TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO
Gabinete da Presidência

RESOLUÇÃO GP N. 409, 12 DE DEZEMBRO DE 2025

Altera a Resolução GP n. 134, de 19 de dezembro de 2019, que institui a Política de Segurança da Informação e Comunicação do Tribunal Regional do Trabalho da 3ª Região (POSIC-TRT3).

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 3ª REGIÃO, no uso de suas atribuições legais e regimentais,

RESOLVE:

Art. 1º O Anexo III da Resolução GP n. 134, de 19 de dezembro de 2019, passa a vigorar com a seguinte redação:

ANEXO III
(art. 18 da Resolução GP n. 134, de 19 de dezembro de 2019)

NORMA COMPLEMENTAR N. 3
GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS

1. Objetivos

1.1. Estabelecer diretrizes e definir o Processo de Gestão de Incidentes de Segurança da Informação e Proteção de Dados Pessoais(PGI-DP) no âmbito do Tribunal, em alinhamento com o Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ), do Conselho Nacional de Justiça (CNJ).

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 409, de 12 de dezembro de 2025. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 4374, 17 dez. 2025. Caderno Administrativo, p. 34-36.

1.2. Assegurar a identificação, o registro, a avaliação e a resposta em tempo hábil aos incidentes de segurança, com foco na proteção da disponibilidade, integridade, confidencialidade e autenticidade dos ativos.

1.3. Definir os procedimentos para tratamento de incidentes de segurança que envolvam dados pessoais, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo a avaliação de risco ou dano relevante e a comunicação obrigatória à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares, quando cabível.

2. Referências normativas

2.1. Lei n. 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

2.2. Resolução CD/ANPD n. 15, de 24 de abril de 2024, que aprova o Regulamento de Comunicação de Incidente de Segurança.

2.3. Resolução CNJ n. 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário - ENSEC-PJ.

2.4. Portaria CNJ n. 162, de 10 de junho de 2021, que aprova protocolos e manuais criados pela Resolução CNJ n. 396/2021.

2.5. Ato Conjunto TST.CSJT.GP n. 41, de 25 de julho de 2025, que institui o Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho - PCIC.

3. Conceitos e definições

3.1. Ativos: sistemas de informação, meios de armazenamento, transmissão e processamento, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 409, de 12 de dezembro de 2025. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 4374, 17 dez. 2025. Caderno Administrativo, p. 34-36.

3.2. Risco ou dano relevante: aquele que pode afetar significativamente interesses e direitos fundamentais dos titulares, avaliado conforme os parâmetros estabelecidos na Resolução CD/ANPD n. 15/2024.

3.3. Encarregado de dados: pessoa formalmente indicada pelo Tribunal para atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD, sendo responsável pela avaliação final de risco e pela decisão de notificação externa.

3.4. Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR):equipe técnica responsável pela condução da investigação técnica, contenção, erradicação e recuperação do incidente.

3.5. Comitê de Segurança da Informação e Proteção de Dados (CSIPD): comitê responsável pela governança, deliberação em casos de alta complexidade/crise e supervisão das ações de adequação à LGPD.

4. Escopo

4.1. A gestão de incidentes de segurança da informação abrange eventos confirmados ou suspeitos relacionados ao ambiente, ativos, projetos e processos que suportam o Tribunal, incluindo aqueles que envolvam dados pessoais.

5. Diretrizes

5.1. A gestão de incidentes de segurança da informação visa, primariamente, minimizar o impacto de eventos adversos nos ativos e processos críticos do Tribunal, assegurando que a resposta seja conduzida em tempo hábil, por meio da execução coordenada e documentada das fases de identificação, contenção, erradicação e recuperação.

5.2. O tratamento da informação deve ser realizado de forma a viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, com retorno das operações à normalidade no menor prazo possível.

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 409, de 12 de dezembro de 2025. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 4374, 17 dez. 2025. Caderno Administrativo, p. 34-36.

5.3. O Tribunal efetuará a comunicação inicial do incidente e o envio do relatório final ao Conselho Superior da Justiça do Trabalho (CSJT), conforme definido no Ato conjunto TST.CSJT.GP n. 41/2025.

6. Fases do Processo de Gestão de Incidentes de Segurança da Informação e Proteção de dados

6.1. Descrição geral das fases do processo, que compõem o ciclo de resposta:

6.1.1. Fase 1: detecção e registro:

I - qualquer detecção de evento adverso deve ser imediatamente registrada pela DISI, acionando-se a ETIR, quando necessário; e

II - confirmada a suspeita de envolvimento de dados pessoais, a DISI deverá acionar o CSIPD.

6.1.2. Fase 2: análise, contenção e avaliação de risco:

I - a ETIR conduzirá a investigação técnica para determinar a natureza, categoria e volume de dados afetados e adotará as medidas imediatas para a contenção e erradicação do incidente;

II - o CSIPD realizará a avaliação de risco ou dano relevante aos titulares, com base no relatório técnico da ETIR, conforme os parâmetros da ANPD e do art. 48 da LGPD; e

III - se a avaliação indicar risco ou dano relevante, o incidente será classificado como notificável.

6.1.3. Fase 3: notificação e comunicação:

I - sendo o incidente classificado como notificável, o encarregado deverá comunicá-lo à ANPD, nos termos do Regulamento de Comunicação de Incidente de Segurança; e

II - quando determinado pela avaliação de risco, o encarregado comunicará o incidente aos titulares de dados afetados, assegurando que a mensagem seja feita de forma clara, concisa e transparente e contenha, no mínimo:

a) descrição do incidente: a natureza do incidente e os dados pessoais afetados;

b) medidas adotadas pelo Tribunal: as providências tomadas para a contenção e mitigação do incidente;

c) canais de contato: o contato do encarregado e os canais de atendimento para que o titular possa tirar dúvidas; e

d) recomendações ao titular: medidas que o titular deve adotar para se proteger, como troca de senhas e monitoramento de contas.

6.1.4. Fase 4: encerramento:

I - a DISI elaborará o relatório final do incidente; e

II - o relatório final será submetido ao CSIPD para deliberação sobre as ações de melhoria contínua a serem incorporadas nos planos de resposta e de gestão de riscos do Tribunal.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

DENISE ALVES HORTA
Desembargadora Presidente

Fonte: BRASIL. Tribunal Regional do Trabalho da 3ª Região. Resolução n. 409, de 12 de dezembro de 2025. Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 4374, 17 dez. 2025. Caderno Administrativo, p. 34-36.