamento das discussões de deliberação.

Art. 56 As propostas de alteração das normas de funcionamento do CSI-INPI deverão ser formuladas por escrito, inseridas em pauta e submetidas à apreciação pelo CSI-INPI.

Art. 57 Dada a especificidade da matéria, na eventual hipótese de conflito, as disciplinas inerentes ao CSI-INPI prevalecerão em detrimento daquelas relativas ao Comitê de Governança Digital do INPI.

Art. 58 Os casos omissos relacionados à interpretação e aplicação do presente normativo serão resolvidos *ad referendum* pelo Coordenador do CSI-INPI e, automaticamente, incluídos na pauta da próxima reunião do CSI-INPI para deliberação.

Art. 59 Fica revogada a portaria/INPI/PR Nº 65, de 1º DE setembro DE 2022.

Art. 60 Esta Portaria entra em vigor na data da sua publicação.

JÚLIO CÉSAR CASTELO BRANCO REIS MOREIRA
Presidente

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