MODELO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO COM DADOS PESSOAIS

PROTEÇÃO de dados pessoais

PREVIC
Superintendência Nacional de Previdência Complementar

Ministério da Previdência Social
Superintendência Nacional de Previdência Complementar - PREVIC

Diretor-Superintendente
Ricardo Pena Pinheiro

Diretor de Administração
Leonardo Zumpichiatti de Campani Rodrigues

Diretor de Fiscalização e Monitoramento
João Paulo de Souza

Diretor de Licenciamento
Guilherme Capriata Vaccaro Campelo Bezerra

Diretor de Normas
Alcinei Cardoso Rodrigues

Procurador-Chefe da Procuradoria Federal
Leandro Santos da Guarda

Chefe de Gabinete
Almir dos Santos Nolêto Filho

Coordenador-Geral de Tecnologia da Informação
James Taylor Faria Chaves

Encarregado pelo Tratamento de Dados Pessoais
Davi Neemias Cardoso Antunes da Costa

Grupo de Trabalho LGPD PREVIC
Leonardo Zumpichiatti de Campani Rodrigues
Renata Cardoso Fernandes Paz
Antônio Augusto Garcia
Davi Neemias Cardoso Antunes da Costa
Maria das Mercês Guimarães Cantuária
Karina Ericson Araújo Sotero
Silvio Alonso Marques
Roberto de Oliveira Mota
Nathalia de Oliveira Santos

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)
James Taylor Faria Chaves
Alexandre Crusca Pozzetti
Leonardo Fiuza da Silva

Chefe da Assessoria de Comunicação Social e Parlamentar
Francisco José Freire Ribeiro

Coordenadora de Comunicação Social
Monyke Silva Castilho

Diagramação e arte
Louise Guimarães Macau Lopes

Versão 1.0. elaborada em novembro/2025

Aprovado pela Diretoria Colegiada em 02/dezembro/2025

Sumário

1. Contexto

A Lei N.º 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece que os agentes de tratamento de dados — controladores e operadores — devem adotar medidas para prevenir danos aos titulares decorrentes de suas atividades. Em caso de incidente de segurança, uma das principais ações de mitigação é a comunicação da ocorrência aos titulares dos dados afetados, permitindo a adoção de providências para reduzir os riscos.

O Modelo de Comunicação de Incidente de Segurança da Informação com Dados Pessoais na Superintendência Nacional de Previdência Complementar (PREVIC) visa, assim, atender o disposto no art. 48, caput, da LGPD, que estabelece 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."

Tal disposição da LGPD foi regulamentada pela Agência Nacional de Proteção de Dados (ANPD), por meio da Resolução CD/ANPD N.º 15, de 24 de abril de 2024, a qual aprova o Regulamento de Comunicação de Incidente de Segurança. Este tema também é objeto da determinação do Tribunal de Contas da União (TCU), prevista no Acórdão nº 1372/2025/ TCU /Plenário, para que as organizações listadas — dentre elas a PREVIC — "adotem ações para elaborarem e aplicarem modelo de comunicação à ANPD e aos titulares de dados da ocorrência de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, conforme disposto na Lei 13.709/2018, art. 48, caput".

Assim, o presente modelo foi elaborado pelo Grupo de Trabalho (GT) instituído pela Portaria nº 939, de 02 de outubro de 2025 para a continuidade do processo de adequação à LGPD na PREVIC, e figura como entrega parcial do citado GT, conforme art. 5º, incisos VI e XIV da referida portaria. O processo de elaboração deste documento contou com a participação da Coordenação-Geral de Tecnologia da Informação (CGTI) e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR – PREVIC), equipe técnica vinculada à CGTI responsável pela análise, contenção e erradicação de incidentes em sistemas e infraestrutura tecnológica.

Dessa forma, este documento objetiva estabelecer, em alinhamento com os normativos citados, o fluxo de informação diante de incidente de segurança da informação com dados pessoais no âmbito da PREVIC, como ente controlador de dados pessoais. Sua validação e aprovação se deu junto à Diretoria Colegiada da PREVIC, instância máxima deliberativa da autarquia, na 762ª Sessão Ordinária, em 02 de dezembro de 2025.

Cumpre esclarecer que não são todos os incidentes de segurança que devem ser comunicados à ANPD. Cabe às equipes técnicas envolvidas avaliarem os riscos e impactos

aos titulares decorrentes do incidente e verificar a necessidade de realizar a comunicação. Este documento esclarece as situações em que será necessária essa comunicação.

Por fim, registra-se que, seguindo-se a Política de Segurança da Informação da PREVIC (Posin/PREVIC), as demais disposições referentes à gestão, tratamento e resposta a incidente de segurança da informação são de responsabilidade da ETIR-PREVIC, em conjunto com o Comitê Executivo da Tecnologia da Informação (CEXTI).

2. Definições

Para fins de aplicação deste Modelo de comunicação de incidente de segurança da informação com dados pessoais, consideram-se as seguintes definições:

- **Ampla divulgação do incidente em meios de comunicação:** providência que pode ser determinada pela ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança, como a publicação no sítio eletrônico, nas redes sociais do controlador ou em outros meios de comunicação;

- **Autenticidade:** propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

- **Categoria de dados pessoais:** classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros;

- **Comunicação de incidente de segurança:** ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;

- **Confidencialidade:** propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados;

- **Dado de autenticação em sistemas:** qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas;

- **Dado financeiro:** dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;

- **Dado pessoal afetado:** dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;

- **Dado pessoal sensível:** dado pessoal 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;

- **Dado protegido por sigilo legal ou judicial:** dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial;

- **Dado protegido por sigilo profissional:** dado pessoal cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem;

- **Dados em larga escala:** aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares;

- **Disponibilidade:** propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou determinado sistema, órgão ou entidade devidamente autorizados;

- **Incidente de segurança:** qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;

- **Integridade:** propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental;

- **Medidas de segurança:** medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

- **Natureza dos dados pessoais:** classificação de dados pessoais em gerais ou sensíveis;

- **Relatório de tratamento de incidente:** documento fornecido pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos.

3. O que caracteriza um incidente de segurança da informação com dados pessoais

De acordo com o Regulamento de Comunicação de Incidente de Segurança da ANPD, deve ser comunicada à ANPD e ao titular dos dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Mas o que caracteriza esse tipo de incidente?

O incidente de segurança pode acarretar risco ou dano relevante aos titulares quando puder **afetar significativamente interesses e direitos fundamentais dos titulares**, ou seja, quando caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder **impedir 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 roubo de identidade.

Além disso, **deverá envolver cumulativamente pelo menos um dos seguintes critérios:**

I - Dados pessoais sensíveis;

II - Dados de crianças, de adolescentes ou de idosos;

III - Dados financeiros;

IV - Dados de autenticação em sistemas;

V - Dados protegidos por sigilo legal, judicial ou profissional; ou

VI - Dados em larga escala.

Segue abaixo a explicação encontrada na página da ANPD que resume esse tipo de incidente:

- É um evento adverso confirmado que comprometa as propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.

- Incidentes podem ocorrer de forma acidental, como o envio de informações para o destinatário incorreto, ou em decorrência de atos intencionais, como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados.

- Os incidentes de segurança não se restringem às violações da confidencialidade, abrangem também eventos de perda ou indisponibilidade dados pessoais. São exemplos de incidentes de segurança o sequestro de dados (ransomware), o acesso não autorizado a dados armazenados em sistemas de informação e a publicação não intencional de dados dos titulares.

- Nem todo incidente de segurança da informação envolve dados pessoais. Incidentes que envolvam somente dados anonimizados ou que não estejam relacionados a pessoas naturais identificadas ou identificáveis não precisam ser comunicados à ANPD.

- A mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança. A exploração da referida vulnerabilidade, no entanto, pode resultar em um incidente.

- Cabe ao controlador identificar, tratar e avaliar o risco dos incidentes de segurança que afetem suas operações de tratamento de dados pessoais.

3.1 Do recebimento da notificação sobre o incidente de segurança da informação com dados pessoais

O recebimento da notificação sobre um incidente de segurança com dados pessoais pode ter diferentes origens. Para usuários internos à PREVIC, tal notificação deverá ser feita, preferencialmente, via **"Formulário de Notificação de Incidente de Segurança"** (Anexo I), disponível no Sistema Eletrônico de Informações (SEI Previc) a ser preenchido pelo colaborador ou área técnica que primeiramente e imediatamente identificar o incidente. O processo deverá ser aberto no SEI, selecionando-se o tipo de processo **"Gestão da Informação: incidente de segurança"** e classificando-o como restrito (informação pessoal), inserindo-se o citado formulário. Poderá ser instruído com anexos que comprovem a natureza e características do incidente de segurança, e deverá ser encaminhado via SEI, para análise, ao Encarregado pelo Tratamento de Dados Pessoais, na unidade "LGPD". Também poderão ser recebidas notificações por e-mail, chamado da TI ou ligações telefônicas, devendo, nesses casos, ser formalizadas pelo Encarregado pelo Tratamento de Dados Pessoais, via Formulário no SEI.

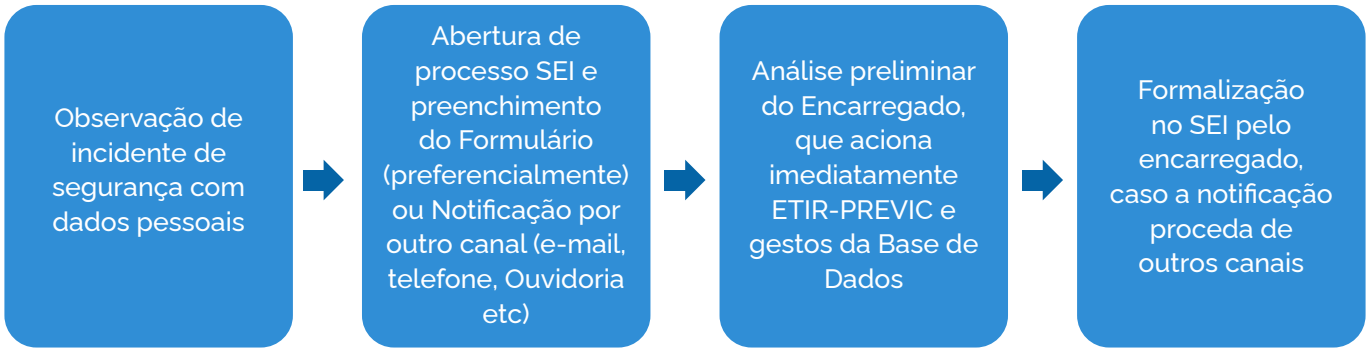
Nos casos em que a constatação de incidente de segurança for feita pela própria equipe de Tecnologia da Informação da PREVIC, seja por meio de chamado de TI, inspeções ou monitoramentos de rotina, ou qualquer outra hipótese de medida de segurança interna, a área responsável também deverá acionar imediatamente o Encarregado para a realização de uma análise conjunta sobre o incidente, e formalizar logo após a instrução de processo no SEI, transcrevendo as informações para o "Formulário de Notificação de Incidente de Segurança" (Anexo I), encaminhando ao Encarregado.

Caso a notificação proceda de ente externo (cidadãos, entidades fechadas de previdência complementar, outros órgãos e entidades, sociedade em geral), solicita-se que seja registrada, preferencialmente, via Manifestação de Ouvidoria, por meio da Plataforma Fala.Br, com o título "Notificação de Incidente de Segurança com dados pessoais", a qual será encaminhada via SEI ao Encarregado pelo Tratamento de Dados Pessoais, para análise. Caso não haja informações suficientes para a caracterização completa do incidente de segurança, o encarregado poderá solicitar ao manifestante as informações complementares.

As manifestações externas também poderão proceder de outros canais, como e-mail, ligações telefônicas, peticionamento eletrônico (SEI Usuário Externo) e Protocolo Digital. Em todos esses, o Encarregado deverá receber as informações, acionar imediatamente a ETIR-PREVIC e/ou o Gestor da base de dados afetada, e, em seguida, transcrever as informações encaminhadas na manifestação para o "Formulário de Notificação de Incidente de Segurança" do SEI.

A depender da relevância, impacto e criticidade do incidente de segurança reportado, o Encarregado poderá, de ofício, realizar ele próprio o devido registro no Formulário do SEI.

Segue abaixo fluxo simplificado do recebimento da notificação de incidente de segurança:



3.2 Da análise do incidente de segurança da informação com dados pessoais

A fim de avaliar a caracterização do incidente de segurança da informação com dados pessoais, é necessário que haja uma análise conjunta **imediata**, tanto do Encarregado pelo tratamento de dados pessoais quanto pelo gestor da base de dados, se for o caso, quanto pela ETIR-PREVIC em caso de sistemas computacionais. Esta análise não poderá ultrapassar o prazo de três dias úteis, que é o prazo estabelecido no Regulamento da ANPD para a comunicação do incidente de segurança à Agência e ao titular.

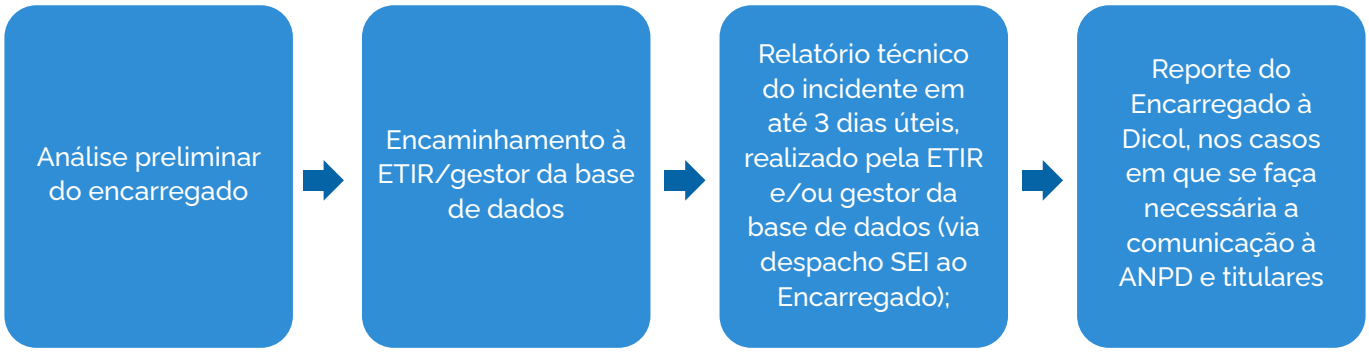
Como descrito no item 3.1., o Encarregado é o agente responsável na PREVIC pelo recebimento das notificações sobre incidente de segurança. Ele irá tanto avaliar a caracterização do incidente de segurança, como iniciar a análise de criticidade, identificando

a descrição da natureza e da categoria de dados pessoais afetados, o volume/número de titulares afetados, os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares, dentre outras informações necessárias.

Após a análise preliminar, o Encarregado acionará a equipe competente pelo tratamento do incidente de segurança, podendo ser o gestor da base de dados afetada e/ou a ETIR-PREVIC, que atuarão na complementação da análise, de forma técnica, subsidiando a confirmação do incidente de segurança, sua extensão, a natureza dos dados afetados, riscos diversos etc.

O resultado da análise será reportado em até três dias úteis via SEI ao Encarregado na forma de Despacho. Em caso de caracterização de incidente de segurança com dados pessoais a ser comunicado, o Encarregado informará imediatamente a Diretoria Colegiada da PREVIC e, após a ciência da Diretoria, providenciará a comunicação à Agência Nacional de Proteção de Dados (ANPD), conforme instruções detalhadas na seção 4 deste documento.

Segue abaixo fluxo simplificado da análise do incidente de segurança:



4. Comunicação do incidente de segurança da informação com dados pessoais à ANPD

A partir da análise conjunta realizada, caso verificada a necessidade de comunicação com base nos critérios listados na seção 3 deste documento, o Encarregado deverá realizar a comunicação do incidente de segurança no prazo de três dias úteis, contados do conhecimento pelo controlador de que o incidente afetou dados pessoais, à Agência Nacional de Proteção de Dados (ANPD), por meio do link Peticionamento Eletrônico ANPD — Agência Nacional de Proteção de Dados. Na Página Comunicação de incidente de segurança — Agência Nacional de Proteção de Dados verifica-se um passo-a-passo para a instrução do processo no sistema SEI da ANPD, com o tipo de processo a ser aberto e o formulário correspondente.

O ato da comunicação deve ser acompanhado, no mesmo prazo citado anteriormente, de documento comprobatório de vínculo funcional do Encarregado (§ 5.º, art. 6.º, Resolução CD/ANPD N.º 15/2024), podendo ser a Declaração de Dados Funcionais (Vínculo) disponível no SouGov, acrescida da Portaria de nomeação para a função de Encarregado pelo Tratamento de Dados Pessoais.

O relatório de comunicação à ANPD deverá conter as seguintes informações:

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

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

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

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

V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto na introdução dessa seção;

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

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

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

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

X - a identificação do operador, quando aplicável;

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

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

As informações acima listadas poderão ser complementadas, de maneira fundamentada, no prazo de 20 dias úteis, a contar da data da comunicação (§ 3.º, art. 6.º, Resolução CD/ANPD Nº 15/2024).

Nos casos que tratem de informações cujo sigilo seja protegido por lei, como dados e informações técnicas, econômico-financeiras, contábeis, operacionais, cuja divulgação possa representar violação a segredo comercial ou a industrial, o Encarregado, em nome do controlador (PREVIC), deverá solicitar à ANPD de maneira fundamentada o respectivo sigilo, indicando aqueles dados/informações cujo acesso deverá ser restringido.

Conforme especificado no próximo item, será necessária, posteriormente, a juntada de declaração de que foi realizada comunicação aos titulares (§ 4.º, art. 9.º, Resolução CD/ANPD N.º 15/2024).

Por fim, ressalta-se que A ANPD poderá, a qualquer tempo, solicitar informações adicionais ao controlador referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.

5. Comunicação do incidente de segurança da informação com dados pessoais ao titular

Assim como a comunicação do incidente de segurança à ANPD, a comunicação do incidente de segurança ao titular deverá ser realizada pelo controlador no prazo de três dias úteis contados do conhecimento pelo controlador de que o incidente afetou dados pessoais. No âmbito da PREVIC, sendo o Encarregado considerado a pessoa designada para atuar como canal de comunicação entre o Controlador, os Titulares dos Dados e a ANPD, conforme disposição da LGPD, é ele também o responsável pela comunicação do incidente de segurança da informação com dados pessoais ao titular.

Dessa forma, o Encarregado providenciará a comunicação ao titular, que conterá as seguintes informações:

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

II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

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

IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo previsto na introdução desta seção;

V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

VI - a data do conhecimento do incidente de segurança; e

VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado.

Essa comunicação ao titular deverá fazer uso de linguagem simples e de fácil entendimento, e de forma direta e individualizada, caso seja possível identificá-los. A comunicação é considerada direta e individualizada quando realizada pelos meios usualmente utilizados para contatar o titular, por exemplo telefone, e-mail ou carta). O conteúdo da mensagem será elaborado pelo Encarregado.

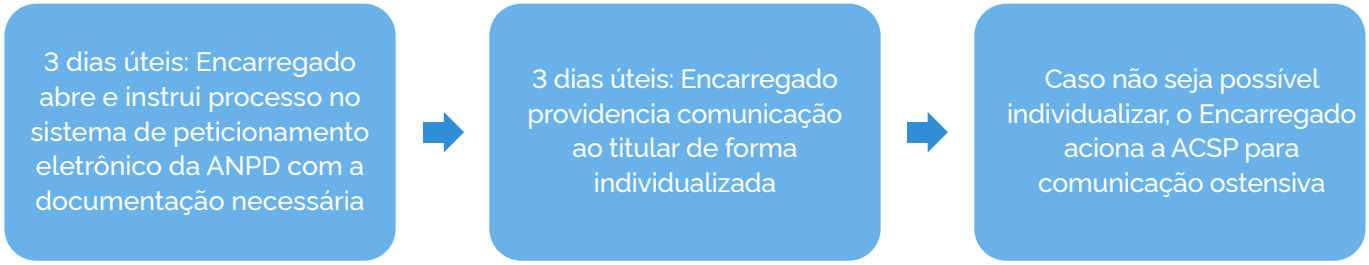
Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados, a comunicação do incidente de

segurança deverá ocorrer no prazo e com as informações definidas acima, pelos meios de divulgação disponíveis, tais como seu sítio eletrônico, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses. Para tal, deverá ser acionada a Assessoria de Comunicação Social e Parlamentar (ACSP), que irá operacionalizar a referida divulgação.

Deverá ser incluído no processo de comunicação de incidente (podendo ser o mesmo processo SEI referente à notificação do incidente de segurança), uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo indicado acima para a comunicação do incidente de segurança ao titular.

Por fim, poderá ser considerada boa prática, para fins do disposto no art. 52, § 1º, IX, da LGPD, a inclusão, na comunicação ao titular, de recomendações aptas a reverter ou mitigar os efeitos do incidente de segurança em questão.

Segue abaixo fluxo simplificado da comunicação do incidente de segurança:



6. Registro do incidente de segurança da informação com dados pessoais

A PREVIC, enquanto ente controlador, deverá manter o registro do incidente de segurança, inclusive daquele não comunicado à ANPD e aos titulares, observadas as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade própria.

O registro do incidente será detalhado no "**Formulário de registro de incidente de segurança"** (Anexo II), no SEI, a ser preenchido pela ETIR-PREVIC em conjunto com o Gestor da base de dados, e deverá conter, no mínimo:

I - a data de conhecimento do incidente;

II - a descrição geral das circunstâncias em que o incidente ocorreu;

III - a natureza e a categoria de dados afetados;

IV - o número de titulares afetados;

V - a avaliação do risco e os possíveis danos aos titulares;

VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;

VII - a forma e o conteúdo da comunicação, se o incidente tiver sido comunicado à ANPD e aos titulares; e

VIII - os motivos da ausência de comunicação, quando for o caso.

7. Disposições acerca do Processo de Comunicação de incidente de segurança

De acordo com o Regulamento de Comunicação de Incidente de Segurança da ANPD, o processo de comunicação de incidente de segurança, instaurado pela ANPD, tem por objeto a fiscalização de atos relacionados ao tratamento e resposta ao incidente que possa acarretar risco ou dano relevante aos titulares de dados, a fim de salvaguardar os direitos dos titulares. Ele abrange o procedimento de apuração de incidente de segurança e o procedimento de comunicação de incidente de segurança.

O processo pode iniciar-se de ofício ou por comunicação formal do controlador, neste caso a PREVIC, e em seu curso, a ANPD pode realizar auditorias ou inspeções para validar informações recebidas. A análise pode ser feita de forma agregada, conforme planejamento da ANPD, que pode determinar medidas preventivas imediatas ao controlador, a fim de prevenir, mitigar ou reverter os efeitos do incidente e evitar a ocorrência de dano grave e irreparável ou de difícil reparação, inclusive com aplicação de multa diária.

No procedimento de apuração de incidente de segurança, a ANPD pode apurar incidentes não comunicados pelo controlador (neste modelo a PREVIC) de que tenha conhecimento. Pode requisitar informações e avaliar o incidente conforme critérios do regulamento. Se confirmado o incidente, a ANPD determinará à PREVIC o envio da comunicação à Agência e aos titulares, podendo instaurar processo sancionador.

Já o procedimento de comunicação de incidente de segurança será iniciado com o recebimento da comunicação do incidente pela ANPD, que após avaliar a gravidade do incidente, poderá exigir medidas do controlador como ampla divulgação em meios de comunicação e medidas para mitigar seus efeitos. A divulgação deve ser proporcional à abrangência do controlador e pode ocorrer por mídia impressa, radiodifusão ou internet.

A ANPD pode divulgar, como medida de transparência ativa, estatísticas agregadas dos incidentes. As medidas exigidas acima pela Agência não se configuram como sanções, mas como ações preventivas. Entretanto o seu não cumprimento nos prazos e condições determinadas pode levar à instauração de processo administrativo sancionador à PREVIC.

8. Papéis e responsabilidades

Papel	Responsabilidade
Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR - PREVIC).	• Comunicar incidente de segurança da informação que envolva dados pessoais ao Encarregado; • Coordenar as atividades de tratamento e resposta a incidentes de SI, adotando todas as medidas reativas e corretivas necessárias, nos termos da Política de Segurança da Informação da PREVIC (Portaria PREVIC nº 295, de 04 de abril de 2023); • Analisar o incidente de segurança da informação com dados pessoais e gerar relatório de tratamento de incidente, encaminhando-o ao Encarregado em até três dias úteis; • Instruir o respectivo processo com o registro do incidente de segurança de que trata o art. 10 da Resolução CD/ANPD N.º 15/2024.
Gestor da base de dados	• Analisar o incidente de segurança da informação com dados pessoais e gerar relatório de tratamento de incidente, identificando os critérios e caracterização constantes do art. 5º da Resolução CD/ANPD N.º 15/2024, encaminhando-o ao Encarregado em até três dias úteis; • Instruir o respectivo processo com o registro do incidente de segurança de que trata o art. 10 da Resolução CD/ANPD N.º 15/2024 em conjunto com a ETIR-PREVIC.
Encarregado pelo Tratamento de Dados Pessoais na PREVIC	• Receber, enquanto canal de comunicação do controlador, as notificações de incidente de segurança encaminhadas interna ou externamente por meio do SEI ou por qualquer outro canal; • Registrar de ofício em formulário próprio do SEI, quando pertinente, notificação de incidente de segurança de que tenha conhecimento por outros canais (e-mail, Teams, carta, etc); • Realizar análise preliminar e encaminhar as informações à análise técnica da ETIR-PREVIC e Gestor da base de dados, quando pertinente; • Analisar as informações enviadas pela ETIR e Gestor da base de dados a fim de verificar a caracterização do incidente de segurança pelos critérios do art. 5.º da Resolução CD/ANPD N.º 15/2024;

	• Comunicar imediatamente à Diretoria Colegiada, e após a ciência da Diretoria, à ANPD, em até 3 dias úteis, a ocorrência de incidente de segurança da informação com dados pessoais, contendo as informações determinadas no §2.º, art. 6.º da Resolução CD/ANPD N.º 15/2024. Importante incluir documento comprobatório de vínculo funcional do Encarregado(a); • Comunicar aos titulares de dados pessoais em até 3 dias úteis a ocorrência de incidente de segurança da informação com dados pessoais, contendo as informações determinadas no art. 9.º da Resolução CD/ANPD N.º 15/2024. em caso de incidente em que seja viável a comunicação direta e individualizada; • Instruir à Assessoria de Comunicação Social e Parlamentar (ACSP) quanto à comunicação aos titulares, quando for o caso de comunicação ampla, conforme §3.º, art. 9.º da Resolução CD/ANPD N.º 15/2024. • Em até 3 dias úteis do término do prazo de comunicação ao titular, juntar ao processo de comunicação de incidente de segurança documentação comprovatória da cientificação aos titulares.
Assessoria de Comunicação Social e Parlamentar (ACSP)	• Realizar comunicação ampla em caso de incidente em que não seja viável a comunicação direta e individualizada, conforme §3.º, art. 9.º da Resolução CD/ANPD N.º 15/2024.

9. Disposições finais

As orientações contidas neste modelo são de observância obrigatória para as unidades da PREVIC envolvidas no processo de comunicação de incidente de segurança.

Será dada ampla divulgação deste documento no portal da PREVIC na internet, bem como internamente, por meio dos canais oficiais de comunicação como e-mail institucional, SEI etc.

Recomenda-se, ainda, que seja realizada periodicamente ação de conscientização em proteção de dados, com ênfase para o procedimento correto de notificação de incidente de segurança com o comprometimento de dados pessoais, junto aos colaboradores e colaboradoras da PREVIC.

Por fim, havendo a necessidade de revisão deste modelo, a proposta poderá ser levada pela unidade proponente à Diretoria Colegiada, ouvida a ETIR-PREVIC e o Encarregado pelo Tratamento de Dados Pessoais.

10. Disposições finais

BRASIL. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em: < http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 22 de outubro de 2025.

BRASIL. Agência Nacional de Proteção de dados. Regulamento de Comunicação de incidentes de segurança. Disponível em: < https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024- 556243024>. Acesso em: 22 de outubro de 2025.

BRASIL. Superintendência Nacional de Previdência Social. PORTARIA PREVIC Nº 295, DE 04 DE ABRIL DE 2023 - Dispõe sobre a Política de Segurança da Informação (Posin), no âmbito da Superintendência Nacional de Previdência Complementar (PREVIC). Disponível em: <https://www.gov.br/previc/pt-br/acesso-a-informacao-1/institucional/normas/portarias-1/2023/portaria-previc-no-295-de-04-de-abril-de-2023.pdf/view>. Acesso em: 22 de outubro de 2025.

Anexo I - Formulário de Notificação de Incidente de Segurança

Processo nº 44011.XXXXXX/XXXX-XX

1. Identificação do Comunicante	
Nome Completo	
Unidade/Lotação	
E-mail de contato	
Telefone para Contato	
Data da comunicação	

2. Descrição Geral do Incidente	
Data e Hora da Ocorrência (ou da suspeita)	[dd/mm/aaaa hh:mm]
Data e Hora da Ciência (quando você descobriu)	[dd/mm/aaaa hh:mm]
Descrição do incidente	[Descreva objetivamente o que aconteceu, como descobriu, em que meio, se há alguém envolvido e qual a localização física ou lógica dos dados afetados]
Causa Principal (se identificada)	[Descrição]

3. Dados Pessoais Afetados	
Natureza dos dados pessoais	( ) Dados pessoais gerais ( ) Dados pessoais sensíveis - 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
Categoria dos dados pessoais	( ) Dados de crianças, de adolescentes ou de idosos; ( ) Dados financeiros; ( ) Dados de autenticação em sistemas; ( ) Dados protegidos por sigilo legal, judicial ou profissional; ou ( ) Dados em larga escala.
Número de titulares afetados	[Total e, se aplicável, número de crianças, adolescentes ou idosos]
Tipo de violação (marque a(s) principal(is) suspeita(s)	( ) Acesso Não Autorizado ( ) Vazamento / Comunicação Indevida ( ) Alteração Indevida ( ) Perda / Destruição ( ) Sequestro de Dados (Ransomware) ( ) Roubo / Furto de Equipamento ( ) Outra: [Especifique]

Anexo II - Formulário de Registro de Incidente de Segurança

Processo nº 44011.XXXXXX/XXXX-XX

1. Descrição Geral do Incidente	
Data de conhecimento do incidente	[dd/mm/aaaa hh:mm]
Descrição geral das circunstâncias em que o incidente ocorreu	[Descrição]
Outras informações relevantes	[Descrição]

2. Dados Pessoais Afetados	
Natureza dos dados afetados	( ) Dados pessoais gerais ( ) Dados pessoais sensíveis ( ) origem racial ou étnica ( ) convicção religiosa ( ) opinião política ( ) filiação a sindicato ou a organização de caráter religioso, filosófico ou político ( ) saúde ( ) vida sexual ( ) dado genético ou biométrico
Categoria dos dados pessoais afetados	( ) Dados de crianças, de adolescentes ou de idosos; ( ) Dados financeiros; ( ) Dados de autenticação em sistemas; ( ) Dados protegidos por sigilo legal, judicial ou profissional; ou ( ) Dados em larga escala.
Avaliação do risco	
Possíveis danos aos titulares	

3. Ações Corretivas e Mitigadoras (quando aplicável)	
Medidas de correção	[Descrição]
Medidas de mitigação	[Descrição]

4. Comunicação do incidente de segurança	
Forma e conteúdo da comunicação à ANPD	[Descrição]
Forma e conteúdo da comunicação aos titulares	[Descrição]
Motivos da ausência de comunicação (quando for o caso)	[Descrição]