§ 4º As diretrizes acerca da gestão de riscos de segurança da informação devem estar alinhadas à Política de Gestão de Riscos do ITI e serão objeto de regulamentação específica pelo SGDSI.

Seção V - Gestão de Incidentes

Art. 31 A gestão de incidentes em segurança da informação e violações à privacidade tem por objetivo assegurar que fragilidades e incidentes de segurança da informação, que tratem ou não dados pessoais (violações à privacidade), sejam identificados, para permitir a tomada de ação corretiva em tempo hábil, bem como a melhoria de controles e processos de segurança da informação.

§ 1º Os incidentes notificados ou detectados deverão ser registrados, classificados de acordo com sua relevância e priorizados pela equipe responsável por seu tratamento.

§ 2º Durante o gerenciamento de incidentes de segurança da informação, havendo indícios de ilícitos criminais, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) em como dever acionar as autoridades competentes para a adoção dos procedimentos legais julgados necessários, observar os procedimentos para preservação das evidências e priorizar a continuidade dos serviços do ITI.

§ 3º Autoridades, servidores, colaboradores do Instituto e quaisquer pessoas que tenham acesso a informações do ITI serão responsáveis por informar imediatamente à ETIR os incidentes em segurança da informação de que tenham ciência ou suspeita, e colaborar, na respectiva área de competência, na identificação e no tratamento de incidentes.

Seção VI - Gestão de Continuidade de Negócios, Segurança em Tecnologia da Informação e Comunicações

Art. 32 A gestão de continuidade de negócios em segurança da informação tem por objetivo garantir níveis adequados de disponibilidade, integridade, confidencialidade e autenticidade das informações essenciais ao funcionamento dos processos críticos de negócio do ITI.

§ 1º O ITI deverá elaborar e manter Programa de Gestão de Continuidade de Negócios (GCN), composto por:

I. Plano de Gerenciamento de Incidentes de Segurança da Informação;

II. Plano de Continuidade e Recuperação de Tecnologia da Informação e Comunicações;

§ 2º Os planos definidos no parágrafo anterior deverão ser avaliados, testados e revisados periodicamente, visando a reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Art. 33 A segurança em tecnologia da informação e comunicações tem por objetivo adotar medidas e controles tecnológicos para proteger as informações, inclusive em meio eletrônico.

§ 1º Diretrizes e procedimentos para o uso de ativos de informação e serviços digitais sujeitam-se, no que couber, aos comandos desta POSIN-ITI, e serão objeto de regulamentação especifica pelo SGDSI.

§ 2º O acesso aos dados e informações produzidas ou custodiadas pelo ITI se submete a controles administrativos e tecnológicos definidos de acordo com a respectiva classificação.

§ 3º A utilização dos ativos de informação e de rede ITI pode ser monitorada pela unidade responsável pela Tecnologia da Informação com vistas a identificar inobservâncias a esta POSIN-ITI e a fornecer evidências no caso de incidentes de segurança da informação, respeitados os direitos e as garantias individuais previstos em lei.

§ 4º Os sistemas de informação desenvolvidos, internalizados e mantidos pelo ITI devem ter sua segurança especificada, analisada e testada em todo seu ciclo de vida e estar em conformidade com os requisitos contratuais e a legislação em vigor.

§ 5º O desenvolvimento e disponibilização de softwares devem:

I. Buscar, de maneira escalonada, a padronização e uniformização dos ambientes de desenvolvimento, homologação e produção do ITI;

II. Buscar a incorporação de princípios de segurança por design e por padrão;

III. Buscar a incorporação de princípios de privacidade por design e por padrão.

Seção VII - Uso Seguro e Responsável da Inteligência Artificial

Art. 34 Os sistemas de inteligência artificial (IA), em uso ou em desenvolvimento, devem ter responsáveis designados, cabendo a eles monitorarem a utilização e o desenvolvimento de forma segura e responsável a fim de garantir o alinhamento com os objetivos estratégicos do ITI.

§ 1º A gestão de riscos relacionados ao uso de inteligência artificial deve ser realizada de maneira contínua, abrangendo as fases de análise, avaliação e tratamento, alinhando-se às diretrizes de IA responsável disponíveis.

§ 2º Os sistemas de IA, que apresentem riscos relevantes, devem passar por análise de impacto algorítmico (AIA), e as recomendações provenientes dessa análise devem ser acompanhadas dentro de um programa de monitoramento formal.

§ 3º O ITI compromete-se a não publicar ou explorar modelos de inteligência artificial que possam causar danos à democracia, gerar desinformação, relacionar-se a armamentos ou violência física, promover vigilância massiva estatal ou privada ou violar direitos fundamentais dos cidadãos.

§ 4º Para assegurar a segurança e a conformidade, será estabelecido um programa de monitoramento contínuo das soluções de inteligência artificial, capaz de detectar e responder a comportamentos suspeitos ou anômalos.

§ 5º As aplicações de inteligência artificial devem implementar controles que garantam a conformidade com as normatizações aplicáveis, prevendo mecanismos de segurança e privacidade que protejam os dados e evitem exposições indevidas de usuários ou terceiros.

§ 6º As diretrizes acerca da implementação de sistemas de IA de forma segura, confiável e responsável serão objeto de regulamentação específica pelo SGDSI.

CAPÍTULO V - VEDAÇÕES E PENALIDADES

Art. 35. É vedada a utilização ativos de informação e de rede disponibilizados pelo ITI para acesso, guarda e divulgação de material incompatível que viole direitos autorais ou que infrinja a legislação vigente.

§1º São vedados o uso, a instalação e a configuração de ativos de informação não autorizados ou permitidos pelo ITI.

§ 2º É vedada a divulgação ou transferência a terceiros de mecanismos de identificação, autenticação e autorização baseados em usuário e senha ou certificação digital, de uso pessoal e intransferível, fornecidos pelo ITI aos seus servidores ou colaboradores.

§ 3º É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas à ETIR assim que identificadas.

§ 4º Compete ao SGDSI estabelecer os requisitos e procedimentos para o uso, instalação e configuração de ativos de informação, a que se refere o §1º.

Art. 36. As denúncias de violação a esta POSIN-ITI devem ser comunicadas à ETIR através dos canais oficiais de comunicação do ITI.

Art. 37. O uso indevido dos recursos tecnológicos ou o descumprimento desta política, causando ou não algum tipo de prejuízo à segurança da informação ou à privacidade de dados pessoais, resultará na aplicação de sanção prevista em normativos internos e na legislação vigente.

Parágrafo único. A não observância dos dispositivos desta POSIN-ITI sujeita os infratores, isolada ou cumulativamente, a sanções administrativas, civis e penais, nos termos da legislação pertinente, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VI - DISPOSIÇÕES FINAIS

Art. 38 As informações produzidas por qualquer pessoa com vínculo permanente ou transitório com o Instituto que tenha acesso, de forma autorizada, às informações ou às dependências do ITI, no exercício de suas atribuições, são patrimônio intelectual do Instituto e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o reconhecimento da autoria, se for o caso.

Art. 39 Esta Política será revisada periodicamente, no mínimo a cada quatro (4) anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente do ITI, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 40 Os casos omissos e as dúvidas sobre esta POSIN-ITI e seus normativos correlatos devem ser submetidos para avaliação do Gestor de Segurança da Informação (GSI).

Art. 41 As adequações às determinações estabelecidas nessa POSIN-ITI devem ser planejadas e implementadas de maneira escalonada e gradativa em planos de ação específicos, elaborados por cada diretoria do ITI, cujo prazo de conclusão não excederá a dois (2) anos.

Parágrafo único. Os planos de ações das diretorias serão apresentados ao SGDSI e submetidos à aprovação pelo CGE.

Art. 42 Esta Minuta de Portaria entra em vigor na data de sua publicação.

ENYLSON FLAVIO MARTINEZ CAMOLESI

[MODELO] TERMO DE CONHECIMENTO E RESPONSABILIDADE (TCR)

Pelo presente Termo, na qualidade de USUÁRIO ou CUSTODIANTE de informações do Instituto Nacional de Tecnologia da Informação (ITI), declaro:

1. DO CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1.1. Declaro ter pleno CONHECIMENTO da Política de Segurança da Informação do ITI (POSIN-ITI), suas normas es e procedimentos correlatos.

2. DAS CREDENCIAIS DE ACESSO

2.1. Declaro que, mediante autorização superior, estou recebendo credenciais de acesso com privilégios adequados ao exercício de minhas atividades funcionais, comprometendo-me a utilizá-las exclusivamente para tal finalidade.

2.2. Comprometo-me a não compartilhar, divulgar ou transferir minhas credenciais de acesso a terceiros, sob qualquer circunstância.

3. DO COMPROMISSO DE SIGILO

3.1. Comprometo-me a manter sigilo absoluto sobre todas as informações a que tiver acesso em razão de minhas atividades, sejam elas classificadas, sensíveis ou de uso interno, não as divulgando a terceiros não autorizados.

3.2. O compromisso de sigilo permanece válido mesmo após o término do vínculo funcional com o ITI, por prazo indeterminado, salvo quando a informação for tornada pública por meio oficial.

3.3. Comprometo-me a observar os preceitos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) no tratamento de dados pessoais a que tiver acesso.

4. DO MONITORAMENTO E AUDITORIA

4.1. Declaro estar ciente de que minhas ações nos sistemas e recursos de tecnologia da informação do ITI poderão ser monitoradas, registradas e auditadas, em conformidade com a POSIN-ITI e a legislação vigente.

4.2. Reconheço que toda ação realizada mediante minha autenticação e autorização é de minha inteira responsabilidade.

5. DAS RESPONSABILIDADES

5.1. Comprometo-me a não realizar, por iniciativa própria, qualquer tentativa de modificação da configuração, física ou lógica, dos recursos computacionais do ITI sem a devida autorização da área técnica competente.

5.2. Responsabilizo-me pelos danos que vier a causar ao ITI, a terceiros ou à Administração Pública em decorrência do descumprimento das normas estabelecidas na POSIN-ITI e neste Termo.

6. DAS SANÇÕES

6.1. Declaro estar ciente de que o descumprimento das obrigações aqui assumidas poderá ensejar a aplicação de sanções administrativas, civis e penais cabíveis, nos termos da legislação vigente.

7. DISPOSIÇÕES FINAIS

7.1. Este Termo entra em vigor na data de sua assinatura e permanece válido durante todo o período de vínculo com o ITI e, no que tange ao sigilo, por prazo indeterminado após seu término.

7.2. Declaro, por fim, ter lido e compreendido integralmente o conteúdo deste Termo, aceitando todas as suas condições.

Brasília - DF, _____ de _____ de _____.

Nome: _____

CPF: _____ Lotação_____

E-mail institucional: _____

_____

Assinado Eletronicamente

PORTARIA Nº 2, DE 9 DE JANEIRO DE 2026

Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos no âmbito do Instituto Nacional de Tecnologia da Informação (ETIR-ITI).

O DIRETOR-PRESIDENTE DO INSTITUTO NACIONAL DE TECNOLOGIA DA INFORMAÇÃO - ITI, no uso das atribuições que lhe conferem o inciso VI do art. 13 do Decreto nº 12.103, de 8 de julho de 2024, o disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), Decreto nº 12.572, de 04 de agosto de 2025 (Política Nacional de Segurança da Informação - PNSI) e no Decreto nº 10.748, de 16 de julho de 2021 (Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC), e o que consta no Processo Administrativo nº 00100.002790/2025-04, resolve:

CAPÍTULO I - DA INSTITUIÇÃO, FINALIDADE E ABRANGÊNCIA

Art. 1º Fica instituída, em caráter permanente, a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Instituto Nacional de Tecnologia da Informação, denominada ETIR-ITI.

Art. 2º A ETIR-ITI tem por missão coordenar e executar as ações de prevenção, detecção, análise e resposta a incidentes cibernéticos e violações à privacidade que possam comprometer os ativos de informação, a continuidade dos serviços negociais e a integridade dos dados, pessoais ou não, do ITI ou sob sua custódia.

Art. 3º. Para efeito desta Portaria, aplicam-se os termos e definições constantes no Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021 e nas normas técnicas ABNT NBR ISO/IEC da família 27000.

Parágrafo único. A ETIR-ITI integra a Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), devendo atuar em conformidade com as normas estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov).

CAPÍTULO II - DA COMPOSIÇÃO E ORGANIZAÇÃO

Art. 3º A ETIR-ITI adotará o Modelo Misto (combinado e descentralizado) de atuação, sendo composta por uma Coordenação Central e Equipes Distribuídas, conforme a seguinte estrutura:

I - Coordenação Central:

a) Agente Responsável pela ETIR (Coordenador);

b) Encarregado pelo Tratamento de Dados Pessoais;

c) Gestor de Segurança da Informação (GSI);

d) Um representante titular da Diretoria de Infraestrutura Tecnológica (DITEC).

II - Equipes Distribuídas - Oficiais de Segurança da Informação e de Resposta a Incidentes (OSIRI):

a) Um representante da Diretoria de Auditoria, Fiscalização e Normalização (DAFN);

b) Um representante da Diretoria de Tecnologias de Identificação (DITI);

c) Um representante da Diretoria de Planejamento, Orçamento e Administração (DPOA);

d) Um representante do Gabinete da Presidência (GABIN).

§ 1º O Agente Responsável pela ETIR será designado formalmente por ato do Diretor-Presidente.

§ 2º A participação na ETIR-ITI é considerada serviço público relevante, não remunerado, e será exercida sem prejuízo das atribuições regulares do cargo do servidor.

§ 3º Os indicados para atuar nas equipes distribuídas devem ser, preferencialmente, os Oficiais de Segurança da Informação e de Resposta a Incidentes (OSIRI) conforme previsto na POSIN-ITI.

§ 4º Os membros titulares e suplentes da ETIR-ITI terão prioridade nas capacitações, eventos e intercâmbios dentro do planejamento anual de capacitação do ITI, desde que relacionados às suas atividades e competências.

CAPÍTULO III - DAS COMPETÊNCIAS E AUTONOMIA

Art. 4º Compete à ETIR-ITI:

I - Atuar como ponto focal único para o recebimento de notificações de incidentes cibernéticos e violações de dados pessoais no âmbito do ITI;

II - Realizar a triagem, classificação de severidade e análise técnica de incidentes;

III - Coordenar as ações de contenção, erradicação e recuperação de serviços afetados;

IV - Elaborar relatórios técnicos e gerenciais sobre os incidentes, incluindo lições aprendidas;

V - Disseminar alertas e recomendações de segurança para a comunidade interna do ITI.