Art. 5º A ETIR-ITI possui Autonomia Operacional para a tomada de decisões técnicas imediatas necessárias à contenção e recuperação de incidentes, visando minimizar danos aos serviços negociais e aos dados, pessoais ou não, sob custódia da Autarquia.

Parágrafo único. As ações tomadas em regime de autonomia devem ser comunicadas imediatamente à Alta Administração e posteriormente documentadas.

CAPÍTULO IV - DA COMUNICAÇÃO E NOTIFICAÇÃO

Art. 6º A comunicação de incidentes deverá observar os seguintes fluxos obrigatórios:

I - Ao CTIR Gov: A ETIR-ITI deve comunicar imediatamente ao CTIR Gov a ocorrência de incidentes cibernéticos relevantes que impactem serviços da APF, conforme normativos vigentes.

II - À ANPD: Em conformidade com a Resolução CD/ANPD nº 15/2024, o incidente de segurança que envolva dados pessoais e possa acarretar risco ou dano relevante aos titulares deve ser comunicado à Autoridade Nacional de Proteção de Dados (ANPD) no prazo de 3 (três) dias úteis, contados da confirmação do evento.

III - Ao CISC Gov.br: Para fins de coordenação operacional no âmbito do SISP, a ETIR-ITI deverá interagir e compartilhar informações técnicas com o Centro Integrado de Segurança Cibernética do Governo Digital.

CAPÍTULO V - DAS DISPOSIÇÕES FINAIS

Art. 7°. A Alta Administração proverá os recursos necessários para o funcionamento da ETIR-ITI, em conformidade com a Instrução Normativa GSI/PR nº 1, de 2020.

Art. 8º O ITI adotará o protocolo Traffic Light Protocol (TLP) versão 2.0 (ou superior) para a classificação e compartilhamento de informações sensíveis sobre incidentes.

Art. 9º O Plano de Gestão de Incidentes Cibernéticos do ITI, contendo os modelos e fluxos detalhados de resposta, deverá ser publicado em até 90 (noventa) dias a partir da publicação desta Portaria, alinhado ao Plano de Gestão de Incidentes Cibernéticos (PlanGIC) da Administração Pública Federal.

Art. 10º Esta Portaria entra em vigor na data de sua publicação.

ENYLSON FLAVIO MARTINEZ CAMOLESI

Ministério da Igualdade Racial

GABINETE DA MINISTRA

PORTARIA GAB/MIR Nº 11, DE 9 DE JANEIRO DE 2026

Institui a Política de Segurança da Informação no âmbito do Ministério da Igualdade Racial e estabelece outras providências.

A MINISTRA DE ESTADO DA IGUALDADE RACIAL, no uso das atribuições conferidas pelo inciso II do parágrafo único do art. 87 da Constituição Federal, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018, com o Decreto nº 12.572, de 4 de agosto de 2025, com o Decreto nº 12.573, de 4 de agosto de 2025, e com a Instrução Normativa PR/GSI nº 1, de 27 de maio de 2020, resolve:

Art. 1º Aprovar a Política de Segurança da Informação do Ministério da Igualdade Racial - POSIN, na forma do Anexo Único.

Art. 2º A POSIN e suas normas complementares serão revisadas dentro do intervalo máximo de 4 (quatro) anos ou sempre que ocorrerem mudanças significativas que afetem a base de avaliação de risco original ou em decorrência de alterações normativas e tecnológicas.

Art. 3º A POSIN, suas atualizações e as demais normas e instrumentos correlatos serão disponibilizados pelo endereço eletrônico https://www.gov.br/ igualdaderacial/pt-br/acesso-a-informacao/privacidade-e-dados-pessoais-1.

Art. 4º Esta portaria entra em vigor na data de sua publicação.

ANIELLE FRANCISCA DA SILVA

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO MINISTÉRIO DA IGUALDADE RACIAL

CAPÍTULO I - DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Art. 1º A Política de Segurança da Informação - POSIN do Ministério da Igualdade Racial - MIR tem por objetivo estabelecer diretrizes, normas, responsabilidades e competências destinadas a garantir a proteção das informações tratadas e custodiadas pelo órgão, assegurando sua integridade, disponibilidade, confidencialidade, autenticidade e conformidade com a legislação e regulamentação vigentes.

Art. 2º A POSIN aplica-se a todas as autoridades, servidores, colaboradores, prestadores de serviços, estagiários e terceiros que, de qualquer forma, acessem, tratem ou utilizem os ativos de informação do MIR, constituídos pelos equipamentos, sistemas e outros meios de armazenamento, transmissão e processamento de informações, bem como os locais onde se encontram esses meios, os recursos humanos que a eles têm acesso e o conhecimento ou dado que tem valor para o MIR.

Art. 3º Aplicam-se as definições constantes do Glossário de Segurança da Informação aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, e suas atualizações.

CAPÍTULO II - DOS OBJETIVOS

Art. 4º São objetivos da Política de Segurança da Informação:

I - proteger as informações tratadas pelo MIR, em qualquer meio ou formato;

II- prevenir incidentes de segurança e danos a pessoas, sistemas e ao órgão;

III - assegurar a conformidade com as normas sobre segurança da informação, cibersegurança, governança de dados, privacidade e tratamento de dados pessoais e acesso à informação e outras sobre temas correlatos;

IV - definir controles e medidas de gestão de riscos relacionados à segurança da informação e temas correlatos;

V - estabelecer mecanismos de resposta a incidentes e continuidade das operações;

VI - promover a conscientização e o treinamento contínuo em segurança da informação; e

VII - fortalecer a governança e a cultura organizacional de segurança, privacidade e proteção de dados pessoais e cibersegurança;

CAPÍTULO III - PRINCÍPIOS

Art. 5º A POSIN é orientada pelos seguintes princípios:

I - necessidade de conhecer;

II - privilégio mínimo;

III - defesa em profundidade;

IV - proteção de dados pessoais e da privacidade;

V - gestão de riscos e melhoria contínua;

VI - simplicidade e objetividade dos controles;

VII - educação e cultura de segurança;

VIII - transparência e responsabilidade; e

IX - articulação entre segurança cibernética, defesa cibernética e proteção de dados.

CAPÍTULO IV - DAS DIRETRIZES GERAIS

Art. 6º As normas e procedimentos complementares deverão abordar, no mínimo:

I - tratamento e classificação da informação;

II - segurança física e lógica;

III - gestão de ativos e acessos;

IV - gestão de riscos e continuidade;

V - gestão de incidentes;

VI - auditoria, conformidade e registro de logs;

VII - uso de recursos tecnológicos e comunicações;

VIII - capacitação e conscientização contínua.

CAPÍTULO V - DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

Art. 7º A governança da segurança da informação no MIR compreende:

I - a alta administração;

II - o Comitê Gerencial de Segurança da Informação - CGSI;

III - o gestor de segurança da informação;

IV - a Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética - ETIR-C; e

V - o encarregado pelo tratamento de dados pessoais.

CAPÍTULO VI - DAS RESPONSABILIDADES

Art. 8º Compete à alta administração:

I - aprovar e divulgar a POSIN;

II - tomar as decisões, implementar as medidas e prover os recursos que sejam necessários à execução da POSIN, especialmente em relação à gestão dos riscos à segurança da informação e privacidade e à catalogação, inventário e curadoria de dados;

III - zelar pela inclusão de cláusulas de segurança nos contratos;

IV - promover cultura institucional de proteção de dados e segurança da informação; e

V - aprovar os demais planos, normas e diretrizes e supervisionar sua execução.

Art. 9º Compete ao CGSI:

I - viabilizar a coordenação da implementação e do monitoramento da POSIN e dos demais componentes da governança de segurança da informação; e

II - deliberar sobre normas complementares, riscos, indicadores e resultados da POSIN; e

III - promover integração com o Comitê de Governança de Tecnologia da Informação e Comunicação e de Dados.

Art. 10. Compete ao gestor de segurança da informação:

I - realizar a coordenação técnica e a integração entre os demais componentes da governança da segurança da informação;

II - conduzir os diagnósticos necessários à segurança da informação, bem como orientar, planejar e monitorar as medidas de segurança da informação.

Art. 11. Compete à ETIR-C:

I - monitorar incidentes e ameaças cibernéticas;

II - registrar, classificar e responder aos incidentes;

III - manter histórico e relatórios periódicos ao CGSI; e

IV - cooperar com a Agência Nacional de Proteção de Dados - ANPD e órgãos de controle quando aplicável.

Art. 12. Compete ao Encarregado pelo Tratamento de Dados Pessoais:

I - receber comunicações da ANPD e dos titulares de dados;

II- participar da formulação e adoção das medidas corretivas com o gestor de segurança da informação e a ETIR-C;

III - conduzir as medidas relativas ao diagnóstico de privacidade, bem como orientar os agentes sobre o planejamento, implementação e monitoramento das medidas de privacidade; e

IV - supervisionar o inventário de dados pessoais.

Art. 13. Todos os servidores, colaboradores e prestadores de serviço devem:

I - cumprir esta Política e as normas complementares;

II - reportar imediatamente incidentes de segurança;

III - utilizar os ativos de informação de forma ética e institucional;

IV - participar dos treinamentos.

CAPÍTULO VII - DA RESPOSTA E DA COMUNICAÇÃO DE INCIDENTES

Art. 14. As medidas de resposta a incidentes de segurança de informação, de cibersegurança e de privacidade devem observar as normas, procedimentos e prazos estabelecidos pela ANPD, pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, pelo Ministério da Gestão e Inovação em Serviços Públicos - MGI, pela Controladoria-Geral da União - CGU e por outros órgãos supervenientes que venham a atuar como responsáveis pela orientação normativa e supervisão de medidas relacionados aos assuntos desta Política.

§ 1º Os incidentes de segurança relacionados a dados pessoais verificados a partir de procedimentos de apuração ou informados pelo recebimento de comunicações serão notificados pelo encarregado de dados pessoais à ANPD e aos titulares de dados pessoais com base nas normas e regulamentos aplicáveis.

§ 2º O MIR adotará as demais normas necessárias para resposta e tratamento de incidentes que especifique os procedimentos, prazos, registros e responsabilidades dos componentes da governança da segurança da informação.

CAPÍTULO VIII - DA GESTÃO DE RISCOS E DO ACESSO À INFORMAÇÃO

Art. 15. O MIR adotará metodologia formal de Gestão de Riscos de Segurança da Informação em consonância com a Política de Gestão de Riscos e Controles Interno e ao Plano de Gestão de Riscos, abrangendo:

I - identificação, análise e avaliação de riscos;

II - definição de medidas de tratamento e aceitação de riscos residuais; e

III - manutenção de registro atualizado dos riscos e dos responsáveis por seu tratamento.

Art. 16. É garantido o acesso público às informações sob custódia do MIR, observadas as exceções elencadas nos artigos 7º, §3º, 22, 23 e 31 da Lei nº 12.527, de 11 de novembro de 2011, e no artigo 13 do Decreto nº 7.724, de 16 de maio de 2012.

CAPÍTULO IX - DA CONTINUIDADE DO NEGÓCIO E DA AUDITORIA

Art. 17. O MIR elaborará e manterá planos e medidas de continuidade de negócio, mitigação e recuperação de incidentes e desastres, que serão revisados periodicamente e testados sempre que houver alteração relevante na infraestrutura tecnológica.

Art. 18. A execução das ações e controles previstos nesta Política estão sujeitos à auditoria do Sistema de Controle Interno do Poder Executivo Federal.

CAPÍTULO X - DAS PENALIDADES

Art. 19. Ações que violem esta Política, normas ou controles de segurança correlatos estarão sujeitas às sanções disciplinares, civis e penais cabíveis, conforme legislação vigente.

CAPÍTULO XI - DAS DISPOSIÇÕES FINAIS

Art. 20. A POSIN, suas normas complementares e planos associados deverão ser amplamente divulgados por meio eletrônico e institucional.

Art. 21. Casos omissos serão resolvidos pelo CGSI, observando a legislação aplicável.

Ministério da Integração e do Desenvolvimento Regional

SECRETARIA NACIONAL DE PROTEÇÃO E DEFESA CIVIL

PORTARIA Nº 3.904, DE 29 DE DEZEMBRO DE 2025

Autoriza o empenho e a transferência de recursos ao Município de Putinga - RS, para execução de ações de Proteção e Defesa Civil

A UNIÃO, por intermédio do MINISTÉRIO DA INTEGRAÇÃO E DO DESENVOLVIMENTO REGIONAL, neste ato representado pelo SECRETÁRIO NACIONAL DE PROTEÇÃO E DEFESA CIVIL, nomeado pela Portaria n.º 190, de 1º de janeiro de 2023, publicada no DOU, de 2 de janeiro de 2023, Seção 2, Edição Extra B, consoante a delegação de competência conferida pela Portaria n.º 1.184, de 15 de abril de 2024, publicada no DOU., de 16 de abril de 2024, Seção 1, e tendo em vista o disposto na Lei n.º 12.340, de 01 de dezembro de 2010, na Lei n.º 12.608, de 10 de abril de 2012 e no Decreto n.º 11.219, de 5 de outubro de 2022 e no Decreto n.º 11.655, de 23 de agosto de 2023, resolve:

Art. 1º Autorizar o empenho e a transferência de recursos ao Município de Putinga - RS no valor de R$ 116.678,88 (cento e dezesseis mil seiscentos e setenta e oito reais e oitenta e oito centavos), para a execução de ações de Resposta, conforme processo Sei n.º 59052.037237/2025-40.

Art. 2º Os recursos financeiros serão empenhados a título de Transferência Obrigatória, conforme a legislação vigente, observando a classificação orçamentária: PT: 06.182.2318.22BO.6504; GND: 3.3.40.41; Fonte: 3000; UG: 530012.

Art. 3º Considerando a natureza emergencial e as ações a serem implementadas, o prazo para a execução será de 180 dias, a partir da publicação desta portaria no Diário Oficial da União (DOU.).

Art. 4º A utilização dos recursos transferidos, pelo ente beneficiário, está vinculada exclusivamente à execução das ações especificadas no Art. 1º desta Portaria.

Art. 5º O ente beneficiário deverá apresentar a Prestação de Contas Final no prazo de 30 dias, contados da data-fim do prazo estabelecido para a execução das ações ou do último pagamento efetuado, quando este ocorrer em data anterior ao encerramento do prazo, nos termos do Art. 32 do Decreto n.º 11.655, de 23 de agosto de 2023.

Art. 6º Esta Portaria entra em vigor na data de sua publicação.

WOLNEI WOLFF BARREIROS