

### Dados do Controlador

Razão Social / Nome:	Fundação Nacional de Artes		
CNPJ/CPF:	26963660-0002-42		
Endereço:	Rua da Imprensa, nº 16, Ed. Palácio Gustavo Capanema		
Cidade:	Rio de Janeiro	Estado:	Rio de Janeiro
CEP:	20030-120		
Telefone:	(21) 99599-2690	E-mail:	
Declara ser Microempresa ou Empresa de Pequeno Porte:	<input type="checkbox"/> Sim	<input type="checkbox"/> Não	
Declara ser Agente de Tratamento de Pequeno Porte <sup>1</sup> :	<input type="checkbox"/> Sim	<input type="checkbox"/> 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 checked="" type="checkbox"/> Sim	<input type="checkbox"/> Não
Nome:	Paulo César Pereira Soares	
CNPJ/CPF:	388.848.877-04	
Telefone:	(21) 99599-2690	E-mail: paulocesarsoares@funarte.gov.br

### 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:

A documentação comprobatória da legitimidade para representação do controlador junto à ANPD deve ser protocolada em conjunto com o formulário de comunicação de incidente.

- *Encarregado*: ato de designação/nomeação/procuração.
- *Representante*: contrato social e procuração, se cabível.

<sup>1</sup> 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>)

## Tipo de Comunicação

☐ Completa

*Todas as informações a respeito do incidente estão disponíveis e a **comunicação aos titulares já foi realizada**.*

☐ Preliminar

*Nem todas as informações sobre o incidente estão disponíveis, justificadamente, ou a **comunicação aos titulares ainda não foi realizada**.*

*A complementação deverá ser encaminhada em até **30 dias corridos** da comunicação preliminar.*

☐ Complementar

*Complementação de informações prestadas em comunicação preliminar.*

**A comunicação complementar deve ser protocolada no mesmo processo que a comunicação preliminar.**

- 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

☐ O incidente de segurança pode acarretar risco ou dano relevante aos titulares.

☐ O incidente não acarretou risco ou dano relevante aos titulares. **(Comunicação Complementar)**

☐ 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?**

☐ Identificado pelo próprio controlador. ☐ Notificação do operador de dados. ☐ Denúncia de titulares/terceiros.

☐ Notícias ou redes sociais. ☐ Notificação da ANPD. ☐ 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 comunicação completa à ANPD e aos titulares 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?

☐ Sim.

☐ Não, por não haver risco ou dano relevante a eles.

☐ Não, mas o processo de comunicação está em andamento.

☐ Não, vez que o risco do incidente ainda está sendo apurado. (**comunicação preliminar**)

Se cabível, quando os titulares serão comunicados sobre o incidente?

De que forma a ocorrência do incidente foi comunicada aos titulares?

☐ Comunicado individual por escrito.  
(mensagem eletrônica / carta / e-mail / etc.)

☐ Anúncio público no sítio eletrônico, mídias sociais ou aplicativos do controlador.

☐ Comunicado individual por escrito com confirmação de recebimento.  
(mensagem eletrônica / carta / e-mail / etc.)

☐ Ampla divulgação do fato em meios de comunicação, por iniciativa do controlador.  
(especifique abaixo)

☐ Outros. (especifique abaixo)

☐ 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:

**O comunicado aos titulares deve utilizar linguagem clara e conter, ao menos, as seguintes informações:**

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?**

☐ Sim

☐ 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.<br>(especifique abaixo)               | <input type="checkbox"/> Outro tipo de incidente não cibernético.<br>(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 (admite 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? (admite 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? (admite mais de uma marcação)

- |   |   |  |
|---|---|--|
| <input type="checkbox"/> Dados básicos de identificação<br>(ex: nome, sobrenome, data de nascimento, matrícula) | <input type="checkbox"/> Número de documentos de identificação oficial.<br>(ex: RG, CPF, CNH, passaporte) | <input type="checkbox"/> Dados de contato.<br>(ex: telefone, endereço, e-mail)           |
| <input type="checkbox"/> Dados de meios de pagamento.<br>(ex: cartão de crédito/débito)                         | <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.<br>(ex: senhas, PIN ou tokens) |
| <input type="checkbox"/> Imagens / Áudio / Vídeo  | <input type="checkbox"/> Dado de geolocalização.<br>(ex: coordenadas geográficas)                         | <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?

☐ Sim

☐ Não

**Qual o número total de titulares cujos dados são tratados nas atividades afetadas pelo incidente?**

**Qual a quantidade aproximada de titulares afetados<sup>2</sup> 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)**

☐ Funcionários.

☐ Prestadores de serviços.

☐ Estudantes/Alunos.

☐ Clientes/Cidadãos.

☐ Usuários.

☐ Inscritos/Filiados.

☐ Pacientes de serviço de saúde.

☐ Ainda não identificadas.

☐ 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)**

☐ Danos morais.

☐ Danos materiais.

☐ Violação à integridade física

☐ Discriminação social.

☐ Danos reputacionais.

☐ Roubo de identidade.

☐ Engenharia social / Fraudes.

☐ Limitação de acesso a um serviço.

☐ Exposição de dados protegidos por sigilo profissional/legal.

☐ Restrições de direitos.

☐ Perda de acesso a dados pessoais.

☐ 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)**

☐ Podem não sofrer danos, sofrer danos negligenciáveis ou superáveis sem dificuldade.

☐ Podem sofrer danos, superáveis com certa dificuldade.

☐ Podem sofrer danos importantes, superáveis com muita dificuldade.

☐ 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.

<sup>2</sup> 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.

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?

☐ Sim, integralmente protegidos por criptografia / pseudonimização.

☐ Sim, parcialmente protegidos por criptografia / pseudonimização.

☐ 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. (backups)	<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. (backups)	<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).

**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?**

☐ Sim

☐ 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>**