Caderno Administrativo
Conselho Superior da Justiça do Trabalho

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

Nº4377/2025 **Data da disponibilização: Segunda-feira, 22 de Dezembro de 2025.**

Conselho Superior da Justiça do Trabalho

Ato

ATO CONJUNTO

ATO CONJUNTO TST.CSJT.GP N.º 84, DE 19 DE DEZEMBRO DE 2025.

Regulamenta os procedimentos de comunicação de incidentes de segurança com dados pessoais à Agência Nacional de Proteção de Dados - ANPD e aos titulares de dados, no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho.

O **PRESIDENTE DO TRIBUNAL SUPERIOR DO TRABALHO** e do **CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO**, no uso de suas atribuições legais e regimentais,

considerando o disposto nos incisos X, XII e LXXIX do art. 5º da Constituição da República, que asseguram como direitos fundamentais a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, e o direito à proteção dos dados pessoais, inclusive nos meios digitais;

considerando a Lei n.º 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), que dispõe sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

considerando o Ato Conjunto TST.CSJT.GP n.º 46, de 4 de novembro de 2020, que atribui o exercício das funções de controlador e encarregado do tratamento de dados pessoais, na forma exigida pela Lei Geral de Proteção de Dados - LGPD;

considerando o Ato Conjunto TST.CSJT.GP n.º 4, de 12 de março de 2021, que institui a Política de Privacidade e Proteção de Dados Pessoais (PPPDP) no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho e estabelece as diretrizes gerais para o tratamento de dados pessoais;

considerando o Ato TST.GP n.º 142, de 21 de março de 2025, que dispõe sobre o Comitê de Proteção de Dados Pessoais (CLGPD) e sua função de assessoramento na implementação e fiscalização das políticas de proteção de dados no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho;

considerando a Resolução n.º 15, de 24 de abril de 2024, do Conselho Diretor (CD) da Autoridade Nacional de Proteção de Dados (ANPD) (atualmente denominada Agência Nacional de Proteção de Dados, nos termos da Medida Provisória n.º 1.317, de 17 de setembro de 2025), que aprova o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais e estabelece procedimentos, prazos e critérios para o cumprimento da obrigação prevista no art. 48 da LGPD;

considerando a necessidade de estabelecer um procedimento formal, célere e eficaz para a gestão e para a comunicação de incidentes de segurança, a fim de mitigar riscos e danos aos titulares de dados, assegurar a responsabilização e a prestação de contas e proteger a integridade institucional do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho; e

considerando o teor do Processo Administrativo SEI n.º 6014093/2025-00;

RESOLVE:

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Ato regulamenta o procedimento para a gestão, apuração e comunicação de incidentes de segurança que envolvam dados pessoais sob o controle do Tribunal Superior do Trabalho (TST) e do Conselho Superior da Justiça do Trabalho (CSJT), com vistas à proteção dos direitos dos titulares e à prevenção de danos, mediante a formalização dos fluxos internos e externos de resposta a incidentes de segurança com dados pessoais.

§ 1º O disposto neste Ato aplica-se a todas as operações de tratamento de dados pessoais realizadas no âmbito do TST e do CSJT, tanto em suas atividades jurisdicionais quanto administrativas, em meios físicos ou digitais.

§ 2º O âmbito de aplicação abrange os dados pessoais de todos os titulares com os quais o TST e o CSJT se relacionam incluindo Ministros, magistrados, servidores, advogados, partes processuais, membros do Ministério Público, estagiários, prestadores de serviços, fornecedores e demais usuários dos serviços do Tribunal e do Conselho.

§ 3º As disposições deste Ato não afastam os procedimentos previstos na Política de Segurança da Informação do TST e nas normas de resposta a incidentes cibernéticos, devendo ambos os fluxos atuar de forma complementar quando houver envolvimento de dados pessoais.

§ 4º Serão observadas no TST e no CSJT as disposições previstas na Resolução CD/ANPD n.º 15, de 24 de abril de 2024, inclusive no que se refere aos objetivos e definições, com os esclarecimentos e detalhamentos previstos no presente Ato.

Art. 2º Para os fins deste Ato, adotam-se as seguintes definições, em alinhamento com a legislação de proteção de dados pessoais:

I - agentes de tratamento: o Controlador e o operador;

II - Comitê de Proteção de Dados Pessoais (CLGPD): colegiado responsável por assessorar o Controlador nas questões pertinentes à proteção de dados pessoais;

III - Controlador: o TST e o CSJT, representados por seu Presidente, a quem compete as decisões referentes ao tratamento de dados pessoais;

IV - Divisão de Integridade e de Gestão de Riscos (DINGER): unidade responsável por assessorar o(a) Encarregado(a) e o CLGPD;

V - Encarregado(a): pessoa designada pelo Controlador para atuar como canal de comunicação entre o Controlador, os titulares dos dados e a Agência Nacional de Proteção de Dados;

VI - incidente de segurança com dados pessoais: evento adverso confirmado que resulte em comprometimento de confidencialidade, integridade ou disponibilidade de dados pessoais;

VII - Operadores: as pessoas naturais ou jurídicas, de direito público ou privado, que realizam o tratamento de dados pessoais em nome do Controlador;

VIII - risco ou dano relevante: a condição que se configura quando um incidente de segurança puder afetar significativamente interesses e direitos fundamentais dos titulares e, cumulativamente, envolver, pelo menos, um dos seguintes critérios:

a) dados pessoais sensíveis, assim considerados os que revelam informações íntimas e potencialmente discriminatórias sobre a pessoa natural, tais como origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, bem como dados referentes a saúde, vida sexual, genética ou biometria;

b) dados de crianças, de adolescentes ou de idosos;

c) dados financeiros, assim considerados aqueles relacionados a transações financeiras, informações bancárias, números de cartão de crédito, entre outros;

d) dados de autenticação em sistemas, como credenciais de acesso (logins, senhas, tokens) que possibilitem o acesso à conta do titular;

e) dados protegidos por sigilo legal, judicial ou profissional; ou

f) dados tratados em larga escala, caracterizada quando abranger número significativo de titulares, volume considerável de dados, longa duração, frequência relevante ou ampla extensão geográfica de localização dos titulares.

DO FLUXO INTERNO DE NOTIFICAÇÃO

Art. 3º São admitidos como meios formais de notificação de incidente de segurança com dados pessoais, para fins de apuração e adoção das providências previstas neste Ato:

I - as manifestações registradas pela Ouvidoria em seus canais oficiais;

II - a comunicação encaminhada diretamente ao(à) Encarregado(a), por e-mail institucional ou por outros meios oficiais de contato disponibilizados;

III - o Formulário de Comunicação Interna de Incidente de Segurança com Dados Pessoais, mediante registro no Sistema Eletrônico de Informações (SEI).

Parágrafo único. A notificação recebida por quaisquer dos meios previstos nos incisos I a III será registrada em processo SEI, para fins de análise preliminar, preservação de evidências, classificação e adoção das providências estabelecidas neste Ato.

Art. 4º Qualquer magistrado(a), servidor(a), estagiário(a), fornecedor(a) ou prestador(a) de serviço que, no exercício de suas funções no âmbito do Tribunal Superior do Trabalho e do Conselho Superior da Justiça do Trabalho, identificar a ocorrência ou a suspeita de incidente de segurança com dados pessoais, tem o dever de comunicar o fato de forma imediata à sua chefia e, concomitantemente, ao(à) Encarregado(a) de Dados.

Parágrafo único. A comunicação de que trata o caput é compulsória e visa garantir que a estrutura de governança de dados do Tribunal e do CSJT seja acionada no menor tempo possível para a adoção das medidas cabíveis.

Art. 5º A comunicação ao(à) Encarregado(a) deverá ocorrer de forma imediata por meio do SEI, não podendo exceder o prazo de 1 (um) dia útil a contar da ciência do evento.

Art. 6º A comunicação interna do incidente de segurança com dados pessoais deverá ser realizada por meio do preenchimento do "Formulário de Comunicação Interna de Incidente de Segurança com Dados Pessoais", o qual estará disponibilizado no SEI, devendo ser classificado como restrito, na forma da lei.

§ 1º O Formulário deverá ser preenchido com o maior detalhamento possível, contendo todas as informações disponíveis no momento da notificação.

§ 2º A ausência de informações detalhadas não impede a comunicação, que deverá ser feita com os elementos conhecidos, e complementada posteriormente assim que novos dados estiverem disponíveis.

Art. 7º Nos casos em que o incidente de segurança com dados pessoais envolver empresa contratada, conveniada ou prestadora de serviços que atue como operadora de dados pessoais do TST/CSJT, caberá à unidade gestora do contrato:

I - comunicar imediatamente o fato ao(à) Encarregado(a), nos termos deste Ato;

II - exigir da contratada relatório de apuração e plano de contenção, com a indicação das medidas corretivas adotadas;

III - assegurar que o contrato celebrado com o terceiro contenha cláusulas específicas de proteção de dados e obrigações quanto à comunicação e ao tratamento de incidentes, conforme a Lei n.º 13.709, de 14 de agosto de 2018; e

IV - avaliar a eventual aplicação de sanções contratuais ou administrativas.

Parágrafo único. A omissão ou o atraso injustificado da empresa contratada na comunicação ou na preservação das evidências poderá ensejar a adoção das medidas sancionatórias cabíveis, inclusive rescisão contratual, bem como comunicação do fato à ANPD e aos órgãos de controle competentes.

DA ANÁLISE E DA GESTÃO DO INCIDENTE

Art. 8º Recebida a comunicação interna de possível incidente de segurança com dados pessoais, o(a) Encarregado(a), com o apoio técnico e administrativo da DINGER, adotará as seguintes providências:

I - realizar análise preliminar do fato comunicado, a fim de:

a) verificar se envolve operador, observado o art. 7º deste Ato;

b) verificar se há envolvimento de dados pessoais;

c) aferir se o evento identificado pode acarretar risco ou dano relevante aos titulares, com base nos critérios definidos no art. 2º, inciso VIII, deste Ato;

d) identificar as categorias de dados pessoais e o número estimado de titulares potencialmente afetados;

e) propor medidas imediatas de contenção e mitigação de eventuais impactos; e

f) indicar, motivadamente, o arquivamento do processo quando constatada a inexistência de dados pessoais ou de risco/dano relevante, ou sugerir o encaminhamento à unidade responsável, registrando as providências adotadas;

II - caso confirmada a ocorrência do incidente, conforme os critérios definidos no art. 2º, inciso VIII, deverá:

a) dar ciência imediata ao Presidente, ao Corregedor-Geral da Justiça do Trabalho e ao CLGPD;

b) instituir a Sala de Situação;

c) determinar a preservação de dados e evidências relacionados ao incidente; e

d) proceder às comunicações aos titulares e à ANPD;

III - em qualquer hipótese, confirmada ou não a ocorrência do incidente de segurança com dados pessoais, o(a) Encarregado(a) deverá comunicar o resultado da análise preliminar, em relatórios semestrais, para ciência, ao CLGPD, indicando as providências adotadas e, se for o caso, recomendando ações adicionais.

Art. 9º Nos casos de incidente de segurança com dados pessoais, as unidades técnicas e administrativas envolvidas deverão preservar todos os registros físicos e eletrônicos, logs de acesso, arquivos temporários, imagens de disco, relatórios de sistema e demais artefatos físicos e digitais relacionados ao evento.

§ 1º A preservação das evidências deverá ocorrer imediatamente após a ciência do incidente.

§ 2º O processo de coleta, guarda e manuseio das evidências observará os princípios da integridade, da autenticidade, da rastreabilidade e da confidencialidade, de modo a assegurar sua validade em auditorias, sindicâncias ou comunicações à ANPD.

§ 3º A eliminação ou descarte das evidências digitais somente poderá ocorrer após o encerramento definitivo da apuração e mediante registro formal no processo SEI correspondente.

DA SALA DE SITUAÇÃO

Art. 10. A Sala de Situação será instituída pelo(a) Encarregado(a) e funcionará como comitê de crise ad hoc para a gestão de incidentes de segurança com dados pessoais que acarretem risco ou dano relevante, nos termos do art. 2º, inciso VIII, deste Ato.

Art. 11. A Sala de Situação será coordenada pelo(a) Encarregado(a) e terá a seguinte composição mínima:

I - Chefe da Divisão de Integridade e de Gestão de Riscos;

II - Secretário(a) de Tecnologia da Informação e Comunicação do TST;

III - Secretário(a) de Comunicação Social;

IV - representantes de unidades administrativas ou judiciárias cujos sistemas ou bases de dados tenham sido afetados pelo incidente; e

V - representantes de outras áreas, conforme a necessidade e a natureza do incidente.

Art. 12. Compete à Sala de Situação:

I - aprofundar a investigação para determinar a causa, a extensão e os efeitos do incidente;

II - definir e coordenar a implementação de medidas de remediação e contenção;

III - elaborar a comunicação aos titulares e à ANPD;

IV - produzir relatórios sobre o incidente e a resposta adotada; e

V - recomendar melhorias nos processos, sistemas e controles de segurança para prevenir futuros incidentes.

Art. 13. A Sala de Situação e a DINGER, para o cumprimento de suas atribuições, terão prioridade na requisição de informações, acesso a sistemas, registros de logs e documentos de quaisquer unidades do Tribunal e do CSJT que estejam relacionadas ao incidente.

Parágrafo único. As unidades demandadas deverão responder às solicitações com a máxima urgência, em detrimento de outras demandas não emergenciais, a fim de viabilizar o cumprimento dos prazos legais e regulamentares.

DA COMUNICAÇÃO

Art. 14. Confirmada a ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares, o(a) Encarregado(a) efetuará a comunicação aos titulares no prazo de 3 (três) dias úteis, contados da data da ciência do incidente pelo Controlador, contendo as informações dispostas no art. 9º da Resolução CD/ANPD n.º 15, de 24 de abril de 2024.

Art. 15. A comunicação aos titulares dos dados afetados deverá ocorrer de forma direta e individualizada, caso seja possível identificá-los, pelos meios usualmente utilizados pelo Controlador, tais como telefone, e-mail, mensagem eletrônica ou carta.

§ 1º A comunicação deverá ser realizada em linguagem clara e de fácil compreensão, contendo as informações indicadas no art. 9º da Resolução CD/ANPD n.º 15, de 24 de abril de 2024.

§ 2º Caso a comunicação direta e individualizada mostre-se inviável ou não seja possível identificar, parcial ou integralmente, os titulares afetados,

deverá ser realizada, no prazo e com as informações definidas no art. 9º, da Resolução CD/ANPD n.º 15, de 24 de abril de 2024, pelos meios de divulgação disponíveis, tais como sítio eletrônico, aplicativos, mídias sociais e canais de atendimento ao titular, de modo que permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, três meses.

Art. 16. A comunicação aos titulares poderá ser motivadamente adiada, mediante decisão fundamentada da Sala de Situação, conforme o art. 16 da Resolução CD/ANPD n.º 15/2024, caso sua divulgação imediata possa:

I - comprometer a apuração do incidente ou a adoção de medidas de contenção;

II - incentivar a prática de outros atos lesivos por terceiros contra os sistemas do TST e do CSJT; e

III - comprometer a segurança das redes e dos sistemas de informação.

Parágrafo único. Cessados os motivos que justificaram o adiamento, a comunicação aos titulares deverá ser realizada imediatamente.

Art. 17. Nos casos em que o incidente de segurança com dados pessoais envolver titulares em situação de vulnerabilidade, como crianças, adolescentes, idosos, pessoas com deficiência ou indivíduos com limitações de compreensão, de comunicação ou de acesso a meios digitais, a comunicação deverá ser realizada de forma assistida, preferencialmente com o apoio ou com a intermediação de seus representantes legais, responsáveis, curadores, assegurando a efetiva compreensão das informações e a adoção das medidas cabíveis para a proteção dos dados e dos direitos desses titulares.

Parágrafo único. Sempre que tecnicamente possível, a comunicação deverá ser adaptada ao grau de compreensão do titular vulnerável e feita por meios acessíveis, respeitando as diretrizes de linguagem clara e inclusiva.

Art. 18. Após a comunicação aos titulares, o(a) Encarregado(a) deverá realizar a comunicação completa à ANPD em prazo concomitante de 3 (três) dias úteis, contados da data da ciência do incidente pelo Controlador.

§ 1º Caso não seja possível realizar a comunicação completa à ANPD, deverá ser realizada a comunicação preliminar, no prazo do caput, conforme o § 2º, do art. 6º da Resolução CD/ANPD n.º 15, de 24 de abril de 2024.

§ 2º A comunicação de incidente de segurança com dados pessoais deverá ocorrer por meio de formulário eletrônico disponibilizado pela ANPD.

§ 3º As informações da comunicação preliminar deverão ser complementadas e enviadas à ANPD pelo(a) Encarregado(a), de maneira fundamentada, no prazo de 20 (vinte) dias úteis, a contar da data da comunicação preliminar à ANPD.

Art. 19. Constatada a existência de indícios de atividade criminosa ou risco institucional significativo, o Controlador comunicará:

I - à autoridade policial, para fins de persecução penal;

II - ao Conselho Nacional de Justiça, para ciência e adoção de providências no âmbito da segurança do Poder Judiciário; e

III - ao Ministério Público, para providências cabíveis.

DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 20. O(A) Encarregado(a), com o apoio da DINGER, deverá manter um registro interno no Sistema Eletrônico de Informações (SEI) de todos os incidentes de segurança com dados pessoais ocorridos nos últimos cinco anos, independentemente de terem sido comunicados à ANPD e aos titulares, observando-se a rastreabilidade e os princípios de prestação de contas.

Parágrafo único. O registro de que trata o caput deverá conter, no mínimo, a descrição do incidente, a data da ciência, a natureza e a categoria de dados afetados, o número de titulares afetados, riscos e possíveis danos aos titulares, a forma e o conteúdo da comunicação à ANPD e aos titulares e os motivos da ausência de comunicação, quando for o caso, e será utilizado como subsídio para atualização e elaboração do Relatório de Impacto de Dados Pessoais.

Art. 21. Este Ato e os procedimentos nele descritos serão objeto de revisão periódica pelo Comitê de Proteção de Dados Pessoais, para garantir sua contínua adequação às normas e às melhores práticas de segurança da informação.

Art. 22. Os casos omissos serão resolvidos pela Presidência.

Art. 23. Este Ato entra em vigor na data de sua publicação.

VIEIRA DE MELLO FILHO
Ministro Presidente do Tribunal Superior do Trabalho
e do Conselho Superior da Justiça do Trabalho

ÍNDICE