



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

ANPD - Auto de Infração nº 1/2023/FIS/CGF/ANPD

00261.001888/2023-21

### 1. IDENTIFICAÇÃO DO AUTUADO

#### Natureza do Autuado

(  )  
Pessoa  
Jurídica      (  ) Pessoa Física

#### Agente de Tratamento

(  ) Controlador      (  ) Operador

**Nome  
Completo  
/  
Razão  
Social**

**CPF / CNPJ**

INSTITUTO  
NACIONAL  
DO  
SEGURO  
SOCIAL

29.979.036/0001-40

#### Endereço

SAUS QUADRA 02 BLOCO "O"

**Município**

**CEP**

BRASÍLIA

70.070-946

**UF**

**Telefone para contato (celular / comercial)**

DF

(61) 3313-4509

## E-mail para comunicações processuais

edson.alvarista@inss.gov.br  
carlos.eduardosimao@inss.gov.br  
encarregado@inss.gov.br

## 2. DESCRIÇÃO DOS FATOS E DOS DISPOSITIVOS NORMATIVOS INFRINGIDOS

### Descrição do(s) Fato(s)

1. Em 19/10/2022, o Instituto Nacional do Seguro Social (doravante INSS ou autuado) apresentou Comunicação de Incidente de Segurança (CIS) preliminar, o Anexo nota (SEI nº 3701050). Em 30/12/2022, após requerimentos dessa CGF por meio do E-mail (SEI nº 3725180) e do E-mail (SEI nº 3760075), o autuado apresentou CIS complementar por meio de Formulário de Incidente de Segurança - ANPD em atendimento 3847370 - ANPD - Aviso (SEI nº 3850818).

2. O autuado tomou ciência do incidente de segurança em 23/09/2022 durante a atividade de monitoramento de rotina do desempenho do computador de grande porte, o autuado identificou um aumento expressivo no número de consultas a dados durante os meses de setembro e agosto, sem justificativa operacional aparente. O aumento de volumetria de consulta a dados ocorreu por acesso realizado por credencial válida vinculada à Advocacia-Geral da União (AGU) e originária de uma rede autorizada. Por meio dessa consulta, foi possível acessar dados de comprovação de identidade oficial, dados financeiros e de saúde de um número indeterminado de beneficiários e segurados do INSS.

3. Nos meses de agosto e setembro de 2022, foram realizadas mais de 90 milhões de consultas ao Sistema Corporativo de Benefícios do INSS (SISBEN) e 9 milhões de consultas ao Sistema Único de Benefícios DATAPREV (BLH00), quantidade quase três vezes maior que a registrada no mês de junho do mesmo ano. A maior parte dos acessos no período foi realizada por três usuários do sistema pertencentes ao grupo de acesso gerido pela AGU, que teria acesso ao sistema em razão de um convênio firmado com o INSS. O autuado afirmou que a gestão de acesso aos sistemas se daria de forma descentralizada, pelos órgãos conveniados, sem qualquer validação por parte do INSS.

4. Em 29/12/2022, a CGF emitiu o ANPD - Aviso 33/2022 (SEI nº 3847370) em que determina que o autuado apresente (a) esclarecimentos a respeito da atuação do agente de tratamento notificante, ou seja, se atua como controlador ou operador dos dados pessoais; (b) formulário de

incidente de segurança com informações complementares; (c) relatório técnico de tratamento do incidente; e (d) comunicação aos titulares a respeito da possível violação do sigilo dos dados no incidente, se cabível.

5. Em resposta ao Aviso, por meio do Formulário de Incidente de Segurança - ANPD em atendimento 3847370 - ANPD - Aviso (SEI nº 3850818), o autuado apresentou os documentos solicitados e justificou a não realização da CIS aos titulares sob alegação de ainda estar analisando a legitimidade dos acessos suspeitos. Ressaltou que as medidas de contenção do incidente foram adotadas imediatamente após o registro do incidente pela Comissão de Tratamento e Resposta a Incidentes Cibernéticos (CTIR) da Empresa de Tecnologia e Informações da Previdência (DATAPREV).

6. A apuração do incidente de segurança está sob análise desta CGF no processo 00261.002177/2022-93. A despeito da existência dessa apuração, algumas medidas já deveriam ter sido implementadas pelo controlador que sofreu incidente de segurança sobre dados pessoais que possa acarretar risco ou dano relevante aos titulares. Existe urgência na comunicação aos titulares possivelmente afetados, já que o incidente em questão os coloca em risco imediato e elevado de serem vítimas de furto de identidade, fraudes, assédios comerciais entre outros danos desde a sua ocorrência.

7. A análise da necessidade de comunicação de incidente foi realizada na Nota Técnica 13 (SEI nº 4046230) que, em síntese, sugeriu, novamente, que fosse determinado ao INSS a comunicação do incidente de segurança aos titulares de dados. A comunicação ao titular deve ser feita em razão do elevadíssimo número de titulares potencialmente afetados, pois trata-se de sistemas que armazenam uma grande quantidade de dados pessoais, tais como Nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes. No mesmo sentido, o próprio INSS informou como critério para comunicação à ANPD que "o incidente de segurança pode acarretar risco ou dano relevante aos titulares".

8. Mesmo após determinação expressa e específica no ANPD - Aviso 33/2022 (SEI nº 3847370) e Despacho Decisório 3 (SEI nº 4055193), o autuado não realizou CIS ao titular. Dessa forma, há fortes indícios de violação do dever de comunicar ao titular a respeito de incidente de segurança que este tenha sido atingido e possa acarretar risco ou dano relevante.

9. Em resposta, no Despacho DESPACHO DTIR - INSS (SEI nº 4190914) e no OFICIO (SEI nº 4190913), o autuado pleiteou pela inviabilidade da comunicação a todos os titulares afetados em razão da impossibilidade

técnica de levantamento dos nomes dos segurados e da desproporcionalidade da comunicação universal. Solicitou, ainda, prorrogação do prazo até a conclusão do relatório pela AGU para reavaliação da ação a ser executada. No OFÍCIO Nº 2/2023/COPDP/CGCONF/DIGOV (SEI nº 4199132), o INSS solicitou prazo indeterminado para a adequação e estruturação do plano de comunicação do INSS e atendimento da determinação.

10. O Despacho (SEI nº 4229589) deferiu o solicitação de prazo até 12/05/2023 para que o referido plano fosse apresentado, assim como fosse indicada a data prevista da realização da comunicação da ocorrência do incidente aos titulares de dados. Ao fim do prazo concedido, a determinação não foi cumprida. Entretanto, foram protocolados, no dia 24/05/2023, os documentos Anexo Plano Estratégico de Comunicação Externa (SEI nº 4279581) e Anexo Plano Estratégico de Comunicação Interno (SEI nº 4279582), que não versam sobre a comunicação ao titular do incidente de segurança em questão.

11. Por fim, adverte-se que de acordo com o art. 12, III, do Regulamento de Dosimetria da ANPD ([RESOLUÇÃO CD/ANPD Nº 4, DE 24 DE FEVEREIRO DE 2023](#)), e com o art. 32, §2º, II, do Regulamento de Fiscalização ([RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021](#)), o não cumprimento da medida preventiva, ou seja, o ANPD - Aviso 33/2022 (SEI nº 3847370), poderá ser considerado circunstância agravante em caso de instauração de processo administrativo sancionador.

### Dispositivos Legais e Regulamentares possivelmente infringidos

1. Art. 48 da Lei nº 13.709/2018 - Não comunicou ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

2. Art. 32, §2º, do Regulamento de Fiscalização (Resolução CD/ANPD nº 1/2021) - Não atendimento de medida preventiva.

### 3. SANÇÕES ADMINISTRATIVAS

1. Este **Auto de Infração** informa a abertura, em desfavor do autuado, de Processo Administrativo Sancionador que poderá culminar na aplicação de uma ou mais sanções listadas no art. 52 da LGPD, a saber:

- a) Advertência;
- b) Multa simples;
- c) Multa diária;

- d) Publicização da Infração;
- e) Bloqueio dos dados pessoais;
- f) Eliminação dos dados pessoais;
- g) Suspensão parcial do tratamento do banco de dados;
- h) Suspensão do exercício da atividade de tratamento dos dados pessoais;
- i) Proibição parcial do exercício de atividades relacionadas a tratamento de dados;
- j) Proibição total do exercício de atividades relacionadas a tratamento de dados.

2. A sanção será definida ao fim da análise do processo administrativo sancionador de acordo com o Regulamento de Dosimetria e Aplicação de Sanções Administrativas (aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023).

#### 4. INFORMAÇÕES COMPLEMENTARES

1. O ANPD - Aviso 33/2022 (SEI nº 3847370), a Nota Técnica 54 (SEI nº 4253171) e o Despacho Decisório 30 (SEI nº 4358186) foram lavrados no Processo SEI nº **00261.002177/2022-93**. O presente Auto de Infração tramita no Processo SEI nº **00261.001888/2023-21**. A Nota Técnica e o Despacho foram juntados também aos autos do presente processo.

2. Constitui dever das partes, representantes e procuradores indicar, no primeiro momento que lhes couber falar nos autos, o endereço eletrônico e o endereço residencial ou profissional onde receberão as notificações, bem assim atualizar essas informações sempre que ocorrer qualquer modificação temporária ou definitiva (Art. 12, §2º, Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1, de 28/10/2021 - Regulamento de Fiscalização). Caso não haja solicitação de atualização, as intimações relacionadas a este Processo serão enviadas para o Usuário Externo que protocola documentos em nome do autuado.

3. Conforme o art. 55-J, II da LGPD, e o art. 5, § 1º e § 2º, do Regulamento de Fiscalização, a ANPD realizará análise de sigilo das informações e documentos apresentados mediante solicitação fundamentada e individualizada. Em não havendo tal requisição, as informações fornecidas poderão ser tornadas públicas. No caso de solicitação de acesso restrito, as informações e documentos devem ser apresentados em duas versões: (i) **uma versão integral, classificada como de ACESSO RESTRITO** a qual será apartada

em anexo; e (ii) **uma versão classificada como PÚBLICA** a qual deve ser editada com a omissão ou rasura das informações consideradas sigilosas.

## 5. INTIMAÇÃO

INTIMA-SE o autuado para ciência:

1. de que responde pelo(s) fato(s) em processo administrativo sancionador **e que tem o prazo de 10 (dez) dias úteis, a partir da ciência deste Auto de Infração, para apresentar Defesa** perante a Coordenação-Geral de Fiscalização da Autoridade Nacional de Proteção de Dados, via SEI, conforme instruções do Anexo 01, de acordo com o art. 47, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.
2. da descrição do fato ou do ato constitutivo da infração e do dispositivo legal ou regulamentar infringido (*Item 2. Descrição dos Fatos e dos Dispositivos Normativos Infringidos*);
3. das sanções aplicáveis (*Item 3. Sanções Administrativas*);
4. da finalidade deste Auto de Infração e das providências necessárias (*Item 5. Intimação*);
5. de que os prazos informados neste Auto de Infração correrão independentemente de manifestação do autuado; e
6. das demais informações constantes neste **Auto de Infração**.

### ANEXO 01: Instruções ao autuado

Quanto ao ACESSO AO PROCESSO indicado neste Auto de Infração:

1) O acesso ao processo indicado neste Auto de Infração dar-se-á exclusivamente por meio do Sistema SEI, acessível na Página da Presidência da República (<https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico>).

Informações detalhadas sobre os requisitos para acesso ao sistema (cadastramento e credenciamento); acesso por autoridades públicas, partes ou procuradores; e sobre o uso do sistema estão disponíveis no link acima. A

visualização de processos e documentos sigilosos depende de autorização da área técnica responsável, após solicitação formal da parte.

2) Constitui dever das partes, representantes e procuradores indicar, no primeiro momento que lhes couber falar nos autos, o endereço eletrônico e o endereço residencial ou profissional onde receberão as notificações, bem assim atualizar essas informações sempre que ocorrer qualquer modificação temporária ou definitiva (Art. 3º, II, III e IV, e Art. 4º, IV da Lei nº 9.784/1999).

#### Quanto à apresentação de DEFESA:

3) No caso de o autuado oferecer Defesa ao Auto de Infração, esta deverá ser formalmente dirigida à Coordenação-Geral de Fiscalização e protocolada no respectivo processo administrativo sancionador no Sistema SEI;

4) O autuado deverá indicar seu faturamento no último exercício concluído, excluídos os tributos de que trata o inciso III do § 1º do art. 12 do Decreto-Lei nº 1.598, de 26 de dezembro de 1977, relativo ao ramo de atividade empresarial em que ocorreu a infração;

5) O autuado deverá utilizar o peticionamento eletrônico do Sistema SEI acessível por meio da página da Presidência da República. Documento que, em razão do formato, do tamanho ou de outra característica, não possa ser encaminhado por meio desse canal, deve ser apresentado por cópia ou segunda via, ou mídia digital, exceto nos casos em que houver determinação legal para apresentação de originais, cabendo ao responsável e/ou interessado manter os originais sob sua guarda;

6) A defesa pode ser apresentada diretamente pelo destinatário do Auto de Infração ou por intermédio de procurador regularmente constituído nos autos, conforme previsto no Art. 3º, IV da Lei nº 9.784/1999; pode, ainda, ser apresentada pelo Encarregado pelo tratamento de dados pessoais, por força do art. 5º, VIII, c/c art. 41, §2º da Lei nº 13.709/2018.

7) Caso haja procurador constituído nos autos, as comunicações processuais subsequentes serão dirigidas ao Encarregado com cópia a esse representante, conforme disposto no Art. 41, § 2º, da Lei nº 13.709/2018 c/c art. 3º, IV da Lei

nº 9.784/1999. Se houver mais de um procurador, deve ser indicado o nome daquele a quem deverão ser encaminhadas as comunicações.

8) Caso haja interesse do autuado, as provas a serem produzidas na fase de instrução devem ser indicadas na Defesa de forma individualizada e devidamente justificadas.

Quanto ao pagamento de MULTA, se aplicada:

9) Em caso de aplicação de pena de MULTA, o não pagamento da multa aplicada implicará na inscrição do devedor no cadastro de não quitados do Setor Público Federal (Cadin) em 75 dias contados da data da intimação, bem como em dívida ativa da União e, se for o caso, cobrança judicial através de órgão competente da Advocacia-Geral da União.

Outras informações:

10) Os prazos informados neste Auto de Infração correrão independentemente de manifestação do autuado, consoante exposto no art. 10, II do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

11) Conforme disposto no art. 48 do Regulamento de Fiscalização, a ANPD poderá realizar diligências e juntar novas provas aos autos, independentemente do prazo de defesa do autuado, visando à celeridade processual e à mitigação de riscos, assegurado o contraditório.



Documento assinado eletronicamente por **Ravvi Augusto de Abreu Coutinho Madruga, Coordenador(a)**, em 03/08/2023, às 11:42, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida informando o código



verificador **4411917** e o código CRC **1C8C48A8** no site:  
[https://super.presidencia.gov.br/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

---

Referência: Processo nº 00261.001888/2023-21

SUPER nº 4411917

		
<b>REPÚBLICA FEDERATIVA DO BRASIL</b>		
<b>CADASTRO NACIONAL DA PESSOA JURÍDICA</b>		
NÚMERO DE INSCRIÇÃO <b>29.979.036/0001-40</b> MATRIZ	<b>COMPROVANTE DE INSCRIÇÃO E DE SITUAÇÃO CADASTRAL</b>	DATA DE ABERTURA <b>13/04/1978</b>
NOME EMPRESARIAL <b>INSTITUTO NACIONAL DO SEGURO SOCIAL</b>		
TÍTULO DO ESTABELECIMENTO (NOME DE FANTASIA) <b>COORDENACAO GERAL DE ORCAMENTO FINANÇAS E CONTABILIDADE</b>		PORTE <b>DEMAIS</b>
CÓDIGO E DESCRIÇÃO DA ATIVIDADE ECONÔMICA PRINCIPAL <b>84.30-2-00 - Seguridade social obrigatória</b>		
CÓDIGO E DESCRIÇÃO DAS ATIVIDADES ECONÔMICAS SECUNDÁRIAS <b>Não informada</b>		
CÓDIGO E DESCRIÇÃO DA NATUREZA JURÍDICA <b>110-4 - Autarquia Federal</b>		
LOGRADOURO <b>ST SAUS QUADRA 02 BLOCO O</b>	NÚMERO <b>6</b>	COMPLEMENTO <b>ANDAR</b>
CEP <b>70.070-946</b>	BAIRRO/DISTRITO <b>ASA SUL</b>	MUNICÍPIO <b>BRASILIA</b>
		UF <b>DF</b>
ENDEREÇO ELETRÔNICO <b>CGOFC@PREVIDENCIA.GOV.BR</b>		TELEFONE <b>(61) 3313-4509</b>
ENTE. FEDERATIVO RESPONSÁVEL (EFR) <b>UNIÃO</b>		
SITUAÇÃO CADASTRAL <b>ATIVA</b>		DATA DA SITUAÇÃO CADASTRAL <b>03/11/2005</b>
MOTIVO DE SITUAÇÃO CADASTRAL		
SITUAÇÃO ESPECIAL *****		DATA DA SITUAÇÃO ESPECIAL *****

Aprovado pela Instrução Normativa RFB nº 1.863, de 27 de dezembro de 2018.

Emitido no dia 12/07/2023 às 14:20:08 (data e hora de Brasília).

Página: 1/1



**AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS**  
**Coordenação-Geral de Fiscalização**

Nota Técnica nº 54/2023/CGF/ANPD

**1. INTERESSADO**

1.1. Instituto Nacional do Seguro Social (INSS).

**2. ASSUNTO**

2.1. Comunicação de Incidente de Segurança com Dados Pessoais.

**3. REFERÊNCIAS**

- 3.1. Anexo nota (3701050);
- 3.2. ANPD - Aviso 33/2022 (3847370);
- 3.3. Certidão de Intimação Cumprida (3849789);
- 3.4. Formulário de Incidente de Segurança - ANPD em atendimento 3847370 - ANPD - Aviso (3850818);
- 3.5. Nota Técnica em atendimento 3847370 - ANPD - Aviso (3850819);
- 3.6. Manifestação INSS (3860331);
- 3.7. Despacho atendimento 3847370 - ANPD - Aviso (3850820);
- 3.8. Nota Técnica 13 (4046230);
- 3.9. Despacho Decisório 3 (4055193);
- 3.10. ANPD - Ofício 58 (4055455);
- 3.11. Certidão de Intimação Cumprida (4139331);
- 3.12. Recibo Ofício Nº 58/2023/CGF/ANPD (4157752);
- 3.13. Portaria PRES/INSS Nº 30, de 15 de fevereiro de 2023 (4145024);
- 3.14. Ofício SEI Nº 1/2023/COPDP/CGCONF/DIGOV-INSS (4190913);
- 3.15. Despacho DTIR - INSS (4190914);
- 3.16. Ofício SEI Nº 2/2023/COPDP/CGCONF/DIGOV (4199132);
- 3.17. Despacho (4229589).

**4. RELATÓRIO**

4.1. Trata-se de Comunicação de Incidente de Segurança (CIS) apresentada pelo Instituto Nacional do Seguro Social (INSS), com fulcro no art. 48 da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), por meio de seu encarregado, indicado pela Portaria PRES/INSS nº 618, de 26 de julho de 2021 (3850817). A comunicação foi realizada em fases, tendo sido a preliminar (3701050) protocolada no dia 19/10/2022.

4.2. Apesar de o agente ter sido orientado, através do e-mail (3725180), datado de 03/11/2022, não foi apresentada a comunicação complementar e o relatório técnico de tratamento do incidente no prazo de 30 dias corridos da preliminar. No dia 22/11/2022, foi encaminhado novo e-mail (3760075) reiterando a necessidade de apresentação das informações solicitadas anteriormente, conferindo 5 (cinco) dias úteis.

4.3. Considerando a inércia do agente e a potencial gravidade do incidente, que teria afetado a base de beneficiários e segurados do INSS, que inclui dados financeiros e sensíveis relacionados à saúde, foi solicitado ao INSS, por meio do Aviso CGF/ANPD 33/2022 (3847370), a apresentação de informações complementares sobre o incidente e, se cabível, a comunicação aos titulares de dados a respeito do incidente, no prazo de 10 (dez) dias úteis.

4.4. O agente foi intimado validamente a respeito do Aviso, no dia 30/12/2022, conforme certidão (3847370). Nesta mesma data, o INSS protocolou a complementação da comunicação do incidente (3850818), acompanhada do Despacho (3850820) de resposta ao Aviso, e dos anexos (3850817, 3850819, 3850821, 3850822, 3850823 e 3850824).

4.5. Justificou o não atendimento ao prazo de comunicação sugerido pela ANPD em razão da necessidade de se realizar uma análise complexa e minuciosa dos dados e do ambiente afetado.

4.6. No entanto, não realizou a comunicação aos titulares sob alegação de ainda estar analisando a legitimidade dos acessos suspeitos vez que originados de usuários credenciados pela Advocacia-Geral da União (AGU). Ressaltou que as medidas de contenção do incidente foram adotadas imediatamente após o registro do incidente pela Comissão de Tratamento e Resposta a Incidentes Cibernéticos (CTIR) da Empresa de Tecnologia e Informações da Previdência (DATAPREV).

4.7. Solicitou, por meio de e-mail (3860326), o apensamento ao processo do Relatório Conclusivo do Incidente (3860331) em 04/01/2023.

4.8. Conforme relatado no formulário presente na manifestação final do controlador (3860331), no dia 23/09/2022, durante monitoramento de rotina de desempenho do servidor [REDACTED] foi identificado um aumento de 4 a 6 vezes no volume de acessos às aplicações em relação aos meses anteriores, sem justificativa operacional aparente. Em razão disso, foi realizada investigação para apuração de possível incidente de segurança com dados pessoais.

4.9. O volume extraordinário de acessos teve origem em uma rede autorizada, conectada por meio [REDACTED] com o uso de credenciais válidas. Nos meses de agosto e setembro de 2022, foram realizadas mais de 90 milhões de consultas ao Sistema Corporativo de Benefícios do INSS (SISBEN) e 9 milhões de consultas ao BLH00, quantidade quase três vezes maior que a registrada no mês de junho do mesmo ano.

4.10. O tratamento do incidente cibernético, identificado pela operadora DATAPREV como [REDACTED] foi documentado na NT/CTIR/001/2023 às fls. 11-26 da manifestação final do INSS (3860331).

4.11. As aplicações afetadas estão identificadas na Tabela 1 como BLH00.12 e STP05\_SISBEN. SISBEN é o Sistema Corporativo de Benefícios do INSS e, conforme Figura 3 da NT/CTIR/001/2023 (3860331), o BLH00 é o Sistema Único de Benefícios DATAPREV.

4.12. A maior parte dos acessos no período foi realizada por três usuários do sistema, pertencentes ao grupo de acesso [REDACTED]. Tais usuários pertenceriam à Advocacia Geral da União (AGU), que teria acesso ao sistema em razão de um convênio firmado com o INSS. Afirmou-se que a gestão de acesso aos sistemas se daria de forma descentralizada, pelos órgãos conveniados, sem qualquer validação por parte do INSS.

4.13. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais de acesso dos três usuários e o fato foi reportado, no dia 28/09/2022, à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do INSS e ao servidor da AGU responsável pela gestão do grupo de acesso [REDACTED] a fim de verificar a legitimidade dos acessos volumétricos. Foi realizada, na mesma data, a captura do tráfego do sistema por 30 minutos a fim de identificar eventuais consultas volumétricas automatizadas realizadas no sistema.

4.14. O responsável na AGU pela gestão do referido grupo de acesso não reconheceu as consultas como válidas e ainda teria informado que 44 dos 66 usuários cadastrados poderiam ser excluídos. Desses, 39 seriam pessoas desconhecidas e 5 seriam ex-estagiários, sem vínculo atual com a instituição, indicando que 2/3 dos usuários do grupo de acesso estavam cadastrados indevidamente.

4.15. A análise da captura do tráfego de rede entre a AGU e o servidor de aplicação comprovou a execução de consultas volumétricas ao sistema. Identificou-se acesso a dados pessoais diversos dos

beneficiários do INSS, tais como Nome, CPF, NIT, Identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes, conforme ilustrado na Figura 3 da NT/CTIR/001/2023 (3860331).

4.16. Foi possível identificar que 84% das 486.503 pesquisas realizadas no período analisado originaram-se de somente 22 estações de trabalho, que estariam realizando mais de 17 mil consultas a cada 30 minutos. Informou, no entanto, que o identificador da estação de trabalho de origem da conexão

4.17. Tal padrão de acesso automatizado guardaria semelhança com um incidente de segurança anterior, ocorrido em 24/11/2021 e cadastrado sob o número EVTD n. 202111003583. Foi observada, em ambos os casos, a utilização de uma mesma senha para diversos usuários distintos.

4.18. Foram identificadas, ainda, consultas suspeitas realizadas por um segundo grupo de usuários denominado . Foram realizados , que também identificou a existência de 12 usuários desconhecidos cadastrados, além de pessoas já desligadas do setor. A sanitização dos grupos de acesso estaria sendo realizada.

4.19. Concluiu-se, portanto, que apesar do uso de credenciais válidas, as consultas automatizadas provavelmente foram realizadas por agentes maliciosos para a captura dos dados dos sistemas do INSS. A captura de credenciais seria facilitada pelo uso

4.20. Diante da recorrência de incidentes, a CTIR da DATAPREV recomendou a adoção de medidas enfáticas para proteção dos dados tais . O acompanhamento dessas implementações correrá por meio do Plano de Segurança entre o INSS e a DATAPREV.

4.21. Em 30/10/2022 a DATAPREV teria decidido bloquear o tráfego da AGU . INSS estaria negociando com os demais entes conveniados a migração para a conexão criptografada e segura.

4.22. No formulário de comunicação de incidente, às fls. 3-10 de sua manifestação (3860331), o INSS afirma desconhecer o nível de risco do incidente aos titulares, apesar de reconhecer que o incidente afetou dados sensíveis referente à saúde, de comprovação oficial e financeiro de um número indeterminado de seus beneficiados e segurados.

4.23. Reconheceu, no entanto, a possibilidade de os dados virem a ser utilizados para cometimento de fraudes ou assédio comercial aos beneficiários. Apesar disso, por não possuir registros detalhados dos acessos realizados que permitam individualizar os titulares afetados no incidente, não comunicou a nenhum deles o ocorrido.

4.24. Afirmou que o Relatório de Impacto à Proteção de Dados dos sistemas hospedados encontra-se em elaboração e que seria de alta complexidade.

4.25. Como medidas de segurança prévias ao incidente, mencionou adotar as melhores práticas e ter restringido o acesso ao sistema a entes autorizados que façam . Reforçou que a gestão de credenciais é feita de forma descentralizada, sendo cada órgão conveniado responsável pelo cadastro e governança de seus usuários.

4.26. Após o incidente, informa que adotará medidas para suspender os grupos de usuários envolvidos no incidente, recadastrar os usuários,

4.27. A análise da comunicação de incidente foi realizada na Nota Técnica 13 (4046230) que, em síntese, sugeriu que fosse determinado ao INSS a comunicação do incidente de segurança aos titulares de dados. Tal sugestão foi embasada em razão do elevadíssimo número de titulares potencialmente afetados, pois trata-se de sistemas que armazenam uma grande quantidade de dados pessoais tais como Nome, CPF, NIT, Identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes, que poderiam expor os titulares a riscos de fraudes e roubo de identidade. No mesmo sentido, o próprio INSS informou como critério para comunicação à ANPD que "O incidente de segurança

pode acarretar risco ou dano relevante aos titulares".

4.28. A determinação de comunicação aos titulares, no prazo de 10 (dez) dias úteis foi formalizada no Despacho Decisório 3 (4055193) e encaminhada ao INSS por meio do ANPD - Ofício 58 (4055455). O INSS foi intimado da referida decisão por via eletrônica no dia 10/04/2023, conforme Certidão de Intimação Cumprida (4139331). O agente de tratamento também confirmou o recebimento do Ofício, conforme e-mail do INSS (4157752), de 12/4/2023 e e-mail do DATAPREV (4158098), de 13/04/2023.

4.29. Em resposta, o INSS apresentou a Portaria PRES/INSS N° 30, de 15 de fevereiro de 2023 (4145024), com a alteração do encarregado, protocolou Ofício (4190913) e Despacho (4190914) em 25/04/2023. Em resumo, pleiteou pela inviabilidade da comunicação a todos os titulares afetados em razão da impossibilidade técnica de levantamento dos nomes dos segurados e da desproporcionalidade da comunicação universal. Solicitou, ainda, prorrogação do prazo até a conclusão do relatório pela AGU para reavaliação da ação a ser executada.

4.30. Em Ofício (4199132) de 27/04/2023, o INSS solicitou prazo indeterminado para a adequação e estruturação do plano de comunicação do INSS e atendimento da determinação. O prazo foi deferido até o dia 12/05/2023 para que o referido plano fosse apresentado, assim como fosse indicada a data prevista da realização da comunicação da ocorrência do incidente aos titulares de dados, nos termos do art. 48 da LGPD, conforme o Despacho (4229589) encaminhado por e-mail (4232805 e 4246163) ao controlador.

4.31. Ao fim do prazo concedido, 12/05/2023, a determinação não foi cumprida. Entretanto, foram protocolados, no dia 24/05/2023, o Ofício SEI-INSS (4279580), juntamente com o Plano Estratégico de Comunicação Externa (4279581) e Plano Estratégico de Comunicação Interna (4279582).

4.32. É o relatório

## 5. ANÁLISE

5.1. Considerando o disposto no art. 73 do Regimento Interno da Autoridade Nacional de Proteção de Dados c/c o art. 59 da Lei nº 9.784/1999, o prazo para apresentação de recurso à decisão proferida no Despacho CGF/ANPD (4055193) é de 10 (dez) dias corridos. O agente não apresentou recurso à decisão.

5.2. Considerando-se a data da intimação, 10/04/2023, e o prazo de 10 (dez) dias úteis conferido para cumprimento da decisão constante do Despacho Decisório 3 (4055393), a manifestação (4190913) do agente de tratamento foi apresentada tempestivamente. Entretanto, a determinação de comunicação aos titulares não foi cumprida.

5.3. Na manifestação (4190913), o controlador prestou esclarecimentos para cumprimento da decisão, sustentando não haver possibilidade técnica de levantamento de quais dados pessoais foram acessados e quais titulares afetados pelo incidente em questão, já que os dados pessoais acessados estavam em várias telas do Sistema. Adicionalmente, argumenta que o monitoramento efetuado pela DATAPREV envolve somente a volumetria dos acessos. Assim, não haveria *log* que demonstrasse quais dados foram acessados. Apesar disso, em razão do volume de acesso e quantidade de telas consumidas, subentende que o volume de dados expostos tenha sido elevado.

5.4. Quanto a possibilidade de emitir comunicado geral, o controlador defende que não se justifica o comunicado geral a todos os titulares, diante de um acesso volumétrico superior ao normal em apenas uma semana, volume que seria mínimo em relação ao quantitativo de titulares que seriam comunicados.

5.5. Sustenta também que a comunicação seria desproporcional e inviável tecnicamente, gerencialmente e financeiramente, pois causaria um dano colateral litigioso para o Estado.

5.6. Apesar das justificativas apresentadas para não efetuar a comunicação aos titulares, o controlador se comprometeu, por fim, a atender a determinação, tendo solicitado prazo para a adequação e estruturação do Plano de Comunicação do INSS. Ainda que não cumprido o prazo deferido para apresentação das informações, findado em 12/05/2023, foram apresentados o Plano Estratégico de Comunicação Externa (4279581) e o Plano Estratégico de Comunicação Interna (4279582), do Programa de Governança em Privacidade (PGP), no dia 24/05/2023.

5.7. Após análise dos planos de comunicação apresentados, verificou-se que em nada se assemelham à comunicação do incidente de segurança aos titulares afetados, conforme disposto no art. 48 da LGPD. O plano designado como de comunicação interna destina-se a "*promover uma mudança da cultura organizacional do INSS no que tange o manejo e tratamento das informações dos cidadãos envolvidos nas atividades do Instituto*", sendo direcionado a seus servidores, colaboradores terceirizados e estagiários. No mesmo sentido, o plano de comunicação externa tem como público-alvo os "*cidadãos de todo o país*" e visa "*comunicar à população geral o conteúdo estabelecido no PGP, o qual está alinhado à LGPD, evidenciando o cuidado e preocupação do INSS no que tange o manejo e tratamento das informações dos cidadãos*".

5.8. Embora no Ofício SEI Conjunto nº 1/COPDP/CGCONF/DIGOV/INSS (4279580) se afirme atender às determinações do Despacho Decisório 3 (4055193), o conteúdo das comunicações planejadas e o detalhamento das ações dos planos de comunicação não se reportam ao incidente de segurança com dados pessoais de que trata o processo em questão. Assim, não é possível afirmar, com base nos planos apresentados, que há um planejamento de comunicação a ser realizada aos titulares afetados, conforme determinado previamente.

5.9. A comunicação aos titulares afetados deve ser feita em linguagem clara e simplificada e mencionar, no mínimo, os elementos aplicáveis previstos no §1º do art. 48 da LGPD e outras informações que possam auxiliar os titulares a prevenir possíveis danos, tais como:

- a) a descrição geral do incidente e a data da ocorrência;
- b) a natureza dos dados pessoais afetados e os riscos relacionados ao incidente;
- c) as medidas tomadas e recomendadas para mitigar os efeitos do incidente; e
- d) o contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente.

5.10. Conforme já consignado na Nota Técnica 13 (4046230), em razão do elevadíssimo número de titulares potencialmente afetados; da grande quantidade de dados pessoais que os referidos sistemas armazenam, tais como Nome, CPF, NIT, Identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes; da possibilidade de expor os titulares a riscos de fraudes e roubo de identidade; e do próprio INSS ter informado como critério para comunicação à ANPD que "o incidente de segurança pode acarretar risco ou dano relevante aos titulares", persiste a necessidade de comunicação do incidente aos titulares dos dados, nos termos do art. 48 da Lei Geral de Proteção de Dados Pessoais (LGPD).

5.11. Se, pelas circunstâncias do incidente ou do ambiente de tecnologia da informação do INSS, não for possível identificar individualmente os titulares afetados pelo incidente, é razoável que não se possa exigir do controlador a comunicação individual. Independente disso, é certo que subsiste a obrigação do controlador de comunicar os titulares. A contrario sensu, se fosse permitido não realizar a comunicação em razão de falta de registros de acesso ou de limitação de mecanismos de controle e de governança dos sistemas de informações, haveria um incentivo ao descuido pelo controlador com seus sistemas de informação, para que nunca houvesse coleta ou guarda de registros, uma vez que isso ocorreria em seu benefício. Tal postura é incompatível com a previsão dos artigos 46 e 49 da LGPD.

5.12. Nesse sentido, é preciso entender que as consequências da limitação dos mecanismos de controle, registro e governança dos sistemas de informação do controlador não podem ser imputadas senão ao próprio controlador, já que resultantes de suas próprias escolhas. Por conseguinte, se não é possível individualizar os titulares afetados e permanece o dever de realizar a comunicação, cabe ao controlador realizar a comunicação a todos os titulares potencialmente afetados pelo incidente até o limite de todos os titulares constantes da base de dados, se não for possível ao controlador estabelecer um conjunto menor de titulares potencialmente afetados.

5.13. Portanto, entende-se presentes indícios de que o controlador deixou de atender ao comando do art. 48 da LGPD, em razão de não ter realizado, no prazo concedido, a comunicação aos titulares, conforme determinado pela CGF/ANPD.

## 6. CONCLUSÃO

6.1. Por todo exposto, com base no inciso I do art. 17 do Regimento Interno da Autoridade

Nacional de Proteção de Dados, c/c o inciso I do art. 37 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no Âmbito da ANPD, sugere-se a instauração de processo administrativo sancionador em razão do possível descumprimento do art. 48 da Lei nº 13.709, de 14/08/2018 (LGPD).

6.2. À consideração superior.

**ROSEMARY DE FÁTIMA ANDRADE**  
Coordenadora-Substituta de Tratamento de Incidentes de Segurança

---



Documento assinado eletronicamente por **Rosemary de Fátima Andrade, Coordenador(a) substituto(a)**, em 23/06/2023, às 10:26, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).

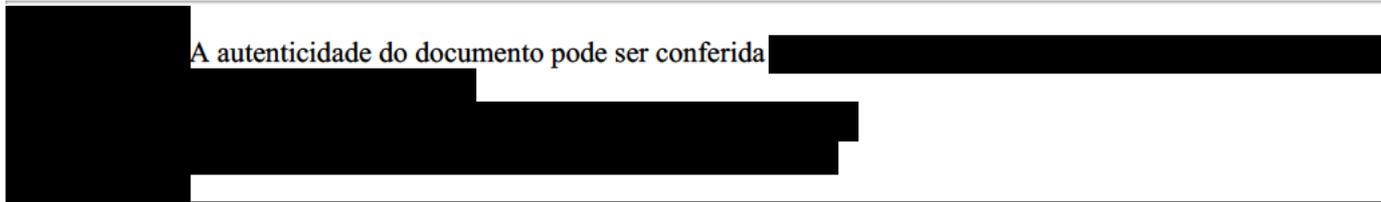
---



Documento assinado eletronicamente por **Mariana Hermínia da Costa, ANPD - Autoridade Nacional de Proteção de Dados**, em 27/06/2023, às 09:04, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).

---

A autenticidade do documento pode ser conferida



Referência: Processo nº 00261.002177/2022-93

SUPER nº 4253171

PRESIDÊNCIA DA REPÚBLICA  
Coordenação-Geral de Fiscalização

Brasília, 23 de junho de 2023.

Despacho Decisório nº 30/2023/CGF/ANPD

Processo nº 00261.002177/2022-93

Interessado: Instituto Nacional do Seguro Social (INSS).

**O COORDENADOR GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)**, no uso de suas atribuições legais e regulamentares, em especial a disposta no art. 17, incisos I e III do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 08/03/2021, examinando os autos do Processo em epígrafe, acata as razões da Nota Técnica 54/2023/CGF/ANPD (SEI nº 4253171) e decide pela instauração de processo administrativo sancionador em desfavor do **INSTITUTO NACIONAL DO SEGURO SOCIAL (INSS)**.

FABRÍCIO GUIMARÃES MADRUGA LOPES  
Coordenador-Geral de Fiscalização



Documento assinado eletronicamente por **Fabricio Guimarães Madruga Lopes, Coordenador(a)-Geral**, em 23/06/2023, às 10:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida informando o código verificador **4358186** e o código CRC **7F79F8EA** no site:

[https://super.presidencia.gov.br/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

Referência: Processo nº 00261.002177/2022-93

SUPER nº 4358186

## Certidão de Intimação Cumprida - 4464285

<b>Tipo de Destinatário:</b>	Pessoa Física
<b>Destinatário:</b>	EDSON PINHEIRO ALVARISTA
<b>Tipo de Intimação:</b>	Apresentação de Defesa
<b>Documento Principal da Intimação:</b>	ANPD - Auto de Infração 1 (4411917)
<b>Data de Expedição da Intimação:</b>	03/08/2023 11:53:53
<b>Tipo de Cumprimento da Intimação:</b>	Consulta Direta
<b>Data do Cumprimento:</b>	03/08/2023
<b>Usuário Responsável pelo Cumprimento:</b>	EDSON PINHEIRO ALVARISTA

Esta Certidão formaliza o cumprimento da intimação eletrônica referente aos dados acima, observado o seguinte:

- O Tipo de Cumprimento "Consulta Direta" indica que o "Destinatário" realizou a consulta aos documentos da intimação diretamente no sistema antes do término do Prazo Tácito para intimação.
  - O Prazo Tácito para intimação é definido conforme normativo aplicável ao órgão, em que, a partir da "Data de Expedição da Intimação", o Destinatário possui o referido prazo para consultar os documentos diretamente no sistema, sob pena de ser considerado automaticamente intimado na data de término desse prazo.
- O Tipo de Cumprimento "Por Decurso do Prazo Tácito" indica que não ocorreu a mencionada consulta aos documentos da intimação diretamente no sistema, situação na qual a Certidão é gerada automaticamente na data de término desse prazo.
  - No caso do Prazo Tácito terminar em dia não útil, a geração automática da Certidão ocorrerá somente no primeiro dia útil seguinte.
- Conforme regras de contagem de prazo processual e normas afetas a processo eletrônico, tanto no Prazo Tácito para intimação como nos possíveis prazos externos para Peticionamento de Resposta:
  - sempre é excluído da contagem o dia do começo e incluído o do vencimento;
  - o dia do começo e o do vencimento nunca ocorrem em dia não útil, prorrogando-o para o primeiro dia útil seguinte;
  - a consulta a intimação ocorrida em dia não útil tem a correspondente data apresentada em linha separada, sendo a "Data do Cumprimento" a do primeiro dia útil seguinte.
- Para todos os efeitos legais, somente após a geração da presente Certidão e com base exclusivamente na "Data do Cumprimento" é que o Destinatário, ou a Pessoa Jurídica ou Física por ele representada, é considerado efetivamente intimado e são iniciados os possíveis prazos externos para Peticionamento de Resposta.
  - Caso a intimação se dirija a Pessoa Jurídica, ela será considerada efetivamente intimada na "Data do Cumprimento" correspondente à primeira Certidão gerada referente a Usuário Externo que possua poderes de representação.



ADVOCACIA-GERAL DA UNIÃO  
PROCURADORIA-GERAL FEDERAL  
PROCURADORIA FEDERAL ESPECIALIZADA JUNTO AO INSTITUTO NACIONAL DO SEGURO SOCIAL -  
PFE/INSS - SEDE  
SUBPROCURADORIA-GERAL  
SETOR DE AUTARQUIAS SUL QUADRA 2 BLOCO O 3º ANDAR

**ILUSTRÍSSIMO SENHOR COORDENADOR-GERAL DE FISCALIZAÇÃO DA AGÊNCIA NACIONAL DE  
PROTEÇÃO DE DADOS - ANPD**

**Processo nº 00261.001888/2023-21**

O **INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS**, autarquia federal com sede em Brasília no Setor de Autarquias Sul, Bloco O, devidamente representada por seu Presidente e pela Procuradoria Federal Especializada do INSS, vem perante V. Senhoria apresentar **DEFESA** em face do Auto de Infração nº 1/2023/FIS/CGF/ANPD, consoante os fatos e fundamentos a seguir aduzidos.

## **1. DA AUTUAÇÃO**

1. O INSS foi autuado pela Coordenação de Fiscalização da ANPD sob a perspectiva do suposto cometimento das seguintes infrações à Lei nº 13.709, de 14 de agosto de 2019 – denominada Lei Geral de Proteção de Dados – LGPD:

a) Não comunicação de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados, conforme artigo 48 da LGPD; e

b) Não atendimento de medida preventiva, conforme artigo 32, § 2º, do Regulamento de Fiscalização da ANPD, aprovada por meio da Resolução CD/ANPD nº 1/2021.

2. Nada obstante as considerações da fiscalização da ANPD, reputa-se que a autuação e a correspondente pretensão sancionatória não devam subsistir.

## **2. DA TEMPESTIVIDADE DA DEFESA**

3. Convém ressaltar que, acessada a comunicação do auto de infração no dia 03/08/2023, no Sistema Eletrônico de Informações – SEI, o prazo de 10 (dez) dias úteis tem por termo final o dia 17/08/2023, em face do que deve ser considerada tempestiva a defesa ora apresentada, observados os termos do artigo 8º do Anexo da Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

## **3. DO INCIDENTE CIBERNÉTICO**

4. No que diz respeito ao mérito da questão, a atuação ora impugnada está assentada no aumento volumétrico atípico de consultas de dados contidos no Sistema PLENUS, do INSS, a partir de acessos realizados por meio da rede da Advocacia-Geral da União.

5. O Sistema Plenus consiste em ferramenta de gestão de benefícios previdenciários e assistenciais, atuando como uma interface completa para gerir, consultar e solucionar pendências relativas a esses benefícios. **Não é o sistema por meio do qual o INSS concede os benefícios**, mas concentra informações decorrentes. **Não compreende a gestão de senhas ou de acesso** dos segurados ou beneficiários aos canais, sistemas ou aplicativos de atendimento e de requerimento de serviços ao INSS.

6. De acordo com Empresa de Tecnologia e Informações da Previdência – DATAPREV, às 17h46 do dia 23/09/2022, durante acompanhamento de rotina do mainframe do INSS, “... foram observadas consultas a dados de 4 a 6 vezes acima do comportamento normal, [REDACTED], e outros elementos com possibilidade de intenção maliciosa, originados da rede da AGU [REDACTED], com destino [REDACTED] [REDACTED]”

7. O evento foi classificado como o [REDACTED]

### 3.1. **A interlocução do INSS com a ANPD**

8. De acordo com o Recibo Eletrônico de Protocolo – 3701051, datado de 19/10/2022, o Encarregado de Dados do INSS providenciou o preenchimento e o encaminhamento do formulário disponibilizado pela ANPD.

9. A ANPD entrou em contato com o encarregado do INSS em 26/10/2022 via e-mail, sugerindo reunião em função da comunicação de incidente encaminhada (35014.528489/2022-29, seq. 4, fls. 11).

10. Novo e-mail da ANPD foi encaminhado aos 03/11/2022 (35014.528489/2022-29, seq. 4, fls. 9), informando a necessidade de comunicação dos titulares e solicitando alguns documentos complementares, a saber:

- a) Formulário de incidente de segurança com informações complementares; e
- b) Relatório técnico de tratamento do incidente

11. A solicitação foi reiterada em 22/11/2022 alertando para a caracterização de obstrução da fiscalização pela ausência de resposta (35014.528489/2022-29, seq. 4, fls. 10).

12. O encarregado respondeu a ANPD por e-mail encaminhado em 22/11/2022, informando que providências estavam sendo tomadas nas esferas do INSS, da AGU e da DATAPREV e concluiu esclarecendo que o relatório seria confeccionado e encaminhado.

13. A DATAPREV encaminhou ao INSS, via e-mail, nota técnica de caráter conclusivo em atendimento ao Incidente de Segurança 202209004099, em 12/12/2022 (35014.528489/2022-29, seq. 3).

14. A ANPD então emitiu o AVISO nº 33/2022/CGF/ANPD (35014.528489/2022-29, seq. 4, fls. 15), em 29/12/2022, com base no artigo 55-J, inciso IV, da LGPD, no artigo 17 do Regimento Interno da ANPD (Portaria nº 1, de 8 de março de 2021) e no artigo 34 do Regulamento de Fiscalização (Resolução CD/ANPD nº1/2021). Ao referido aviso foi determinada a juntada dos documentos que seguem:

- a) esclarecimentos a respeito da atuação do agente de tratamento notificante, ou seja, se atua como controlador ou operador dos dados pessoais;
- b) formulário de incidente de segurança com informações complementares;
- c) relatório técnico de tratamento do incidente; e
- d) comunicação aos titulares a respeito da possível violação do sigilo dos dados no incidente, se cabível.

15. Ao final do texto do aviso mencionado a ANPD fez constar exortação no sentido da instauração de Processo Administrativo Sancionador, caso não fossem atendidas suas requisições (35014.528489/2022-29, seq. 4, fls. 15).

16. A Coordenadora de Proteção de Dados Substituta encaminhou via e-mail, em 04/01/2023, Relatório Conclusivo de Incidente confeccionado pela DATAPREV (35014.528489/2022-29, seq. 4, fls. 113).

17. A DATAPREV confeccionou ainda memorando com objetivo de atender os questionamentos e as solicitações formuladas ao AVISO nº 33/2022/CGF/ANPD (35014.528489/2022-29, seq. 4, fls. 113). Esses documentos foram encaminhados para o Encarregado pelo Tratamento de Dados Pessoais do INSS por e-mail (35014.528489/2022-29, seq. 4, fls. 140).

18. A DATAPREV ainda encaminhou ofício ao INSS em 06/02/2023 recomendando, a título de providências de curto prazo, o fechamento da INFOVIA destinada aos acessos da Advocacia-Geral da União - AGU à plataforma previdenciária (Seq. 13, NUP 35014.528489/2022-29).

19. A ANPD editou a Nota Técnica nº 13/2023/CGF/ANPD em 17/03/2023 (35014.528489/2022-29, seq. 4, fls. 141). Da referida Nota é possível extrair os aspectos que seguem:

- a) apontou que o INSS não demonstrou a comunicação aos titulares dos dados vazados e determinou a comunicação de “todos os titulares presentes na base de dados”;
- b) indeferiu o pedido de sigilo dos autos do processo administrativo pertinente à autuação à medida que, não foi realizada referência a qualquer informação sigilosa específica que justificasse o pedido; e
- c) previu notificar a AGU para manifestar-se sobre os fatos dos autos;

20. A conclusão da Nota Técnica nº 13/2023/CGF/ANPD trouxe o conteúdo que segue:

## 6. CONCLUSÃO

6.1. Ante o exposto, sugere-se que seja determinado ao Instituto Nacional do Seguro Social (INSS) a comunicação do incidente de segurança aos titulares de dados, nos termos do previsto no art. 48 da Lei Geral de Proteção de Dados c/c o inciso XXII do art. 17 do Regimento Interno da Autoridade Nacional de Proteção de Dados - ANPD.

6.2. Ainda, que seja encaminhado ofício à Advocacia-Geral da União (AGU) para que se manifeste no presente processo quando ao incidente reportado pelo INSS requisitando, com base no inciso I do art. 5º do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dado, as seguintes informações:

- a) O instrumento que prevê o compartilhamento de dados entre o INSS e a AGU.
- b) Esclarecimento sobre a finalidade do tratamento de dados realizado com os dados do INSS e, especificamente, se atua como controlador em relação a tais atividades de tratamento.
- c) Se reconhece como válidos os acessos volumétricos apontados como irregulares pela DATAPREV e INSS ao sistema SISBEN.
- d) Se foi consultada pelo INSS a respeito da possível irregularidade dos acessos volumétricos ao sistema SISBEN e, se cabível, quando foi consultada e em que data foi transmitida a resposta.
- e) O relatório de tratamento do incidente de segurança produzido pela AGU e as conclusões da apuração a que se referiu o INSS.
- f) Apresente a política ou, alternativamente, explicação sobre como é feita a gestão de acessos aos sistemas do INSS pela AGU.
- g) Se elaborou relatório de impacto à proteção de dados pessoais referentes às atividades de tratamento de dados afetadas no incidente.

21. A AGU foi então instada pela ANPD por meio do Ofício N° 53/2023/CGF/ANPD, 09/04/2023, a prestar informações sobre o incidente em questão (35014.528489/2022-29, seq. 4, fls. 146).

22. Acolhendo sugestões constantes da Nota Técnica n° 13/2023/CGF/ANPD, por meio do DESPACHO DECISÓRIO N° 3/2023/CGF/ANPD (35014.528489/2022-29, seq. 4, fls. 148) de 09/04/2023, foi determinada ao INSS que promovesse no prazo de 10 (dez) dias comunicação pretendida.

23. A ANPD, por meio do Ofício N° 58/2023/CGF/ANPD conferiu ciência ao encarregado de dados do INSS acerca do DESPACHO DECISÓRIO N° 3/2023/CGF/ANPD e estabeleceu prazo de 10 (dez) dias úteis para apresentação de informações (certidão de intimação cumprida – 4139331 consta de fls. 154 do seq. 4 do NUP 35014.528489/2022-29).

24. Com o objetivo de prover a avaliação das determinações constantes da Nota Técnica n° 13/2023/CGF/ANPD, o encarregado de dados do INSS solicitou à Divisão de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - DTIR do INSS esclarecimento sobre a possibilidade de identificar as pessoas a serem eventualmente comunicadas (35014.528489/2022-29, seq. 6).

25. A Chefe da DTIR esclareceu no Despacho de 17/04/2023 (SEI/INSS 11355158) “... que **não há possibilidade técnica de levantamento dos nomes dos segurados** envolvidos no incidente ...”. (35014.528489/2022-29, seq. 7).

26. O encarregado de dados do INSS, por meio de Despacho de 19/04/2023 (SEI/INSS 11379737), entendeu oportuno pedir esclarecimentos à AGU, em especial no sentido de certificar a ocorrência de casual vazamento, da natureza dos dados e a eventual identificação dos titulares (35014.528489/2022-29, seq. 8).

27. Por meio do DESPACHO n. 00072/2023/GAB/PFE-INSS-SEDE/PGF/AGU constante do seq. 9 do NUP 35014.528489/2022-29, foram solicitados esclarecimentos à AGU.

28. Nada obstante, a ANPD considerou descumprida medida preventiva e instaurou procedimento sancionador e intimou o INSS para apresentar defesa em 10 (dez) dias (SUPER/PR - 4411917 - ANPD - Auto de Infração, 03/08/2023, doc. SEI 12729700, 35014.293086/2023-34).

29. A partir do AVISO n° 33/2022/CGF/ANPD, da Nota Técnica n° 13/2023/CGF/ANPD, do DESPACHO DECISÓRIO N° 3/2023/CGF/ANPD, evidencia-se que o ponto nodal do presente processo sancionador é o aventado descumprimento do dever de comunicação aos titulares dos dados pretensamente vazados conforme caput do artigo 48 da LGPD, seja de forma individual ou ampla na forma do §2º do mesmo artigo.

30. Quando da abordagem dos fundamentos jurídicos da defesa, o dever de comunicar os titulares será abordado.

### 3.2. Medidas preventivas adotadas pelo INSS

31. Como medidas preventivas de acessos não autorizados o INSS vem adotando a obrigatoriedade de uso de certificado digital para todos os acessos a sistemas de benefícios aos servidores do INSS e usuários externos, incluindo os ambientes por meio do qual se consegue acesso ao Sistema Plenus.

32. Isso foi estabelecido por meio da Portaria DTI/INSS n° 67, de 21/12/2021.

33. Além da certificação digital, adquirida do Serpro no modelo A3 - token [\[1\]](#), foi estabelecido também que os acessos aos sistemas pelos usuários em teletrabalho ocorreriam ainda com o [REDACTED]

34. Quanto ao Sistema Plenus, ambas as providências foram implementadas em agosto de 2022.

35. Ademais, no mês de dezembro de 2022 houve o [REDACTED] utilizada pela AGU para acesso ao Sistema Plenus, [REDACTED]

36. Tais medidas, segundo a DATAPREV, [REDACTED]

37. Contemporaneamente, a DTIR articulou a intermediação entre a DATAPREV e a AGU para o saneamento dos acessos [REDACTED]. Assim, foram [REDACTED]

38. Após esse evento, não houve registro de incidentes relacionados aos sistemas do INSS utilizados pela AGU.

39. Vale ainda mencionar que o INSS aprovou seu Plano de Dados Abertos por meio da Resolução CEGOV/INSS nº 29, de 1º de junho de 2023<sup>[2]</sup> e está por aprovar seu Programa de Governança em Privacidade, por meio da Resolução CEGOV/INSS nº 32, de 15 de agosto de 2023.

### 3.3. Contribuições da AGU para o tratamento do incidente.

40. Por meio da Nota Técnica n. 00027/2023/SGE/AGU, confeccionada em 24/04/2023, a AGU esclareceu que desempenhava a função de operador de dados pessoais. Considere-se a argumentação:

[REDACTED]

41. A AGU complementou as informações prestadas por meio da Nota Técnica n. 00002/2023/SGE/AGU, elaborada em 24/04/2023, com o relatório técnico acerca do incidente. A referida nota definiu seu objeto conforme segue:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

42. Na sequência, estabeleceu a cronologia precisa dos fatos a partir da identificação do incidente cibernético conforme segue:

[REDACTED]

43. A Nota Técnica n. 00002/2023/SGE/AGU evidenciou ainda as recomendações realizadas pela DATAPREV conforme segue:

[REDACTED]

44. Por outro lado, como a origem do incidente se deu em ambiente externo, em especial em uma unidade da AGU, é importante trazer ao conhecimento da ANPD as iniciativas investigativas desenvolvidas por este órgão.

45. De acordo com a Nota Técnica n. 00002/2023/SGE/AGU [\[3\]](#) a AGU apontou a título de resultados investigativos o quanto segue:

[REDACTED]

46. A título de providências de caráter complementar implementadas pela AGU foram mencionadas na Nota Técnica n. 00002/2023/SGE/AGU as seguintes medidas:

[REDACTED]

[REDACTED]

[REDACTED]

47. No que toca às conclusões e recomendações a AGU pontou que:

[REDACTED]

[REDACTED]

#### 4. DOS FUNDAMENTOS DA DEFESA

48. Apresentados os fatos, que já são de conhecimento da ANPD, posto que devidamente comunicados e tratados a tempo e modo, passe-se ao desenvolvimento da defesa.

##### 4.1. O INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS

49. O INSS é uma autarquia federal criada pela Lei nº 8.029, de 12 de abril de 1990, a partir da fusão dos extintos Instituto de Administração da Previdência e Assistência Social - IAPAS, com o Instituto Nacional de Previdência Social - INPS.

50. Nessa condição, consideradas as diversas alterações legislativas que trataram de suas atribuições específicas ao longo do tempo, atualmente tem suas competências previstas no artigo 2º do Decreto nº 10.995, de 14 de março de 2022, nele assim disposto:

*Art. 2º Ao INSS compete operacionalizar:*

*I - reconhecimento do direito, a manutenção e o pagamento de benefícios e os serviços previdenciários do Regime Geral de Previdência Social - RGPS;*

*II - o reconhecimento do direito, a manutenção e o pagamento de benefícios assistenciais previstos na legislação; e*

*III - o reconhecimento do direito e a manutenção das aposentadorias e das pensões do regime próprio de previdência social da União, no âmbito das autarquias e das fundações públicas, nos termos do disposto no Decreto nº 10.620, de 5 de fevereiro de 2021.*

51. Segundo o Boletim Estatístico da Previdência Social de junho de 2023 [\[4\]](#), o INSS mantém atualmente cerca de **38 milhões de benefícios previdenciários do RGPS e assistenciais**, que projetam um gasto anual estimado de **R\$800 bilhões de reais**.

52. No ano de 2022 o INSS processou aproximadamente **10 milhões de requerimentos de benefícios**.

53. Segundo o mesmo Boletim, considera-se que existam aproximadamente **54 milhões de segurados contribuintes** vinculados ao RGPS, de uma população economicamente ativa ocupada de 89 milhões de pessoas, conforme dados populacionais de 2021.

54. Tais números demonstram a dimensão extraordinária da atuação do INSS, pressupondo-se uma **infinidade de dados e de relações jurídicas acumuladas ao longo do tempo, muito maior que os dados acima apresentados**, que representam um retrato do momento atual, especialmente pelos mais de 100 (cem) anos da Previdência Social Brasileira que, juntamente com a Assistência Social, consubstanciam **o maior programa de distribuição de renda**

**permanente do mundo.**

55. A **segurança social** é certamente uma marca distintiva e indelével do INSS, comprometido com a **proteção das pessoas e seus dados e com a pontualidade histórica dos pagamentos dos benefícios** .

56. É válido também mencionar que o INSS conta com **sede** em Brasília, **6 Superintendências Regionais** (Brasília, Belo Horizonte, Rio de Janeiro, São Paulo e Florianópolis), **97 Gerências Executivas, 1.586 Agências da Previdência Social, 18 Serviços de Centralização de Atendimento de Benefícios** (reconhecimento de direitos, manutenção e monitoramento), **6 Serviços de Centralização de Atendimento de Benefícios de Demandas Judiciais** e aproximadamente **18 mil servidores**, menos da metade do contingente de pessoal que dispunha há 10 anos.

57. Quanto aos canais remotos de atendimento, o INSS atua com o aplicativo “Meu INSS”, que oferece mais de 100 serviços e registra **62 milhões de acessos por mês**, e com a “Central 135” (*call center*), havendo registros de **10 milhões de chamadas por mês**. As Agências da Previdência Social registram **1,8 milhões de atendimentos presenciais**.

58. Também é relevante ainda pontuar que o INSS conta atualmente com uma **fila de espera de 1,8 milhões de pedidos de reconhecimento inicial de direitos**<sup>[5]</sup>.

59. Noutro ver, a representação judicial e extrajudicial, consultoria e assessoramento jurídicos do INSS são prestados pela **Procuradoria-Geral Federal - PGF**, órgão da **AGU**, conforme artigo 10 da Lei nº 10.480, de 2 de julho de 2002, que mantém entre si protocolos para compartilhamentos de informações, considerado o volume expressivo de demandas judiciais em que o INSS figura como parte e determina celeridade na obtenção de subsídios e cumprimento de decisões judiciais.

60. Vale o registro de que nos últimos 12 (doze) meses foram **concedidos judicialmente cerca de 1,18 milhões de benefícios** (14,5% do total de concessões), mediante atuação de aproximadamente **1.100 servidores do INSS**. Na representação judicial do INSS há cerca de **1.500 procuradores federais**, quase a metade do contingente ativo da PGF na ocasião, responsáveis pela atuação em alguns milhões de ações previdenciárias e assistenciais.

61. Por outro lado, a **DATAPREV**, empresa pública vinculada ao Ministério da Gestão e Inovação em Serviços Públicos, é a empresa que presta serviços de informação ao INSS, com a produção e manutenção de sistemas e banco de dados, responsável pela operacionalização do controle dos acessos.

62. Esse contexto é relevante para se compreender a **expressividade dos números e a repercussão que a atuação** pode ocasionar.

## 4.2. **DA RAZOABILIDADE DA CONDUTA DO INSS EM NÃO COMUNICAR OS TITULARES DOS DADOS PRETENSAMENTE VAZADOS**

### 4.2.1 **Matriz normativa e a supremacia do interesse público sobre o privado**

63. De início é preciso delinear a matriz normativa dos incidentes em ambiente digital. O Direito, enquanto conjunto de normas e princípios editados com objetivo de reger dada sociedade, incide sobre os fatos na sua integralidade, como um monólito. Com efeito, a aplicação da LGPD ao caso sob análise deve se dar em conjunto com os demais normativos destinados a reger a matéria.

64. Sob a perspectiva constitucional, o inciso LXXIX do artigo 5º previu o direito à proteção de dados pessoais, nos termos da Lei.

65. E a proteção de dados pessoais atualmente é regulamentada por um conjunto de leis que devem ser

levadas em consideração quando da análise do presente caso, a se destacar:

a) a Lei nº 12.682, de 9 de julho de 2012, que trata da elaboração e o arquivamento de documentos em meios eletromagnéticos, prevendo-se que "os meios de armazenamento dos documentos digitais deverão protegê-los de acesso, uso, alteração, reprodução e destruição não autorizados" (parágrafo único do art. 3º);

b) a Lei nº 12.527, de 18 de novembro de 2011, a Lei de Acesso à Informação (LAI), que estabelece, dentre outros, que o "tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais" (art. 31);

c) a Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, dentre os quais, "a proteção dos dados pessoais, na forma da lei" (art. 3º, III);

d) especialmente a Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), prevendo, dentre outras garantias, que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" (art. 46); e

e) a Lei nº 14.129, de 29 de março de 2021, que dispõe sobre princípios, regras e instrumentos para o Governo Digital, nela previsto como princípios "a proteção de dados pessoais, nos termos da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais)"

66. Desse contexto normativo, como regra, infere-se que os incidentes cibernéticos, definidos no inciso V do artigo 4º do Decreto nº 10.748, de 16 de julho de 2021, submetem-se ao tratamento disposto no artigo 48 da LGPD, segundo o qual "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".

67. No § 2º de tal dispositivo também consta que a ANPD *verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente.*

68. Nada obstante, a LAI, ao tratar de hipóteses restritivas ao acesso de informações, em seu artigo 23, estabeleceu a possibilidade de serem classificadas como sigilosas informações "**imprescindíveis à segurança da sociedade ou do Estado**".

69. E o Decreto nº 10.748, de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos, considera que as informações sobre incidentes cibernéticos são imprescindíveis à segurança da sociedade e do Estado. Confira-se o disposto em seu artigo 15:

*Art. 15. As informações específicas sobre os incidentes cibernéticos e sobre as configurações e características técnicas de ativos de informação de cada órgão ou entidade da administração pública federal direta, autárquica e fundacional são consideradas **imprescindíveis à segurança da sociedade e do Estado.**" (gn)*

70. E o §1º do mesmo dispositivo reforçou a necessidade de sigilo apontando o quando segue:

*§ 1º As informações de que trata o caput somente poderão ser acessadas por profissionais autorizados pelas autoridades responsáveis pelos ativos de informação dos órgãos ou das entidades da administração pública federal direta, autárquica e fundacional.*

71. O cotejo entre o artigo 23 da LAI c/c com o artigo 15 do Decreto nº 10.748, de 2021 e o artigo 48 da Lei nº 13.709, de 2018 revelam uma antinomia aparente. Antinomia que não resiste à aplicação do critério da

especialidade.

72. Com efeito, o controlador tem o dever de comunicar à ANPD e aos titulares dos dados sobre os incidentes cibernéticos, **na presença de riscos ou danos relevantes**.

73. E a divulgação aos titulares supostamente afetados, quando possível, deve ser avaliada pela Administração Pública Federal e, **não havendo comprometimento dos interesses maiores do Estado**, as comunicações devem ser realizadas. Isso se dá dessa forma em razão do prevalectimento do interesse público sobre os interesses individuais.

74. Celso Antônio Bandeira de Mello<sup>[6]</sup> sustenta de forma incisiva o princípio supremacia do interesse público sobre o interesse privado, em seu clássico “Curso de Direito Administrativo”. E quando se propõe a traçar o conteúdo do referido princípio aduz:

O princípio da supremacia do interesse público sobre o interesse privado é princípio geral de Direito inerente a qualquer sociedade. É a própria condição de sua existência. Assim, não se radica em dispositivo específico algum da Constituição, ainda que inúmeros aludam ou impliquem manifestações concretas dele, como, por exemplo, os princípios da função social da propriedade, da defesa do consumidor ou do meio ambiente (art. 170, III, V e VI), ou tantos outros.

Afinal, o princípio em causa é um pressuposto lógico do convívio social. Para o Direito Administrativo interessam apenas os aspectos de sua expressão na esfera administrativa. Para não deixar sem referência constitucional algumas aplicações concretas especificamente dispostas na Lei Maior e pertinentes ao Direito Administrativo, basta referir os institutos da desapropriação e da requisição (art. 5u, XXIV e XXV), nos quais é evidente a supremacia do interesse público sobre o interesse privado.

75. A supremacia do interesse público sobre o privado aparece defendido por José dos Santos Carvalho Filho<sup>[7]</sup> em sua obra clássica “Manual de Direito Administrativo”. À referida obra o autor leciona o seguinte:

As atividades administrativas são desenvolvidas pelo Estado para benefício da coletividade. Mesmo quando age em vista de algum interesse estatal imediato, o fim último de sua atuação deve ser voltado para o interesse público. E se, como visto, não estiver presente esse objetivo, a atuação estará inquinada de desvio de finalidade.

Desse modo, não é o indivíduo em si o destinatário da atividade administrativa, mas sim o grupo social num todo. Saindo da era do individualismo exacerbado, o Estado passou a caracterizar-se como o Welfare State (Estado/bem-estar), dedicado a atender ao interesse público. Logicamente, as relações sociais vão ensejar, em determinados momentos, um conflito entre o interesse público e o interesse privado, mas, ocorrendo esse conflito, há de prevalecer o interesse público.

Trata-se, de fato, do primado do interesse público. O indivíduo tem que ser visto como integrante da sociedade, não podendo os seus direitos, em regra, ser equiparados aos direitos sociais. Vemos a aplicação do princípio da supremacia do interesse público, por exemplo, na desapropriação, em que o interesse público suplanta o do proprietário; ou no poder de polícia do Estado, por força do qual se estabelecem algumas restrições às atividades individuais.

76. Maria Sylvia Zanella Di Pietro<sup>[8]</sup> segue sustentando a sobrevivência do princípio da supremacia do interesse público sobre o particular e nesse sentido pontua:

Esse princípio está presente tanto no momento da elaboração da lei como no momento da sua execução em concreto pela Administração Pública. Ele inspira o legislador e vincula a autoridade administrativa em toda a sua atuação.

No que diz respeito à sua influência na elaboração da lei, é oportuno lembrar que uma das distinções que se costuma fazer entre o direito privado e o direito público (e que vem desde o Direito Romano) leva em conta o interesse que se tem em vista proteger; o direito privado contém normas de interesse individual e, o direito público, normas de interesse público.

Esse critério tem sido criticado porque existem normas de direito privado que objetivam defender o interesse público (como as concernentes ao Direito de Família) e existem normas de direito público que defendem também interesses dos particulares (como as normas de segurança, saúde pública, censura, disposições em geral atinentes ao poder de polícia do Estado e normas no capítulo da Constituição consagrado aos direitos fundamentais do homem).

Apesar das críticas a esse critério distintivo, que realmente não é absoluto, algumas verdades permanecem: em primeiro lugar, as normas de direito público, embora protejam reflexamente o interesse individual, têm o objetivo primordial de atender ao interesse público, ao bem-estar coletivo. Além disso, pode-se dizer que o direito público somente começou a se desenvolver quando, depois de superados o primado do Direito Civil (que durou muitos séculos) e o individualismo que tomou conta dos vários setores da ciência, inclusive a do Direito, substituiu-se a ideia do homem como fim único do direito (própria do individualismo) pelo princípio que hoje serve de fundamento para todo o direito público e que vincula a Administração em todas as suas decisões: o de que os interesses públicos têm supremacia sobre os individuais.

Com efeito, já em fins do século XIX começaram a surgir reações contra o individualismo jurídico, como decorrência das profundas transformações ocorridas nas ordens econômica, social e política, provocadas pelos próprios resultados funestos daquele individualismo exacerbado. O Estado teve que abandonar a sua posição passiva e começar a atuar no âmbito da atividade exclusivamente privada.

O Direito deixou de ser apenas instrumento de garantia dos direitos do indivíduo e passou a ser visto como meio para consecução da justiça social, do bem comum, do bem-estar coletivo.

77. No caso, **o incidente de segurança que ensejou a abertura do presente processo sancionador foi tempestivamente comunicado à ANPD**, que determinou e insistiu na comunicação dos titulares dos dados potencialmente acessados, o que não ocorreu em razão de não se vislumbrar sua pertinência.

78. Por um lado, **não foi possível determinar os potenciais dados acessados e seus correspondentes titulares**, de modo que comunicações individualizadas seriam materialmente impossíveis.

79. Por outro, uma divulgação ampla e indistinta do incidente cibernético, que teria atingido um percentual ínfimo das milhões de pessoas com as quais o INSS manteve algum tipo de relação ao longo de décadas, contaria apenas com **o potencial de gerar pânico e desconfiança em todo o contingente de segurados e beneficiários vinculados ao INSS**.

80. Qualquer comunicado a respeito do incidente, antes de proteger efetivamente os segurados e beneficiários, ocasionaria um **caos nos canais de atendimento do INSS**, que não teria condições sequer de indicar objetivamente se dados foram efetivamente acessados, quais dados e de quais pessoas, caso fosse demandado a fazê-lo.

81. Em verdade, no momento em que a missão do INSS é a de buscar debelar suas **filas de atendimento**, como diretriz governamental, num contexto de infraestrutura logística e de pessoal ainda não favorável, não se revelaria apropriado considerar minimamente tal medida, que dispersaria significativos esforços administrativos para tratá-las.

82. Com efeito, a juízo do INSS, as informações sobre o incidente cibernético em apuração são fundamentais para a **manutenção do equilíbrio, da credibilidade e do funcionamento** de atividades estratégicas para as

políticas sociais desenvolvidas pelo Brasil.

83. Vale ainda mencionar que **não foram evidenciados quaisquer prejuízos concretos** a segurados e beneficiários cujos benefícios estejam sob a gestão do INSS, o que descaracterizaria a presença de riscos e danos relevantes como fator determinante da comunicação pretendida pela ANPD, tal como previsto no artigo 48 da LGPD.

84. Isso não quer dizer que se desprestigia a garantia constitucional da proteção de dados constante do inciso LXXIX do artigo 5º da Constituição Federal<sup>[9]</sup>. Esse princípio foi concretizado e observado no presente processo sancionador a partir do seguinte:

- a) atuação do INSS, DATAPREV e AGU com absoluta transparência;
- b) manutenção de estrutura de controle diligente que, diante de eventual suspeita, prontamente identificou o problema e bloqueou os acessos pertinentes;
- c) alteração da forma de acesso dos órgãos da AGU aos bancos de dados mantido pelo INSS, passando a se estabelecer a conexão por VPN e com utilização de certificado digital e token; e
- d) migração da base de dados para plataforma mais moderna, que permitirá acompanhamento por log da navegação.

#### **4.2.2. O devido processo legal substantivo - controle de razoabilidade e de proporcionalidade**

85. Noutro ver, é importante pontuar que o processo administrativo sancionador deve observar o conteúdo da Lei nº 9.784, de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

86. Dentre seus diversos dispositivos, relevante rememorar os princípios que deverão ser observados pela Administração Pública quando da gestão de processos administrativos.

87. No artigo 2º da Lei nº 9.784, de 1999 tem-se que a “... Administração Pública obedecerá, dentre outros, aos princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência.”.

88. Relevante ponderar acerca dos princípios da razoabilidade e da proporcionalidade que são concretizadores do devido processo legal substantivo.

89. A razoabilidade foi tratada por Celso Antônio Bandeira de Mello <sup>[10]</sup> conforme segue:

13. Enuncia-se com este princípio que a Administração, ao atuar no exercício de discricção, terá de obedecer a critérios aceitáveis do ponto de vista racional, em sintonia com o senso normal de pessoas equilibradas e respeitosa das finalidades que presidiram a outorga da competência exercida. Vale dizer: pretende-se colocar em claro que não serão apenas inconvenientes, mas também ilegítimas - e, portanto, jurisdicionalmente invalidáveis-, as condutas desarrazoadas, bizarras, incoerentes ou praticadas com desconsideração às situações e circunstâncias que seriam atendidas por quem tivesse atributos normais de prudência, sensatez e disposição de acatamento às finalidades da lei atributiva da discricção manejada.

90. Há na doutrina quem estabeleça uma relação bastante próxima entre a razoabilidade e a legalidade, o que tornaria assim sensivelmente mais grave a afronta aos padrões de razoabilidade. Nesse sentido José dos Santos Carvalho Filho<sup>[11]</sup> aduz:

Razoabilidade é a qualidade do que é razoável, ou seja, aquilo que se situa dentro de limites aceitáveis, ainda que os juízos de valor que provocaram a conduta possam dispor-se de forma um pouco diversa.

Ora, o que é totalmente razoável para uns pode não o ser para outros. Mas, mesmo quando não o seja, é de reconhecer-se que a valoração se situou dentro dos standards de aceitabilidade. Dentro desse quadro, não pode o juiz controlar a conduta do administrador sob a mera alegação de que não a entendeu razoável.

Não lhe é lícito substituir o juízo de valor do administrador pelo seu próprio, porque a isso se coloca o óbice da separação de funções, que rege as atividades estatais. Poderá, isto sim, e até mesmo deverá controlar os aspectos relativos à legalidade da conduta, ou seja, verificar se estão presentes os requisitos que a lei exige para a validade dos atos administrativos. Esse é o sentido que os Tribunais têm emprestado ao controle.

Desse modo, quando alguns estudiosos indicam que “a razoabilidade vai se atrelar à congruência lógica entre as situações postas e as decisões administrativas”,<sup>125</sup> parece-nos que a falta da referida congruência viola, na verdade, o princípio da legalidade, porque, no caso, ou há vício nas razões impulsionadoras da vontade, ou o vício estará no objeto desta.

A falta de razoabilidade, na hipótese, é puro reflexo da inobservância de requisitos exigidos para a validade da conduta. Por outro lado, quando a falta de razoabilidade se calca em situação na qual o administrador tenha em mira algum interesse particular, violado estará sendo o princípio da moralidade, ou o da impessoalidade, como tivemos a oportunidade de examinar.

Com esses elementos, desejamos frisar que o princípio da razoabilidade tem que ser observado pela Administração à medida que sua conduta se apresente dentro dos padrões normais de aceitabilidade. Se atuar fora desses padrões, algum vício estará, sem dúvida, contaminando o comportamento estatal. Significa dizer, por fim, que não pode existir violação ao referido princípio quando a conduta administrativa é inteiramente revestida de licitude.

91. Maria Sylvia Zanella Di Pietro<sup>[12]</sup> por sua vez, trata em conjunto os princípios da razoabilidade e proporcionalidade conforme segue:

Trata-se de princípio aplicado ao Direito Administrativo como mais uma das tentativas de impor-se limitações à discricionariedade administrativa, ampliando-se o âmbito de apreciação do ato administrativo pelo Poder Judiciário.

Segundo Gordillo (1977:183-184), “a decisão discricionária do funcionário será ilegítima, apesar de não transgredir nenhuma norma concreta e expressa, se é ‘irrazoável’, o que pode ocorrer, principalmente, quando:

- a) não dê os fundamentos de fato ou de direito que a sustentam ou;
- b) não leve em conta os fatos constantes do expediente ou públicos e notórios; ou
- c) não guarde uma proporção adequada entre os meios que emprega e o fim que a lei deseja alcançar, ou seja, que se trate de uma medida desproporcionada, excessiva em relação ao que se deseja alcançar”.

92. A proporcionalidade por sua vez, foi elucidada por Bandeira de Mello<sup>[13]</sup> conforme trecho que segue:

15. Este princípio enuncia a ideia- singela, aliás, conquanto frequentemente desconsiderada - de que as competências administrativas só podem ser validamente exercidas na extensão e intensidade correspondentes ao que seja realmente demandado para cumprimento da finalidade de interesse público a que estão atreladas. Segue-se que os atos cujos conteúdos ultrapassem o necessário para alcançar o objetivo que justifica o uso da competência ficam maculados de ilegitimidade, porquanto desbordam do âmbito da competência; ou seja, superam os limites que naquele caso lhes corresponderiam.

Sobremodo quando a Administração restringe situação jurídica dos administrados além do que caberia, por imprimir às medidas tomadas uma intensidade ou extensão supérfluas,

prescindendas, ressalta a ilegalidade de sua conduta. É que ninguém deve estar obrigado a suportar constrições em sua liberdade ou propriedade que não sejam indispensáveis à satisfação do interesse público.

93. Bandeira de Mello toca o ponto fulcral que caracteriza a desproporcionalidade da ampla comunicação do caso concreto. É desproporcional, pois imprime às medidas tomadas uma intensidade ou extensão supérfluas.

94. Nesse passo, a determinação para a comunicação dos titulares, **além de sobrepujar o princípio da supremacia do interesse público** no caso concreto, também consistiria em medida **irrazoável**, posto que impossível de execução material em função da indeterminação de dados e seus titulares, e **desproporcional**, a considerar que impõe obrigação em medida superior àquelas estritamente necessárias ao atendimento do interesse público, que já foram tomadas pelos agentes de tratamento, a saber, o INSS, DATAPREV e AGU, que agiram com total transparência e atenderam aos preceitos legais e normativos da LGPD.

95. A ponderação entre o ônus imposto pela determinação/sanção e o benefício trazido (proporcionalidade em sentido estrito) ainda se apresenta indissociável de uma leitura consequentialista do caso concreto, tema que será tratado a seguir.

#### 4.2.3. O Consequencialismo e a LINDB

96. A Lei nº 13.655, de 25 de abril de 2018 introduziu de forma incisiva ao ordenamento pátrio o chamado consequentialismo.

97. O consequentialismo, de acordo com José dos Santos Carvalho Filho <sup>[14]</sup>, encerra um “*método interpretativo que leva em conta, como fundamental, a antevisão dos efeitos oriundos da decisão.*”

98. A novidade ficou bem marcada nos art. 20 a 22 do Decreto-Lei nº. 4.657, de 4 de setembro de 1942 (Lei de Introdução às normas de Direito Brasileiro - LINDB) cujo conteúdo segue:

*Art. 20. Nas esferas administrativa, controladora e judicial, não se decidirá com base em valores jurídicos abstratos sem que sejam consideradas as consequências práticas da decisão.*

*Parágrafo único. A motivação demonstrará a **necessidade e a adequação** da medida imposta ou da invalidação de ato, contrato, ajuste, processo ou norma administrativa, inclusive em face das possíveis alternativas.*

*Art. 21. A decisão que, nas esferas administrativa, controladora ou judicial, decretar a invalidação de ato, contrato, ajuste, processo ou norma administrativa **deverá indicar de modo expresso suas consequências jurídicas e administrativas.***

*Parágrafo único. A decisão a que se refere o caput deste artigo deverá, quando for o caso, indicar as condições para que a **regularização ocorra de modo proporcional e equânime e sem prejuízo aos interesses gerais**, não se podendo impor aos sujeitos atingidos **ônus ou perdas que, em função das peculiaridades do caso, sejam anormais ou excessivos.***

*Art. 22. Na interpretação de normas sobre gestão pública, **serão considerados os obstáculos e as dificuldades reais do gestor e as exigências das políticas públicas a seu cargo**, sem prejuízo dos direitos dos administrados.*

*§ 1º Em decisão sobre regularidade de conduta ou validade de ato, contrato, ajuste, processo ou norma administrativa, serão consideradas as **circunstâncias práticas que houverem imposto, limitado ou condicionado a ação do agente.***

*§ 2º Na aplicação de sanções, serão consideradas a natureza e a gravidade da infração cometida, os danos que dela provierem para a administração pública, as circunstâncias agravantes ou atenuantes e os antecedentes do agente. (Incluído pela Lei nº 13.655, de 2018)*

*§ 3º As sanções aplicadas ao agente serão levadas em conta na dosimetria das demais*

99. O caput do artigo 20 da LINB atraiu a necessidade de a Administração avaliar a consequência de suas decisões.

100. O parágrafo único do artigo 20 por sua vez, repetiu a Lei nº 9.784, de 29 de janeiro de 1999, ao exigir que decisões administrativas impondo razoabilidade e proporcionalidade às decisões administrativas.

101. Trabalhando a proporcionalidade instituída ao artigo 20 da LINDB José dos Santos Carvalho Filho<sup>[15]</sup> aduz:

Apesar disso, o legislador enunciou que a motivação será o elemento de comprovação da necessidade e da adequação de medida imposta ou de invalidação de ato, contrato, processo ou norma administrativa (art. 20, parágrafo único). O preceito, conquanto relevante, não traz, a rigor, nenhuma novidade. Com efeito, a moderna interpretação das decisões administrativas já há muito considera fundamentais os elementos justificativos da conduta, com base no art. 93, IX, da CF, porquanto o aplicador poderá aferi-los em confronto com os efeitos da decisão. Incide aqui o princípio da proporcionalidade, cabendo à autoridade demonstrar a inviabilidade de alternativas.

102. O parágrafo único do artigo 21 da LINDB reforça a ideia de que, a rigor, o procedimento corretivo de eventuais anomalias identificadas deve ser “... **proporcional e equânime e sem prejuízo aos interesses gerais**, não se podendo impor aos sujeitos atingidos ônus ou perdas que, em função das peculiaridades do caso, sejam anormais ou excessivos”.

103. Do caput do artigo 22 observa-se que, as **dificuldades reais do gestor e as exigências das políticas públicas** a seu cargo deverão ser consideradas quando da interpretação das normas.

104. Tais dispositivos, em suma, buscam promover uma abordagem holística para a aplicação do direito, considerando tanto os fundamentos normativos e suas **possíveis interpretações** quanto as **implicações práticas das decisões tomadas**, com o objetivo final de alcançar **resultados justos e equitativos**.

105. Segundo Carlos Henrique Benedito Nitão Loureiro<sup>[16]</sup>:

Nesse ambiente, a LINDB, na qualidade de norma de sobre direito, irradia seus efeitos sobre as esferas administrativa e controladora, além da judicial, como se depreende da leitura dos seus artigos, notadamente ser referencial normativo para interpretação de normas jurídicas, afastando, no seu artigo 20, a possibilidade de decisão com base em valores jurídicos abstratos **sem que sejam observadas as consequências práticas da decisão**  
(...)

Não se trata de refutar abstratamente a aplicação dos princípios. Trata-se, pois, da definição de parâmetro relevante que pretende afastar a insegurança jurídica decorrente de decisões puramente principiológicas adaptáveis à solução pretendida pelo controlador, sem que este tenha que motivar de forma adequada a sua decisão a partir da **análise da situação concretamente vivenciada pelo agente público**.

No que concerne ao dever de motivação, Palmas recorda que "os ônus de fundamentação não são constrangimentos aos controladores, mas antes respostas que devem ser fornecidas em função do tipo de decisão que será tomada", seja pela administração, seja pelo controlador. É certo que não há qualquer inovação no que tange ao dever de motivar, posto que este é inerente à prática de atos administrativos. Entretanto, a LINDB almeja promover uma **delimitação do espaço decisório**, especialmente na hipótese de a motivação ser norteada por valores jurídicos abstratos.

106. Dado esse contexto, impõe-se ponderar que a comunicação aos titulares, **além de impossível materialmente, não alcançaria resultados úteis** à sociedade caso fosse realizada de modo indistinto nos termos do § 2º, I, do artigo 48 da LGPD.

107. Aliás, a ampla divulgação exigiria uma motivação específica por parte da ANPD a respeito das condições estabelecidas em tal dispositivo. Confira-se o dispositivo:

*Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.*

*(...)*

*§ 2º A autoridade nacional **verificará** a gravidade do incidente e **poderá, caso necessário para a salvaguarda dos direitos dos titulares**, determinar ao controlador a adoção de providências, tais como:*

*I - ampla divulgação do fato em meios de comunicação; e*

*II - medidas para reverter ou mitigar os efeitos do incidente.*

*§ 3º No **juízo de gravidade do incidente**, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. (gn)*

108. Os vocábulos “**verificará**”, “**poderá**” e “**juízo**” certamente encerram uma necessidade de motivação expressa das medidas previstas nos incisos do § 2º do artigo 48 da LGPD, nas hipóteses em que houver **riscos** ou **danos relevantes** para os titulares de dados, ponderada a **atuação dos controladores** dos dados na adoção de medidas técnicas necessárias para resolver as disfunções.

109. Dado esse cenário, observa-se que a Coordenação de Fiscalização da ANPD **não aferiu objetivamente** os elementos presentes no dispositivo acima transcrito, **deixando de ponderar** os aspectos do incidente de dados de que trata este processo sancionador, como a gravidade, os riscos e danos, e menos ainda em pensar nas **consequências de sua determinação**.

110. Com efeito, não se revela razoável e proporcional a exigência em publicizar o incidente, sob a perspectiva de um **incerto acesso de dados indeterminados** e envolvendo um **número também indeterminado de pessoas**, observada dimensão dos números que envolvem o INSS, cujo pequeno resumo foi apresentado no **item 4.1 desta defesa**.

111. Por outro lado, a Coordenação de Fiscalização da ANPD não emprestou qualquer valor às medidas que foram tomadas incontinentemente no sentido de investigar, comunicar e sanear o problema identificado, num ambiente de absoluta **boa-fé e transparência nos processos administrativos**.

#### **4.2.4. Da razoabilidade e proporcionalidade na aplicação das sanções previstas na LGPD**

112. De qualquer modo, convém ainda observar que o devido processo legal substantivo, do qual emana o controle da razoabilidade e da proporcionalidade enquanto parâmetro para própria constitucionalidade do ato administrativo, é um elemento que estabelece uma fronteira que limita as ações da ANPD sobre o poder público.

113. Tal fronteira diz respeito à relação entre o suposto ilícito e a efetividade, dosimetria e consequências da sanção que se pretende aplicar. Para serem razoáveis e proporcionais, as sanções da ANPD sobre o poder público devem considerar a (i) adequação, ou seja, a sanção deve ser apta a atingir o objetivo pretendido; (ii) necessidade, ou seja, a sanção deve decorrer da inexistência de meio menos gravoso para atingir a finalidade; e a (iii) proporcionalidade em sentido estrito, ou seja, a ponderação entre o ônus imposto pela sanção e o benefício trazido<sup>[17]</sup>.

114. Ademais, a LGPD adotou o modelo de regulação responsiva, segundo o qual há um estímulo à

conscientização e persuasão, à autorregulação dos setores, à adoção de boas práticas e à progressividade das sanções, refletindo claramente as denominadas pirâmides de *enforcement* – com bases mais largas de mecanismos preventivos, e que avançam em camadas menores e progressivamente mais severas até o topo. Assim, a maior parte dos conflitos potenciais entre a ANPD e entidades e órgãos públicos será dirimida nas partes inferiores das pirâmides, em que prevalece a atuação preventiva, o esclarecimento, a coordenação entre as diferentes instâncias de controle, e, mesmo na perspectiva sancionatória, medidas de alerta, como advertência<sup>[18]</sup>.

115. O artigo 52 da LGPD elenca as sanções aplicáveis aos agentes de tratamento, a saber:

*I - advertência, com indicação de prazo para adoção de medidas corretivas;*

*II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;*

*III - multa diária, observado o limite total a que se refere o inciso II;*

*IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;*

*V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;*

*VI - eliminação dos dados pessoais a que se refere a infração;*

*VII - (VETADO);*

*VIII - (VETADO);*

*IX - (VETADO)*

*X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; (Incluído pela Lei nº 13.853, de 2019)*

*XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei nº 13.853, de 2019)*

*XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)*

116. Os incisos II e III do artigo 52 supra são inaplicáveis ao INSS em razão da previsão do §3º do mesmo dispositivo legal que excluiu a possibilidade da aplicação de multa simples e a multa diária a entidades e aos órgãos públicos.

117. Anote-se que a proteção de dados pessoais no setor público é muito importante, mas não será, em todos os casos concretos, o bem jurídico necessariamente mais relevante. No presente processo sancionador, é claro que eventual vazamento de dados de beneficiários da previdência social não legitima, pelo critério da razoabilidade e proporcionalidade, sanções administrativas da ANPD que inviabilizem o funcionamento do INSS.

118. Dessa forma, o bloqueio e a eliminação de dados constantes dos incisos V e VI, bem como a suspensão parcial do funcionamento do banco de dados, a suspensão do exercício da atividade de tratamento de dados pessoais e a proibição do exercício de atividades relacionadas a tratamento de dados, previstas nos incisos X, XI e XII, todos do artigo 52 da LGPD mostram-se absolutamente impraticáveis à medida que o tratamento de dados pessoais constitui o cerne da atividade da autarquia previdenciária. Eventual inviabilização do acesso a dados dos beneficiários impossibilitaria a gestão do RGPS e ameaçaria a subsistência de milhares de trabalhadores em intensa desproporção à alegada infração praticada.

119. O inciso IV do artigo 52 supra igualmente não pode ser aplicado, uma vez que a informação foi classificada como sigilosa pelo INSS nos termos do artigo 23 da LAI e artigo 15 do Decreto nº 10.748, de 2021, inviabilizando a sanção de publicização da infração aventada.

120. Pelo exposto, no caso concreto e, por absoluta exclusão e de forma subsidiária, a advertência encerraria a única sanção possível de ser cogitada, em caso de manutenção do auto de infração.

## 5. CONCLUSÃO

121. Considerando todo o exposto nesta defesa, conclui-se que:

a) o incidente de dados de que trata este processo consistiu no aumento volumétrico atípico e não autorizado de consulta de dados no Sistema Plenus do INSS, não havendo como precisar quais dados foram potencialmente acessados, consultados e eventualmente compartilhados, nem as pessoas casualmente afetadas.

b) o acesso dos dados do INSS pela AGU envolve uma necessidade ordinária de obtenção de informações de segurados e beneficiários visando sua atuação na representação judicial do INSS, cujo significativo volume de demandas determina a adoção dos meios tecnológicos disponíveis para compartilhamento de modo ágil e seguro.

c) os agentes de tratamento, a saber, o INSS, a DATAPREV e a AGU, tomaram todas as precauções no sentido de atuar em conjunto para investigar, comunicar e sanear o problema identificado, demonstrando absoluta boa-fé e transparência nos processos administrativos.

d) não há registros de que o incidente tenha ocasionado prejuízo aos segurados ou beneficiários que contam com dados no Sistema Plenus.

e) considerados os princípios da supremacia do interesse público, a decisão do INSS em não comunicar individual ou indistintamente o incidente é legal, razoável e proporcional, observada a indeterminação de dados e pessoas envolvidas e os efeitos deletérios de tal medida, sob a perspectiva de ser potencialmente capaz de gerar um prejuízo incomensurável na gestão do atendimento dos serviços previdenciários e assistenciais, sem gerar qualquer benefício individual ou coletivo ao conjunto de segurados e beneficiários, observado o consequentialismo previsto nos artigos 20 a 22 da LINDB.

f) a ampla divulgação aos titulares dos dados que possam ser afetados em incidentes de segurança não é uma consequência legal necessária e automática, dependendo da presença das condições do § 2º do artigo 48 da LGPD, cuja interpretação e aplicação deve ser motivada sob a perspectiva dos princípios da razoabilidade e da proporcionalidade e do consequentialismo.

g) a Coordenação de Fiscalização da ANPD não motivou sua determinação de comunicação do incidente segundo os aspectos contidos no § 2º do artigo 48 da LGPD, nos termos dos artigos 20 a 22 da LINDB.

h) o auto de infração deve ser considerado nulo por falta de motivação, observado o disposto no artigo 2º da Lei nº 4.717, de 29 de junho de 1965, e o disposto no artigo 50, I e II, da Lei nº 9.784, de 1999, ou insubsistente em relação ao mérito, dada a inobservância da supremacia do interesse público, dos princípios da proporcionalidade e da razoabilidade e do consequentialismo tratado na LINDB.

i) na hipótese de não ser considerada a nulidade ou insubsistência do auto de infração, entende-se que o episódio possa importar, no máximo, em sanção de advertência, em atenção à adequação, necessidade e a proporcionalidade em sentido estrito.

122. Em face de todo o exposto, requer o acolhimento desta defesa, com **declaração de nulidade ou insubsistência do auto de infração e o consequente arquivamento do processo sancionador.**

123. Por cautela, caso não acolhida tal pretensão, mantendo-se o auto de infração, postula-se pela aplicação dos princípios da razoabilidade e proporcionalidade da eventual especificação de sanção, considerada sobretudo a natureza jurídica do INSS, que limita as hipóteses previstas no artigo 52 da LGPD.

Brasília, 17 de agosto de 2023

BRUNO JÚNIOR BISINOTO  
Procurador-Geral

ALESSANDRO ANTÔNIO STEFANUTTO  
Presidente do INSS

---

Notas

1. <sup>^</sup> A solicitação de token e certificados digitais aos servidores do INSS foi regulamentada pela PORTARIA DTI/INSS N° 67, DE 21 DE DEZEMBRO DE 2021 que segue anexa. A obrigatoriedade do uso de token e certificado digital foi ainda publicizada por meio do OFÍCIO SEI CIRCULAR N° 6/2022/DTI/DTI-INSS, que também segue anexo.
2. <sup>^</sup> Disponível em: < <https://www.gov.br/inss/pt-br/acao-a-informacao/dados-abertos/dados-abertos>>.
3. <sup>^</sup> A íntegra da Nota Técnica n. 00002/2023/SGE/AGU segue anexa à presente defesa, mostrando-se útil sua consulta em função das gráficos e tabelas que a compõe.
4. <sup>^</sup> Disponível em: <<https://www.gov.br/previdencia/pt-br/assuntos/previdencia-social/dados-estatisticos-previdencia-social-e-inss>>.
5. <sup>^</sup> Disponível em: <<https://www.gov.br/inss/pt-br/portal-de-transparencia>>.
6. <sup>^</sup> BANDEIRA DE MELLO, Celso Antônio. Curso de Direito Administrativo. 35ª ed. rev. e atual. até a EC 109/2021 e Lei 14.133/2021. São Paulo: Malheiros, 2021. p. 81.
7. <sup>^</sup> CARVALHO FILHO, José dos Santos. Manual de direito administrativo. 37. ed. – Barueri [SP]: Atlas, 2023. p. 75.
8. <sup>^</sup> DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 36ª ed. Rio de Janeiro: Forense, 2023, p. 118.
9. <sup>^</sup> LXXVIII - a todos, no âmbito judicial e administrativo, são assegurados a razoável duração do processo e os meios que garantam a celeridade de sua tramitação. (Incluído pela Emenda Constitucional n° 45, de 2004).
10. <sup>^</sup> Op. Cit. p. 91.
11. <sup>^</sup> Op. Cit. p. 81.
12. <sup>^</sup> Op. Cit. p. 81.
13. <sup>^</sup> Op. Cit. p. 93.
14. <sup>^</sup> Op. Cit. p. 93.
15. <sup>^</sup> Op. Cit. p. 922.
16. <sup>^</sup> LOUREIRO, Carlos Henrique Benedito Nitão. Entre as alternativas possíveis e o erro grosseiro nas contratações públicas: a LINDB e os impactos na responsabilização do agente público. Londrina, PR: Thoth, 2022, p. 51-52.
17. <sup>^</sup> MALDONADO, Viviane. 4. Especificidades das Sanções na LGPD para o Poder Público. In: LGPD: Sanções e Decisões Judiciais. São Paula (SP): Editora Revista dos Tribunais, 2022. Disponível em: <https://www.jusbrasil.com.br/doutrina/secao/4-especificidades-das-sancoes-na-lgpd-para-o-poder-publico-ii-as-sancoes-previstas-na-lgpd-e-a-autoridade-nacional-de-protecao-de-dados-lgpd-sancoes-e-decisoes-judiciais/1590357425#ftn.DTR.2022.3965-n21>. Acesso em 15 de ago. de 2023.



Documento assinado eletronicamente por **BRUNO JUNIOR BISINOTO, Procurador-Geral da PFE/INSS**, em 17/08/2023, às 12:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **ALESSANDRO ANTONIO STEFANUTTO, Presidente**, em 17/08/2023, às 14:20, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



<b>Usuário Externo (signatário):</b>	EDSON PINHEIRO ALVARISTA
<b>Data e Horário:</b>	17/08/2023 16:36:27
<b>Tipo de Peticionamento:</b>	Resposta a Intimação
<b>Número do Processo:</b>	00261.001888/2023- 21
<b>Tipo de Intimação:</b>	Apresentação de Defesa
<b>Documento Principal da Intimação:</b>	ANPD - Auto de Infração 1 (4411917)
<b>Tipo de Resposta:</b>	Defesa
<b>Interessados:</b>	
INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS	
<b>Protocolos dos Documentos (Número SEI):</b>	
- Defesa SEI_12906070	4500984
- Processo SEI_35014.293086_2023_34	4500985
- Processo SEI_35014.437670_2022_27	4500986
- Processo SEI_35014.528489_2022_29	4500987

O Usuário Externo acima identificado foi previamente avisado que o peticionamento importa na aceitação dos termos e condições que regem o processo eletrônico, além do disposto no credenciamento prévio, e na assinatura dos documentos nato-digitais e declaração de que são autênticos os digitalizados, sendo responsável civil, penal e administrativamente pelo uso indevido. Ainda, foi avisado que os níveis de acesso indicados para os documentos estariam condicionados à análise por servidor público, que poderá alterá-los a qualquer momento sem necessidade de prévio aviso, e de que são de sua exclusiva responsabilidade:

- a conformidade entre os dados informados e os documentos;
- a conservação dos originais em papel de documentos digitalizados até que decaia o direito de revisão dos atos praticados no processo, para que, caso solicitado, sejam apresentados para qualquer tipo de conferência;
- a realização por meio eletrônico de todos os atos e comunicações processuais com o próprio Usuário Externo ou, por seu intermédio, com a entidade porventura representada;
- a observância de que os atos processuais se consideram realizados no dia e hora do recebimento pelo SEI, considerando-se tempestivos os praticados até as 23h59min59s do último dia do prazo, considerado sempre o horário oficial de Brasília, independente do fuso horário em que se encontre;
- a consulta periódica ao SEI, a fim de verificar o recebimento de intimações eletrônicas.

A existência deste Recibo, do processo e dos documentos acima indicados pode ser conferida no Portal na Internet do(a) Presidência da República.





PRESIDÊNCIA DA REPÚBLICA  
Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização da Coordenação-Geral de Fiscalização da ANPD

ANPD - Ofício Nº 72/2023/FIS/CGF/ANPD

Brasília, 18 de dezembro de 2023.

Ao Sr.

**EDSON PINHEIRO ALVARISTA**

COORDENADOR DE PROTEÇÃO DE DADOS PESSOAIS - COPDP

INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS

CNPJ nº 29.979.036/0001-40

ST SAUS QUADRA 02 BLOCO "O"

BRASÍLIA-DF CEP 70.070-946

[edson.alvarista@inss.gov.br](mailto:edson.alvarista@inss.gov.br)

[encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)

**Assunto: Apresentação de alegações finais no Processo SUPER nº  
00261.001888/2023-21 - Auto de Infração nº 1/2023/CGF/ANPD**

Senhor Coordenador de Proteção de Dados Pessoais -  
COPDP,

1. A Autoridade Nacional de Proteção de Dados, no âmbito do processo SUPER nº 00261.001888/2023-21, em 03/05/2023, lavrou o Auto de Infração nº 1/2023/CGF/ANPD (SUPER nº 4411917), em desfavor do INSS, por possível infringência do artigo 48 da Lei nº 13.709/2018 e do artigo 32, §2º, do Regulamento de Fiscalização CD/ANPD nº 1, de 28 de outubro de 2021.

2. O INSS, desse modo, foi intimado a apresentar **Defesa** perante a Coordenação-Geral de Fiscalização da Autoridade Nacional de Proteção de Dados, via SEI, de acordo com o disposto no art. 47, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1/2021, no prazo de 10 dias úteis.

3. Observa-se que, em 17/08/2023, a entidade pública regulada apresentou a sua Defesa em face do Auto de Infração nº 1/2023/FIS/CGF/ANPD (SUPER nº 4500984), com seus respectivos anexos. Tem-se, no entanto, que não foram apresentadas novas provas pela entidade regulada após a intimação desta ANPD.

4. Diante disso, tendo em vista o disposto no art. 53 do Regulamento de Fiscalização, fica o INSS intimado a apresentar **alegações finais** neste processo, via acesso externo, no prazo de 10 (dez) dias úteis, a partir da ciência deste Ofício, perante a Coordenação-Geral de Fiscalização da ANPD. As instruções para acesso externo podem ser obtidas no link <https://www.gov.br/secretariageral/pt-br/sei-peticionamento-eletronico>.

5. Por conseguinte, informamos que, caso o INSS opte por apresentar alegações finais, poderá indicar quais as informações constantes no presente processo sancionatório encontram-se, a seu ver, protegidas por hipótese legal de sigilo. Nesse caso, deverá indicar as razões de fato e de direito que sustentariam eventual restrição de acesso a

informações.

6. Por oportuno, informa-se que o processo terá seu prosseguimento regular independentemente da apresentação das alegações finais.

7. A CGF coloca-se à disposição para prestar informações adicionais que se fizerem necessárias por meio do endereço eletrônico [fiscalizacao@anpd.gov.br](mailto:fiscalizacao@anpd.gov.br).

Atenciosamente,

**MARIDELIA MOURA DE ARRUDA MOREIRA**  
Coordenadora de Fiscalização



Documento assinado eletronicamente por **Maridélia Moura de Arruda Moreira, Coordenador(a)**, em 18/12/2023, às 11:53, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida informando o código verificador **4836919** e o código CRC **976C2728** no site: [https://super.presidencia.gov.br/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

**Referência:** Caso responda este Ofício, indicar expressamente o Processo nº 00261.001888/2023-21 SUPER nº 4836919

SCN, Quadra 6, Conjunto "A" - Ed. Venâncio 3000, Bloco "A", 9º andar

Telefone: (61) 2025-8168

CEP 70.716-900 Brasília/DF - <https://www.gov.br/planalto/pt-br>

## Certidão de Intimação Cumprida - 4871007

<b>Tipo de Destinatário:</b>	Pessoa Física
<b>Destinatário:</b>	EDSON PINHEIRO ALVARISTA
<b>Tipo de Intimação:</b>	Apresentação de Alegações Finais
<b>Documento Principal da Intimação:</b>	ANPD - Ofício 72 (4836919)
<b>Data de Expedição da Intimação:</b>	18/12/2023 11:57:02
<b>Tipo de Cumprimento da Intimação:</b>	Por Decurso do Prazo Tácito
<b>Data do Cumprimento:</b>	02/01/2024

Esta Certidão formaliza o cumprimento da intimação eletrônica referente aos dados acima, observado o seguinte:

- O Tipo de Cumprimento "Consulta Direta" indica que o "Destinatário" realizou a consulta aos documentos da intimação diretamente no sistema antes do término do Prazo Tácito para intimação.
  - O Prazo Tácito para intimação é definido conforme normativo aplicável ao órgão, em que, a partir da "Data de Expedição da Intimação", o Destinatário possui o referido prazo para consultar os documentos diretamente no sistema, sob pena de ser considerado automaticamente intimado na data de término desse prazo.
- O Tipo de Cumprimento "Por Decurso do Prazo Tácito" indica que não ocorreu a mencionada consulta aos documentos da intimação diretamente no sistema, situação na qual a Certidão é gerada automaticamente na data de término desse prazo.
  - No caso do Prazo Tácito terminar em dia não útil, a geração automática da Certidão ocorrerá somente no primeiro dia útil seguinte.
- Conforme regras de contagem de prazo processual e normas afetas a processo eletrônico, tanto no Prazo Tácito para intimação como nos possíveis prazos externos para Peticionamento de Resposta:
  - sempre é excluído da contagem o dia do começo e incluído o do vencimento;
  - o dia do começo e o do vencimento nunca ocorrem em dia não útil, prorrogando-o para o primeiro dia útil seguinte;
  - a consulta a intimação ocorrida em dia não útil tem a correspondente data apresentada em linha separada, sendo a "Data do Cumprimento" a do primeiro dia útil seguinte.
- Para todos os efeitos legais, somente após a geração da presente Certidão e com base exclusivamente na "Data do Cumprimento" é que o Destinatário, ou a Pessoa Jurídica ou Física por ele representada, é considerado efetivamente intimado e são iniciados os possíveis prazos externos para Peticionamento de Resposta.
  - Caso a intimação se dirija a Pessoa Jurídica, ela será considerada efetivamente intimada na "Data do Cumprimento" correspondente à primeira Certidão gerada referente a Usuário Externo que possua poderes de representação.

Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

## FORMULÁRIO PARA EXPEDIÇÃO DE DOCUMENTOS PARA O PROTOCOLO CENTRAL

**Ao Protocolo da ANPD.**

Encaminho o presente processo para expedição conforme a seguir:

**Enviar o processo integralmente;**

Enviar apenas os documentos listados abaixo:

Indicação da forma de remessa	
<input checked="" type="checkbox"/>	<p><b>Barramento - envio à caixa CGF</b></p> <ul style="list-style-type: none"><li>· Solução que permite a comunicação entre os órgãos públicos que utilizam o SUPER ou outras soluções de processo eletrônico (desde que também estejam integrados ao Barramento).</li><li>· Envio de todo o processo.</li><li>· O processo eletrônico enviado fica bloqueado no SUPER-PR e não pode ser editado nem tramitado, mas fica disponível para consulta.</li></ul>

Em caso de dúvida, por favor, entre em contato com o Protocolo Central: 2487/2488 ou acesse o menu [Documentação e Arquivo, opção PROTOCOLO CENTRAL](#) na Intranet.



Documento assinado eletronicamente por **Ulliana Cervigni Martinelli**, **Coordenador(a) substituto(a)**, em 16/01/2024, às 21:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida informando o código verificador **4904180** e o código CRC **87543620** no site: [https://super.presidencia.gov.br/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)

Referência: Processo nº 00261.001888/2023-21

SUPER nº 4904180



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

Relatório de Instrução nº 01/2024/CGF/ANPD

Brasília/DF, na data da assinatura.

**1. IDENTIFICAÇÃO**

- 1.1. Nome/Razão Social do Autuado: Instituto Nacional do Seguro Social (INSS)
- 1.2. CNPJ do Autuado: 29.979.036/0001-40
- 1.3. Porte do Autuado: - *Grande porte*
- 1.4. Agente de Tratamento: (  ) Controlador (  ) Operador
- 1.5. Nome do Encarregado ou Responsável Jurídico: Edson Pinheiro Alvarista
- 1.6. Contado do Encarregado: [edson.alvarista@inss.gov.br](mailto:edson.alvarista@inss.gov.br); [encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)

**2. REFERÊNCIAS**

- 2.1. Lei nº 13.709, de 14 de agosto de 2018 – Lei de Geral de Proteção de Dados Pessoais (LGPD);
- 2.2. Regimento Interno da Autoridade Nacional de Proteção de Dados, aprovado pela Portaria nº 01, de 08/03/2021 (RI-ANPD);
- 2.3. Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28/10/2021 (Regulamento de Fiscalização);
- 2.4. Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24/02/2023 (Regulamento de Dosimetria);
- 2.5. Processo 1.1. de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93.

2.6. Processo Administrativo Sancionador nº 00261.001888/2023-21.

### 3. SUMÁRIO EXECUTIVO DO PROCESSO

3.1. Auto de Infração: 03/08/2023 – Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146)

Dispositivo(s) Infringido(s)	Descrição da Infração
Art. 48 da Lei nº 13.709/2018.	Não comunicar aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
Art. 32, §2º da Resolução CD/ANPD nº 1/2021	Não atendimento às determinações da ANPD.

3.2. Intimação: 03/08/2023 – *Certidão de Intimação Cumprida (SEI nº 0048150)*;

3.3. Dados de quem recebeu a Intimação: Edson Pinheiro Alvarista.

3.4. Forma da Intimação: ( X ) Meio eletrônico ( ) Via postal ( ) Pessoal ( ) Comparecimento pessoal ( ) Por edital ( ) Cooperação internacional ( ) Outro meio

3.5. Data da Apresentação da Defesa: 17/08/2023 – Recibo Eletrônico de Protocolo ([SEI nº 0048155](#));

3.5.1. Defesa ([SEI nº 0048151](#));

3.5.2. Processo SEI 35014.293086/2023-34 ([SEI nº 0048152](#));

3.5.3. Processo SEI 35014.437670/2022-27 ([SEI nº 0048153](#)); e

3.5.4. Processo SEI 35014.528489/2022-29 ([SEI nº 0048154](#)).

3.6. Produção de Prova(s) pelo Autuado: ( X ) Não ( ) Sim;

3.7. Produção de Prova(s) pelo Denunciante/ Titular: ( X ) Não ( ) Sim;

3.8. Produção de Prova(s) pela ANPD: ( X ) Não ( ) Sim;

3.9. Terceiro(s) Interessado(s): ( X ) Não ( ) Sim;

3.10. Termo de Ajustamento de Conduta: ( X ) Não ( ) Sim;

3.11. Alegações Finais: ( X ) Não ( ) Sim;

3.12. Medida(s) Preventiva(s) Aplicada(s) com base no Art. 32 do Regulamento de Fiscalização: ( ) Não ( X ) Sim. - Aviso nº 33/2022/CGF/ANPD ([SEI nº 0045825](#)) e Despacho decisório nº 3/2023/CGF/ANPD ([SEI nº 0045840](#))

3.13. Medida(s) Preventiva(s) Aplicada(s) com base no Art. 7º, IV, do RI-ANPD: ( X ) Não ( ) Sim.

## 4. RELATÓRIO

4.1. Conforme disposto no art. 37 do Regulamento de Fiscalização da ANPD, o processo administrativo sancionador destina-se à apuração de infrações à legislação de proteção de dados que sejam de competência da ANPD, nos termos do artigo 55-J, IV, da LGPD. De acordo com o art. 54 do mencionado regulamento, o Relatório de Instrução subsidiará a decisão de primeira instância, a ser proferida pela Coordenação-Geral de Fiscalização (CGF). Assim, em consonância com os ditames normativos aplicáveis ao caso e demais documentos que constam dos autos, passa-se ao detalhamento dos atos processuais até a presente data, com o objetivo de avaliar os motivos da atuação e os argumentos apresentados pela atuada face à legislação e às normas de proteção de dados.

4.2. O Instituto Nacional do Seguro Social (INSS) apresentou, em 19/10/2022, à Coordenação-Geral de Fiscalização (CGF), com fundamento no art. 48 da Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD), Comunicação de Incidente de Segurança (CIS) preliminar (0045818). A entidade pública atuada identificou aumento no número de consultas a dados sem justificativa operacional ou de negócio aparente. Os acessos teriam origem em uma rede autorizada, por órgão da administração pública, e com utilização de credenciais de acesso válidas, concedidas por meio de convênio pelo controlador Instituto Nacional do Seguro Social (INSS) à Advocacia Geral da União (AGU). Além disso, o atuado informou que, nos meses de agosto e setembro de 2022, foram realizadas mais de 90 milhões de consultas ao Sistema Corporativo de Benefícios do INSS (SISBEN) e 9 milhões de consultas ao Sistema Único de Benefícios DATAPREV (BLH00), quantidade quase três vezes maior que a registrada no mês de junho do mesmo ano.

4.3. Por se tratar de comunicação preliminar, no dia 3/11/2022, a Coordenação-Geral de Fiscalização encaminhou comunicação eletrônica ao atuado E-mail - 3725180 (SEI nº 0045820) solicitando a apresentação da complementação da comunicação em até 30 (trinta) dias corridos da comunicação inicial. Decorrido o prazo estabelecido sem que houvesse manifestação do agente de tratamento, a solicitação de complementação foi reiterada no dia 22/11/2022, por intermédio do E-mail - 3760075 (SEI nº 0045821), e concedido prazo adicional de 5 (cinco) dias úteis para resposta.

4.4. Embora o atuado tenha respondido à solicitação da CGF, em 22/11/2022 (SEI nº 0045823), afirmando que iria encaminhar o relatório e informar as ações efetivadas, o prazo se findou sem que as solicitações fossem atendidas. Diante do descumprimento das determinações desta Coordenação-Geral de Fiscalização, a CGF emitiu, em 29/12/2022, o **Aviso nº 33/2022/CGF/ANPD** (SEI nº 0045825), em que determinou que o atuado apresentasse (a) esclarecimentos a respeito da atuação do agente de tratamento

notificante, ou seja, se atua como controlador ou operador dos dados pessoais; (b) formulário de incidente de segurança com informações complementares; (c) relatório técnico de tratamento do incidente; e **(d) comunicação aos titulares a respeito da possível violação do sigilo dos dados no incidente, se cabível.**

4.5. Em cumprimento parcial ao **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825), o autuado apresentou os documentos solicitados em 30/12/2022, por meio do Formulário de Comunicação de Incidente de Segurança Complementar - ANPD - Aviso (SEI nº 0045828). O INSS, porém, justificou a não realização da CIS aos titulares sob alegação de ainda estar analisando a legitimidade dos acessos suspeitos. Ressaltou, ademais, que as medidas de contenção do incidente foram adotadas imediatamente após o registro do incidente pela Comissão de Tratamento e Resposta a Incidentes Cibernéticos (CTIR) da Empresa de Tecnologia e Informações da Previdência (DATAPREV).

4.6. A CGF, em 09/04/2023, por meio do **Despacho Decisório nº 3/2023/CGF/ANPD** (SEI nº 0045840), que acatou a Nota Técnica nº 13/2023/CGF/ANPD (SEI nº 0045838), determinou ao INSS que realizasse, no **prazo de 10 (dez) dias úteis**, nos termos dispostos no art. 48 da Lei nº 13.709 de 14 de agosto de 2018 (LGPD), a comunicação a todos os titulares afetados pelo incidente de segurança comunicado à ANPD e juntasse aos autos do Processo de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93 comprovação do cumprimento da presente determinação.

4.7. O autuado, no entanto, não realizou a comunicação do incidente de segurança aos titulares afetados. Em resposta, tanto no Despacho DTIR - INSS (SEI nº 0045857) quanto no Ofício 1/2023/COPDP/CGCONF/DIGOV-INSS (SEI nº 0045856), o INSS pleiteou pela inviabilidade da comunicação a todos os titulares afetados em razão da impossibilidade técnica de levantamento dos nomes dos segurados, bem como pela desproporcionalidade da comunicação universal. Solicitou, ainda, prorrogação do prazo de cumprimento das medidas preventivas até a conclusão do relatório pela AGU para reavaliação da ação a ser executada. No Ofício 2/2023/COPDP/CGCONF/DIGOV-INSS (SEI nº 0045859), o INSS solicitou prazo indeterminado para a adequação e estruturação do plano de comunicação da entidade pública e atendimento da determinação.

4.8. A CGF, por meio do Despacho (SEI nº 0045861), deferiu a solicitação de prazo adicional para que o referido plano fosse apresentado até 12/05/2023. Do mesmo modo, indicou-se que fosse apontada a data prevista para a comunicação da ocorrência do incidente aos titulares de dados, nos termos do art. 48 da LGPD. Em resposta, foram protocolados pela autuada, no dia 24/05/2023, os documentos Anexo Plano Estratégico de Comunicação Externa (SEI nº 0045866) e Anexo Plano Estratégico de Comunicação Interno (SEI nº 0045867). Entretanto, os documentos enviados à CGF não versam sobre a comunicação ao titular do incidente de segurança em questão, de maneira que a

medida preventiva determinada pela ANPD não foi cumprida.

4.9. A CGF, finalmente, em 23/06/2023, acatou as razões da Nota Técnica nº 54/2023/CGF/ANPD (SEI nº 0045864) e, diante da inércia do autuado em adotar as medidas preventivas determinadas pelo **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825) e pelo Despacho Decisório nº 3/2023/CGF/ANPD (SEI nº 0045840), decidiu pela instauração de processo administrativo sancionador em desfavor do Instituto Nacional do Seguro Social (INSS), nos termos do art. 17, incisos I e III do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 08/03/2021.

4.10. Em 03/08/2023, foi exarado o Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146), devidamente recebido pelo autuado no mesmo dia, conforme a certidão de intimação cumprida (SEI nº 0048150). Conforme o Auto de Infração nº 1/2023/CGF/ANPD (SEI nº 0048146), os dispositivos infringidos pela autuada têm como fundamento (i) a ausência de comunicação de incidente de segurança aos titulares – art. 48 da LGPD; e (ii) a falta de atendimento de medida preventiva – art. 32, §2º, do Regulamento de Fiscalização (Resolução CD/ANPD nº 1/2021).

4.11. Ato contínuo, foi conferido ao autuado o prazo de 10 (dez) dias úteis, a partir da ciência do Auto de Infração em tela, para apresentar **Defesa** perante a Coordenação-Geral de Fiscalização da Autoridade Nacional de Proteção de Dados, via SEI, conforme instruções do Anexo 01, de acordo com o art. 47, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

4.12. Em 17/08/2023, portanto, dentro do prazo indicado, foram encaminhados à CGF os seguintes documentos: Defesa SEI\_12906070 (SEI nº 0048151); Processo SEI\_35014.293086\_2023\_34 (SEI nº 0048152); Processo SEI\_35014.437670\_2022\_27 (SEI nº 0048153); e Processo SEI\_35014.528489\_2022\_29 (SEI nº 0048154). No entanto, não foram apresentadas novas provas pela entidade regulada após a intimação. Com isso, em virtude da faculdade disposta no art. 53 do Regulamento de Fiscalização, foi encaminhado ao Coordenador de Proteção de Dados Pessoais (COPDP) do INSS, por meio do Ofício nº 72/2023/FIS/CGF/ANPD (SEI nº 0048156), intimação para que o autuado apresentasse **alegações finais**, no prazo de 10 (dez) dias úteis, a partir da ciência deste Ofício, perante a Coordenação-Geral de Fiscalização da ANPD.

4.13. Do mesmo modo, informou-se à entidade pública autuada que ela poderia indicar eventuais informações constantes no presente processo sancionatório que, a seu ver, encontrar-se-iam protegidas por hipótese legal de sigilo, devendo-se indicar as razões de fato e de direito que sustentariam

eventual restrição de acesso a informações.

4.14. O autuado foi considerado intimado, em 02/01/2024, por decurso do prazo tácito, conforme Certidão de Intimação Cumprida (SEI nº 0048157).

4.15. É o relatório.

## **5. PRELIMINARES**

### **5.1. Competência.**

5.1.1. A Lei nº 13.709/18, Lei Geral de Proteção de Dados (LGPD), art. 5º, I, considera dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável". Os dados envolvidos no incidente de segurança aqui tratado – CPF, nome completo, data de nascimento, diagnóstico, data de encaminhamento médico, responsável pela criança, números de telefone e endereço – são dados pessoais (alguns até mesmo sensíveis), pois consistem em informação relacionada a pessoa natural identificada ou identificável.

5.1.2. Diante disso, resta claro que o incidente de segurança informado à ANPD envolve o tratamento de dados pessoais de terceiras pessoas, uma vez que o evento adverso teria afetado a base de beneficiários e segurados do INSS, que inclui dados pessoais como Nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes. Além disso, observa-se que, por se tratar de banco de dados com informações sobre benefícios previdenciários, o incidente de segurança potencialmente envolve dados pessoais sensíveis. Nos termos do inciso II do art. 5º da LGPD, considera-se dados pessoais sensíveis os dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

5.1.3. No que se refere ao papel dos agentes de tratamento responsáveis pela base de dados envolvida no incidente de segurança, verifica-se que a DATAPREV atua como a operadora do Sistema Corporativo de Benefícios do INSS (SISBEN), por se tratar de pessoa jurídica de direito privado, vinculada ao Ministério da Gestão e Inovação em Serviços Públicos (MGI), responsável pelo tratamento de dados pessoais em nome do controlador. O INSS, por sua vez, atua como a entidade controladora da referida base de dados, por se tratar de, nos termos do art. 5º, VI, pessoa jurídica de direito público a quem compete as decisões referentes ao tratamento de dados pessoais dos beneficiários.

5.1.4. A Lei nº 13.709, de 14/08/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), por sua vez, determina no art. 48 que "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares". O §1º, por

sua vez, estabelece que a comunicação deve ocorrer em prazo razoável e indicar a natureza dos dados pessoais afetados, os titulares envolvidos, as medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente, os motivos da demora e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

5.1.5. Ainda, cabe à ANPD, de acordo com o art. 55-J, I, da LGPD "zelar pela proteção dos dados pessoais, nos termos da legislação", bem como "IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso".

5.1.6. De acordo com o Regimento Interno da ANPD:

Art. 17. São competências da Coordenação-Geral de Fiscalização, sem prejuízo de outras previstas na Lei nº 13.709, de 2018, no Decreto nº 10.474, de 2020, e na legislação aplicável:

I - fiscalizar e aplicar as sanções previstas no artigo 52 da Lei nº 13.709, de 2018, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;

(...)

III - promover ações de fiscalização sobre as ações de tratamento de dados pessoais efetuadas pelos agentes de tratamento, incluído o Poder Público;

(...)

IX - requisitar aos agentes de tratamento de dados a apresentação de Relatório de Impacto à Proteção de Dados Pessoais;

5.1.7. O art. 48 do Regimento Interno da ANPD, ainda, determina que as "atividades da ANPD obedecerão, além dos princípios estabelecidos na Lei nº 13.709, de 2018, aos princípios da legalidade, motivação, moralidade, eficiência, celeridade, interesse público, impessoalidade, igualdade, devido processo legal, ampla defesa, contraditório, razoabilidade, proporcionalidade, imparcialidade, publicidade, economicidade, segurança jurídica, entre outros". Esta é, portanto, a justificativa para análise do suposto incidente de segurança ocorrido no Instituto de Pesquisas Jardim Botânico do Rio de Janeiro em processo administrativo próprio, pois é necessário observar as diretrizes e os princípios incidentes sobre a atuação administrativa no cumprimento da atribuição de fiscalização.

5.1.8. O Regulamento de Fiscalização da ANPD, aprovado pela Resolução CD/ANPD nº 1, de 28/10/2021, dispõe de forma fundamental sobre a estruturação das atividades previstas no art. 17 do Regimento Interno da ANPD. De acordo com o art. 2º do Regulamento, a fiscalização volta-se à orientação, à prevenção e à repressão das infrações à LGPD, de sorte a,

conforme o art. 3º, proteger os direitos dos titulares de dados, promover a implementação da legislação de proteção de dados pessoais e zelar pelo cumprimento das disposições da LGPD.

5.1.9. Por força do art. 4º, I, do mencionado Regulamento, o Instituto de Pesquisas Jardim Botânico do Rio de Janeiro é considerado agente regulado pela ANPD, haja vista ser um agente de tratamento (ver. art. 5º, IX da LGPD). Cumpre especificar as atividades a que os agentes regulados estão submetidos, a teor do art. 5º:

Art. 5º Os agentes regulados submetem-se à fiscalização da ANPD e têm os seguintes deveres, dentre outros:

I - fornecer cópia de documentos, físicos ou digitais, dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais, no prazo, local, formato e demais condições estabelecidas pela ANPD;

II - permitir o acesso às instalações, equipamentos, aplicativos, facilidades, sistemas, ferramentas e recursos tecnológicos, documentos, dados e informações de natureza técnica, operacional e outras relevantes para a avaliação das atividades de tratamento de dados pessoais, em seu poder ou em poder de terceiros;

III - possibilitar que a ANPD tenha conhecimento dos sistemas de informação utilizados para tratamento de dados e informações, bem como de sua rastreabilidade, atualização e substituição, disponibilizando os dados e as informações oriundos destes instrumentos;

IV - submeter-se a auditorias realizadas ou determinadas pela ANPD;

V - manter os documentos físicos ou digitais, os dados e as informações durante os prazos estabelecidos na legislação e em regulamentação específica, bem como durante todo o prazo de tramitação de processos administrativos nos quais sejam necessários; e

VI - disponibilizar, sempre que requisitado, representante apto a oferecer suporte à atuação da ANPD, com conhecimento e autonomia para prestar dados, informações e outros aspectos relativos a seu objeto.

5.1.10. Pelo exposto, não há dúvidas quanto à competência da ANPD no caso concreto para avaliar a conduta do Instituto de Pesquisa Jardim Botânico do Rio de Janeiro, controlador de dados e agente regulado, à luz da LGPD.

## 5.2. **Prescritibilidade.**

5.2.1. No presente processo, não há que se analisar a prescrição intercorrente, a qual pode ser verificada quando existe paralisação do processo por mais de 3 (três) anos, a teor do Art. 1º, §1º, Lei nº 9.873/99. Com

efeito, os documentos recebidos pela ANPD e que subsidiaram a abertura do processo de fiscalização foram recebidos em 26/01/2022, e considerando as ações desenvolvidas, bem como a data de apresentação do presente relatório, não há que se falar em paralisação do processo por mais de 3 (três) anos. Tampouco foi verificada a prescrição punitiva, a qual incide após cinco anos da data do ato, consoante disposto no art. 1º, *caput*, da Lei nº 9.873/99.

5.3. No mais, o autuado não arguiu questões preliminares de mérito em sua defesa e em nossas análises preliminares não verificamos questões relevantes a serem trazidas a este Relatório de Instrução.

## 6. ANÁLISE

### 6.1. *Circunstâncias da infração*

6.1.1. Os documentos apresentados aos autos são suficientes para afirmar que houve um incidente de segurança, envolvendo dados do Sistema Corporativo de Benefícios do INSS (SISBEN), conforme detalhado na Nota Técnica 13/2023/CGF/ANPD (SEI nº 0045838), Processo de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93. Conforme disposto no documento, a comunicação do evento adverso aos titulares afetados justificar-se-ia em virtude do elevadíssimo número de pessoas naturais potencialmente afetadas, uma vez que a base de dados envolvida armazena uma grande quantidade de dados pessoais, tais como nome, CPF, NIT, RG, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes, cuja publicação indevida poderia expor os titulares a riscos de fraudes e roubo de identidade. O próprio autuado, nesse sentido, informou que utilizou como critério de comunicação à ANPD que "O incidente de segurança pode acarretar risco ou dano relevante aos titulares".

6.1.2. A determinação de comunicação aos titulares, no prazo de 10 (dez) dias úteis, foi formalizada no Despacho Decisório 3 (SEI nº 0045840) e encaminhada ao INSS por meio do Ofício 58 (SEI nº 0045841). O INSS foi intimado da referida decisão por via eletrônica no dia 10/04/2023, conforme Certidão de Intimação Cumprida (SEI nº 0045844). O agente de tratamento também confirmou o recebimento do Ofício, conforme e-mail do INSS (SEI nº 0045852), de 12/04/2023 e e-mail do DATAPREV (SEI nº 0045853), de 13/04/2023.

6.1.3. Em resposta, o INSS apresentou a Portaria PRES/INSS nº 30, de 15 de fevereiro de 2023 (SEI nº 0045847), com a alteração do Encarregado, protocolou Ofício (SEI nº 0045856) e Despacho (SEI nº 0045857), em 25/04/2023. Em resumo, pleiteou pela inviabilidade da comunicação a todos os titulares afetados em razão da impossibilidade técnica de levantamento dos nomes dos segurados e da desproporcionalidade da comunicação universal. Solicitou, ainda, prorrogação do prazo até a conclusão do relatório pela AGU para reavaliação da ação a ser executada.

6.1.4. Entretanto, mesmo com o deferimento da prorrogação do prazo de cumprimento da medida preventiva determinada pela CGF, conforme o Despacho (SEI nº 0045861), o INSS não comunicou o incidente de segurança aos titulares de dados pessoais afetados, em claro descumprimento das obrigações legais exaradas no art. 48 da LGPD e do art. 32, §2º, do Regulamento de Fiscalização (Resolução CD/ANPD nº 1/2021).

6.1.5. Restam comprovados, assim, os fatos que ensejaram a instauração deste PAS e a autoria por parte da autuada, nos termos do art. 43, inciso I, da Lei Geral de Proteção Dados Pessoais.

## 6.2. **Análise da defesa apresentada pelo Autuado**

6.2.1. O INSS, em sede de defesa (SEI nº 0048151), apresentou os argumentos abaixo:

6.2.2. Decisão sobre comunicação do incidente de segurança ao titular deve passar por juízo de pertinência pela Administração Pública.

"[A] divulgação aos titulares supostamente afetados, quando possível, deve ser avaliada pela Administração Pública Federal e, não havendo comprometimento dos interesses maiores do Estado, as comunicações devem ser realizadas. Isso se dá dessa forma em razão do preavalecimento do interesse público sobre os interesses individuais. No caso, o incidente de segurança que ensejou a abertura do presente processo sancionador foi tempestivamente comunicado à ANPD, que determinou e insistiu na comunicação dos titulares dos dados potencialmente acessados, o que não ocorreu em razão de não se vislumbrar sua pertinência."

6.2.3. A comunicação do incidente de segurança ao titular é medida irrazoável e prejudicial ao interesse público.

"Por um lado, não foi possível determinar os potenciais dados acessados e seus correspondentes titulares, de modo que comunicações individualizadas seriam materialmente impossíveis. Por outro, uma divulgação ampla e indistinta do incidente cibernético, que teria atingido um percentual ínfimo das milhões de pessoas com as quais o INSS manteve algum tipo de relação ao longo de décadas, contaria apenas com o potencial de gerar pânico e desconfiança em todo o contingente de segurados e beneficiários vinculados ao INSS. Qualquer comunicado a respeito do incidente, antes de proteger efetivamente os segurados e beneficiários, ocasionaria um caos nos canais de atendimento do INSS, que não teria condições sequer de indicar objetivamente se dados foram efetivamente acessados, quais dados e de quais pessoas, caso fosse demandado a fazê-lo. Nesse passo, a determinação para a comunicação dos titulares, além de sobrepujar o princípio da supremacia do interesse público no caso concreto, também

consistiria em medida irrazoável, posto que impossível de execução material em função da indeterminação de dados e seus titulares, e desproporcional, a considerar que impõe obrigação em medida superior àquelas estritamente necessárias ao atendimento do interesse público, que já foram tomadas pelos agentes de tratamento, a saber, o INSS, DATAPREV e AGU, que agiram com total transparência e atenderam aos preceitos legais e normativos da LGPD."

6.2.4. A consequência danosa da comunicação do incidente de segurança ao titular, em vista do art. 20 da LINDB.

"A ampla divulgação aos titulares dos dados que possam ser afetados em incidentes de segurança não é uma consequência legal necessária e automática, dependendo da presença das condições do § 2º do artigo 48 da LGPD, cuja interpretação e aplicação deve ser motivada sob a perspectiva dos princípios da razoabilidade e da proporcionalidade e do consequencialismo."

6.2.5. A determinação que obriga comunicação do incidente de segurança ao titular deve ser motivada pela ANPD.

"No § 2º de tal dispositivo também consta que a ANPD verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente. [...] A ampla divulgação exigiria uma motivação específica por parte da ANPD a respeito das condições estabelecidas em tal dispositivo. Por outro lado, a Coordenação de Fiscalização da ANPD não emprestou qualquer valor às medidas que foram tomadas incontinentem no sentido de investigar, comunicar e sanar o problema identificado, num ambiente de absoluta boa-fé e transparência nos processos administrativos. [...] A Coordenação de Fiscalização da ANPD não motivou sua determinação de comunicação do incidente segundo os aspectos contidos no § 2º do artigo 48 da LGPD, nos termos dos artigos 20 a 22 da LINDB. [...] O auto de infração deve ser considerado nulo por falta de motivação, observado o disposto no artigo 2º da Lei nº 4.717, de 29 de junho de 1965, e o disposto no artigo 50, I e II, da Lei nº 9.784, de 1999, ou insubsistente em relação ao mérito, dada a inobservância da supremacia do interesse público, dos princípios da proporcionalidade e da razoabilidade e do consequencialismo tratado na LINDB."

6.2.6. O Decreto 10.748, de 16 de julho de 2021, impede a divulgação de informações sobre incidente de segurança sofrido pela Administração Pública Federal.

"[A] LAI, ao tratar de hipóteses restritivas ao acesso de informações, em seu artigo 23, estabeleceu a possibilidade de serem classificadas

como sigilosas informações “imprescindíveis à segurança da sociedade ou do Estado”. E o Decreto nº 10.748, de 2021, que institui a Rede Federal de Gestão de Incidentes Cibernéticos, considera que as informações sobre incidentes cibernéticos são imprescindíveis à segurança da sociedade e do Estado. Confirma-se o disposto em seu artigo 15 [...]. O cotejo entre o artigo 23 da LAI c/c com o artigo 15 do Decreto nº 10.748, de 2021 e o artigo 48 da Lei nº 13.709, de 2018 revelam uma antinomia aparente. Antinomia que não resiste à aplicação do critério da especialidade. Com efeito, o controlador tem o dever de comunicar à ANPD e aos titulares dos dados sobre os incidentes cibernéticos, na presença de riscos ou danos relevantes. E a divulgação aos titulares supostamente afetados, quando possível, deve ser avaliada pela Administração Pública Federal e, não havendo comprometimento dos interesses maiores do Estado, as comunicações devem ser realizadas. Isso se dá dessa forma em razão do prevalectimento do interesse público sobre os interesses individuais.”

### 6.3. ***Das alegações finais apresentadas pelo Autuado***

6.3.1. Foi encaminhado ao Coordenador de Proteção de Dados Pessoais (COPDP) do INSS, por meio do Ofício nº 72/2023/FIS/CGF/ANPD (SEI nº 0048156), intimação para que o autuado apresentasse **alegações finais**, no prazo de 10 (dez) dias úteis, a partir da ciência deste Ofício, perante a Coordenação-Geral de Fiscalização da ANPD, conforme os termos facultados no art. 53 do Regulamento de Fiscalização. O autuado, porém, não respondeu à solicitação, motivo pelo qual foi considerado intimado, em 02/01/2024, por decurso do prazo tácito, conforme Certidão de Intimação Cumprida (SEI nº 0048157).

### 6.4. ***Subsunção do fato ao tipo infracional correspondente***

#### **I - Da obrigação de comunicar o titular sobre o incidente de segurança em questão: descumprimento do art. 48 da LGPD pelo INSS.**

6.4.1. A LGPD inaugurou um sistema jurídico para tutelar os direitos e garantias dos titulares de dados pessoais, a fim de resguardar que qualquer tratamento de dados referente à pessoa natural identificada ou identificável ocorra em acordo com as determinações legais previstas no ordenamento jurídico. Dessa forma, a LGPD estabelece uma série de determinações que devem ser cumpridas pelos agentes de tratamento para que sejam garantidos a autodeterminação informativa, a privacidade, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, entre outros elencados em seu art. 2º.

6.4.2. O artigo 48 da LGPD, nesse sentido, estabelece a obrigação do controlador de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e

ao titular de dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Observe-se abaixo:

**Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.**

§ 1º A comunicação será feita em **prazo razoável**, conforme definido pela autoridade nacional, e deverá mencionar, **no mínimo**:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, **caso necessário para a salvaguarda dos direitos dos titulares**, determinar ao controlador a adoção de providências, tais como:

I - **ampla divulgação do fato em meios de comunicação**; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. (Grifo nosso)

6.4.3. Pode-se compreender pela leitura do *caput* do artigo que o controlador não se encontra obrigado a comunicar aos destinatários de direito (ANPD e titulares) a ocorrência de todo e qualquer tipo de incidente de segurança, mas apenas em relação ao *incidente de segurança qualificado*, isto é, aquele cuja ocorrência, em virtude da natureza dos dados pessoais envolvidos ou do número de pessoas naturais afetadas, por exemplo, possa gerar lesões potencialmente danosas aos direitos dos indivíduos afetados<sup>[1]</sup>.

6.4.4. Em caso de ocorrência de incidente de segurança, desse modo, cabe ao controlador avaliar se as consequências do evento podem ocasionar danos materiais ou morais relevantes aos titulares, como discriminação, violação aos direitos à imagem, honra e privacidade, fraudes financeiras e roubos de identidades. É importante destacar, nesse sentido, que o controlador deve sempre agir com cautela ao avaliar as probabilidades de danos a terceiros, de maneira a adotar as medidas preventivas contidas no artigo 48 da LGPD mesmo

nos casos em que houver dúvidas quanto à gravidade dos riscos e danos envolvidos. Isso ocorre uma vez que a comunicação do incidente de segurança qualificado tem como objetivo não apenas o cumprimento do dever de mitigação do prejuízo pelo próprio controlador, mas sobretudo permitir que a pessoa natural afetada possa tomar medidas preventivas para conter os eventuais danos provocados pelo evento[2]. Observe-se, nesse sentido, a conduta defendida por MODENESI (Brasil, 2022):

“Eventualmente, diante de um caso concreto em que o controlador esteja em dúvida sobre a consumação do incidente de segurança, deve-se, mediante conduta cautelosa e preventiva, **comunicar à autoridade nacional e ao titular** as circunstâncias da ocorrência apurada, o que desvela uma renovada aplicação, no âmbito dos direitos civis, do brocardo *in dubio pro societate*, pois proteger dados pessoais e pessoas humanas é, ao fim e ao cabo, proteger toda a sociedade. ***Essa orientação interpretativa induz à criação de uma máxima adequada à sociedade da informação: in dubio pro titular dos dados, que, inclusive, já vem sendo reconhecida como um princípio apto a compensar as assimetrias de poder e de conhecimento entre titular e agentes de tratamento***”. (Grifo nosso).

6.4.5. Desse modo, verificado que o incidente de segurança pode gerar risco ou dano relevante aos titulares de dados pessoais, o controlador não pode se eximir de fazer a devida comunicação do evento adverso, nos termos do *caput* do art. 48 da LGPD, tanto para a ANPD quanto para os titulares afetados. Desse modo, uma vez que a comunicação aos titulares de dados, conforme já destacado, visa a possibilidade de mitigação de eventuais impactos negativos decorrentes do incidente, ela deve ser feita o mais rapidamente possível[3].

6.4.6. Assim, além da obrigação de comunicação do incidente aos sujeitos destinatários, a LGPD também estabelece que as informações pertinentes ao evento adverso devem ser prestadas em tempo razoável, nos termos do §1º do art. 48 da LGPD. Ainda que a norma não imponha prazo específico para a comunicação, a demora injustificada na tomada de ação pelo controlador deve ser compreendida como infração ao dever exarado pelo *caput* da norma em comento, pois impede que o titular possa tomar medidas que garantam a segurança de seus dados pessoais, apesar da ocorrência do incidente. É importante ressaltar, nesse sentido, que a ANPD recomenda que o incidente de segurança seja comunicado em até 2 (dois) dias úteis da ciência do fato[4].

6.4.7. Diante do exposto, não há que se falar em exercício do poder discricionário da Administração quando observado que o incidente de segurança ocorrido é potencialmente lesivo aos titulares, por ensejar relevante risco de dano a seus direitos e garantias fundamentais. O poder

discricionário pode ser exercido pela Administração quando o agente administrativo, dentre várias condutas possíveis, pode optar pela ação que traduz maior conveniência e oportunidade para o interesse público[5]. A norma do art. 48 da LGPD *não* confere ao controlador liberdade para fixar juízo de ordem técnica quanto à possibilidade de comunicação do incidente de segurança qualificado aos titulares quando identificado o potencial de ocorrência de danos relevantes decorrentes do evento adverso.

6.4.8. O *caput* do art. 48, na verdade, impõe ao controlador uma atuação vinculada, pois obriga-o a realizar conduta rigorosamente nos termos do parâmetro definido em lei, qual seja, a comunicação tanto à ANPD quanto ao titular de ocorrência do incidente de segurança qualificado que envolva dados pessoais. É importante destacar, nesse sentido, que os sujeitos destinatários da obrigação de comunicação são tanto a Autoridade Nacional de Proteção de Dados quanto os titulares afetados pelo incidente, não cabendo ao controlador optar a quem encaminhará a devida comunicação.

6.4.9. Logo, verificada a ocorrência do incidente de segurança qualificado envolvendo dados pessoais, o controlador deve necessariamente comunicar os titulares sobre a ocorrência do evento, nos termos do *caput* do art. 48 da LGPD. Não há que se falar, desse modo, em exercício legítimo do poder discricionário pelo controlador, uma vez que o agente de tratamento se encontra vinculado à determinação da norma supracitada.

6.4.10. Percebe-se, portanto, conforme destacado no **Auto de Infração nº 1/2023/FIS/CGF/ANPD**(SEI nº 0048146), **que o INSS** agiu em desconformidade com o disposto no *caput* do art. 48 da LGPD, uma vez que não comunicou aos titulares afetados a ocorrência de incidente de segurança qualificado, consoante verificado por esta Autoridade Nacional de Proteção de Dados no âmbito do Processo de Apuração de Incidente de Segurança (PAI) nº 00261.002177/2022-93.

6.4.11. Conforme verificado durante a tramitação do referido PAI, ademais, o INSS não refutou ou questionou a ocorrência do incidente de segurança ou a possibilidade deste acarretar risco ou dano relevante aos titulares. Na verdade, a própria entidade pública autuada admitiu que o incidente de segurança em comento poderia ensejar riscos e danos aos titulares de dados envolvidos. Tais riscos estão associados ao teor dos dados pessoais contidos na base de dados objeto do incidente, que abrangem dados de comprovação de identidade oficial, bem como dados financeiros e referentes à saúde dos titulares, segundo o Formulário de Comunicação de Incidente de Segurança Complementar - ANPD - Aviso (SEI nº 0045828). O vazamento desses dados pessoais, portanto, pode causar aos titulares tanto danos patrimoniais quanto extrapatrimoniais.

6.4.12. No caso concreto, portanto, caberia ao INSS comunicar as pessoas naturais cujos dados pessoais compunham as bases de dados atingidas pelo incidente de segurança relatado à ANPD, indicando todas as informações referidas no §1º do art. 48 da LGPD. No entanto, a entidade pública regulada resistiu até o momento em cumprir a determinação legal em comento, mesmo após diversas determinações feitas pela Coordenação Geral de Fiscalização (CGF), evidenciando o descumprimento da obrigação legal inserida no art. 48 da Lei Geral de Proteção de Dados Pessoais.

**II - Do não atendimento às requisições da ANPD pela entidade autuada: Art. 32, §2º da Resolução CD/ANPD nº 1/2021.**

6.4.13. A comunicação do incidente de segurança é medida preventiva importante, pois, a partir da ação do controlador, o próprio titular pode realizar ações acautelatórias que o protejam de eventuais furtos de identidade, fraudes, assédios comerciais, dentre outros danos que possam o atingir desde a ocorrência do incidente. A Resolução CD/ANPD nº 1/2021, nesse sentido, confere à Coordenação Geral de Fiscalização, no exercício do poder de fiscalização conferido pelo art. 55-J, IV, da LGPD, o poder de determinar ao agente de tratamento medidas preventivas que visem remediar situações que acarretem riscos ou danos aos titulares de dados. Dentre tais medidas, encontra-se a divulgação de informações.

6.4.14. Conforme já relatado nos itens 4.4 e 4.6 do presente Relatório de Instrução, a Coordenação Geral de Fiscalização determinou ao autuado que realizasse a comunicação do incidente de segurança qualificado aos titulares em duas oportunidades. Primeiramente, foi encaminhado o **Aviso nº 33/2022/CGF/ANPD**(SEI nº 0045825). Posteriormente, a determinação foi exarada por meio do **Despacho Decisório nº 3/2023/CGF/ANPD** (SEI nº 0045840). Em ambas as oportunidades, no entanto, houve a recusa do INSS em cumprir a determinação desta Autarquia Federal, o que implica a subsunção do fato à infração disposta no art. 32, §2º da Resolução CD/ANPD nº 1/2021.

6.4.15. Deve-se, contudo, analisar mais detalhadamente os argumentos trazidos ao conhecimento da CGF pela entidade pública autuada para justificar a sua inércia. Para esse fim, os argumentos apresentados na defesa foram divididos em três blocos: *(i) a comunicação do incidente de segurança qualificado como medida necessária para a proteção dos direitos do titular; (ii) o interesse público subjacente à comunicação do incidente de segurança e da razoabilidade da medida preventiva; e (iii) a inaplicabilidade do art. 15 do Decreto nº 10.748/2021 ao caso concreto.*

**(i) A comunicação do incidente de segurança qualificado como medida necessária para a proteção dos direitos do titular:**

6.4.16. O INSS, em defesa apresentada no presente processo administrativo sancionador (SEI nº0048151), indicou não haver "como precisar quais dados foram potencialmente acessados, consultados e eventualmente compartilhados, nem as pessoas casualmente afetadas", e que "não foi possível determinar os potenciais dados acessados e seus correspondentes titulares, de modo que comunicações individualizadas seriam materialmente impossíveis". Diante eventual impossibilidade de rastrear os titulares afetados pelo incidente, o autuado arguiu que não seria logicamente possível que a comunicação do incidente fosse realizada de maneira individual, sob pena de não se alcançar o objetivo da medida.

6.4.17. O autuado, desse modo, afirmou não haver conseguido mapear um grupo específico potencialmente atingido pelo incidente, motivo pelo qual a comunicação individual do incidente de segurança ao titular, que seria a solução adequada para a conformidade com o disposto no *caput* da norma, não foi cumprida.

6.4.18. O INSS, além disso, argumentou que eventual "divulgação ampla e indistinta do incidente cibernético (...) **contaria apenas com o potencial de gerar pânico e desconfiança em todo o contingente de segurados e beneficiários vinculados ao INSS**". Desse modo, advertiu que "(q)ualquer comunicado a respeito do incidente, antes de proteger efetivamente os segurados e beneficiários, ocasionaria **um caos nos canais de atendimento do INSS**, que não teria condições sequer de indicar objetivamente se dados foram efetivamente acessados, quais dados e de quais pessoas, caso fosse demandado a fazê-lo" (Grifo original).

6.4.19. Em que pese os argumentos trazidos pelo INSS, compete à entidade, no papel de controladora, empregar todos seus esforços para cumprir a norma de proteção de dados pessoais de forma eficaz. Por conseguinte, a falta de mecanismos de segurança que permitam o rastreamento dos dados acessados no incidente ou a impossibilidade técnica de individualização dos titulares afetados pelo incidente, conforme alegado, não deve ser justificativa suficiente para a inaplicabilidade da obrigação legal exarada pelo art. 48 da LGPD, bem como pelo descumprimento da determinação deste órgão fiscalizador.

6.4.20. O objetivo da comunicação ao titular, como já ressaltado neste RI, é garantir ao titular a possibilidade de tomar medidas preventivas para se proteger de eventuais furtos de identidade, fraudes, assédios comerciais, entre outros danos que possam o atingir desde a ocorrência do incidente. Além disso, a inobservância desse dever pelo autuado pode incentivar postura de pouco cuidado com segurança da informação por parte dos agentes de tratamento, uma vez que, não sendo possível a comunicação individualizada ao titular, a obrigação de comunicação não persistiria. Neste cenário, o agente

se valeria do próprio descuido (negligência) para justificar o não cumprimento da lei. Tal conduta, do mesmo modo, exacerba a assimetria informacional existente entre o agente de tratamento e o titular dos dados, ao privar a pessoa natural afetada de receber informações pertinentes quanto ao tratamento de seus dados pessoais pelo controlador, em especial no que se refere aos procedimentos de segurança aos quais os dados são submetidos.

6.4.21. O princípio da boa-fé objetiva, previsto no *caput* do art. 6º da LGPD, nesse sentido, estabelece que as operações de tratamento de dados pessoais devem ser realizadas pelo controlador com observância dos deveres de lealdade e de transparência com o titular, isto é, o controlador precisa orientar as suas ações com base nos interesses legítimos e expectativas razoáveis do titular, no contexto de tratamento que não lhe cause qualquer tipo de abuso, lesão ou desvantagem[6]. Frazão, Prata de Carvalho e Milanez (Brasil, 2022), inclusive, definem que o princípio da boa-fé objetiva possui função limitadora ao restringir, de certa forma, a liberdade de conduta dos agentes de tratamento ao considerar certas práticas como possivelmente abusivas e ao incentivar a transparência e a previsibilidade nas relações jurídicas[7].

6.4.22. A recusa do controlador em comunicar o titular sobre a ocorrência de incidente de segurança qualificado, desse modo, vai de encontro ao princípio da boa-fé objetiva, uma vez que há expectativa razoável do titular em ser devidamente informado sobre incidentes de segurança que possam ensejar resultados danosos para o exercício de seus direitos individuais. Ademais, como um dos objetivos da comunicação é justamente permitir que o titular possa tomar medidas acautelatórias para proteger seus dados pessoais, a falta proposital de comunicação pelo controlador evidencia claro desrespeito ao princípio da prevenção, inscrito no inciso VIII do art. 6º da LGPD. No caso concreto, configura-se uma exacerbação da assimetria informacional entre controlador e titulares de dados, quanto aquele impede que estes tenham todas as informações necessárias para a proteção da tutela de seus direitos e garantias fundamentais.

6.4.23. A impossibilidade técnica de comunicação individual do incidente de segurança qualificado, portanto, não exime o controlador da obrigação legal de comunicação do evento adverso aos titulares, uma vez que a divulgação do incidente pode ser feita por meios indiretos, como uma comunicação individualizada a todos os titulares potencialmente afetados (100% dos titulares cujos dados são tratados no sistema ou na base de dados comprometida), como uma comunicação difusa em seus canais de atendimento e relacionamento (independentemente de ser um titular potencialmente afetado) ou, por fim, como a ampla publicação em meios de comunicação, este último conforme admitido pelo §2º do art. 48 da LGPD.

Nessa transição gradual do mais 'discreto e preciso' ao mais 'exposto e difuso' é possível observar a proporcionalidade entre o ônus que recai sobre o controlador em função de seu preparo e adequação à LGPD: um controlador preparado com sistemas adequados à LGPD (art. 46 e 49) possui governança o suficiente para identificar quem e quando foi afetado e direcionar sua comunicação somente às pessoas efetivamente afetadas, consequentemente reduzindo sua exposição; um controlador que não tomou o devido cuidado em se adequar à LGPD não será capaz de individualizar as pessoas e por conseguinte necessita se expor mais para atingir o comando legal de comunicar às pessoas que seus dados foram potencialmente afetados. Admitir qualquer leitura em sentido oposto constitui uma lógica perversa que estimula o descaso com a segurança da informação, a insensibilidade com o impacto de incidentes nas vidas das pessoas e converte em 'sanção' financeira o investimento realizado pelo controlador que agiu corretamente. Em situações de mercado concorrencial, isso pode até causar abalos significativos no equilíbrio concorrencial entre os agentes econômicos.

6.4.24. Não se deve, ademais, impugnar o Auto de Infração nº 1/2023/FIS/CGF/ANPD por falta de transparência quanto à motivação que levou ao referido ato administrativo, conforme alegado pelo autuado. Os motivos determinantes que fundamentaram a medida regulatória foram devidamente informados à entidade autuada no âmbito da Nota Técnica 13/2023/CGF/ANPD (SEI nº 0045838), conforme consta no item 7. da Descrição dos fatos e dos dispositivos infringidos do Auto de Infração nº 1/2023/FIS/CGF/ANPD. Nesse sentido, foi informado ao autuado que "(a) comunicação ao titular deve ser feita em razão do elevadíssimo número de titulares potencialmente afetados, pois trata-se de sistemas que armazenam uma grande quantidade de dados pessoais, tais como Nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes. No mesmo sentido, o próprio INSS informou como critério para comunicação à ANPD que "o incidente de segurança pode acarretar risco ou dano relevante aos titulares"".

*(ii) Do interesse público subjacente à comunicação do incidente de segurança e da razoabilidade da medida preventiva:*

6.4.25. O princípio da razoabilidade está implícito na Constituição da República Federativa do Brasil e expresso na legislação infraconstitucional, como na Lei nº 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal. De acordo com esse princípio, a Administração Pública deve atuar dentro de certos padrões médios de aceitabilidade pela sociedade, de maneira que será compreendida como razoável a conduta do Estado quando legítima perante o corpo social. Do mesmo modo, não se poderia esperar da Administração a adoção de condutas que resultassem em desacordo

com os princípios gerais do direito.

6.4.26. Pode-se compreender, desse modo, que o princípio da razoabilidade aplicado às atividades de fiscalização da ANPD visaria explicitar a necessidade do uso moderado dos meios administrativos disponíveis para a aplicação da Lei Geral de Proteção de Dados Pessoais. Assim, por meio da observância do princípio da razoabilidade, buscar-se-ia evitar que o atendimento às determinações da ANPD, no exercício das suas atividades fiscalizatória e sancionatória, gerasse encargo excessivamente oneroso para a entidade regulada, especialmente quando o atendimento da determinação estatal se mostrasse em desconformidade com o interesse público preponderante ou os princípios gerais do direito.

6.4.27. Segundo o princípio da supremacia do interesse público, presume-se que a atuação do Estado está pautada pelo interesse geral, consubstanciado nas leis e na Constituição, sendo, desse modo, um resultado da “vontade geral”. Decorre deste princípio o fato de que, em havendo conflito entre os interesses privados e o interesse público, representado pelo Estado, prevalecerá este último, resguardando-se os direitos dos particulares.

6.4.28. De acordo com Barroso (Barroso, 2015)[\[8\]](#), ao se analisar a incidência do princípio da supremacia do interesse público em determinada relação jurídica, deve-se primeiramente distinguir o interesse público primário do interesse público secundário. O interesse público primário pode ser compreendido como a própria razão de ser do Estado, ou seja, caracteriza-se como os interesses de toda a sociedade, como a promoção da justiça e do bem-estar social. O interesse público secundário, por sua vez, pode ser entendido como a vontade da pessoa jurídica de direito público exarada em determinada relação jurídica. Para o autor, é o interesse público primário que desfruta de supremacia em um sistema constitucional e democrático, uma vez que ele não é passível de ponderação, uma vez que constitui o próprio parâmetro para a ponderação com outros direitos e garantias fundamentais. O interesse público secundário, por outro lado, ao entrar em aparente colisão com outros valores jurídicos, deve ser ponderado com base nas condições fáticas e de direito presentes no caso concreto.

6.4.29. A avaliação acerca da razoabilidade da ação fiscalizatória da ANPD exige, portanto, uma reflexão qualitativa a respeito da plausibilidade da determinação em análise, ou seja, deve-se avaliar se o objeto da resolução estatal se encontra dentro dos limites impostos pelos princípios gerais do direito e pelo meio social com que o direito à proteção de dados pessoais dialoga. Desse modo, é preciso avaliar as opções disponíveis, no caso concreto, com o objetivo de atingir a solução mais adequada à consecução do interesse público.

6.4.30. Observa-se que no caso em análise a medida determinada pela

ANPD à entidade autuada encontra-se dentro das alternativas legais dispostas em norma jurídica específica, isto é, o art. 48 da LGPD, motivo pelo qual a determinação encontra-se dentro dos limites legais impostos pelo ordenamento jurídico. Conforme já discutido na seção anterior, uma vez identificadas as premissas legais para realização da comunicação do incidente de segurança, não cabe à entidade escolher a qual destinatário irá encaminhar os avisos pertinentes, de maneira que a divulgação aos titulares afetados é obrigatória. Por conseguinte, conforme já destacado, a necessidade de comunicação aos titulares, ainda que de forma indireta, encontra-se amparada pelos princípios gerais de proteção de dados pessoais, especialmente no que se refere à boa-fé e à prevenção. Há, desse modo, legítima expectativa dos titulares de dados em ser devidamente informados sobre incidentes cibernéticos que envolvam seus dados pessoais, sobretudo quando o evento adverso puder provocar riscos e danos relevantes a seus direitos. Assim, é certo que a medida preventiva determinada por esta Autarquia federal encontra-se de acordo com a racionalidade inscrita na Lei Geral de Proteção de Dados Pessoais, motivo pelo qual não se vislumbra ilegalidade ou ilegitimidade na ação fiscalizatória.

6.4.31. Percebe-se, ademais, que as alegações trazidas pelo INSS para indicar a irrazoabilidade da ampla divulgação do incidente de segurança em meios de comunicação, em virtude da impossibilidade técnica de se proceder à comunicação individual dos titulares, baseia-se em eventuais dificuldades administrativas a serem absorvidas pela entidade, como o aumento da sua capacidade de atendimento ao público externo. Trata-se, portanto, de justificativa que visa proteger um interesse público secundário da pessoa jurídica de direito público, o que não se confunde com a aplicação do princípio da supremacia do interesse público no caso concreto.

6.4.32. Ao contrário do que indica o INSS, a comunicação do incidente de segurança, nos termos do inciso I do §2º do art. 48 da LGPD, é, na verdade, medida adequada e proporcional que objetiva a subsunção do interesse público no caso concreto. Primeiramente, deve-se compreender que a tutela do direito à privacidade e o direito à proteção de dados pessoais, ambos valores normativos materializados como garantias fundamentais, nos termos dos incisos X e LXXIX do art. 5º da Constituição Federal, respectivamente, não deve mais ser percebida como o mero exercício de uma garantia individual pelo titular, em que a atuação do Estado ocorreria apenas de maneira negativa. De acordo com essa visão anacrônica, a ação estatal na proteção dos direitos de personalidade, dentre os quais se encontra a privacidade e a proteção de dados pessoais, existiria apenas para salvaguardar um direito individual do cidadão, no contexto de uma tutela remedial.

6.4.33. Tal acepção da proteção do direito à privacidade, no entanto, não mais encontra guarida no arcabouço jurídico de sociedades democráticas, pois

ignora o desenvolvimento das premissas que permeiam a tutela da privacidade nas últimas décadas, em especial, no contexto da digitalização crescente das relações sociais[9], o que resultou no desenvolvimento de um novo direito a proteção de dados pessoais. Observe-se, nesse sentido, lição de Danilo Doneda[10]:

“A trajetória percorrida pelo direito à privacidade reflete tanto uma mudança de perspectiva da tutela da pessoa quanto a sua progressiva adequação às novas tecnologias de informação. **Não basta pensar na privacidade nos moldes de um direito subjetivo, a ser tutelado conforme as conveniências individuais, nem da privacidade como uma “predileção” individual, associada basicamente ao conforto e comodidade.** A própria noção da privacidade como algo de que um cidadão respeitável poderia abrir mão (ou que ao menos se esperasse isto de um cidadão honesto e de bons costumes), a presumida “transparência de quem não tem nada a temer”, deixa de fazer sentido dada a crescente complexidade das situações que tais arroubos podem desencadear e das suas consequências para os cidadãos. Uma esfera privada, dentro da qual a pessoa tenha condições de desenvolver a própria personalidade, livre de ingerências externas, ganha hoje ainda mais importância: passa a ser pressuposto para que a pessoa não seja submetida a formas de controle social que, em última análise, anulariam sua individualidade, cerceariam sua autonomia privada (para tocar em um conceito caro ao direito privado) e, em última análise, inviabilizariam o livre desenvolvimento de sua personalidade.

**A privacidade assume, portanto, posição de destaque na proteção da pessoa humana, não somente tomada como escudo contra o exterior – na lógica da exclusão – mas como elemento indutor da autonomia, da cidadania, da própria atividade política em sentido amplo e dos direitos de liberdade de uma forma geral. Nesse papel, ela é pressuposto de uma sociedade democrática moderna, da qual o dissenso e o anticonformismo são componentes orgânicos.**

(...)

**A tutela remedial**, típica do direito subjetivo, não é mais do que um instrumento entre outros que podem ser utilizados para a tutela da privacidade, e de forma alguma é a estrutura na qual deva necessariamente se concretizar. **A ela faltam os instrumentos adequados à realização da função promocional da tutela da privacidade como meio de proteção da pessoa humana e da atuação da cláusula geral da proteção da personalidade; nela igualmente não é concebida a dimensão coletiva na qual se insere a problemática da privacidade.** Nesse sentido, deve ser entendida a tutela da privacidade através da responsabilidade civil que, se é uma perspectiva que não deve de forma alguma ser descartada como opção em uma série de situações, por si só não promove o avanço necessário na tutela da privacidade. Nessa perspectiva, ela continuaria a ser encarada como mera liberdade negativa, isto é, desconsiderando tanto a evolução da matéria como o alcance da norma constitucional, que, ao considerar a privacidade em seu aspecto positivo, destaca sua função promocional – para o que deve lançar mão de outros institutos”.

6.4.34. Tem-se, desse modo, que o INSS, ao entender que a determinação da ANPD, no âmbito do PAI nº 00261.002177/2022-93, iria de encontro ao

interesse público, por supostamente trazer ônus elevado a sua atuação administrativa, em favor de interesses de particulares, desconsidera completamente a evolução doutrinária e jurisprudencial dos Tribunais Superiores no que se refere ao sentido conferido à proteção de dados pessoais no ordenamento jurídico pátrio e o seu papel instrumental para o livre desenvolvimento da personalidade dos indivíduos e, portanto, da dignidade humana.

6.4.35. A proteção de dados pessoais, a partir de uma evolução do direito à privacidade<sup>[11]</sup>, possui como razão de ser a salvaguarda de um valor normativo que irradia direitos a toda a coletividade, para além da mera tutela individual, visto que possui fundamento direto com o princípio da dignidade da pessoa humana, de maneira que não se pode mais separar o interesse público primário da proteção da garantia fundamental em comento. Essa concepção já foi, inclusive, reconhecida pelo Supremo Tribunal Federal, no âmbito do julgamento da ADI 6.649, quanto à ADPF 695, que analisou a constitucionalidade do Decreto nº 10.046/2019, que instituiu normas para o compartilhamento de dados pessoais pelo Poder Público. O Ministro Gilmar Mendes, em seu voto seminal, asseverou que<sup>[12]</sup>:

**“(...) Todavia, diferentemente do que assevera o ente público, a discussão sobre a privacidade nas relações com a Administração Estatal não deve partir de uma visão dicotômica que coloque o interesse público como bem jurídico a ser tutelado de forma totalmente distinta e em confronto com o valor constitucional da privacidade e proteção de dados pessoais.**

Como bem destacado por Gillian Black e Leslie Stevens, pesquisadores britânicos dedicados a essa temática, “se a privacidade for tratada simplesmente como um direito ou interesse individual, sempre será possível para o setor público controlar dados para suas finalidades públicas, já que isso será sempre reputado como necessário e proporcional” (tradução livre) (BLACK, Gillian e STEVENS, Leslie. “Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest”. In: Scripted. Vol. 10, n. 1, 2013, p. 95).

Nesse sentido, **assentam os autores a necessidade de se conferir uma abordagem comunitária e institucional ao direito à proteção de dados pessoais, evitando-se que este valor sempre sucumba diante da invocação do interesse público.**

A consciência de que os governos devem tratar o regime jurídico de privacidade como um objetivo coletivo de estruturação dos regimes democráticos, e não como um valor contraposto de proteção de interesses individuais, é corolário do próprio reconhecimento da autonomia do direito fundamental à proteção de dados pessoais.

Sobre esse ponto, destaca-se mais uma vez o escólio de Miriam Wimmer:

‘A aplicação da legislação de proteção de dados no tratamento de dados pelo Poder Público – tanto no caso de atos individuais e concretos como também na edição de atos normativos –

traz, portanto, o desafio de conciliação entre os princípios tradicionalmente aplicáveis à Administração Pública e aqueles contidos na própria LGPD, sem que se determine a precedência *prima facie* de um interesse público abstratamente caracterizado e reconhecendo também a importância da proteção de dados pessoais para além da sua dimensão individual. A eficiência demandada da Administração Pública e o interesse público tutelado pelo Estado devem, portanto, ser compreendidos no contexto de um conjunto mais amplo de princípios e com elementos integrantes do compromisso que o Estado deve ter com a democracia e com a concretização de direitos fundamentais”. (WIMMER, Miriam. “Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público”. In: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel; RODRIGUES JÚNIOR, Octavio Luís. (Org.). Tratado da Proteção de dados no Brasil, no Direito Estrangeiro e Internacional. Rio de Janeiro, Editora Forense, 2021, pp. 271-288)”. (Grifo meu)

6.4.36. Acredita-se, portanto, que a realização do interesse público primário ocorre, ao contrário do que fora alegado pelo INSS, com a comunicação do incidente de segurança aos titulares afetados, seja por meio direto, seja por meio indireto, por se tratar de procedimento que visa a garantia do direito fundamental de proteção de dados pessoais, insculpido no art. 5º, inciso LXXIX, da Constituição Federal.

(iii) Da inaplicabilidade do art. 15 do Decreto nº 10.748/2021 ao caso concreto:

6.4.37. A entidade pública atuada afirma que o disposto no artigo 15 do Decreto nº 10.748, de 16 de julho de 2021, impediria a divulgação de informações sobre incidente de segurança sofrido pela Administração Pública Federal. De acordo com o dispositivo, as informações sobre os incidentes cibernéticos são consideradas imprescindíveis à segurança da sociedade e do Estado, sendo classificadas como informações sigilosas, segundo o art. 4º, III, e o art. 23 e 24, da Lei de Acesso à Informação (LAI). Argumenta-se, desse modo, que as informações relativas aos comunicados de incidentes de segurança seriam informações classificadas, nos termos do art. 23 da Lei nº 12.527/2011, Lei de Acesso à Informação – LAI. Tal interpretação, no entanto, não pode prosperar.

6.4.38. O artigo 23 da Lei nº 12.527/2011 dispõe de modo exaustivo as informações que podem ser classificadas pela Administração Pública, por serem consideradas imprescindíveis à segurança da sociedade ou do Estado. Desse modo, consideram-se informações classificadas aquelas submetidas temporariamente à restrição de acesso público, em razão de sua imprescindibilidade para a segurança da sociedade e do Estado, as informações que se enquadrem nos incisos do referido dispositivo legal:

Art. 23. São consideradas imprescindíveis à segurança da sociedade ou do Estado e, portanto, passíveis de classificação as informações cuja divulgação ou acesso irrestrito possam:

I - pôr em risco a defesa e a soberania nacionais ou a integridade do território nacional;

II - prejudicar ou pôr em risco a condução de negociações ou as relações internacionais do País, ou as que tenham sido fornecidas em caráter sigiloso por outros Estados e organismos internacionais;

III - pôr em risco a vida, a segurança ou a saúde da população;

IV - oferecer elevado risco à estabilidade financeira, econômica ou monetária do País;

V - prejudicar ou causar risco a planos ou operações estratégicos das Forças Armadas;

VI - prejudicar ou causar risco a projetos de pesquisa e desenvolvimento científico ou tecnológico, assim como a sistemas, bens, instalações ou áreas de interesse estratégico nacional;

VII - pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares; ou

VIII - comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações.

6.4.39. Observa-se, inicialmente, que o art. 23 da LAI não constitui hipótese autônoma de sigilo, ou seja, o enquadramento de determinada informação ou documento em uma das hipóteses descritas no artigo não é suficiente para se determinar a restrição de acesso. Para que seja feita a devida restrição de acesso à informação, por meio de procedimento de classificação, a autoridade classificadora competente (art. 27 da LAI) deve estabelecer o prazo de restrição de acesso ao documento salvaguardado no ato de produção do Termo de Classificação de Informação (TCI), documento formal que oficializa esse ato administrativo. É a partir da produção do TCI que a Administração Pública pode determinar a restrição de acesso a documento classificado[13].

6.4.40. Verifica-se, desse modo, que a hipótese de restrição de acesso com fundamento no art. 23 da LAI guarda diferenças com a hipótese presente no art. 22 da norma de transparência. A restrição de acesso a informações protegidas por hipótese de sigilo prevista em lei, por sua vez, encontra-se prevista no artigo 22 da Lei nº 12.527/2011, bem como é regulamentada no Poder Executivo Federal por meio do artigo 6º, inciso I do Decreto nº 7.724/2012, abaixo:

Lei nº 12.527/2011:

Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.

Decreto nº 7.724/2012:

Art. 6º O acesso à informação disciplinado neste Decreto não se aplica: I - às hipóteses de sigilo previstas na legislação, como fiscal, bancário, de operações e serviços no mercado de capitais,

6.4.41. Ao contrário do que ocorre com as informações classificadas, a restrição de acesso a informações cuja publicidade se encontra limitada por legislação específica prescinde da produção de ato administrativo subsequente para produzir os seus efeitos. Outra característica que difere esta base legal daquela relacionada às informações classificadas é que o termo final da restrição de acesso em leis específicas não depende necessariamente de um lapso temporal pré-definido pela Administração Pública. Há restrições decorrentes de lei específica cujo termo final é um evento ou a cessação de uma condição, assim como há hipóteses de restrição sem evento claro que a defina.

6.4.42. O art. 15 do Decreto nº 10.748, de 16 de julho de 2021, nesse sentido, estabelece que as informações específicas sobre os incidentes cibernéticos e sobre as configurações e características técnicas de ativos de informação de cada órgão ou entidade da administração pública federal direta, autárquica e fundacional são consideradas imprescindíveis à segurança da sociedade e do Estado. Desse modo, o §1º do Decreto determina que as informações supramencionadas somente poderão ser acessadas por profissionais autorizados pelas autoridades responsáveis pelos ativos de informação dos órgãos ou das entidades da administração pública federal direta, autárquica e fundacional.

6.4.43. Observa-se, portanto, que o artigo 15 do Decreto nº 10.748, de 16 de julho de 2021 possui como finalidade precípua determinar que a Administração tome as medidas técnicas e administrativas necessárias para que as informações específicas relacionadas a incidentes cibernéticos sejam acessadas somente por agentes públicos devidamente autorizados, de modo a se resguardar dos olhos públicos informações estratégicas sobre o evento adverso. Nesse sentido, como medida mitigadora, seriam disponibilizados ao público em geral apenas dados estatísticos gerais relativos aos incidentes cibernéticos.

6.4.44. A restrição de acesso a tais informações, assim, ao ser considerada como imprescindível à segurança da sociedade e do Estado, encontra seu fundamento de validade infraconstitucional nos termos do inciso VI do artigo 23 da LAI. Desse modo, a restrição de acesso à informação exarada pelo artigo 15 do Decreto nº 10.748, de 16 de julho de 2021 não constitui hipótese autônoma de sigilo nos termos do art. 22 da LAI, motivo pelo qual a reserva das informações somente poderá ser considerada legal se adotado pelo órgão ou entidade pública o correto procedimento de classificação a que essas informações se submetem.

6.4.45. Isso é o que se depreende da inteligência do artigo 19 do Decreto nº 7.845/2012, que regulamentou no âmbito do Poder Executivo Federal os

procedimentos para o credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo. De acordo com a norma, a decisão de classificação, desclassificação, reclassificação ou redução do prazo de sigilo de informação classificada em qualquer grau de sigilo observará os procedimentos previstos nos artigos 31 e 32 do Decreto nº 7.724 de 16 de maio de 2012, que regulamentou a aplicação da LAI no Poder Executivo Federal<sup>[14]</sup>.

6.4.46. Tem-se, finalmente, que a decisão administrativa que resolver pela classificação de informações específicas envolvendo incidentes cibernéticos, nos termos do art. 23, inciso VI da Lei nº 12.527/2011 c/c o artigo 15 do Decreto nº 10.748/ 2021, deverá necessariamente ser formalizada em decisão consubstanciada em Termo de Classificação de Informação, conforme determinado pelo artigo 31 do Decreto nº 7.724/12, respeitando-se a previsão de apenas três níveis de restrição de acesso por classificação de informações: reservado, secreto e ultrassecreto. É importante enfatizar, nesse sentido, que, em nenhum momento deste processo sancionador - ou no processo de fiscalização que deu ensejo à confecção do Auto de Infração nº 01/2023/CGF/ANPD -, o INSS indicou a existência de TCI que comprovasse a classificação das informações específicas envolvendo o incidente de segurança objeto da medida sancionatória em análise.

6.4.47. Deve-se enfatizar, ademais, que o artigo 15 do Decreto nº 10.748/2021 limita a restrição de acesso apenas a *informações específicas* relacionadas a eventuais incidentes cibernéticos. Isso significa que a opacidade informacional temporária se refere somente a dados e informações de caráter técnico e administrativo cuja divulgação geral puder fragilizar a segurança do próprio sistema que se pretende salvaguardar, o que geraria prejuízos para a sociedade e o Estado.

6.4.48. Assim, a partir de uma interpretação sistemática da norma, compreende-se que a comunicação das informações constantes do §1º do artigo 48 da LGPD aos titulares afetados por incidentes de segurança qualificados não seria passível de restrição de acesso por classificação, seja por sua generalidade, seja por se tratar de um dos objetivos da Rede Federal de Gestão de Incidentes Cibernéticos, qual seja, divulgar medidas de prevenção, tratamento e resposta a incidentes cibernéticos, presente no I do art 3º do Decreto nº 10.748/ 2021.

## **7. DOSIMETRIA DA(S) SANÇÃO(ÕES)**

### **7.1. Classificação da infração.**

7.1.1. Conforme já relatado, a autuada incorreu em violação à obrigação estabelecida no art. 48 da LGPD. Além disso, a entidade autuada deixou de realizar medida preventiva determinada Autoridade Nacional de Proteção de Dados Pessoais, no âmbito de Processo de Apuração de Incidente de Segurança, conforme o disposto no artigo 32 do Regulamento de Fiscalização, sendo

observada, portanto, a circunstância agravante do inciso II, § 2º do art. 32 do Regulamento de Fiscalização.

7.1.2. Diante do exposto, cabe, inicialmente, realizar a classificação da infração cometida pela entidade autuada (leve, média ou grave), conforme indica o art. 8º da Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, doravante Regulamento de Dosimetria:

Art. 8º As infrações são classificadas, segundo a gravidade e a natureza das infrações e dos direitos pessoais afetados, em:

I - leve;

II - média; ou

III - grave.

§ 1º A infração será considerada leve quando não verificada nenhuma das hipóteses relacionadas nos §§ 2º ou 3º deste artigo.

**§ 2º A infração será considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais**, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave.

§ 3º A infração será considerada grave quando:

I - verificada a hipótese estabelecida no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes:

a) envolver tratamento de dados pessoais em larga escala, caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado;

b) o infrator auferir ou pretender auferir vantagem econômica em decorrência da infração cometida;

c) a infração implicar risco à vida dos titulares;

d) **a infração envolver tratamento de dados sensíveis** ou de dados pessoais de crianças, de adolescentes ou de idosos;

e) o infrator realizar tratamento de dados pessoais sem amparo em uma das hipóteses legais previstas na LGPD;

f) o infrator realizar tratamento com efeitos discriminatórios ilícitos ou abusivos; ou

g) verificada a adoção sistemática de práticas irregulares pelo infrator;

II - constituir obstrução à atividade de fiscalização.

7.1.3. O art. 48 da LGPD, caput e incisos, determina que o controlador deve apresentar CIS adequada, tanto à ANPD quanto ao titular, em prazo

razoável, sempre que o incidente de segurança puder acarretar risco ou dano relevante aos titulares. Conforme visto nos itens 6.4.1 a 6.4.12, a entidade pública autuada não realizou a comunicação do incidente de segurança qualificado aos titulares afetados, mesmo após as determinações exaradas pela Coordenação-Geral de Fiscalização.

7.1.4. A falta de CIS ao titular, especialmente quando resulta na exposição de dados pessoais em espaço não controlado de acesso, inclusive de dados de saúde e de benefícios previdenciários, pode afetar significativamente interesses e direitos fundamentais dos titulares. Isso porque o titular não sabe que seus dados foram expostos e, com isso, se encontra impossibilitado de tomar por conta própria medida preventivas que possam evitar o uso indevido de identidade, fraudes financeiras e outros danos que a exposição de dados possa causar. No caso concreto, os dados expostos permitem que o titular sofra esse tipo de dano, além de perturbações por ligações indevidas e fraudes em processos de autenticação ou validação de identidade em serviços específicos.

7.1.5. Logo, a infração ao art. 48 ora analisada se enquadra nos requisitos do art. 8º, §2º, do Regulamento de Dosimetria, atendendo ao critério para ser classificada como média. No entanto, no presente caso, a infração de falta de comunicação aos titulares versa sobre quantidade significativa de dados sensíveis relacionados à saúde e benefícios previdenciários, conforme item 4.3 da Nota Técnica 54/2023 (SEI nº 0048148). Essas características elevam o grau de classificação da infração que, por esse motivo, passa a ser considerada como **grave**, segundo art. 8º, §3º, "a" e "d", do Regulamento de Dosimetria:

Art. 8º

§ 2º A infração será considerada média quando puder afetar significativamente interesses e direitos fundamentais dos titulares de dados pessoais, caracterizada nas situações em que a atividade de tratamento puder impedir ou limitar, de maneira significativa, o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação; violação à integridade física; ao direito à imagem e à reputação; fraudes financeiras ou uso indevido de identidade, desde que não seja classificada como grave.

§ 3º A infração será considerada grave quando:

I - verificada a hipótese estabelecida no § 2º deste artigo e cumulativamente, pelo menos, uma das seguintes:

a) envolver tratamento de dados pessoais em larga escala, caracterizado quando abranger número significativo de titulares, considerando-se, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica do tratamento realizado;

(...)

d) a infração envolver tratamento de dados sensíveis ou de dados pessoais de crianças, de adolescentes ou de idosos

## 7.2. ***Definição do tipo de sanção administrativa.***

7.2.1. O art. 52 da LGPD define as sanções administrativas aplicáveis pela ANPD aos agentes de tratamento de dados que cometerem infrações às normas previstas na lei. Nesse sentido, a LGPD estabelece que a Autoridade de Proteção de Dados Pessoais, após o devido processo administrativo que possibilite o contraditório e a ampla defesa, poderá aplicar os seguintes tipos de sanção administrativa:

- I) advertência, com indicação de prazo para adoção de medidas corretivas;
- II) multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;
- III) multa diária, observado o limite total a que se refere o inciso II;
- IV) publicização da infração após devidamente apurada e confirmada a sua ocorrência;
- V) bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
- VI) eliminação dos dados pessoais a que se refere a infração;
- VII) (VETADO);
- VIII) (VETADO);
- IX) (VETADO);
- X) suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
- XI) suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; e
- XII) proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

7.2.2. O Regulamento de Dosimetria, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023, por sua vez, regulamentou a aplicação das sanções administrativas previstas na LGPD, assim como os parâmetros e critérios para a dosimetria das eventuais sanções aplicadas. As penalidades, conforme os preceitos indicados tanto na LGPD quanto no Regulamento de Dosimetria, devem ser aplicadas de forma gradativa, levando-se em consideração critérios específicos dispostos na norma.

7.2.3. A sanção de advertência, regulamentada no art. 9º do Regulamento de Dosimetria, nesse sentido, será aplicada quando a infração observada for considerada de natureza leve ou média e não caracterizar reincidência específica ou quando houver a necessidade de imposição de medida corretiva que tenha como finalidade corrigir a infração e reconduzir o infrator à plena conformidade à LGPD e aos regulamentos aplicados por esta Autarquia federal.

7.2.4. Observou-se, no entanto, que as infrações cometidas pela entidade autuada foram consideradas de natureza grave, por envolver o tratamento de dados pessoais em larga escala e dados pessoais sensíveis. Além disso, a ocorrência de uma circunstância agravante, nos termos do art. 32, §2º, II, do Regulamento de Fiscalização, ou seja, o não atendimento de medida preventiva determinada pela autoridade fiscalizatória, indica a necessidade de aplicação de medida sancionatória mais grave. Assim, em virtude da circunstância agravante, compreende-se que não se aplica ao caso concreto a sanção de advertência.

7.2.5. O Regulamento de Dosimetria, por sua vez, define, em seu art. 20, que a ANPD poderá aplicar sanção administrativa de publicização da infração ao autuado, considerando a relevância e o interesse público da matéria. A sanção de publicização consiste na divulgação da infração pelo próprio infrator, após devidamente apurada e confirmada sua ocorrência. Considerando que a realização do interesse público primário, no caso concreto, ocorre com a devida comunicação do incidente de segurança aos titulares afetados, ainda que por meio indireto, conforme consta nos itens a 7.31 a 7.43 deste RI, bem como a natureza grave da infração, acredita-se que a sanção de publicização da infração seja mais adequada à inobservância pelo autuado da conduta do art. 48 da LGPD e do dever de comunicação aos titulares afetados.

7.2.6. Deve-se ressaltar, nesse sentido, que a sanção de publicização deverá indicar o teor, o meio, a duração e o prazo para o seu cumprimento, nos termos do art. 20, §2º do Regulamento de Dosimetria. Além disso, conforme o disposto no art. 21 do Regulamento de Dosimetria, é importante enfatizar que a sanção de publicização da infração não se confunde com a publicação de decisão de aplicação de sanção administrativa no Diário Oficial da União ou com os demais atos realizados pela ANPD, para fins de atendimento ao princípio da publicidade administrativa. Nesse sentido, o ônus relacionado à publicização da infração deve ser suportado exclusivamente pelo infrator. Assim, de acordo com as normas que regulamentam a matéria, sugere-se o seguinte texto de comunicação ao titular a ser adotado pelo infrator:

O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto

de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.

Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: [encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)."

7.2.7. Para se atingir o objetivo da comunicação, sugere-se que o comunicado fique disponível por 180 (cento e oitenta) dias corridos contados a partir da data do cumprimento da intimação da decisão que determinar a sanção administrativa, ou seja, contados a partir do início da publicização do comunicado. Igualmente, sugere-se que a comunicação esteja disponível:

- na primeira página do sítio do INSS (<https://www.gov.br/inss/pt-br>) ou até, no máximo, a um clique de distância da página inicial, sob pena da comunicação não atingir seu objetivo de informar o titular sobre o incidente de segurança; e
- no menu de 'notificações' do aplicativo Meu INSS, com indicação visual de que há mensagem pendente de leitura/visualização.

7.2.8. Em relação às demais sanções previstas na norma, percebe-se que não deve ser aplicação ao caso concreto a sanção de multa simples, prevista no art. 10, incisos I e II, do Regulamento de Dosimetria. Ainda que esta sanção administrativa seja prevista em caso de descumprimento pelo infrator de medidas preventivas a ele impostas, o art. 52, §3º da LGPD, ao estabelecer as sanções que podem ser impostas a entidade ou a órgãos públicos, afasta, por omissão, a possibilidade de aplicação de multa ou de multa diária a esses agentes de tratamento, motivo pelo qual deixa-se de se aplicar tal sanção. Igualmente, muito embora seja uma infração grave, as outras sanções previstas na LGPD (no caso, os incisos V a XII do art. 52) tampouco são adequadas para a infração ora analisada, em função do interesse público que justifica a necessidade do tratamento dos dados, bem como necessidade de aplicação proporcional da medida sancionatória. Igualmente, muito embora seja uma infração grave, as outras sanções

previstas na LGPD (no caso, os incisos V a XII do art. 52) tampouco são adequadas para a infração ora analisada, em função do interesse público que justifica a necessidade do tratamento dos dados, bem como necessidade de aplicação proporcional da medida sancionatória

7.2.9. Fica, portanto, cominada a **sanção de publicização da infração**, exarada nos termos do art. 20 da Resolução CD/ANPD nº 4/2023, para a infração ao art. 48 da LGPD, considerando-se como circunstância agravante a falta de atendimento pela autuada de determinação exarada pela ANPD, nos termos do art. 32, §2º, II, da Resolução CD/ANPD nº 1/2021

## 8. CONCLUSÃO

8.1. Ante o exposto, considerando que o conjunto probatório demonstra que a autoria e a materialidade restam devidamente comprovadas nos autos, e que os fatos descritos correspondem às infrações tipificadas pelos enquadramentos indicados no Auto de Infração nº 1/2023/CGF/ANPD (4411917), conclui-se pela seguinte recomendação:

8.1.1. Por violação ao art. 48 da LGPD, com circunstância agravante nos termos do art. 32, §2º, II, da Resolução CD/ANPD nº 1/2021, a aplicação da sanção de PUBLICIZAÇÃO DA INFRAÇÃO ao INSS. A entidade pública autuada, assim, deverá, em até 10 dias úteis, contados a data da intimação:

a) Publicar comunicado, na primeira página do sítio (<https://www.gov.br/inss/pt-br>), que deverá permanecer acessível pelo prazo de 60 dias, contados a partir da intimação da decisão que determinar a sanção administrativa, com o seguinte teor:

O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.

Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada

no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: [encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)."

- b) Enviar mensagem, via recurso de notificação, a todos os usuários do aplicativo Meu INSS, para que fique disponível no menu de 'notificações' do aplicativo Meu INSS, com indicação visual de que há mensagem pendente de leitura/visualização, com o seguinte teor:

"O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica a ocorrência de incidente de segurança entre agosto e setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS, saiba mais no link:" [apontar para o link criado para atender a determinação 8.1.1.a]

8.2. Por fim, é importante registrar que a classificação das infrações, a definição das sanções (inclusos agravantes e atenuantes) e a adoção de medidas corretivas restringem-se às circunstâncias deste caso em concreto. Tais decisões não vinculam, naturalmente, a análise e o posicionamento da CGF em futuros processos sancionadores.

8.3. Caso a entidade pública autuada não cumpra a referida decisão nos termos definidos pela Autoridade Nacional de Proteção de Dados, recomenda-se que o presente processo administrativo sancionador seja encaminhado para os órgãos de controle interno competentes, nos termos do art. 55-J, XXII, da LGPD, para que sejam tomadas as medidas administrativas necessárias em relação aos agentes públicos que deram causa ao descumprimento do disposto na legislação de proteção de dados pessoais.

## **9. ENCAMINHAMENTOS**

9.1. Este Relatório de Instrução encerra a fase de instrução da atuação repressiva prevista no Art. 54, parágrafo único, do Regulamento de Fiscalização.

9.2. O presente Relatório de Instrução deve ser encaminhado à CGF para decisão, de acordo com Art. 55 do Regulamento de Fiscalização.

9.3. Após a decisão, o autuado deverá ser intimado para cumprimento da sanção e/ou apresentação de recurso, em até 10 dias, em consonância com o Art. 44, da Lei nº 9.784/99, e o Art. 58, do Regulamento de Fiscalização. Em caso de sanção de multa, o autuado deverá pagá-la no prazo de até 20 (vinte) dias úteis, contados a partir da ciência oficial da decisão de aplicação de sanção.

9.4. A decisão deve ser publicada no DOU, segundo o Art. 55, do Regulamento de Fiscalização.

9.5. Por derradeiro, deve-se informar que a entidade autuada, mesmo após consultada, nos termos do Ofício nº 72/2023/FIS/CGF/ANPD (SEI nº 4836919), não indicou eventuais informações constantes no presente processo administrativo sancionatório que pudessem estar protegidas por hipótese de sigilo exaradas pela Lei nº 12.527/2011 (Lei de Acesso à Informação – LAI).

9.6. Encaminhado, por fim, o presente Relatório de Instrução para aprovação superior.

**JORGE ANDRÉ FERREIRA FONTELLES DE LIMA**  
Auditor federal de finanças e controle

**De acordo.**

**ULLIANA CERVIGNI MARTINELLI**  
Coordenadora de Fiscalização, Substituta

---

[1] MODENESI, Pedro; Art. 48. In *Comentários à lei geral de proteção de dados pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 452.

[2] MODENESI, Pedro; Art. 48. In *Comentários à lei geral de proteção de dados pessoais*. Indaiatuba, SP: Editora Foco, 2022. p. 455.

[3] SOMBRA, Thiago Luís. Planos de resposta a incidentes de segurança com dados pessoais e a construção de uma governança responsável. In *Compliance e políticas de proteção de dados [livro eletrônico]*, 1º. ed. São Paulo: Thomson Reuters Brasil, 2021. RB-25.5

[4] ANPD. Qual o prazo para comunicar um incidente de segurança? Comunicação de Incidentes de Segurança, 2022. Disponível em: [https://www.gov.br/anpd/pt-br/canais\\_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis](https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis). Acessado em 22/01/2024.

[5] RITA TOURINHO, *Discricionariedade administrativa*, Juruá, 2º ed. 2009, p 127. In CARVALHO FILHO, José dos Santos, *Manual de direito administrativo*, 31º ed., atual. E ampl. – São Paulo: Atlas, 2017. p 53.

[6] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de proteção de dados pessoais, fundamentos da LGPD*. 1º ed. Rio de Janeiro: Forense, 2022. p. 72.

[7] FRAZÃO, Ana; PRATA DE CARVALHO, Angelo; MILANEZ, Giovanna. *Curso de proteção de dados pessoais, fundamentos da LGPD*. 1º ed. Rio de Janeiro: Forense, 2022. p. 73.

[8] BARROSO, Luís Roberto. *Curso de direito constitucional contemporâneo: os conceitos fundamentais e a construção do novo modelo*. 5. ed. São Paulo: Saraiva, 2015. P. 94-97.

[9] MEJIAS, U.A.; COULDRY, N. *Datafication*. Internet Policy Review, 8 (4), 2019.

[10] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais: fundamentos da lei geral de proteção de dados pessoais*. 2º ed. -- São Paulo: Thomson Reuters Brasil, 2021.

[11] MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. (Saraiva 2014).

[12] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade n. 6.649 e Arguição de Descumprimento de Preceito Fundamental n. 695**. Lei nº 13.709/2018 e Decreto nº 10.046/2019. Controvérsia relativa aos limites, ao âmbito de proteção e à dimensão axiológica dos direitos fundamentais à privacidade e ao livre desenvolvimento da personalidade, especificamente no que diz respeito ao uso compartilhado de dados pessoais pelo Estado brasileiro. ReQte(s). Conselho Federal da Ordem dos Advogados do Brasil e Partido Socialista Brasileiro (PSB). Intdo. Presidente da República. Rel. Min. Gilmar Mendes, em 15 de setembro de 2022. Disponível em <https://portal.stf.jus.br/>. Acessado em 19/01/2024.

[13] BRASIL. Controladoria-Geral da União. *Parecer sobre acesso à informação para atender ao Despacho Presidencial de 1º de janeiro de 2023*. Disponível em [https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-conclui-revisao-dos-sigilos-impostos-a-documentos-de-acesso-publico/copy\\_of\\_PARECERFINALSOBREACESSOINFORMAO\\_CGU\\_FEV2023.pdf](https://www.gov.br/cgu/pt-br/assuntos/noticias/2023/02/cgu-conclui-revisao-dos-sigilos-impostos-a-documentos-de-acesso-publico/copy_of_PARECERFINALSOBREACESSOINFORMAO_CGU_FEV2023.pdf). Acessado em 23/01/2024. Pgs 59-60.

[14] Art. 31. A decisão que classificar a informação em qualquer grau de sigilo deverá ser formalizada no Termo de Classificação de Informação - TCI, conforme modelo contido no Anexo, e conterá o seguinte:

I - código de indexação de documento;

II - grau de sigilo;

III - categoria na qual se enquadra a informação;

IV - tipo de documento;

V - data da produção do documento;

VI - indicação de dispositivo legal que fundamenta a classificação;

VII - razões da classificação, observados os critérios estabelecidos no art. 27, com a justificativa para o grau de sigilo adotado; ([Redação dada pelo Decreto nº 11.527, de 2023](#))

VII-A - assunto a que se refere a informação, com a descrição de elementos mínimos que permitam a identificação do tema de que trata a classificação; ([Incluído pelo Decreto nº 11.527, de 2023](#))

VIII - indicação do prazo de sigilo, contado em anos, meses ou dias, ou do evento que defina o seu termo final, observados os limites previstos no art. 28;

IX - data da classificação; e

X - identificação da autoridade que classificou a informação.

§ 1º O TCI seguirá anexo à informação.

§ 2º As informações previstas no inciso VII do **caput** deverão ser mantidas no mesmo grau de sigilo que a informação classificada.

§ 3º A ratificação da classificação de que trata o § 5º do art. 30 deverá ser registrada no TCI.

Art. 32. A autoridade classificadora ou outro agente público que classificar a informação deverá enviar, no

prazo de trinta dias, contado da data da decisão de classificação ou de sua ratificação, as informações previstas no **caput** do art. 31 à: [\(Redação dada pelo Decreto nº 11.527, de 2023\)](#)

I - Comissão Mista de Reavaliação de Informações, no caso de informações classificadas no grau ultrassecreto ou secreto; ou [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

II - Controladoria-Geral da União, no caso de informações classificadas em qualquer grau de sigilo, ressalvado o envio das informações de que trata o inciso VII do **caput** do art. 31. [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

#### Vigência

§ 1º Na hipótese de que trata o inciso II do **caput**, quando identificar, no desempenho das competências previstas no art. 68, a partir do exame dos elementos públicos que compõem o TCI, indícios de erro na classificação da informação, a Controladoria-Geral da União deverá: [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

I - notificar a autoridade classificadora, que decidirá sobre a reavaliação da classificação no prazo de trinta dias; e [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

II - informar a Comissão Mista de Reavaliação de Informações, no caso de informações classificadas no grau ultrassecreto ou secreto, para fins do disposto no inciso I do **caput** do art. 47. [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

§ 2º Os indícios de erro a que se refere o § 1º serão considerados quanto: [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

I - ao não enquadramento do assunto de que trata o inciso VII-A do **caput** do art. 31 nas hipóteses legais de sigilo; e [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)

II - a não adequação do grau de sigilo. [\(Incluído pelo Decreto nº 11.527, de 2023\)](#)



Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Assessor(a)**, em 25/01/2024, às 15:00, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Ulliana Cervigni Martinelli, Coordenador(a), Substituto(a)**, em 25/01/2024, às 17:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0053354** e o código CRC **1E8C7722**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8168 e Fax: @fax\_unidade@ - <https://www.gov.br/anpd/pt-br>

Referência: Caso responda a este documento, indicar expressamente o Processo nº  
00261.001888/2023-21

SEI nº 0053354



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

Ofício nº 7/2024/FIS/CGF/ANPD

Brasília-DF, na data da assinatura.

À Coordenação-Geral de Administração - CGA

**Assunto: Publicação no Diário Oficial da União**

1. Encaminho o presente processo para que a decisão constante no Despacho Decisório nº 1/2024/FIS/CGF (SEI nº 0063073) seja publicada no D.O.U., consoante comando do art. 55 do Regulamento de Fiscalização.

Atenciosamente,

**MARIDELIA MOURA DE ARRUDA MOREIRA**  
Coordenadora de Fiscalização

Anexos: I - Relatório de Instrução nº 01/2024/CGF/ANPD (SEI nº 0053354).  
II - Despacho decisório nº 1/2024/FIS/CGF (SEI nº 0063073).



Documento assinado eletronicamente por **Maridélia Moura de Arruda Moreira, Coordenador(a)**, em 30/01/2024, às 11:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0060910** e o código CRC **A3998A7E**.

---

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8168 e Fax: @fax\_unidade@ - <https://www.gov.br/anpd/pt-br>

---

**Referência:** Caso responda este Ofício, indicar expressamente o Processo nº  
00261.001888/2023-21

SEI nº 0060910

Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização**Despacho Decisório nº 1/2024/FIS/CGF**

Brasília/DF, na data da assinatura.

Processo nº 00261.001888/2023-21

Interessado: INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, EDSON PINHEIRO ALVARISTA

**O COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD** no uso de suas atribuições legais e regulamentares, com fundamento no art. 17, inciso I, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do processo em epígrafe, instaurado em face do **INSTITUTO NACIONAL DO SEGURO SOCIAL (INSS)** inscrito no CNPJ/MF sob o nº 29.979.036/0001-40, em razão dos indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD); e

CONSIDERANDO o teor do Relatório de Instrução nº 1/2024/CGF/ANPD (SUPER nº 0053354), cujas razões acolho e integro à presente decisão, inclusive como motivação, com fulcro no §1º do art. 50 da Lei nº 9.784/1999 c/c o art. 55 e seguintes do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021;

**DECIDE:**

1. Aplicar ao INSS a sanção de:
2. **PUBLICIZAÇÃO DA INFRAÇÃO** por violação ao art. 48 da LGPD, com circunstância agravante nos termos do art. 32, §2º, II, da Resolução CD/ANPD nº 1/2021, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor ao INSS a obrigação de:
  - 2.1. Publicar comunicado, na primeira página do sítio (<https://www.gov.br/inss/pt-br>), que deverá permanecer acessível pelo prazo de 60 (sessenta) dias, contados a partir da intimação da decisão que

determinar a sanção administrativa, com o seguinte teor:

O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.

Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: [encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)."

2.2. Enviar mensagem, via recurso de notificação, a todos os usuários do aplicativo Meu INSS, para que fique disponível no menu de 'notificações' do aplicativo Meu INSS, pelo período de 60 (sessenta) dias, com indicação visual de que há mensagem pendente de leitura/visualização, com o seguinte teor:

"O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica a ocorrência de incidente de segurança entre agosto e setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS, saiba mais no link:" [apontar para o link criado para atender a determinação 2.1.]

3. **Pela intimação do autuado** para cumprimento das sanções e medidas corretivas e/ou apresentação de recurso, em até 10 (dez) dias úteis, em consonância com o art. 56 da Lei nº 9.784/99 c/c o art. 58 do Regulamento de Fiscalização.

4. Aguarde-se o trânsito em julgado. Após, em caso de não cumprimento desta decisão, encaminhe-se este Processo Administrativo Sancionador para a Procuradoria Federal Especializada - PFE da ANPD para a execução das medidas corretivas, bem como para a Controladoria Geral da União, nos termos do art. 55-J, XXII, da LGPD, para que sejam tomadas as medidas administrativas necessárias em relação aos agentes públicos que

deram causa ao descumprimento do disposto na legislação de proteção de dados pessoais.

5. Publique-se no DOU, segundo o art. 55 da Resolução CD/ANPD nº 1/2021.

**FABRÍCIO GUIMARÃES MADRUGA LOPES**  
Coordenador-Geral de Fiscalização



Documento assinado eletronicamente por **Fabício Guimarães Madruga Lopes, Coordenador(a)-Geral de Fiscalização**, em 29/01/2024, às 17:48, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0063073** e o código CRC **20377BB1**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8168 e Fax: @fax\_unidade@ - <https://www.gov.br/anpd/pt-br>

**Referência:** Processo nº 00261.001888/2023-21

SEI nº 0063073



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

Ofício nº 13/2024/FIS/CGF/ANPD

Brasília-DF, na data da assinatura.

Ao Sr.

**EDSON PINHEIRO ALVARISTA**

COORDENADOR DE PROTEÇÃO DE DADOS PESSOAIS - COPDP

INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS

CNPJ nº 29.979.036/0001-40

ST SAUS QUADRA 02 BLOCO "O"

BRASÍLIA-DF CEP 70.070-946

[edson.alvarista@inss.gov.br](mailto:edson.alvarista@inss.gov.br)

[encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)

Assunto: **Comunica decisão em Processo Administrativo Sancionador.**

Referência: **Caso responda este Ofício, indicar expressamente o Processo nº 00261.001888/2023-21.**

Senhor Coordenador de Proteção de Dados Pessoais,

1. Em atenção ao disposto no art. 58 do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021, e no art. 17, I e II, do Regimento Interno da Autoridade Nacional de Proteção de Dados (ANPD), aprovado pela Portaria nº 1, de 8 de março de 2021, fica essa entidade **intimada** da decisão ocorrida no processo em epígrafe, consubstanciada no **Despacho Decisório nº 1/2024/FIS/CGF 0063073**), que acolheu as razões contidas no **Relatório de Instrução nº 1/2024/CGF 0053354**), ambos documentos em anexo.

2. Resulta da referida decisão a aplicação de **SANÇÃO DE PUBLICIZAÇÃO DA INFRAÇÃO** de acordo com o art. 44, da Lei nº 9.784, de 29 de janeiro de 1999, e art. 58, do Regulamento de Fiscalização, este Ofício intima o infrator para ciência e, se for o caso, apresentação de recurso em até 10 (dez) dias úteis contados do recebimento, perante a Coordenação-Geral de Fiscalização da ANPD.

4. Esta Coordenação de Fiscalização permanece à disposição, inclusive pelo e-mail [fiscalizacao@anpd.gov.br](mailto:fiscalizacao@anpd.gov.br).

Atenciosamente,

**JORGE ANDRÉ FERREIRA FONTELLES DE LIMA**  
Auditor Federal de Finanças e Controle

Anexos: I - Despacho Decisório nº 1/2024/FIS/CGF (0063073)

II - Relatório de Instrução nº 1/2024/CGF/ANPD (0053354)



Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Assessor(a)**, em 30/01/2024, às 17:06, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0067329** e o código CRC **3FD9B9F6**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8168 e Fax: @fax\_unidade@ - <https://www.gov.br/anpd/pt-br>

**Referência:** Caso responda este Ofício, indicar expressamente o Processo nº 00261.001888/2023-21

SEI nº 0067329



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

## Formulário para Expedição de Documentos para o Protocolo

Processo nº 00261.001888/2023-21

Brasília, 30 de janeiro de 2024

Ao Protocolo da ANPD.

Encaminho o presente processo para expedição conforme a seguir:

( ) Enviar o processo integralmente;

( X ) Enviar apenas os documentos listados abaixo:

Identificação do documento PRINCIPAL 1		Link SUPER do documento PRINCIPAL 1	
Ofício nº 13/2024/FIS/CGF/ANPD		0067329	
Identificação do anexo do documento PRINCIPAL 1		Link SUPER do anexo do documento PRINCIPAL 1	
Despacho Decisório nº 1/2024/FIS/CGF		0063073	
Relatório de Instrução nº 1/2024/CGF/ANPD		0053354	
Prazo de envio			
( )	Urgente	( x )	Não urgente
Nível de Acesso			
( x )	Público	(	Restrito

)		)	
<b>Indicação da forma de remessa</b>			
( )	E-mail · Informar e-mail (s) de destino: _____		
( x )	Protocolo Digital ou Peticionamento Eletrônico para Instituto Nacional do Seguro Social - INSS. · Solução que possibilita aos órgãos e entidades da Administração Pública de todas as esferas, pessoas físicas e jurídicas, encaminhar documentos pela Internet, de forma eletrônica. · Envio de documentos avulsos. · O processo eletrônico que possui o(s) documento(s) continua aberto na Unidade no SUPER-ANPD.		
( )	Barramento · Solução que permite a comunicação entre os órgãos públicos que utilizam o SUPER/SEI ou outras soluções de processo eletrônico (desde que também estejam integrados ao Barramento). · Envio de todo o processo. · O processo eletrônico enviado fica bloqueado no SUPER-ANPD e não pode ser editado nem tramitado, mas fica disponível para consulta.		
( )	Via Postal * Colocar endereço(s) do(s) destinatário(s)	( )	SEDEX
		( )	Aviso de recebimento
( )	Qualquer das opções		

**ATENÇÃO: Caso a opção escolhida seja envio por meio de protocolo digital ou de peticionamento eletrônico, barramento ou e-mail e o Órgão de destino não ofereça essas opções de recebimento, o documento será enviado fisicamente ou por via postal.**

**INSTRUÇÕES:**

a) este formulário deve ser assinado pelo colaborador responsável e o

respectivo processo encaminhado à unidade **Protocolo** da ANPD para atendimento;

b) não é necessário incluir despacho de encaminhamento - apenas o formulário devidamente preenchido e assinado é suficiente para o atendimento da demanda;

c) os documentos a serem expedidos devem compor os autos dos processos enviados à expedição. Havendo documentos em processo diverso, estes deverão estar disponíveis para consulta da unidade **Protocolo** da ANPD.

**Em caso de dúvida, por favor, entre em contato com o Protocolo: [protocolo@anpd.gov.br](mailto:protocolo@anpd.gov.br)**



Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Assessor(a)**, em 30/01/2024, às 17:14, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0067346** e o código CRC **3A48CCD3**.

**Referência:** Caso responda a este documento, indicar expressamente o Processo nº 00261.001888/2023-21

SEI nº 0067346

**Data de Envio:**

31/01/2024 20:18:00

**De:**

ANPD/Protocolo da ANPD <protocolo@anpd.gov.br>

**Para:**

edson.alvarista@inss.gov.br  
encarregado@inss.gov.br

**Assunto:**

Comunica decisão em Processo Administrativo Sancionador

**Mensagem:**

Prezados,

Trata-se de encaminhamento do Ofício nº 13/2024/FIS/CGF/ANPD e seus anexos:

I - Despacho Decisório nº 1/2024/FIS/CGF

II - Relatório de Instrução nº 1/2024/CGF/ANPD

Favor confirmar o recebimento.

Atenciosamente,

Protocolo

Coordenação-Geral de Administração

Autoridade Nacional de Proteção de Dados - ANPD

**Anexos:**

Oficio\_0067329.html

Despacho\_Decisorio\_0063073.html

Relatorio\_de\_Instrucao\_0053354.html

# DIÁRIO OFICIAL DA UNIÃO

Publicado em: 01/02/2024 | Edição: 23 | Seção: 1 | Página: 42

Órgão: Ministério da Justiça e Segurança Pública/Autoridade Nacional de Proteção de Dados/Coordenação-Geral de Fiscalização

## DESPACHO DECISÓRIO Nº 1/2024/FIS/CGF

Processo nº 00261.001888/2023-21

Interessado: INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS, EDSON PINHEIRO ALVARISTA

O COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD, no uso de suas atribuições legais e regulamentares, com fundamento no art. 17, inciso I, do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, examinando os autos do processo em epígrafe, instaurado em face do INSTITUTO NACIONAL DO SEGURO SOCIAL (INSS), inscrito no CNPJ/MF sob o nº 29.979.036/0001-40, em razão dos indícios de infração à Lei Geral de Proteção de Dados Pessoais (LGPD); e

CONSIDERANDO o teor do Relatório de Instrução nº 1/2024/CGF/ANPD (SUPER nº 0053354), cujas razões acolho e integro à presente decisão, inclusive como motivação, com fulcro no §1º do art. 50 da Lei nº 9.784/1999 c/c o art. 55 e seguintes do Regulamento de Fiscalização, aprovado pela Resolução CD/ANPD nº 1/2021, decide:

1. Aplicar ao INSS a sanção de:

2. PUBLICIZAÇÃO DA INFRAÇÃO, por violação ao art. 48 da LGPD, com circunstância agravante nos termos do art. 32, §2º, II, da Resolução CD/ANPD nº 1/2021, com imposição da seguinte medida corretiva, nos termos do art. 55, §2º, I do Regulamento de Fiscalização, para impor ao INSS a obrigação de:

2.1. Publicar comunicado, na primeira página do sítio (<https://www.gov.br/inss/pt-br>), que deverá permanecer acessível pelo prazo de 60 (sessenta) dias, contados a partir da intimação da decisão que determinar a sanção administrativa, com o seguinte teor:

"O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica que tomou conhecimento da ocorrência de incidente de segurança entre os meses de agosto de setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS por conta de acesso a volume extraordinário de dados por meio de consultas volumétricas ao sistema. Dentre os dados que podem ter sido afetados, estariam dados de comprovação de identidade oficial, dados financeiros e de saúde (tais como nome, CPF, NIT, identidade, data de nascimento, sexo, ramo de atividade profissional, dados bancários e quantidade de dependentes) de um número indeterminado de beneficiários e segurados do INSS, o que poderia acarretar o risco de furto de identidade, fraudes, assédios comerciais, entre outros danos.

Informamos que o Instituto realizou, imediatamente, ações preventivas e corretivas nos processos e sistemas informatizados da entidade visando mitigar a vulnerabilidade detectada no sistema. A fim de conter o possível incidente de segurança, foi realizado o bloqueio das credenciais dos usuários que possivelmente permitiram o acesso e consequente consulta. Além disso, o Instituto comunicou à ANPD do incidente em questão. Dúvidas ou outras solicitações podem ser encaminhadas à encarregada pelo Tratamento dos Dados no e-mail: [encarregado@inss.gov.br](mailto:encarregado@inss.gov.br)."

2.2. Enviar mensagem, via recurso de notificação, a todos os usuários do aplicativo Meu INSS, para que fique disponível no menu de 'notificações' do aplicativo Meu INSS, pelo período de 60 (sessenta) dias, com indicação visual de que há mensagem pendente de leitura/visualização, com o seguinte teor:

"O INSS, tendo em vista que foi condenado pela Autoridade Nacional de Proteção de Dados por infração ao dever de comunicar os titulares a ocorrência de incidente de segurança, comunica a ocorrência de incidente de segurança entre agosto e setembro de 2022. O incidente pode ter comprometido a confidencialidade dos dados pessoais tratados pelo INSS, saiba mais no link:" [apontar para o link criado para atender a determinação 2.1.]

3. Pela intimação do autuado para cumprimento das sanções e medidas corretivas e/ou apresentação de recurso, em até 10 (dez) dias úteis, em consonância com o art. 56 da Lei nº 9.784/99 c/c o art. 58 do Regulamento de Fiscalização.

4. Aguarde-se o trânsito em julgado. Após, em caso de não cumprimento desta decisão, encaminhe-se este Processo Administrativo Sancionador para a Procuradoria Federal Especializada - PFE da ANPD para a execução das medidas corretivas, bem como para a Controladoria Geral da União, nos termos do art. 55-J, XXII, da LGPD, para que sejam tomadas as medidas administrativas necessárias em relação aos agentes públicos que deram causa ao descumprimento do disposto na legislação de proteção de dados pessoais.

**FABRÍCIO GUIMARÃES MADRUGA LOPES**

Este conteúdo não substitui o publicado na versão certificada.



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Administração  
Protocolo

Despacho Protocolo/CGA

Brasília/DF, na data da assinatura.

À Coordenação-Geral de Fiscalização - CGF

Assunto: **Comunica decisão em Processo Administrativo Sancionador, Ofício nº 13/2024/FIS/CGF/ANPD.**

Prezados(as),

1. Trata-se de expedição do Ofício nº 13/2024/FIS/CGF/ANPD e seus anexos, nos termos do Formulário para Expedição de Documentos (0067346).
2. Informamos que, em 31 de janeiro de 2024, os documentos foram encaminhados aos destinatários por e-mail (0070060).
  - 2.1. Ocorre que, em virtude da não confirmação de recebimento em tempo, foi gerado o Processo nº 00261.000903/2024-03 (relacionado), contendo os documentos informados no Formulário para Expedição de Documentos, então o processo foi encaminhado nesta data ao destinatário por meio do Tramita GOV.BR (anteriormente conhecido como Barramento - ferramenta destinada à tramitação de processos administrativos eletrônicos e documentos avulsos, em meio eletrônico, com incrementos de segurança, integridade, agilidade e redução de custos no serviço público).
3. Sendo assim, restitui-se ao setor responsável para os devidos registros e encaminhamentos.

Atenciosamente,



---

Documento assinado eletronicamente por **Thiago Ramos de Souza, Coordenador(a)-Geral**, em 02/02/2024, às 18:59, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).

---



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0074965** e o código CRC **5ADC43C1**.

---

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8115 e Fax: @fax\_unidade@ - <https://www.gov.br/anpd/pt-br>

---

**Referência:** Caso responda a este documento, indicar expressamente o Processo nº 00261.001888/2023-21

SEI nº 0074965



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

**Despacho Decisório nº 14/2024/FIS/CGF** Brasília/DF, na data da assinatura.

Processo nº 00261.001888/2023-21

Interessado: Instituto Nacional do Seguro Social (INSS)

**O COORDENADOR-GERAL DE FISCALIZAÇÃO DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS – ANPD** o uso de suas atribuições legais e regulamentares, em especial as dispostas no §2º do art. 58 e no art. 61, todos do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da ANPD (Regulamento de Fiscalização), aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021, examinando os autos do processo epígrafe, que tratam de Processo Administrativo Sancionador (PAS) instaurado em face do INSTITUTO NACIONAL DO SEGURO SOCIAL (INSS), inscrita no CNPJ/MF sob o nº 29.979.036/0001-40, em razão dos indícios de infração à Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), profere o presente despacho:

**1. Análise de admissibilidade do recurso administrativo (SEI nº 0101772) interposto pelo INSS.**

*Tempestividade – art. 61, I, do Regulamento de Fiscalização*

1.1. Observa-se que o recurso administrativo foi impetrado pelo Instituto Nacional do Seguro Social (INSS) em 16/02/2024, conforme recibo de protocolo eletrônico (SEI nº 0101773). Desse modo, o recurso é tempestivo, tendo sido encaminhado pela entidade pública autuada dentro do prazo instituído pelo art. 58 do Regulamento de Fiscalização.

*Legitimidade recursal – art. 61, II, do Regulamento de Fiscalização*

1.2. Além disso, o recurso foi subscrito por autoridade pública legitimada para representar a entidade em procedimentos administrativos, por se tratar de seu presidente, conforme a Portaria do nº 2.633, de 4 de julho de 2023, publicada no Diário Oficial da União, em 05/07/2023, na seção 2,

página 1.

Cabimento – arts. 61, III e V, do Regulamento de Fiscalização

1.3. Percebe-se, em seguida, que **não houve o esgotamento da via administrativa**, uma vez que cabe ao Conselho Diretor da ANPD a decisão final em matéria de processo sancionador no âmbito desta Autarquia Federal, conforme o disposto no art. 58 do Regulamento de Fiscalização.

1.4. Do mesmo modo, o Despacho Decisório nº 1/2024/FIS/CGF (SEI nº 0063073) não é ato de mero expediente ou ato preparatório de decisão, mas **decisão administrativa** tomada no curso de processo administrativo sancionador instituído por norma específica.

Interesse recursal – art. 61, IV, do Regulamento de Fiscalização

1.5. Igualmente, eventual reversão da decisão proferida em juízo de reconsideração pela Coordenação-Geral de Fiscalização ou em instância recursal pelo Conselho Diretor traria claro **benefício à entidade autuada**, que teria revertida sanção de advertência proferida contra si. Entende-se, assim, que há interesse recursal da parte irressignada.

Regularidade formal – art. 58, §2º, do Regulamento de Fiscalização

1.6. Observa-se, ainda, que o recurso administrativo foi direcionado ao Coordenador-Geral de Fiscalização, autoridade da ANPD responsável pelo Despacho Decisório nº 1/2024/FIS/CGF (SEI nº 0063073), e protocolado conforme orientado por esta ANPD.

Admissibilidade do recurso

1.7. Cumpridos, assim, os requisitos de admissibilidade, entende-se que **o recurso administrativo deve ser conhecido pela Coordenação-Geral de Fiscalização**, para que sejam analisadas as razões de fato e de direito alegadas pela entidade pública autuada para a revisão do Despacho Decisório nº 1/2024/FIS/CGF (SEI nº 0063073).

2. **Efeito suspensivo.**

2.1. No presente feito, o recurso atendeu aos critérios objetivos de conhecimento, motivo pelo qual não se vislumbram elementos que ensejem afastar o efeito suspensivo previsto no art. 60 do Regulamento de Fiscalização.

3. **Mérito**

3.1. O mérito do recurso, para fins de juízo de reconsideração, nos termos admitidos pelo art. 62 do Regulamento de Fiscalização, será analisado

em apartado.

4. **ANTE O EXPOSTO, DECIDE:**

4.1. CONHECER o recurso administrativo interposto pelo autuado (SEI nº **0101772**).

4.2. CONCEDER o efeito suspensivo ao recurso, conforme determinado pelo art. 60 do Regulamento de Fiscalização.

5. Intime-se a autuada.



Documento assinado eletronicamente por **Fabício Guimarães Madruga Lopes, Coordenador(a)-Geral de Fiscalização**, em 12/06/2024, às 18:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0126836** e o código CRC **4A1199F8**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8168 - <https://www.gov.br/anpd/pt-br>

**Referência:** Processo nº 00261.001888/2023-21

SEI nº 0126836



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

Despacho FIS/CGF

Brasília-DF, na data da assinatura.

1. De acordo com a Nota Técnica nº nº 20/2024/FIS/CGF/ANPD (0123131).
2. Mantém-se o Despacho Decisório nº nº 1/2024/FIS/CGF (SEI nº 0063073).
3. Encaminhe-se o processo ao Conselho Diretor, nos termos do art. 62, §3º, do Regulamento de Fiscalização.
4. Intime-se a autuada, para conhecimento.



Documento assinado eletronicamente por **Fabício Guimarães Madruga Lopes, Coordenador(a)-Geral de Fiscalização**, em 12/06/2024, às 18:47, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0126902** e o código CRC **D57CC8E3**.

**Referência:** Caso responda a este documento, indicar expressamente o Processo nº 00261.001888/2023-21

SEI nº 0126902



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

Ofício nº 93/2024/FIS/CGF/ANPD

Brasília-DF, na data da assinatura.

À Sra.

**ROBERTA DOS SANTOS LEMOS**

ENCARREGADA DE TRATAMENTO DE DADOS PESSOAIS

INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS

CNPJ nº 29.979.036/0001-40

ST SAUS QUADRA 02 BLOCO "O"

BRASÍLIA-DF CEP 70.070-946

roberta.lemos@inss.gov.br

edson.alvarista@inss.gov.br

**Assunto: Comunica decisão - recurso administrativo recebido com efeito suspensivo; decisão inicial mantida; envio de recurso ao Conselho Diretor da ANPD.**

**Referência: caso responda este ofício, favor indicar expressamente o processo nº 00261.001888/2023-21.**

Senhora Encarregada de dados pessoais do Instituto Nacional do Seguro Social - INSS,

1. Encaminho, para conhecimento, o Despacho Decisório nº 14/2024/FIS/CGF (0126836), por meio do qual a Coordenação-Geral de Fiscalização recebeu, com efeitos suspensivos, o recurso administrativo interposto contra a decisão proferida no presente Processo Administrativo Sancionador (PAS) em face do Instituto Nacional do Seguro Social - INSS.

2. Compartilho, ademais, o Despacho (0126902), que manteve o Despacho Decisório nº 1/2024/CGF/ANPD (0071087), tendo em vista os fundamentos apresentados na Nota Técnica nº 20/2024/FIS/CGF/ANPD (0123131); e que, conseqüentemente, encaminhou o recurso administrativo em questão para análise do Conselho Diretor, nos termos do art. 62, §3º, do Regulamento de Fiscalização.

3. Esta Coordenação de Fiscalização permanece à disposição, inclusive pelo e-mail [fiscalizacao@anpd.gov.br](mailto:fiscalizacao@anpd.gov.br).

Atenciosamente,

**JORGE ANDRÉ FERREIRA FONTELLES DE LIMA**  
Coordenador de Fiscalização

Anexos: Despacho Decisório nº 14/2024/FIS/CGF  
(0126836)  
Nota Técnica nº 20/2024/FIS/CGF/ANPD  
(0123131)  
Despacho (0126902)



Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Coordenador(a)**, em 14/06/2024, às 12:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0127116** e o código CRC **ADA2052E**.

SCN Quadra 06, Conjunto A, Ed. Venâncio 3000, Bloco A, 9º andar, - Bairro Asa Norte, Brasília/DF, CEP 70716-900  
Telefone: (61) 2025-8168 - <https://www.gov.br/anpd/pt-br>

**Referência:** Caso responda a este documento, indicar expressamente o Processo nº 00261.001888/2023-21

SEI nº 0127116



Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

Despacho CGF

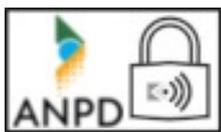
Brasília-DF, na data da assinatura.

À Secretaria-Geral

Assunto: **Recurso contra decisão em Processo Administrativo Sancionador**

1. Tendo em vista o Despacho (0126902), assinado pelo Coordenador-Geral de Fiscalização, encaminho o processo à Secretaria-Geral, para as providências cabíveis.

Atenciosamente



Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Coordenador(a)**, em 13/06/2024, às 18:29, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0127117** e o código CRC **278227DE**.





Autoridade Nacional de Proteção de Dados  
Coordenação-Geral de Fiscalização  
Coordenação de Fiscalização

## Formulário para Expedição de Documentos para o Protocolo

Processo nº 00261.001888/2023-21

Brasília, 14 de junho de 2024

Ao Protocolo da ANPD.

Encaminho o presente processo para expedição conforme a seguir:

( ) Enviar o processo integralmente;

( X ) Enviar apenas os documentos listados abaixo:

Identificação do documento PRINCIPAL 1		Link SUPER do documento PRINCIPAL 1	
Ofício nº 93/2024/FIS/CGF/ANPD		0127116	
Identificação do anexo do documento PRINCIPAL 1		Link SUPER do anexo do documento PRINCIPAL 1	
Despacho Decisório nº 14/2024/FIS/CGF		0126836	
Nota Técnica nº 20/2024/FIS/CGF/ANPD		0123131	
Despacho		0126902	
Prazo de envio			
( X )	Urgente	( )	Não urgente
Nível de Acesso			
( X )	Público	( )	Restrito

)		)	
<b>Indicação da forma de remessa</b>			
( )	E-mail · Informar e-mail (s) de destino:		
( X )	Protocolo Digital ou Peticionamento Eletrônico · Solução que possibilita aos órgãos e entidades da Administração Pública de todas as esferas, pessoas físicas e jurídicas, encaminhar documentos pela Internet, de forma eletrônica. · Envio de documentos avulsos. · O processo eletrônico que possui o(s) documento(s) continua aberto na Unidade no SUPER-ANPD.		
( )	Barramento · Solução que permite a comunicação entre os órgãos públicos que utilizam o SUPER/SEI ou outras soluções de processo eletrônico (desde que também estejam integrados ao Barramento). · Envio de todo o processo. · O processo eletrônico enviado fica bloqueado no SUPER-ANPD e não pode ser editado nem tramitado, mas fica disponível para consulta.		
( )	Via Postal * Colocar endereço(s) do(s) destinatário(s)	( )	SEDEX
		( )	Aviso de recebimento
( )	Qualquer das opções		

**ATENÇÃO: Caso a opção escolhida seja envio por meio de protocolo digital ou de peticionamento eletrônico, barramento ou e-mail e o Órgão de destino não ofereça essas opções de recebimento, o documento será enviado fisicamente ou por via postal.**

#### **INSTRUÇÕES:**

a) este formulário deve ser assinado pelo colaborador responsável e o respectivo processo encaminhado à unidade **Protocolo** da ANPD para

atendimento;

b) não é necessário incluir despacho de encaminhamento - apenas o formulário devidamente preenchido e assinado é suficiente para o atendimento da demanda;

c) os documentos a serem expedidos devem compor os autos dos processos enviados à expedição. Havendo documentos em processo diverso, estes deverão estar disponíveis para consulta da unidade **Protocolo** da ANPD.

Em caso de dúvida, por favor, entre em contato com o Protocolo: [protocolo@anpd.gov.br](mailto:protocolo@anpd.gov.br)



Documento assinado eletronicamente por **Jorge André Ferreira Fontelles de Lima, Coordenador(a)**, em 14/06/2024, às 14:22, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site [https://anpd-super.mj.gov.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://anpd-super.mj.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **0127263** e o código CRC **9D8AF87F**.

**Referência:** Caso responda a este documento, indicar expressamente o Processo nº 00261.001888/2023-21

SEI nº 0127263

**Data de Envio:**

14/06/2024 14:32:24

**De:**

ANPD/Coordenação-Geral de Fiscalização <fiscalizacao@anpd.gov.br>

**Para:**

roberta.lemos@inss.gov.br  
edson.alvarista@inss.gov.br

**Assunto:**

Comunica decisão - recurso administrativo recebido com efeito suspensivo  
00261.001888/2023-21

**Mensagem:**

À Sra.

ROBERTA DOS SANTOS LEMOS  
ENCARREGADA DE TRATAMENTO DE DADOS PESSOAIS  
INSTITUTO NACIONAL DO SEGURO SOCIAL - INSS  
CNPJ nº 29.979.036/0001-40  
ST SAUS QUADRA 02 BLOCO O  
BRASÍLIA-DF CEP 70.070-946  
roberta.lemos@inss.gov.br  
edson.alvarista@inss.gov.br

Assunto: Comunica decisão - recurso administrativo recebido com efeito suspensivo;  
decisão inicial mantida; envio de recurso ao Conselho Diretor da ANPD.

Referência: caso responda este ofício, favor indicar expressamente o processo nº  
00261.001888/2023-21.

Senhora Encarregada de dados pessoais do Instituto Nacional do Seguro Social - INSS,

Encaminho, para conhecimento, o Despacho Decisório nº 14/2024/FIS/CGF (0126836), por meio do qual a Coordenação-Geral de Fiscalização recebeu, com efeitos suspensivos, o recurso administrativo interposto contra a decisão proferida no presente Processo Administrativo Sancionador (PAS) em face do Instituto Nacional do Seguro Social - INSS.

Compartilho, ademais, o Despacho (0126902), que manteve o Despacho Decisório nº 1/2024/CGF/ANPD (0071087), tendo em vista os fundamentos apresentados na Nota Técnica nº 20/2024/FIS/CGF/ANPD (0123131); e que, conseqüentemente, encaminhou o recurso administrativo em questão para análise do Conselho Diretor, nos termos do art. 62, §3º, do Regulamento de Fiscalização.

Esta Coordenação de Fiscalização permanece à disposição, inclusive pelo email [fiscalizacao@anpd.gov.br](mailto:fiscalizacao@anpd.gov.br).

Atenciosamente,

JORGE ANDRÉ FERREIRA FONTELLES DE LIMA  
Coordenador de Fiscalização

Anexos:

I - Despacho Decisório nº 14/2024/FIS/CGF (0126836)

II - Nota Técnica nº 20/2024/FIS/CGF/ANPD (0123131)

III - Despacho (0126902)

**Anexos:**

Despacho\_Decisorio\_0126836.html

Nota\_Tecnica\_0123131.html

Despacho\_0126902.html

Oficio\_0127116.html

**Processo:**

00261.001888/2023-21 - ANPD: Processo Administrativo Sancionador

**Data da Distribuição:**

14/06/2024 15:19:18

**Colegiado:**

Conselho Diretor da Autoridade Nacional de Proteção de Dados (CD/ANPD)

**Composição do Colegiado:**

Waldemar Gonçalves Ortunho Junior (GABPR) - Impedido: Art. 22 do Regimento Interno da ANPD - O Diretor-Presidente, quando em exercício, fica impedido de receber processos para relatoria.

Arthur Pereira Sabbat (DIR-AS) - Impedido: Art. 22 do Regimento Interno da ANPD - O Diretor que estiver no exercício do encargo de substituto do Diretor-Presidente, fica impedido de receber processos para relatoria.

Joacil Basílio Rael (DIR-JR)

Miriam Wimmer (DIR-MW)

**Relator:**

Joacil Basílio Rael (DIR-JR)

**Re: Ofício nº 93/2024/FIS/CGF/ANPD**

ROBERTA DOS SANTOS LEMOS &lt;roberta.lemos@inss.gov.br&gt;

Ter, 18/06/2024 19:24

Para:ANPD - Protocolo <protocolo@anpd.gov.br>;Presidencia <pres@inss.gov.br>;CGRLOG - Coord Geral de Recursos Logísticos - CGRLOG - INSSDF <cgrlog@inss.gov.br>;Coordenação Geral de Licitações e Contratos - DGDF <cglco@inss.gov.br>

Cc:EDSON PINHEIRO ALVARISTA <edson.alvarista@inss.gov.br>;LUIZ CLAUDIO SENA SANTOS <luz.sena@inss.gov.br>;ANA CAROLINA TIETZ <ana.tietz@inss.gov.br>

Boa noite,

Confirmando recebimento dos 4 documentos em anexo.

Informo que, na data de sábado, foram inseridos em processo interno SEI sobre o assunto e encaminhado para conhecimento.

**Atenciosamente,****ROBERTA DOS SANTOS LEMOS**

Coordenação de Proteção de Dados - COPDP

Coordenação- Geral de Conformidade

Diretoria de Governança, Planejamento e Inovação

SAS, Quadra 2, Bloco O, sala 807, CEP 70.070-946

(61)3313-4153 (81) 98991-8355

Instituto Nacional do Seguro Social

---

**De:** ANPD - Protocolo <protocolo@anpd.gov.br>**Enviado:** terça-feira, 18 de junho de 2024 18:18**Para:** Presidencia <pres@inss.gov.br>; CGRLOG - Coord Geral de Recursos Logísticos - CGRLOG - INSSDF <cgrlog@inss.gov.br>; Coordenação Geral de Licitações e Contratos - DGDF <cglco@inss.gov.br>**Cc:** ROBERTA DOS SANTOS LEMOS <roberta.lemos@inss.gov.br>; EDSON PINHEIRO ALVARISTA <edson.alvarista@inss.gov.br>**Assunto:** Ofício nº 93/2024/FIS/CGF/ANPD

Algumas pessoas que receberam esta mensagem não costumam receber emails de protocolo@anpd.gov.br. [Saiba por que isso é importante](#)

Prezado(a),

Por ordem, encaminho o Ofício nº 93/2024/FIS/CGF/ANPD e anexos.

Solicito confirmação de recebimento desta mensagem eletrônica para fins de controle interno.

Atenciosamente,



Autoridade Nacional de Proteção de Dados - ANPD

[protocolo@anpd.gov.br](mailto:protocolo@anpd.gov.br)

<https://www.gov.br/anpd/pt-br>