MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

COORDENAÇÃO DE ASSESSORAMENTO NORMATIVO E DOCUMENTAL

SERVIÇO DE ATOS NORMATIVOS E GESTÃO DOCUMENTAL

PORTARIA Nº 466/2021/SEI-INPE

Dispõe sobre a Política de Segurança da Informação e Comunicação do INPE (POSIC-INPE).

A Diretora do Instituto Nacional de Pesquisas Espaciais - INPE, substituta, no uso de suas atribuições conforme o disposto na Portaria/MCT nº 407, de 29 de junho de 2006 e considerando o disposto no Processo 01340.008677/2021-31, resolve aprovar a Política de Segurança da Informação e Comunicação do INPE (POSIC-INPE).

CAPÍTULO I
ESCOPO

Art. 1º A Política de Segurança da Informação e Comunicação do Instituto Nacional de Pesquisas Espaciais (POSIC-INPE) tem por objetivo garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações produzidas ou custodiadas pelo INPE e encontra-se alinhada aos objetivos estratégicos do Instituto e às orientações para gestão de segurança da informação e comunicação do Governo Federal.

Art. 2º A POSIC-INPE define as diretrizes, competências e responsabilidades relativas ao uso e compartilhamento de dados, informações e documentos em conformidade com a Legislação vigente, com as normas técnicas pertinentes, com valores éticos e com as melhores práticas de segurança da informação e comunicação.

Art. 3º Integram também a POSIC-INPE, os documentos que a complementam, destinados à proteção da informação e comunicação e à disciplina de sua utilização.

Art. 4º Esta Política aplica-se a todos os servidores e demais usuários que, oficialmente, executem atividades vinculadas à atuação institucional do INPE.

Parágrafo único. Todos os citados neste artigo são responsáveis e devem estar comprometidos com a segurança da informação e comunicação do INPE e sujeitos às penalidades descritas no Capítulo VIII.

Art. 5º Esta Política também se aplica, no que couber, ao relacionamento do INPE com outros órgãos e entidades públicos ou privados.

Art. 6º Os contratos, convênios, acordos e outros instrumentos congêneres

celebrados pelo INPE devem se adequar a esta POSIC.

CAPÍTULO II
CONCEITOS E DEFINIÇÕES

Art. 7º Para fins deste documento, entende-se por:

I - Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do órgão;

II - Agente público: toda pessoa que exerce cargo, emprego ou função no INPE, ainda que transitoriamente, com ou sem remuneração, ou que por força de lei, contrato ou de qualquer outro ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual;

III - Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um ativo de informação;

IV - Ativo: qualquer bem, tangível ou intangível, que tenha valor para a organização;

V - Ativo de Informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

VI - Ativo sob restrição de acesso: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito;

VII - Auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;

VIII - Auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões;

IX - Autenticidade: garantia de que a informação foi produzida, expedida, modificada ou destruída dentro de preceitos legais e normativos, por pessoa física, equipamento ou sistema, órgão ou entidade vinculados ao INPE;

X - Celeridade: as ações de segurança da informação devem oferecer respostas rápidas a incidentes e falhas;

XI - Clareza: as regras de segurança dos ativos de segurança da informação e comunicação devem ser precisas, concisas e de fácil entendimento;

XII - Comitê de Segurança da Informação e Comunicação (COSIC): Comitê instituído com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicação no âmbito deste órgão;

XIII - Confidencialidade: garantia de que a informação não esteja disponível ou revelada à pessoa física, sistema, órgão ou entidade não autorizados pelo INPE;

XIV - Contingência: descrição de medidas a serem tomadas em caso de um incidente de segurança, incluindo a ativação de processos manuais, para fazer com que seus processos vitais voltem a funcionar plenamente, ou num estado minimamente aceitável, o mais rápido possível, evitando assim, uma paralisação prolongada que possa gerar maiores prejuízos à corporação;

XV - Criticidade: grau de importância da informação;

XVI - Custodiante do ativo de informação: é aquele que administra o ativo de

informação. Ele faz a guarda, mas não necessariamente usa a informação;

XVII - Dado: representa o elemento a ser processado, operado e transmitido por um sistema ou programa de computador;

XVIII - Disponibilidade: garantia de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema em todas as unidades do INPE;

XIX - Eficácia: ato de realizar um trabalho que atinja totalmente os resultados esperados;

XX - Eficiência: ato de realizar um trabalho correto, sem erros e de boa qualidade;

XXI - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR): grupo de pessoas com conhecimentos técnicos na área de Segurança da Informação, responsável por receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em ativos de informação;

XXII - Ética: atuação do agente público em manter a dignidade, segurança, privacidade e outros valores no ambiente virtual, seguindo tanto os valores morais quanto as legislações a respeito do assunto;

XXIII - Gestão de continuidade de negócios: execução do plano de documentação dos procedimentos e informações necessárias para que os órgãos ou entidades da Administração Pública Federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo num nível previamente definido, em casos de incidentes;

XXIV - Gestão de riscos de segurança da informação: conjunto de processos que permitem identificar e implementar medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação, equilibrando os custos operacionais e financeiros envolvidos;

XXV - Gestão de segurança da informação e comunicação: ações e métodos para a integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos;

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

XXVII - Gestor de área: responsável pela área funcional (titular de nível A) ou unidade (titular da unidade) onde a informação é criada, comunicada, manuseada, armazenada, custodiada, transportada ou descartada;

XXVIII - Gestor de Segurança da Informação e Comunicação (Gestor de SIC) do INPE: servidor responsável pelas ações de segurança da informação e comunicação no INPE;

XXIX - Gestor do ativo de informação: autoridade responsável pelo ativo de informação e pela concessão de acesso a este;

XXX - Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de informação, de computação ou das redes de computadores, provocando a perda de um ou mais dos princípios básicos de Segurança da Informação - Confidencialidade, Integridade e Disponibilidade - aos ativos de informação;

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

XXXII - Integridade: garantia de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, seja na sua origem, no trânsito e no seu destino;

XXXIII - Legalidade: garantia da legalidade jurídica da informação, assegurando que todos os seus dados estão de acordo com as cláusulas contratuais pactuadas ou com a legislação nacional ou internacional vigente;

XXXIV - Não repúdio: garantia de que a informação não tenha seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;

XXXV - Política de Segurança da Informação e Comunicação (POSIC-INPE): documento aprovado pela autoridade responsável pelo INPE, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicação neste órgão;

XXXVI - Princípios: ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;

XXXVII - Privacidade: garantia de que a informação privada só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata;

XXXVIII - Publicidade: dar transparência no trato das informações, observados os critérios legais;

XXXIX - Recursos de TIC: recursos de Tecnologia da Informação e Comunicação (TIC) por meio dos quais são processadas, armazenadas e transmitidas informações, incluindo: computadores e periféricos, estações de trabalho, notebooks, servidores de rede, sistemas de armazenamento de dados, equipamentos de conectividade de rede, comunicação de dados e infraestrutura, aplicações, sistemas de informação, rede de computadores corporativa, serviços de TIC corporativos, software ou bancos de dados direta ou indiretamente administrados ou utilizados pelas unidades organizacionais do INPE;

XL - Segurança da Informação e Comunicação (SIC): conjunto de ações que visam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos ativos de informação e comunicação do órgão;

XLI - Sistemas de informação: conjunto de meios de comunicação, computadores e redes de computadores, assim como dados e informações que podem ser armazenados, processados, recuperados ou transmitidos por serviços de telecomunicações, inclusive aplicativos, especificações e procedimentos para sua operação, uso e manutenção;

XLII - Termo de Compromisso: Termo assinado pelo usuário que registra estar ciente de seu compromisso com a disponibilidade, a integridade, a confidencialidade e a autenticidade dos ativos de informação a que tiver acesso, bem como assume as responsabilidades decorrentes de tal acesso, em conformidade com esta Política e com as Normas de Segurança da Informação e Comunicação do INPE;

XLIII - Tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da

informação;

XLIV - Tratamento de incidentes de segurança em redes computacionais: serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

XLV - Usuário: qualquer indivíduo ou instituição autorizado(a) a acessar e utilizar os ativos administrados e/ou disponibilizados pelo INPE;

XLVI - Vulnerabilidade: é qualquer fraqueza de um ativo de informação, ou conjunto de ativos, que permita que seja explorado por uma ou mais ameaças.

CAPÍTULO III
REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 8º O desenvolvimento da POSIC-INPE considera os dispositivos legais e normativos apresentados a seguir:

I - Instruções Normativas do Gabinete de Segurança Institucional da Presidência da República e Normas Complementares;

II - Decreto Nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

III - Decreto Nº 10.332, de 28 de abril de 2020, que institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências;

IV - Decreto Nº 9.832, de 12 de junho de 2019, que altera o Decreto nº 9.637, de 26 de dezembro de 2018, e o Decreto nº 7.845, de 14 de novembro de 2012, para dispor sobre o Comitê Gestor da Segurança da Informação;

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

VI - Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);

VII - Decreto Nº 9.319, de 21 de março de 2018, que institui o Sistema Nacional para a Transformação Digital e estabelece a estrutura de governança para a implantação da Estratégia Brasileira para a Transformação Digital;

VIII - Norma ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, levando em consideração os ambientes de risco da segurança da informação da organização;

IX - Instrução Normativa nº 02, de 5 de fevereiro de 2013, do Gabinete de Segurança Institucional da Presidência da República, que dispõe sobre o credenciamento de segurança para o tratamento de informação classificada, em qualquer grau de sigilo, no âmbito do Poder Executivo Federal;

X - Decreto Nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação

classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

XI - Lei Nº 12.527, de 18 de novembro de 2011 – Lei de Acesso a Informações (LAI), que dispõe sobre o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal, e o Decreto nº 7.724, de 16 de maio de 2012, que a regulamenta.

CAPÍTULO IV
PRINCÍPIOS

Art. 9º As ações relacionadas com Segurança da Informação e Comunicação do INPE são norteadas pelos princípios de auditabilidade, autenticidade, celeridade, clareza, confidencialidade, disponibilidade, eficácia, eficiência, ética, integridade, legalidade, não repudio, privacidade, publicidade e responsabilidade.

Art. 10. Os dados, informações e conhecimentos produzidos ou custodiados no INPE, e classificados com qualquer grau de sigilo, devem ser protegidos de acordo com o disposto nesta Política e nos seus documentos complementares.

CAPÍTULO V
DIRETRIZES GERAIS

Art. 11. A segurança da informação e comunicação tem como principal diretriz a proteção da informação, garantindo a continuidade do negócio, minimizando seus riscos, maximizando o retorno sobre os investimentos e as oportunidades pertinentes.

Art. 12. As diretrizes de segurança da informação e comunicação devem considerar, prioritariamente, objetivos estratégicos, processos, requisitos legais, normas e legislação existentes sobre segurança da informação e a estrutura organizacional do INPE.

Art. 13. As diretrizes de segurança da informação e comunicação descritas nesta Política devem ser observadas por todos os usuários que executem atividades vinculadas a este Instituto durante todas as etapas do tratamento da informação, a saber: produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

Art. 14. O cumprimento desta Política, bem como das normas e procedimentos que a complementam, destinados à proteção da informação e comunicação e à disciplina de sua utilização, deverá ser avaliado periodicamente por meio de verificações de conformidade realizadas pelo COSIC, buscando a certificação do cumprimento dos requisitos de segurança da informação e comunicação e garantia de cláusula de responsabilidade e sigilo.

Art. 15. O INPE deve observar as diretrizes estabelecidas nesta Política e deve se orientar pelas melhores práticas e procedimentos de segurança da informação e comunicação recomendadas por órgãos e entidades públicas e privadas responsáveis pelo estabelecimento de padrões.

Art. 16. O INPE deve criar, gerir e avaliar critérios de tratamento da informação de acordo com o sigilo requerido, relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 17. Os recursos de TIC, os sistemas de informação e as suas aplicações devem ser protegidos contra acessos indevidos, furtos e roubos.

Art. 18. É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações criadas, manuseadas,

armazenadas, transportadas, descartadas ou custodiadas pelo INPE.

Art. 19. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor do ativo de informação é o próprio custodiante.

Art. 20. Os contratos, convênios, acordos e instrumentos congêneres celebrados entre o INPE e terceiros devem conter cláusulas que determinem a observância desta Política e de seus documentos complementares.

Art. 21. Todos os mecanismos de proteção utilizados para a segurança da informação e comunicação devem ser mantidos para preservar a continuidade do negócio, provendo regular exercício das funções institucionais.

Art. 22. Os gestores dos ativos de informação e comunicação deverão observar normas operacionais e procedimentos específicos, a fim de garantir operação segura e contínua dos ativos.

Art. 23. As medidas de proteção devem ser planejadas e os gastos na aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Art. 24. O acesso às informações, sistemas e instalações depende da apresentação de identificador único, pessoal, intransferível e com validade estabelecida, que permita de maneira clara e indiscutível o seu reconhecimento.

Art. 25. A aquisição, contratação de serviços de desenvolvimento, instalação e uso de sistemas e equipamentos devem ser homologados e/ou autorizados pela administração.

Art. 26. Para garantir o cumprimento das normas, os responsáveis pelas unidades deverão auxiliar no controle do uso dos recursos de TIC.

CAPÍTULO VI
COMPETÊNCIAS E RESPONSABILIDADES

Art. 27. Ao Comitê de Segurança da Informação e Comunicação (COSIC) compete:

I - Assessorar a implementação das ações de segurança da informação e comunicação no INPE;

II - Constituir grupos de trabalho para tratar de temas e propor soluções específicas relacionados à segurança da informação e comunicação;

III - Participar da elaboração da Política de Segurança da Informação e Comunicação – POSIC e das normas internas de segurança da informação e comunicação;

IV - Propor alterações à Política de Segurança da informação e Comunicação – POSIC e às normas internas de segurança da informação e comunicação;

V - Deliberar sobre normas internas de segurança da informação e comunicação.

Art. 28. Ao Gestor de Segurança da Informação e Comunicação (Gestor de SIC) compete:

I - Coordenar o Comitê de Segurança da Informação e Comunicação - COSIC-INPE;

II - Coordenar a elaboração da Política de Segurança da Informação e Comunicação - POSIC e das normas internas de segurança da informação e comunicação do INPE, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - Assessorar a alta administração na implementação da Política de Segurança

da Informação - POSIC;

IV - Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação e comunicação;

V - Promover a divulgação da política e das normas internas de segurança da informação e comunicação do INPE a todos os servidores e demais usuários que trabalham no Instituto;

VI - Incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à segurança da informação e comunicação;

VII - Propor recursos necessários às ações de segurança da informação e comunicação;

VIII - Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes em Redes de Computadores (ETIR);

IX - Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação e comunicação;

X - Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação e comunicação; e

XI - Manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação e comunicação.

Art. 29. Aos Usuários compete:

I - Cumprir fielmente a POSIC-INPE, normas e seus documentos complementares;

II - Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação e comunicação;

III - Assinar Termo de Compromisso, formalizando a ciência e o aceite da POSIC e normas de segurança da informação e comunicação vigentes no INPE, bem como assumindo responsabilidade por seu cumprimento;

IV - Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pelo INPE;

V - Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo INPE;

VI - Comunicar imediatamente ao COSIC-INPE (por meio do endereço eletrônico cosic@inpe.br) qualquer descumprimento ou violação da POSIC e das normas de segurança da informação e comunicação do Instituto.

CAPÍTULO VII
NORMAS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Art. 30. As normas de segurança da informação e comunicação (NSIC) indicadas a seguir devem ser implementadas no âmbito do INPE, em suporte à POSIC:

I - NSIC-01: Normas para uso aceitável de recursos computacionais do INPE e Termo de Compromisso;

II - NSIC-02: Normas para implementação de controles de acesso;

III - NSIC-03: Normas para inventário, mapeamento e gestão de ativos de informação em apoio à segurança da informação e comunicação (SIC);

IV - NSIC-04: Normas para o processo de tratamento da informação;

V - NSIC-05: Normas para gerenciamento de incidentes em redes computacionais;

VI - NSIC-06: Normas para gestão de riscos de segurança da informação e comunicação;

VII - NSIC-07: Normas para gestão de continuidade dos negócios, nos aspectos relacionados à segurança da informação e comunicação;

VIII - NSIC-08: Normas para avaliação de conformidade nos aspectos relacionados à segurança da informação e comunicação;

IX - NSIC-09: Normas para utilização de serviços de nuvem privada, comercial ou pública.

Art. 31. As NSIC devem ser divulgadas no Portal Intranet-INPE, estando disponíveis internamente para conhecimento de todos os servidores e demais usuários que utilizam os recursos do INPE. Em hipótese alguma será permitido o descumprimento das normas associadas a POSIC pela alegação de desconhecimento das mesmas por parte do usuário.

Art. 32. As NSIC devem ser elaboradas e atualizadas em conformidade com as diretrizes da POSIC-INPE.

CAPÍTULO VIII
PENALIDADES

Art. 33. O INPE, ao gerir e monitorar seus ativos de informação, pretende garantir a segurança destes, juntamente com suas informações e recursos.

Art. 34. O descumprimento ou inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, às quais o INPE responderá com a aplicação das medidas administrativas, cíveis e judiciais cabíveis.

Art. 35. Toda tentativa de alteração dos parâmetros de segurança da informação e comunicação, por qualquer usuário, sem o devido credenciamento e a autorização para tal, será considerada inadequada e os riscos relacionados serão informados ao usuário e ao respectivo gestor de área.

Art. 36. O uso de qualquer recurso em inobservância das normas vigentes ou para prática de atividades ilícitas poderá acarretar ações administrativas e penalidades decorrentes de processos administrativo, civil e criminal, em que a instituição cooperará ativamente com as autoridades competentes.

Art. 37. Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o INPE e/ou terceiros. Portanto, o usuário vinculado a tais dispositivos identificadores será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), sendo que o uso dos dispositivos e/ou senhas de identificação de outra pessoa viola as regras de segurança e poderá resultar na aplicação de medidas administrativas, cíveis e judiciais cabíveis.

CAPÍTULO IX
ATUALIZAÇÃO

Art. 38. A POSIC-INPE deve ser revisada e atualizada sempre que for necessário, não excedendo o período máximo de dois (2) anos.

CAPÍTULO X
DIVULGAÇÃO

Art. 39. A Política e as NSIC do INPE devem ser amplamente divulgadas a todos os usuários dos recursos disponibilizados pelo INPE, por meio do correio eletrônico e dos Portais Intranet e Internet do INPE.

CAPÍTULO XI
DISPOSIÇÕES FINAIS

Art. 40. Os casos omissos e as dúvidas com relação a essa Política serão submetidos ao Comitê de Segurança da Informação e Comunicação do INPE (COSIC-INPE).

Art. 41. Esta Portaria entra em vigor no dia 10 de janeiro de 2022, em atenção ao disposto no Art. 4º, do Decreto nº 10.139, de 28 de novembro de 2019.

(Assinado Eletronicamente)
Monica Elizabeth Rocha de Oliveira
Diretora Substituta
SIAPE: 1363002

Documento assinado eletronicamente por **Monica Elizabeth Rocha de Oliveira**, **Diretor do Instituto Nacional de Pesquisas Espaciais substituto**, em 31/12/2021, às 12:17 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **8977645** e o código CRC **6058F2E3**.

Referência: Processo nº 01340.008677/2021-31 SEI nº 8977645