Caderno Administrativo
Tribunal Regional do Trabalho da 12ª Região

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

Data da disponibilização: Terça-feira, 12 de Maio de 2026.

Tribunal Regional do Trabalho da 12ª Região Desembargadora Teresa Regina Cotosky Presidente Desembargadora Mirna Uliano Bertoldi Vice-Presidente Desembargador Reinaldo Branco de Moraes Corregedor Regional	Rua Esteves Júnior, 395, Centro, Florianópolis/SC CEP: 88015905 Telefone(s) : (48) 3216-4000

SECRETARIA DE APOIO INSTITUCIONAL

Portaria

Portaria SEAP

Institui o Protocolo Unificado de Prevenção e Gestão de Incidentes Cibernéticos e de Proteção de Dados Pessoais

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO

PORTARIA SEAP N.º 73, DE 11 DE MAIO DE 2026

Institui o Protocolo Unificado de Prevenção e Gestão de Incidentes Cibernéticos e de Proteção de Dados Pessoais no âmbito do Tribunal Regional do Trabalho da 12ª Região.

A **DESEMBARGADORA-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 12ª REGIÃO**, no uso de suas atribuições legais e regimentais;
CONSIDERANDO o disposto nos incisos X e XII do art. 5º da Constituição Federal, que instituem o direito à privacidade;
CONSIDERANDO o disposto na Resolução CNJ n.º 396, de 7 de junho de 2021, que trata da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO a Portaria CNJ n.º 162/2021, que determina a adoção de Protocolo de Prevenção de Incidentes Cibernéticos no âmbito do Poder Judiciário;
CONSIDERANDO o Ato Conjunto TST.CSJT.GP n.º 41/2025, que institui o Processo de Comunicação de Incidentes Cibernéticos na Justiça do Trabalho (PCIC);
CONSIDERANDO a Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD);
CONSIDERANDO a Recomendação CNJ n.º 73, de 20 de agosto de 2020;
CONSIDERANDO a Recomendação CNJ n.º 363, de 12 de janeiro de 2021;
CONSIDERANDO a Portaria PRESI n.º 70/2021, de 25 de março de 2021 do TRT12;
CONSIDERANDO a Resolução CD/ANPD n.º 15, de 24 de abril de 2024;
CONSIDERANDO a Portaria SEAP N.º 149, de 27 de novembro de 2025, que institui a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) no âmbito do Tribunal Regional do Trabalho da 12º Região;

CONSIDERANDO a Portaria SEAP N.º 151, de 27 de novembro de 2025, Institui o Protocolo de Gerenciamento de Crises Cibernéticas no âmbito do Tribunal Regional do Trabalho da 12ª Região;
CONSIDERANDO a necessidade de estabelecer procedimentos claros, céleres e eficazes para a gestão e comunicação de incidentes de segurança com dados pessoais;
CONSIDERANDO a importância de assegurar a transparência, a responsabilização e a proteção dos titulares de dados pessoais;
CONSIDERANDO a necessidade de estabelecer procedimentos céleres para a gestão de incidentes que comprometam a privacidade e a segurança institucional;
CONSIDERANDO a importância de integrar a resposta técnica cibernética com as obrigações de transparência junto à ANPD e aos titulares;,
RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Portaria institui o protocolo unificado para prevenção, detecção, análise, resposta e comunicação de incidentes de segurança da informação, incluindo incidentes que envolvam dados pessoais.
Art. 2º Para fins desta Portaria, adotam-se as seguintes definições:
I. Ciência do incidente: momento em que o Tribunal obtém confirmação razoável da ocorrência de incidente, formalmente registrada no relato oficial à Coordenadoria de Segurança da Informação;
II. Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
III. Dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
IV. Dado pessoal sensível: dado 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;
V. Encarregado(a) de Dados, também chamado de DPO (*Data Protection Officer*): pessoa indicada para atuar como canal de comunicação entre o controlador, os titulares e a Agência Nacional de Proteção de Dados (ANPD);
VI. Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou à infraestrutura computacional, ou ainda evento que viole ou represente ameaça iminente de violação de política de segurança ou de política de uso aceitável para equipamento ou sistema de Tecnologia da Informação. No contexto de proteção de dados, inclui qualquer evento que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais tratados pelo Tribunal;
VII. Incidente de segurança crítico: evento que comprometa a disponibilidade do sistema PJe, envolvam dados pessoais sensíveis ou vazamentos de dados que superem 1.000 dados, bem como aquele que interrompa atividades essenciais ou coloque em risco ativos críticos do TRT12. Incluem-se nesta categoria situações supervenientes que, por sua gravidade ou potencial de dano, sejam assim classificadas pela equipe de gestão de incidentes;
VIII. Titular: pessoa natural a quem se referem os dados pessoais;
IX. Unidade gestora dos dados: unidade responsável por processos que envolvam tratamento de dados, competindo-lhe a gestão administrativa e colaboração na análise de incidentes;
X. Violação de dados pessoais: casos que envolvam a destruição, perda, vazamento, alteração, uso para fins comerciais, acesso indevido ou não autorizado, bem como a divulgação não autorizada ou incompatível com a legislação vigente.

CAPÍTULO II
DA PREVENÇÃO, DETECÇÃO E MONITORAMENTO

Art. 3º Deverão ser adotados controles administrativos e tecnológicos, promovendo ações contínuas de prevenção, controle, capacitação e conscientização com relação à Segurança da Informação e Proteção de Dados.
Art. 4º Qualquer suspeita de incidente de segurança ou violação de dados pessoais deve ser comunicada imediatamente.
§ 1º O público interno deve comunicar os incidentes de segurança mediante abertura de chamado no sistema de registro de demandas de tecnologia da informação, com a descrição detalhada do ocorrido.
§ 2º Na hipótese de o incidente envolver dados pessoais sensíveis ou informações protegidas por sigilo legal, judicial ou profissional, o público interno deverá criar um PROAD sigiloso com informações sobre o vazamento de dados sensíveis, com o assunto “Comunicação de suspeita de incidente de segurança ou violação de dados pessoais”.
§ 3º O público externo deverá comunicar incidentes de segurança da informação e violação de dados via Ouvidoria.
Art. 5º O monitoramento de possíveis incidentes relacionados com a Segurança da Informação, violação dos Dados Pessoais ou Crimes Cibernéticos acontece por meio de supervisão dos canais de comunicação do Tribunal, Ouvidoria, Corregedoria Regional, Processos Administrativos, sistemas de monitoramento de Ativos de Tecnologia da Informação e Comunicação e registros dos sistemas de informática e dos mecanismos de segurança da rede de dados.

CAPÍTULO III
DO REGISTRO E GESTÃO DOS INCIDENTES

Art. 6º O registro e a gestão de incidentes de segurança da informação e violação de dados será realizada por meio do sistema de Gerenciamento de Incidentes de TIC e também do sistema de Processo Administrativo Eletrônico (PROAD) quando houver necessidade de sigilo nas informações.
Art. 7º A Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR) será responsável pela gestão dos incidentes de segurança e de violação de Dados.
Parágrafo Único. A ETIR poderá solicitar apoio multidisciplinar abrangendo as áreas Tribunal Regional do Trabalho da 12ª Região de tecnologia da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, dentre outras necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

CAPÍTULO V
DA CLASSIFICAÇÃO E CRITICIDADE

Art. 8º A criticidade do incidente é apurada de acordo com o que segue:
§ 1º Incidentes que afetam a disponibilidade do sistema PJe e/ou dados pessoais sensíveis sob guarda do TRT12 são classificados como Críticos e devem ser comunicados imediatamente via Sistema de Gestão de Incidentes ou PROAD.
§ 2º Sem prejuízo do disposto no parágrafo anterior, outros incidentes poderão ser classificados como Críticos mediante avaliação discricionária da equipe de gestão de incidentes, considerando a gravidade do impacto, a extensão do dano ou a iminência de risco à continuidade operacional do Tribunal.
Art. 9º Considera-se haver risco ou dano relevante aos titulares de dados quando o incidente afetar dados pessoais sensíveis, dados pessoais de vulneráveis, dados financeiros, ou vazamento autenticação ou em larga escala (superior a 1.000 dados vazados).

CAPÍTULO IV
DO TRATAMENTO

Art. 10. A ETIR (Equipe de Tratamento e Resposta) atuará na gestão, contenção técnica e investigação da causa-raiz.
Art. 11. Sempre que houver violação de dados pessoais, o(a) Encarregado(a) de Dados deve ser envolvido na gestão do incidente.

CAPÍTULO V
DA COMUNICAÇÃO EXTERNA E TRANSPARÊNCIA DOS INCIDENTES DE SEGURANÇA SEM VIOLAÇÃO DE DADOS PESSOAIS

Art. 12. Toda a indisponibilidade no sistema PJe deve ser comunicada no portal do TRT12 na Internet.
Art. 13. O(a) Gestor(a) de Segurança comunicará o incidente ao Subcomitê Nacional de Comunicação e Acompanhamento de Incidentes Cibernéticos da Justiça do Trabalho (SNCAIC-JT) e ao CNJ, detalhando ativos afetados e evidências coletadas.

CAPÍTULO VI
DA COMUNICAÇÃO EXTERNA E TRANSPARÊNCIA DOS INCIDENTES DE SEGURANÇA COM VIOLAÇÃO DE DADOS PESSOAIS

Art. 14. Os incidentes de segurança que possam acarretar risco ou dano relevante aos titulares deverão ser comunicados à Autoridade Nacional de Proteção de Dados – ANPD, e, aos(às) titulares afetados(as), nos termos do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).
Parágrafo único. A comunicação à ANPD deverá ser realizada pelo(a) Encarregado(a) de Dados por meio do sistema eletrônico disponibilizado pela Autoridade.
Art. 15. Quando o incidente envolver dados pessoais que possam acarretar risco ou dano relevante, a comunicação à autoridade nacional e ao titular deverá mencionar, no mínimo:
I - A descrição da natureza e da categoria dos dados pessoais afetados, incluindo a descrição do incidente e sua causa;
II - As informações sobre os(as) titulares envolvidos(as), incluindo o seu número e a discriminação de crianças, adolescentes e idosos, se houver;
III - A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, adotadas antes e após o incidente, observados os segredos comercial e industrial;
IV - Os riscos relacionados ao incidente e os dados do encarregado para contato;
V - Os motivos da demora e a exposição das razões, no caso de a comunicação não ter sido encaminhada tempestivamente (após os três dias úteis); e
VI - As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos, bem como as datas da ocorrência do incidente e de seu conhecimento pelo controlador.
Art. 16. Devem ser observados os seguintes prazos mandatórios após a ciência de incidentes de segurança que envolvem dados pessoais:
I - Até 2 (dois) dias úteis: para conclusão da análise preliminar conjunta;
II - Até 3 (três) dias úteis: para comunicação à ANPD e aos titulares, quando constatado risco ou dano relevante;
III – na hipótese de o Tribunal não dispor de informações completas no prazo previsto no inciso II, a comunicação poderá ser realizada em duas etapas:
a) comunicação preliminar, dentro do prazo estabelecido;
b) comunicação complementar;
IV - As informações poderão ser complementadas, de forma fundamentada, no prazo de até 20 (vinte) dias úteis, contado da data da comunicação preliminar;
V **–** na hipótese de a comunicação não ser realizada no prazo previsto no inciso II, o Tribunal deverá apresentar à Autoridade Nacional de Proteção de Dados – ANPD justificativa fundamentada quanto aos motivos da demora, incluindo, quando for o caso, a impossibilidade de dispor de informações completas no momento da comunicação.
Art. 18. A comunicação aos(as) titulares deve utilizar linguagem simples e, caso a notificação individual seja inviável, o aviso deve permanecer visível nos canais oficiais por, no mínimo, 3 (três) meses.

CAPÍTULO VII
DAS RESPONSABILIDADES

Art. 19. Compete a ETIR: Gerenciar os incidentes, acionar o(a) Encarregado(a) de Dados (DPO) quando o incidente envolver violação dos Dados Pessoais, acionar o protocolo de Crise Cibernética.
Art. 20. Compete ao(à) Encarregado(a) de Dados (DPO): Coordenar a análise, orientar, e quando o caso, encaminhar as comunicações oficiais e acompanhar as providências.
Art. 21. Compete às Unidades Administrativas e Judiciárias do TRT12: Prestar informações para análise técnica e adotar medidas administrativas imediatas.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 22. Todos os incidentes de segurança e proteção de dados devem ter seus registros mantidos por, no mínimo, 5 (cinco) anos, contados a

partir da data de registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

Art. 23. Esta Portaria será revista anualmente para fins de melhoria contínua.

Art. 24. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria SEAP n.º 148, de 27 de novembro de 2025.

TERESA REGINA COTOSKY
Desembargadora do Trabalho-Presidente