



MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS

COORDENAÇÃO DE ASSESSORAMENTO NORMATIVO E DOCUMENTAL

SERVIÇO DE ATOS NORMATIVOS E GESTÃO DOCUMENTAL

PORTARIA Nº 1917/2026/SEI-INPE

Institui o procedimento de comunicação de incidente de segurança com dados pessoais à ANPD e aos titulares de dados pessoais, no âmbito do INPE.

O Diretor do Instituto Nacional de Pesquisas Espaciais - INPE, no uso da competência que lhe foi delegada pelo Ministro de Estado da Ciência, Tecnologia e Inovação - MCTI, por meio da Portaria/MCT nº 407, de 29 de junho de 2006, e tendo em vista o disposto no Acórdão nº 1372/2025 - TCU - Plenário, bem como no art. 48, da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), e na Resolução CD/ANPD nº 15, de 24 de abril de 2024, resolve:

Art. 1º Fica instituído, no âmbito do INPE, o procedimento a ser observado para a comunicação de incidente de segurança com dados pessoais à Agência Nacional de Proteção de Dados - ANPD e aos titulares de dados pessoais, nos termos desta Portaria.

CAPÍTULO I DAS DISPOSIÇÕES GERAIS

Art. 2º Esta Portaria aplica-se aos incidentes de segurança envolvendo dados pessoais tratados pelo INPE na condição de controlador, em quaisquer sistemas, bases de dados, processos de trabalho ou soluções contratadas, próprios ou de terceiros.

Art. 3º O tratamento técnico do incidente, incluindo investigação, contenção e recuperação, seguirá a Política de Segurança da Informação e demais normas correlatas deste Instituto.

Art. 4º Para os fins desta Portaria, aplicam-se as definições constantes da Lei Geral de Proteção de Dados - LGPD e do Regulamento de Comunicação de Incidente de Segurança - RCIS, aprovado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024, especialmente as seguintes:

I - controlador: pessoa jurídica de direito público que toma decisões referentes ao tratamento de dados pessoais;

II - incidente de segurança: qualquer evento adverso confirmado relacionado à

violação das propriedades de confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais;

III - comunicação de incidente de segurança: ato pelo qual o controlador comunica à Agência Nacional de Proteção de Dados - ANPD e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante;

CAPÍTULO II DO FLUXO INTERNO E DAS RESPONSABILIDADES

Art. 5º Compete às unidades do INPE responsáveis por sistemas, bases de dados ou processos de trabalho que envolvam o tratamento de dados pessoais, bem como às pessoas naturais ou jurídicas, internas ou externas, que atuem como operadoras de dados pessoais em nome deste Instituto, detectar e registrar a ocorrência de incidente de segurança que envolva ou possa envolver dados pessoais.

Art. 6º As pessoas naturais ou jurídicas, internas ou externas, referidas no art. 5º, deverão comunicar ao Encarregado pelo Tratamento de Dados Pessoais, no prazo máximo de 1 (um) dia útil, informações preliminares que permitam a adequada compreensão inicial do incidente, contendo, no mínimo:

I - descrição sucinta do incidente de segurança;

II - identificação dos sistemas, bases de dados ou processos de trabalho afetados;

III - a indicação preliminar das categorias de dados pessoais possivelmente envolvidas;

IV - estimativa, ainda que aproximada, do número de titulares potencialmente afetados; e

V - a indicação das medidas emergenciais eventualmente adotadas.

Parágrafo único. As informações inicialmente comunicadas ao Encarregado pelo Tratamento de Dados Pessoais devem ser complementadas, conforme a evolução da apuração, fornecendo dados técnicos, esclarecimentos e evidências adicionais sobre o incidente, de modo a viabilizar a adequada avaliação do risco ou dano relevante e o atendimento das exigências de comunicação à ANPD e aos titulares de dados pessoais.

Art. 7º Compete ao Encarregado pelo Tratamento de Dados Pessoais ou ao representante legalmente constituído pelo controlador receber e analisar as comunicações encaminhadas nos termos do art. 6º, avaliando, em conformidade com a legislação aplicável e com as orientações da Agência Nacional de Proteção de Dados, se o incidente de segurança:

I - está devidamente confirmado;

II - envolve dados pessoais;

III - pode acarretar risco ou dano relevante aos titulares de dados pessoais.

§ 1º A análise deve apurar, ainda, as categorias de dados afetados, o número de titulares e a possibilidade de impactos materiais, morais ou reputacionais.

§ 2º Concluída a avaliação prevista no caput, caberá ao Encarregado pelo Tratamento de Dados Pessoais realizar, em nome do controlador, a comunicação do incidente de segurança à ANPD, no prazo de 3 (três) dias úteis, a contar da ciência pelo controlador do incidente de segurança que tenha afetado dados

peçoais, nos termos do art. 6º da Resolução CD/ANPD nº 15, de 24 de abril de 2024.

§ 3º Na hipótese de não ser possível a conclusão integral da apuração do incidente no prazo regulamentar, a comunicação poderá ser realizada com as informações disponíveis, em caráter preliminar, com posterior complementação das informações relevantes.

Art. 8º A comunicação de incidente de segurança aos titulares de dados pessoais deverá ser realizada pelo controlador, quando verificada a possibilidade de risco ou dano relevante, nos termos da legislação aplicável e do Regulamento de Comunicação de Incidente de Segurança - RCIS, e deverá conter, no mínimo:

- I - a descrição da natureza e da categoria de dados pessoais afetados;
- II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- III - os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;
- IV - as medidas que foram ou que serão adotadas para mitigar os efeitos do incidente, quando cabíveis;
- V - a data do conhecimento do incidente de segurança; e
- VI - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

Parágrafo único. A comunicação do incidente aos titulares de dados deverá ser redigida em linguagem clara e acessível, sendo realizada, sempre que viável, de forma direta e individualizada.

CAPÍTULO III DO PADRÃO DE COMUNICAÇÃO À ANPD

Art. 9º A comunicação de incidente de segurança à Agência Nacional de Proteção de Dados - ANPD e aos titulares de dados pessoais afetados será realizada pelo Encarregado pelo Tratamento de Dados Pessoais ou por representante legalmente constituído pelo controlador, em estrita observância aos instrumentos, padrões e modelos definidos pela ANPD.

Parágrafo único. A realização da comunicação não exime as unidades responsáveis por sistemas, bases de dados ou processos de trabalho que envolvam o tratamento de dados pessoais do dever de continuar prestando ao Encarregado pelo Tratamento de Dados Pessoais informações adicionais e atualizadas, sempre que necessárias ao esclarecimento do incidente ou ao atendimento de solicitações da ANPD.

Art. 10. O Encarregado pelo Tratamento de Dados Pessoais deverá manter registros atualizados dos incidentes de segurança com dados pessoais analisados, abrangendo as comunicações realizadas e as decisões adotadas.

§ 1º Os registros de que trata o caput deverão conter, sempre que aplicável, informações essenciais relativas à descrição do incidente, à avaliação de risco, à decisão quanto à necessidade de comunicação e à comprovação da comunicação à ANPD, quando realizada, com referência ao processo administrativo correspondente.

§ 2º As decisões de não comunicação deverão ser devidamente motivadas e

registradas, de modo a demonstrar a conformidade com a legislação aplicável, com o Regulamento de Comunicação de Incidente de Segurança - RCIS e com as orientações da Agência Nacional de Proteção de Dados.

Art. 11. O padrão de comunicação de incidente de segurança à ANPD, a ser obrigatoriamente observado pelo INPE, consistirá em:

I - abertura de novo processo no sistema SEI da ANPD, com o tipo "ANPD - Comunicados de Incidentes à Agência Nacional de Proteção de Dados";

II - utilização do Formulário de Comunicação de Incidente de Segurança - CIS, disponibilizado pela ANPD, como documento principal do processo, conforme espelho constante do Anexo I desta Portaria;

III - inclusão, como documento complementar, do Resumo Executivo do Incidente, elaborado de acordo com o modelo constante do Anexo II, destinado a apresentar, de forma sintética, as principais informações sobre o incidente;

IV - anexação de eventuais evidências técnicas e documentos adicionais necessários à adequada descrição do incidente e das medidas adotadas.

Art. 12. O Formulário de Comunicação de Incidente de Segurança - CIS, quando devidamente preenchido, deverá contemplar as informações mínimas exigidas pela LGPD e pelo RCIS para a comunicação de incidente de segurança à ANPD, conforme a Resolução CD/ANPD nº 15, de 24 de abril de 2024:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no artigo 7º;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;

VIII - os dados do encarregado ou de quem represente o controlador;

IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;

X - a identificação do operador, quando aplicável;

XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e

XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Art. 13. O Resumo Executivo do Incidente terá caráter complementar e sintético, com a finalidade de:

I - apresentar, em poucas linhas, a identificação básica do incidente, a linha do tempo principal, o escopo afetado e a avaliação resumida de risco;

II - fornecer à ANPD uma visão geral imediata do evento, sem reproduzir de forma exaustiva as informações já detalhadas no Formulário CIS e nos documentos técnicos anexos.

CAPÍTULO IV DO PADRÃO DE COMUNICAÇÃO AOS TITULARES DE DADOS PESSOAIS

Art. 14. Confirmada a necessidade de comunicação aos titulares, na forma do art. 48 da LGPD e do art. 9º do Regulamento de Comunicação de Incidente de Segurança- RCIS, o Encarregado coordenará o envio de comunicado aos titulares afetados, preferencialmente por meio dos canais já utilizados pelo INPE para contato com esses titulares.

Parágrafo único. Para fins de padronização, deverá ser utilizado como referência o Modelo de Comunicação aos Titulares constante do Anexo II desta Portaria, admitidas as adaptações necessárias ao caso concreto.

Art. 15. O Modelo de Comunicação aos Titulares previsto no Anexo II para a comunicação ao titular de dados pessoais deverá conter, no mínimo:

- I - a descrição da natureza e da categoria de dados pessoais afetados;
- II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- III - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
- IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo previsto no artigo 7º;
- V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
- VI - a data do conhecimento do incidente de segurança; e
- VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do Encarregado.

Art. 16. Quando a comunicação individual não for viável, o Encarregado poderá, observados os parâmetros do RCIS, propor o uso de meios alternativos, como aviso em destaque no sítio eletrônico do INPE, mantendo, sempre que possível, a estrutura informativa do Anexo II.

CAPÍTULO V DO REGISTRO E DA GUARDA DAS INFORMAÇÕES

Art. 17. O Encarregado deverá manter registro dos incidentes de segurança avaliados, comunicados ou não à ANPD, pelo prazo mínimo previsto no RCIS e nas normas de gestão documental aplicáveis, contendo, no mínimo:

- I - descrição do incidente;
- II - avaliação de risco e decisão quanto à necessidade de comunicação; e comprovação da comunicação à ANPD, quando realizada, com referência ao processo SEI correspondente;
- III - comprovação da comunicação aos titulares, quando realizada, com indicação

dos meios utilizados e das datas de envio.

Parágrafo único. Os registros referidos no caput poderão ser solicitados pela ANPD ou por órgãos de controle a qualquer tempo, devendo ser apresentados pelo Encarregado.

CAPÍTULO VI DAS DISPOSIÇÕES FINAIS

Art. 18. As unidades do INPE deverão prestar ao Encarregado pelo Tratamento de Dados Pessoais, de forma completa e à medida que se tornarem disponíveis, as informações e os elementos técnicos que lhes forem solicitados para fins de análise e de comunicação de incidentes de segurança com dados pessoais.

Art. 19. As disposições desta Portaria deverão ser interpretadas e aplicadas em conformidade com a LGPD, com o Regulamento de Comunicação de Incidente de Segurança - RCIS e com as orientações expedidas pela Agência Nacional de Proteção de Dados.

Art. 20. Esta Portaria entrará em vigor sete dias após a data de sua assinatura.

(Assinado Eletronicamente)
Antonio Miguel Vieira Monteiro
Diretor
SIAPE: 0664462

ANEXO I FORMULÁRIO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA - CIS

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS	Formulário de Comunicação de Incidente de Segurança com Dados Pessoais
--	---

Dados do Controlador				
Razão Social / Nome:				
CNPJ/CPF:				
Endereço:				
Cidade:		Estado:		
CEP:				
Telefone:		E-mail:		

Declara ser Microempresa ou Empresa de Pequeno Porte:		<input type="checkbox"/>	<input type="checkbox"/>	
		Sim	Não	
Declara ser Agente de Tratamento de Pequeno Porte[1]:		<input type="checkbox"/>	<input type="checkbox"/>	
		Sim	Não	
Informe o número aproximado de titulares cujos dados são tratados por sua organização:				
Dados do Encarregado				
Possui um encarregado pela proteção de dados pessoais?		<input type="checkbox"/>	<input type="checkbox"/>	
		Sim	Não	
Nome:				
CNPJ/CPF:				
Telefone:			E-mail:	
Dados do Notificante / Representante Legal				
<input type="checkbox"/> O próprio encarregado pela proteção de dados.				
<input type="checkbox"/> Outros (especifique):				
Nome:				
CNPJ/CPF:				
Telefone:				
E-mail:				
<p>A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.</p> <ul style="list-style-type: none"> • <i>Encarregado</i>: ato de designação/nomeação/procuração. • <i>Representante</i>: contrato social e procuração, se cabível. 				

Tipo de Comunicação	
<input type="checkbox"/> Completa	<i>Todas as informações a respeito do incidente estão disponíveis e a comunicação aos titulares já foi realizada.</i>
	<i>Nem todas as informações sobre o incidente estão disponíveis,</i>

<input type="checkbox"/> Preliminar	<i>justificadamente, ou a comunicação aos titulares ainda não foi realizada.</i> <i>A complementação deverá ser encaminhada em até 30 dias corridos da comunicação preliminar.</i>
<input type="checkbox"/> Complementar	<i>Complementação de informações prestadas em comunicação preliminar.</i>
A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.	
<ul style="list-style-type: none"> A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido. 	
Avaliação do Risco do Incidente	
<input type="checkbox"/> O incidente de segurança pode acarretar risco ou dano relevante aos titulares.	
<input type="checkbox"/> O incidente não acarretou risco ou dano relevante aos titulares. (Comunicação Complementar)	
<input type="checkbox"/> O risco do incidente aos titulares ainda está sendo apurado. (Comunicação Preliminar)	
Justifique, se cabível, a avaliação do risco do incidente:	

Da Ciência da Ocorrência do Incidente			
Por qual meio se tomou conhecimento do incidente?			
<input type="checkbox"/> Identificado pelo próprio controlador.	<input type="checkbox"/> Notificação do operador de dados.	<input type="checkbox"/> Denúncia de titulares/terceiros.	
<input type="checkbox"/> Notícias ou redes sociais.	<input type="checkbox"/> Notificação da ANPD.	<input type="checkbox"/> Outros. (especifique)	
Descreva, resumidamente, de que forma a ocorrência do incidente foi conhecida:			
Caso o incidente tenha sido comunicado ao controlador por um operador,			

informe:		
Dados do Operador		
Razão Social / Nome:		
CNPJ/CPF:		
E-mail:		
Cabe ao controlador solicitar ao operador as informações necessárias à comunicação do incidente.		
Da Tempestividade da Comunicação do Incidente		
Informe as seguintes datas, sobre o incidente:		
Quando ocorreu		
Quando tomou ciência		
Quando comunicou à ANPD		
Quando comunicou aos titulares		
Justifique, se cabível, a não realização da <u>comunicação completa</u> à ANPD e aos <u>titulares</u> de dados afetados no prazo sugerido de 2 (dois) dias úteis após a ciência do incidente:		
Se cabível, informe quando e a quais outras autoridades o incidente foi comunicado:		
Da Comunicação do Incidente aos Titulares dos Dados		
Os titulares dos dados afetados foram comunicados sobre o incidente?		
<input type="checkbox"/> Sim.	<input type="checkbox"/> Não, por não haver risco ou dano relevante a eles.	
<input type="checkbox"/> Não, mas o processo de comunicação está em	<input type="checkbox"/> Não, vez que o risco do incidente ainda está sendo apurado. (comunicação	

andamento.	preliminar)	
Se cabível, quando os titulares serão comunicados sobre o incidente?		
De que forma a ocorrência do incidente foi comunicada aos titulares?		
<input type="checkbox"/> Comunicado individual por escrito. <i>(mensagem eletrônica / carta / e-mail / etc.)</i>	<input type="checkbox"/> Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.	
<input type="checkbox"/> Comunicado individual por escrito com confirmação de recebimento. <i>(mensagem eletrônica / carta / e-mail / etc.)</i>	<input type="checkbox"/> Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador. <i>(especifique abaixo)</i>	
<input type="checkbox"/> Outros. <i>(especifique abaixo)</i>	<input type="checkbox"/> Não se aplica.	
Descreva como ocorreu a comunicação:		
Quantos titulares foram comunicados individualmente sobre o incidente?		
Justifique, se cabível, o que motivou a não realização da comunicação individual aos titulares:		
<p>O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:</p> <ol style="list-style-type: none"> 1. resumo e data de ocorrência do incidente; 2. descrição dos dados pessoais afetados; 3. riscos e consequências aos titulares de dados; 4. medidas tomadas e recomendadas para mitigar seus efeitos, se cabíveis; 5. dados de contato do controlador para obtenção de informações adicionais sobre o incidente. 		
O comunicado aos titulares atendeu os requisitos acima?		
<input type="checkbox"/> Sim	<input type="checkbox"/> Não	

- Se não atendidos os requisitos, o comunicado aos titulares deverá ser devidamente retificado.
- Poderá ser solicitada pela ANPD, a qualquer tempo, cópia do comunicado aos titulares para fins de fiscalização.

Descrição do Incidente

Qual o tipo de incidente? (Informe o tipo mais específico)

<input type="checkbox"/> Sequestro de Dados (<i>ransomware</i>) sem transferência de informações.	<input type="checkbox"/> Sequestro de dados (<i>ransomware</i>) com transferência e/ou publicação de informações.
<input type="checkbox"/> Exploração de vulnerabilidade em sistemas de informação.	<input type="checkbox"/> Vírus de Computador / <i>Malware</i> .
<input type="checkbox"/> Roubo de credenciais / Engenharia Social.	<input type="checkbox"/> Violação de credencial por força bruta.
<input type="checkbox"/> Publicação não intencional de dados pessoais.	<input type="checkbox"/> Divulgação indevida de dados pessoais.
<input type="checkbox"/> Envio de dados a destinatário incorreto.	<input type="checkbox"/> Acesso não autorizado a sistemas de informação.
<input type="checkbox"/> Negação de Serviço (DoS).	<input type="checkbox"/> Alteração/exclusão não autorizada de dados.
<input type="checkbox"/> Perda/roubo de documentos ou dispositivos eletrônicos.	<input type="checkbox"/> Descarte incorreto de documentos ou dispositivos eletrônicos.
<input type="checkbox"/> Falha em equipamento (<i>hardware</i>).	<input type="checkbox"/> Falha em sistema de informação (<i>software</i>).
<input type="checkbox"/> Outro tipo de incidente cibernético. (especifique abaixo)	<input type="checkbox"/> Outro tipo de incidente não cibernético. (especifique abaixo)

Descreva, resumidamente, como ocorreu o incidente:

Explique, resumidamente, por que o incidente ocorreu (identifique a causa raiz, se conhecida):

Que medidas foram adotadas para corrigir as causas do incidente?

Impactos do Incidente Sobre os Dados Pessoais

De que forma o incidente afetou os dados pessoais (admita mais de uma marcação):

<input type="checkbox"/> Confidencialidade	Houve acesso não autorizado aos dados, violando seu sigilo.
<input type="checkbox"/> Integridade	Houve alteração ou destruição de dados de maneira não autorizada ou acidental.
<input type="checkbox"/> Disponibilidade	Houve perda ou dificuldade de acesso aos dados por período significativo.

Se aplicável, quais os tipos de dados pessoais sensíveis foram violados? (admita mais de uma marcação)

<input type="checkbox"/> Origem racial ou étnica.	<input type="checkbox"/> Convicção religiosa.	<input type="checkbox"/> Opinião política.
<input type="checkbox"/> Referente à saúde.	<input type="checkbox"/> Biométrico.	<input type="checkbox"/> Genético.
<input type="checkbox"/> Referente à vida sexual.	<input type="checkbox"/> Filiação a organização sindical, religiosa, filosófica ou política.	

Se aplicável, descreva os tipos de dados pessoais sensíveis violados:

Quais os demais tipos de dados pessoais violados? (admita mais de uma marcação)

<input type="checkbox"/> Dados básicos de identificação <i>(ex: nome, sobrenome, data de nascimento, matrícula)</i>	<input type="checkbox"/> Número de documentos de identificação oficial. <i>(ex: RG, CPF, CNH, passaporte)</i>	<input type="checkbox"/> Dados de contato. <i>(ex: telefone, endereço, e-mail)</i>
<input type="checkbox"/> Dados de meios de pagamento. <i>(ex: cartão de crédito/débito)</i>	<input type="checkbox"/> Cópias de documentos de identificação oficial.	<input type="checkbox"/> Dados protegidos por sigilo profissional/legal.
<input type="checkbox"/> Dado financeiro ou econômico.	<input type="checkbox"/> Nomes de usuário de sistemas de informação.	<input type="checkbox"/> Dado de autenticação de sistema. <i>(ex: senhas, PIN ou tokens)</i>
<input type="checkbox"/> Imagens / Áudio / Vídeo	<input type="checkbox"/> Dado de geolocalização. <i>(ex: coordenadas geográficas)</i>	<input type="checkbox"/> Outros (especifique abaixo)

Descreva os tipos de dados pessoais não sensíveis violados:		
Riscos e Consequências aos Titulares dos Dados		
Foi elaborado um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) das atividades de tratamento afetadas pelo incidente?		
<input type="checkbox"/> Sim <input type="checkbox"/> Não		
Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?		
Qual a quantidade aproximada de titulares afetados [2] pelo incidente?		
Total de titulares afetados		
Crianças e/ou adolescentes		
Outros titulares vulneráveis		
Se aplicável, descreva as categorias de titulares vulneráveis afetados:		
Quais as categorias de titulares foram afetadas pelo incidente? (admite mais de uma marcação)		
<input type="checkbox"/> Funcionários.	<input type="checkbox"/> Prestadores de serviços.	<input type="checkbox"/> Estudantes/Alunos.
<input type="checkbox"/> Clientes/Cidadãos.	<input type="checkbox"/> Usuários.	<input type="checkbox"/> Inscritos/Filiados.
<input type="checkbox"/> Pacientes de serviço de saúde.	<input type="checkbox"/> Ainda não identificadas.	<input type="checkbox"/> Outros. (especifique abaixo)
Informe o quantitativo de titulares afetados, por categoria:		

Quais as prováveis consequências do incidente para os titulares? (admite mais de uma marcação)			
<input type="checkbox"/> Danos morais.	<input type="checkbox"/> Danos materiais.	<input type="checkbox"/> Violação à integridade física	
<input type="checkbox"/> Discriminação social.	<input type="checkbox"/> Danos reputacionais.	<input type="checkbox"/> Roubo de identidade.	
<input type="checkbox"/> Engenharia social / Fraudes.	<input type="checkbox"/> Limitação de acesso a um serviço.	<input type="checkbox"/> Exposição de dados protegidos por sigilo profissional/legal.	
<input type="checkbox"/> Restrições de direitos.	<input type="checkbox"/> Perda de acesso a dados pessoais.	<input type="checkbox"/> Outros (especifique abaixo).	
Se cabível, descreva as prováveis consequências do incidente para cada grupo de titulares:			
Qual o provável impacto do incidente sobre os titulares? (admite só uma marcação)			
<input type="checkbox"/> Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.			
<input type="checkbox"/> Podem sofrer danos, superáveis com certa dificuldade.			
<input type="checkbox"/> Podem sofrer danos importantes, superáveis com muita dificuldade.			
<input type="checkbox"/> Podem sofrer lesão ou ofensa a direitos ou interesses difusos, coletivos ou individuais, que, dadas as circunstâncias, ocasionam ou tem potencial para ocasionar dano significativo ou irreversível.			
Se cabível, quais medidas foram adotadas para mitigação dos riscos causados pelo incidente aos titulares?			
Medidas de Segurança Técnicas e Administrativas para a Proteção dos Dados Pessoais			
Os dados violados estavam protegidos de forma a impossibilitar a identificação de seus titulares?			
<input type="checkbox"/> Sim, integralmente protegidos por criptografia / pseudonimização.	<input type="checkbox"/> Sim, parcialmente protegidos por criptografia / pseudonimização.	<input type="checkbox"/> Não.	

Descreva os meios utilizados para proteger a identidade dos titulares, e a quais tipos dados foram aplicados:			
Antes do incidente, quais das seguintes medidas de segurança eram adotadas? (admite mais de uma marcação)			
<input type="checkbox"/> Políticas de segurança da informação e privacidade.	<input type="checkbox"/> Processo de Gestão de Riscos.	<input type="checkbox"/> Registro de incidentes.	
<input type="checkbox"/> Controle de acesso físico.	<input type="checkbox"/> Controle de acesso lógico.	<input type="checkbox"/> Segregação de rede.	
<input type="checkbox"/> Criptografia / Anonimização.	<input type="checkbox"/> Cópias de segurança. (<i>backups</i>)	<input type="checkbox"/> Gestão de ativos.	
<input type="checkbox"/> Antivírus.	<input type="checkbox"/> Firewall.	<input type="checkbox"/> Atualização de Sistemas.	
<input type="checkbox"/> Registros de acesso (logs).	<input type="checkbox"/> Monitoramento de uso de rede e sistemas.	<input type="checkbox"/> Múltiplos fatores de autenticação.	
<input type="checkbox"/> Testes de invasão.	<input type="checkbox"/> Plano de resposta a incidentes.	<input type="checkbox"/> Outras (especifique).	
Descreva as demais medidas de segurança técnicas e administrativas adotadas antes do incidente:			
Após o incidente, foi adotada alguma nova medida de segurança? (admite mais de uma marcação)			
<input type="checkbox"/> Políticas de segurança da informação e privacidade.	<input type="checkbox"/> Processo de Gestão de Riscos.	<input type="checkbox"/> Registro de incidentes.	
<input type="checkbox"/> Controle de acesso físico.	<input type="checkbox"/> Controle de acesso lógico.	<input type="checkbox"/> Segregação de rede.	
<input type="checkbox"/> Criptografia / Anonimização.	<input type="checkbox"/> Cópias de segurança. (<i>backups</i>)	<input type="checkbox"/> Gestão de ativos.	
<input type="checkbox"/> Antivírus.	<input type="checkbox"/> Firewall.	<input type="checkbox"/> Atualização de Sistemas.	
<input type="checkbox"/> Registros de acesso (logs).	<input type="checkbox"/> Monitoramento de uso de rede e sistemas.	<input type="checkbox"/> Múltiplos fatores de autenticação.	
	<input type="checkbox"/> Plano de resposta a		

<input type="checkbox"/> Testes de invasão.	<input type="checkbox"/> Plano de resposta a incidentes.	<input type="checkbox"/> Outras (especifique).	
Se cabível, descreva as medidas de segurança adicionais adotadas após o incidente:			
As atividades de tratamento de dados afetadas estão submetidas a regulações de segurança setoriais?			
<input type="checkbox"/> Sim	<input type="checkbox"/> Não		
Se cabível, indique as regulamentações setoriais de segurança aplicáveis às atividades de tratamento de dados afetadas pelo incidente:			

Declaro, sob as penas da lei, serem verdadeiras as informações prestadas acima.

<ASSINATURA>

ANEXO II MODELO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA AOS TITULARES DE DADOS

Prezado(a) Senhor(a),

Em cumprimento ao art. 48 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)), informamos que foi identificado um incidente de segurança que pode ter afetado seus dados pessoais tratados por esta Entidade.

1. Descrição do Incidente

Data de ocorrência: ____/____/____

Natureza do incidente: _____

Descrição resumida: _____

2. Dados Possivelmente Afetados

Tipos de dados: () Cadastrais () Sensíveis () Funcionais () Outros: _____

3. Riscos e Medidas Adotadas

Riscos identificados: () Uso indevido () Exposição () Outros: _____

Providências adotadas: _____

4. Ações Recomendadas ao Titular

() Ficar atento a comunicações suspeitas.

() Não compartilhar senhas ou dados sigilosos.

() Comunicar uso indevido de suas informações.

5. Canal de Contato

Encarregado de Proteção de Dados

Nome: _____

E-mail: _____

Telefone: _____

Atenciosamente,

Data: ____ / ____ / _____

[Nome do Responsável/Encarregado de Dados]

INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS - INPE

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO - MCTI

[1] Nos termos do REGULAMENTO DE APLICAÇÃO DA LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, aprovado pela RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022. (<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>)

[2] Titular afetado é aquele cujos dados podem ter tido a confidencialidade, integridade ou disponibilidade violadas e que ficará exposto a novos riscos relevantes em razão do incidente.



Documento assinado eletronicamente por **Antonio Miguel Vieira Monteiro, Diretor do Instituto Nacional de Pesquisas Espaciais**, em 16/03/2026, às 16:45 (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 <https://sei.mcti.gov.br/verifica.html>, informando o código verificador **13597112** e o código CRC **59ACE438**.