Seção III

Da segurança física e do ambiente

Art. 10. A segurança física e do ambiente no Ministério da Integração e do Desenvolvimento Regional tem como objetivo prevenir danos, perdas, roubos ou interferências nas instalações que possam comprometer os ativos de informação, garantindo a proteção adequada dos locais e dos equipamentos onde informações sensíveis ou críticas são tratadas.

§ 1º Devem ser adotados controles de acesso físico e salvaguardas nas áreas onde dados e informações são elaborados, processados, armazenados ou manuseados, independentemente do meio utilizado.

§ 2º Equipamentos e áreas destinados ao processamento de informações devem ser protegidos contra acessos não autorizados, danos ou interferências indevidas.

§ 3º A unidade responsável pela segurança organizacional deverá implementar perímetros físicos de segurança que assegurem a separação entre ambientes internos e externos, utilizando mecanismos de registro e autorização de entrada que garantam o acesso exclusivamente a pessoas autorizadas.

Seção IV

Da gestão de incidentes em segurança da informação

Art. 11. Devem ser estabelecidos procedimentos formais para a prevenção, auditoria, detecção, notificação e tratamento de incidentes de segurança da informação, de forma a garantir a continuidade das atividades do Ministério da Integração e do Desenvolvimento Regional e prevenir impactos nos seus objetivos estratégicos.

§ 1º A estruturação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, bem como as medidas de resposta, deverão estar alinhadas às diretrizes desta Política, competindo ao Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais - CGDSP e à ETIR adotar providências dentro de suas respectivas competências.

§ 2º Os incidentes de segurança deverão ser registrados, analisados periodicamente e comunicados imediatamente ao Encarregado pelo Tratamento de Dados Pessoais, que orientará as ações corretivas a serem adotadas.

§ 3º Quando envolverem dados pessoais, os incidentes de segurança deverão ser comunicados, no prazo de 3 (três) dias úteis, à Autoridade Nacional de Proteção de Dados - ANPD e aos titulares afetados, sempre que houver risco ou dano relevante aos direitos desses titulares.

Seção V

Da gestão de ativos

Art. 12. A gestão dos ativos de tecnologia da informação do Ministério da Integração e do Desenvolvimento Regional deve garantir sua proteção, rastreabilidade, uso adequado e integração com os processos de segurança da informação, observando os seguintes requisitos:

I - os ativos devem ser inventariados e protegidos contra indisponibilidade, acessos indevidos, ameaças, alterações, falhas, perdas, danos, furtos, roubos, interrupções não programadas e demais incidentes de segurança;

II - o mapeamento dos ativos deve subsidiar a gestão da segurança da informação, incidentes, riscos, continuidade de negócios, conformidade, auditoria e melhoria contínua;

III - a entrada e a saída de ativos nas dependências do Ministério da Integração e do Desenvolvimento Regional devem ser previamente autorizadas e registradas por autoridade competente;

IV - os ativos devem estar sujeitos a mecanismos de monitoramento e rastreabilidade de uso;

V - deve ser identificado o custodiante responsável por cada ativo;

VI - é vedado o uso de ativos institucionais para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias ou outras em desacordo com a legislação vigente; e

VII - no caso de dispositivos móveis, deve haver registro formal de cessão e uso.

Seção VI

Da gestão do uso dos recursos operacionais e de comunicações

Art. 13. É vedada a instalação de softwares ou sistemas não homologados pela Unidade de Tecnologia da Informação do Ministério da Integração e do Desenvolvimento Regional.

Parágrafo único. Excepcionalmente, mediante justificativa, a instalação de softwares não homologados poderá ser autorizada pela Unidade de Tecnologia da Informação.

Art. 14. O acesso remoto aos recursos computacionais deve ocorrer com mecanismos de segurança definidos pela Unidade de Tecnologia da Informação, mediante autorização formal.

Parágrafo único. O suporte técnico poderá acessar remotamente as estações de trabalho dos usuários, com permissão destes ou por demanda da Unidade de Tecnologia da Informação, exclusivamente para fins de execução de serviços relacionados a recursos computacionais autorizados ou homologados por aquela Unidade de Tecnologia da Informação.

Art. 15. A guarda e o uso das senhas de acesso à rede e aos sistemas são de responsabilidade de cada usuário.

Art. 16. O uso dos recursos operacionais e de comunicação deve seguir as diretrizes desta Política e observar, no mínimo:

I - o correio eletrônico institucional deve ser utilizado como canal oficial exclusivamente para fins funcionais;

II - o acesso à internet deve ser disciplinado para uso restrito às atividades institucionais;

III - a implementação ou contratação de soluções em nuvem deve obedecer à legislação vigente e às normas internas; e

IV - informações classificadas em qualquer grau de sigilo devem ser protegidas com criptografia adequada.

Seção VII

Dos controles de acesso

Art. 17. O controle de acesso, credenciais e perfis dos usuários deve observar os seguintes procedimentos:

I - no ingresso do usuário:

a) criação de perfis com níveis de autorização compatíveis com as atividades;

b) concessão de credenciais de acesso;

c) acesso apenas aos ativos necessários, com rastreabilidade das ações;

d) assinatura de Termo de Compromisso de sigilo sobre informações restritas, inclusive após desligamento ou movimentação; e

e) garantia de que o acesso físico e lógico seja concedido somente a pessoas autorizadas, com base em critérios de negócio e segurança da informação.

II - no desligamento ou movimentação do usuário:

a) desativação dos perfis;

b) revogação das credenciais; e

c) devolução dos ativos de informação sob sua responsabilidade.

Parágrafo único. O princípio do menor privilégio deve ser observado na concessão de acessos.

Art. 18. A proposição de ações de divulgação e conscientização em segurança da informação pode ser feita por qualquer agente público e será submetida à apreciação da Unidade de Tecnologia da Informação.

Art. 19. O acesso à informação e aos ativos que a armazenam será concedido com base nos requisitos de negócio e de segurança, devendo ser monitorado para garantir a rastreabilidade e a auditoria.

Parágrafo único. Os controles de acesso devem observar as disposições da Lei nº 13.709, de 14 de agosto de 2018 e estar alinhados ao Programa de Governança em Privacidade - PGP do Ministério da Integração e do Desenvolvimento Regional, conforme previsto no art. 50 da referida Lei.

Art. 20. Os sistemas que tratam informações restritas devem adotar, sempre que possível, autenticação com mais de um fator.

Art. 21. O credenciamento de usuários para acesso a documentos classificados será regulamentado em norma específica.

Art. 22. O controle de acesso deve abranger tanto o nível físico quanto o lógico, conforme procedimentos definidos pelas áreas competentes.

Parágrafo único. O trabalho remoto, quando autorizado, deve ser realizado em conformidade com os requisitos de segurança da informação definidos nesta PSI e em normativos complementares, garantindo a proteção dos ativos de informação mesmo fora das dependências do Ministério da Integração e do Desenvolvimento Regional.

Seção VIII

Da gestão de riscos e de continuidade

Art. 23. A gestão de riscos de segurança da informação deve ser realizada de forma sistemática e contínua, abrangendo todos os ativos de informação do Ministério da Integração e do Desenvolvimento Regional e considerando os aspectos de disponibilidade, integridade, confidencialidade e autenticidade.

§ 1º Deverá ser observada a Metodologia de Avaliação de Riscos e Controles aprovada pelo colegiado de governança do Ministério da Integração e do Desenvolvimento Regional.

§ 2º A segurança da informação deve contribuir para a continuidade dos negócios, com a definição de medidas de controle e recuperação, com base na priorização de processos críticos e nos riscos identificados.

§ 3º O processo de continuidade visa minimizar impactos decorrentes de falhas, desastres ou indisponibilidades significativas, por meio de ações de resposta a incidentes e recuperação de desastres.

§ 4º As contratações de serviços, convênios, acordos de cooperação e outros instrumentos congêneres que envolvam ativos de informação do Ministério da Integração e do Desenvolvimento Regional deverão conter cláusulas específicas de segurança da informação, observando as diretrizes desta PSI e dos normativos internos complementares.

Seção IX

Da auditoria e da conformidade

Art. 24. O uso dos ativos de informação do Ministério da Integração e do Desenvolvimento Regional deve ser passível de monitoramento e auditoria, devendo existir mecanismos que permitam sua rastreabilidade, controle e verificação de acessos a sistemas e rede interna do Ministério.

Parágrafo único. Fragilidades ou alterações identificadas durante atividades de auditoria ou monitoramento devem ser comunicadas imediatamente ao Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais - CGDSP.

Art. 25. A conformidade das práticas de segurança da informação adotadas pelo Ministério da Integração e do Desenvolvimento Regional deve ser verificada periodicamente, observando as diretrizes desta PSI, bem como as normas elaboradas pelo Gabinete de Segurança Institucional da Presidência da República - GSI/PR, na forma do art. 8º, do Decreto nº 12.572, de 4 de agosto de 2025.

Parágrafo único. As ações de conformidade interna deverão observar diretrizes do Plano Nacional de Cibersegurança - PNCiber, de modo a articular os objetivos institucionais com a estratégia nacional.

CAPÍTULO III

RESPONSABILIDADES E COMPETÊNCIAS

Art. 26. O Ministério da Integração e do Desenvolvimento Regional deverá instituir e manter instâncias e estruturas de governança voltadas à segurança da informação, incluindo a alta administração, os gestores das unidades organizacionais, o Gestor de Segurança da Informação, a Equipe de Tratamento e Resposta a Incidentes Cibernéticos - ETIR, entre outras que se fizerem necessárias, responsáveis por coordenar, implementar, monitorar e promover ações para a proteção dos ativos de informação, conforme legislação vigente e normativos internos específicos.

Art. 27. O Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais - CGDSP exercerá as competências do Comitê de Segurança da Informação - CSI, em atendimento ao art. 20 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I - assessorar a implementação das ações de segurança da informação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da PSI e das normas internas de segurança da informação;

IV - propor alterações à PSI e às normas internas de segurança da informação; e

V - deliberar sobre normas internas de segurança da informação.

CAPÍTULO IV

DAS DISPOSIÇÕES FINAIS

Art. 28. A violação das regras estabelecidas nesta Política e nos normativos internos de segurança da informação poderá acarretar responsabilização administrativa, civil e penal, nos termos da legislação vigente, garantidos a ampla defesa e o contraditório.

Art. 29. As omissões e dúvidas decorrentes da aplicação desta Política serão dirimidas pelo Comitê de Governança Digital, Segurança da Informação e Proteção de Dados Pessoais - CGDSP.

Art. 30. Atos a serem editados, por meio de Portaria, pelo Ministro de Estado, ou por agente público que tenha recebido delegação formal de competência para tal finalidade, observados os limites estabelecidos no respectivo instrumento de delegação, disporão sobre:

I - a designação do gestor de segurança da informação no âmbito do Ministério da Integração e do Desenvolvimento Regional conforme o disposto no art. 18 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

II - a instituição do CGDSP, bem como suas competências, composição e deliberações, de acordo com o art. 15, inciso II, art. 20 e art. 21, da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020; e

III - a constituição, a composição, as atribuições e o escopo de atuação da ETIR, conforme o disposto no art. 15, inciso IV e no art. 22 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

§ 1º A ETIR do Ministério da Integração e do Desenvolvimento Regional adotará procedimentos e guias metodológicos da rede federal coordenada pelo GSI/PR.

§ 2º A ETIR do Ministério da Integração e do Desenvolvimento Regional será responsável por adotar medidas específicas para serviços essenciais inerentes ao seu âmbito de atuação, conforme o Decreto nº 12.572, de 4 de agosto de 2025, art. 4º, inciso II.

Art. 31. Esta Portaria entra em vigor sete dias após a data de sua publicação.

ANTONIO WALDEZ GÓES DA SILVA

SECRETARIA NACIONAL DE PROTEÇÃO E DEFESA CIVIL

PORTARIA Nº 311, DE 29 DE JANEIRO DE 2026

Autoriza o empenho e a transferência de recursos ao Município de Vitória do Xingu/PA, 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, 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, resolve:

Art. 1º Autorizar o empenho e a transferência de recursos ao município de Vitória do Xingu/PA para a execução de ações de Resposta, conforme o protocolo de solicitação registrado no Sistema Integrado de Informações sobre Desastres (S2iD) e contido no processo SEI n.º 59052.038356/2026-09, no valor de R$ 139.150,00 (Cento e trinta e nove mil e cento e cinquenta reais).

Art. 2º Os recursos financeiros serão transferidos em parcela única, a título de Transferência Legal, onerando a classificação orçamentária 06.182.2318.22BO - Ações de Proteção e Defesa Civil no Plano Orçamentário (PO) 0002 - Ações de Resposta e de Recuperação de Infraestrutura danificada ou destruída por Desastres.

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, devendo o ente beneficiário cumprir, nos casos de obra de restabelecimento de serviços essenciais, as disposições do Decreto n.º 7.983, de 8 de abril de 2013 e afixar em local visível a placa da obra elaborada conforme o Manual de Uso da Marca do Governo Federal - Obras, Portaria SECOM/PR n.º 31, de 28 de agosto de 2025 e a Instrução Normativa SECOM n.º 5, de 26 de fevereiro de 2024, mantendo-a em bom estado de conservação durante todo o período de execução da obra.

Art. 5º O ente beneficiário deverá apresentar a Prestação de Contas Final no prazo de 30 dias, contado da data do término 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 11.219, de 5 de outubro de 2022.

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

WOLNEI WOLFF BARREIROS