Caderno Administrativo
Tribunal Regional do Trabalho da 14ª Região

DIÁRIO ELETRÔNICO DA JUSTIÇA DO TRABALHO

PODER JUDICIÁRIO

REPÚBLICA FEDERATIVA DO BRASIL

Data da disponibilização: Quinta-feira, 19 de Fevereiro de 2026.

Gabinete da Presidência

Portaria

Portaria de Regulamentação

PORTARIA TRT GP Nº 0152, DE 19 DE FEVEREIRO DE 2026.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 14º REGIÃO, no uso de suas atribuições legais e regimentais,
CONSIDERANDO a edição da Portaria GP nº 0581, de 29 de maio de 2024, que instituiu a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 14ª Região;
CONSIDERANDO a necessidade de aprimoramento contínuo da Política de Segurança da Informação, especialmente quanto à padronização de procedimentos relacionados ao gerenciamento de patches e softwares, bem como à implantação de novas soluções e aplicações;
CONSIDERANDO a necessidade de estabelecer diretrizes e padrões para garantir um ambiente informatizado controlado e seguro, de forma a oferecer a informação necessária à prestação jurisdicional com integridade, confidencialidade e disponibilidade;
CONSIDERANDO a Resolução CNJ nº 396, de 07 de junho de 2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
CONSIDERANDO os termos da Resolução CNJ nº 370, de 28 de janeiro de 2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
CONSIDERANDO a necessidade de implementar ações voltadas à adequada observância da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no que se refere à Segurança da Informação;
CONSIDERANDO a aprovação, pelo Comitê de Segurança da Informação, das normas complementares NSI07 – Gerenciamento de Patches e Softwares e NSI08 – Implantação de Novas Soluções e Aplicações, conforme ata de reunião constante do doc. 78 do PROAD nº 28.396/2018, de acordo com as recomendações e providências apontadas pela equipe de auditoria;
CONSIDERANDO o constante dos autos do Processo Administrativo Eletrônico (PROAD) nº 2070/2021,
RESOLVE
Art. 1º Alterar o art. 16 da Portaria GP nº 0581, de 29 de maio de 2024, que passa a vigorar acrescido dos incisos VII e VIII, com a seguinte redação:
VII – NSI07 – Gerenciamento de Patches e Softwares;
VIII – NSI08 – Implantação de Novas Soluções e Aplicações
Art. 2º Ficam incluídos os Anexos VII e VIII à Política de Segurança da Informação instituída pela Portaria GP nº 0581, de 29 de maio de 2024, os

quais passam a integrar o referido ato normativo.
Art. 3º Permanecem inalteradas as demais disposições da Portaria GP nº 0581, de 29 de maio de 2024.
Art. 4º Esta Portaria entra em vigor na data de sua publicação.
Publique-se.
(assinado eletronicamente)
Desembargador ILSON ALVES PEQUENO JUNIOR
Presidente, Gestor de Governança e de Metas e Ordenador de Despesas
do TRT da 14ª Região

Anexos
Anexo 1: Download

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

ILSON ALVES PEQUENO JUNIOR
19/02/2026 15:32

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

ANEXO VII

NSI07 – Gerenciamento de Patches e Softwares

1. Introdução

1.1. Esta norma descreve os requisitos para assegurar a atualização constante dos sistemas operacionais e dos programas de terceiros em todas as estações de trabalho do Tribunal que utilizam sistema operacional windows.

1.2. Os fornecedores disponibilizam regularmente atualizações de recursos, corrigem defeitos e emitem patches de segurança para melhorar o desempenho e eliminar vulnerabilidades de segurança em seus produtos, a implementação eficaz deste documento reduz a probabilidade de comprometimento do sistema devido a vulnerabilidades conhecidas.

1.3. Os patches disponibilizados pelos fornecedores são classificados conforme abaixo:

CLASSIFICAÇÃO	
Classificação de vulnerabilidade do fornecedor	Descrição
Crítico	Alta vulnerabilidade, indicando uma ameaça significativa com potencial para impacto generalizado. Essas vulnerabilidades frequentemente têm uma alta probabilidade de exploração e podem resultar no comprometimento do sistema ou vazamento de dados.
Alto	Vulnerabilidades que representam um risco sério, mas podem ter fatores atenuantes, como dificuldade na exploração ou escopo limitado de impacto. Recomenda-se que as organizações priorizem a aplicação de patches para vulnerabilidades importantes prontamente.
Médio	Média vulnerabilidade, indicando um risco menor em comparação com vulnerabilidades altas e críticas. Embora essas vulnerabilidades possam não representar uma ameaça imediata, é aconselhável abordá-las de maneira oportuna para manter um ambiente seguro.
Baixo	Vulnerabilidades com impacto mínimo. Essas vulnerabilidades geralmente são consideradas menos críticas por terem uma exploração extremamente difícil, e as organizações podem escolher abordá-las com base em suas

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

	políticas específicas de gerenciamento de riscos e recursos

2. Âmbito

2.1. Todas as edições do sistema operacional Windows em uso nas estações de trabalho do Tribunal.

2.2. Todos os softwares de terceiros instalados em estações de trabalho

3. Responsabilidades

3.1. O Chefe da Divisão de Infraestrutura e Serviços é responsável por garantir que o Gerenciamento de Patches e softwares seja cumprido.

3.2. O Chefe da Divisão de Segurança da Informação é responsável por avaliar rotineiramente a conformidade com o Gerenciamento de Patches e softwares e fornecerá orientação a todos os grupos de partes interessadas em relação a questões de segurança e gerenciamento de patches.

3.3. Fornecedores terceirizados são responsáveis por garantir que todo software dentro do escopo que eles administram seja mantido por meio de atualizações e patches regulares de software, antes e durante sua implantação operacional.

4. Inventário, Descoberta e Catálogo de Softwares

4.1. O inventário de hardware e software será realizado automaticamente via Endpoint Central.

4.2. A SETIC manterá catálogo oficial de softwares autorizados.

4.3. A instalação de softwares fora do catálogo dependerá de aprovação formal da SETIC.

4.4. Softwares não autorizados identificados no inventário serão removidos automaticamente ou após notificação ao usuário.

4.5. Sistemas sem licença válida, sem suporte do fabricante ou em fim de vida (EoL) serão descontinuados e removidos da rede. Casos excepcionais serão avaliados e gerenciados pela Divisão de Segurança da Informação

5. Da implantação de novas soluções e aplicações

5.1. A implantação de softwares deverá ser feita exclusivamente via Endpoint Central, utilizando:

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

- Pacotes MSI/EXE com parâmetros silenciosos
- Repositório de Software Centralizado
- Grupos de teste
- Logs de instalação.

5.2. Instalações manuais por usuários sem autorização são proibidas.

6. Atualizações e patches de software

6.1. Atualizações e patches categorizados como de importância média, alta ou crítica serão inicialmente implementados em um grupo seleto de computadores. Após um período de observação de 72 horas, na ausência de incompatibilidades ou outros problemas, estes serão então estendidos a todos os computadores na rede.

6.2. A seleção de computadores para o teste inicial de patches e atualizações será realizada pela Divisão de Infraestrutura. Este grupo deve incluir máquinas de diversos departamentos do tribunal para assegurar uma representação abrangente do ambiente de TI.

6.3. Atualizações e patches que não sejam essenciais para correções de segurança ou vulnerabilidades serão agendados de acordo com um cronograma específico, e não serão aplicados automaticamente.

6.4. Informações sobre datas e detalhes específicos das atualizações e patches, incluindo os softwares e computadores afetados, poderão ser consultadas pela equipe de suporte técnico por meio do portal do Endpoint Central.

6.5. Não havendo impedimento à atualização, os computadores e softwares afetados serão atualizados através do processo definido no item 4.2.

6.6. Em se tratando de grande número de máquinas ou de softwares que requeiram procedimentos especiais na instalação e configuração, será definida estratégia de atualização entre os setores envolvidos.

CLASSIFICAÇÃO	
Classificação de vulnerabilidade do fornecedor	Implantação completa em (dias corridos)
Crítico	14
Alto	14
Médio	21

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

Baixo	28

6.7. Quando a implantação de patches de segurança críticos ou de alto risco dentro de 14 dias não for possível, devem ser aplicados controles de compensação apropriados ou um meio temporário de mitigação para reduzir a exposição enfrentada pelos sistemas de TI do Tribunal.

6.8. Novos sistemas devem ser corrigidos para a linha de base atual acordada antes de entrarem em operação a fim de limitar a introdução de novas ameaças.

6.9. Os servidores devem cumprir os requisitos mínimos recomendados especificados pela Secretaria de TI do Tribunal, que incluem o nível padrão do sistema operacional; pacotes de serviços; hotfixes e níveis de patch. Todas as exceções devem ser documentadas pela Secretaria de TI do Tribunal.

6.10. Os patches da Microsoft estão programados para serem implantados na primeira segunda-feira após a “Patch Tuesday”. Este é o nome não oficial usado para se referir ao dia em que a Microsoft lança seus patches de segurança, o que normalmente ocorre na segunda terça-feira de cada mês.

6.11. Os servidores gerenciados pela Secretaria de TI do Tribunal aplicarão patches regulares de acordo com o cronograma definido pela Secretaria de TI:

6.12. Os sistemas removidos da rede como resultado de patches insuficientes só serão reconectados quando for demonstrado que foram atualizados e não representam mais um risco para a rede do Tribunal.

6.13. Exceções à política de gerenciamento de patches exigem aprovação formal documentada da SETIC.

ANEXO VIII

NSI08 – Implantação de Novas Soluções e Aplicações

1. Do objetivo

1.1. Esta Norma de Segurança da Informação estabelece as diretrizes, responsabilidades e procedimentos relativos à implantação, desenvolvimento, homologação, avaliação de segurança e entrada em produção de novas soluções e aplicações no âmbito do Tribunal Regional do Trabalho da 14ª Região (TRT14).

1.2. A norma visa garantir que todo software ou aplicação seja desenvolvido, avaliado e implantado de forma segura, controlada e alinhada à Política de Segurança da Informação.

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

2. Da abrangência

2.1. Esta norma se aplica a todas as unidades do TRT14, incluindo magistrados, servidores, estagiários, contratados e terceiros que desenvolvam, demandem, mantenham ou implantem soluções tecnológicas.

2.2. Envolve soluções produzidas internamente, adquiridas, customizadas, contratadas ou mantidas por terceiros.

3. Das definições

3.1. Solução ou aplicação – software, sistema, serviço digital, módulo, automação ou artefato tecnológico destinado ao atendimento de necessidades institucionais.

3.2. DDSA – Divisão de Desenvolvimento de Soluções e Aplicações, unidade responsável pelo desenvolvimento de software no âmbito da SETIC.

3.3. DSI – Divisão de Segurança da Informação, responsável pela avaliação técnica de segurança das soluções antes de sua entrada em produção.

3.4. Entrada em produção – disponibilização da solução ou aplicação para uso institucional, em ambiente oficial.

3.5. Processo de Desenvolvimento de Software do Tribunal – conjunto de fases, métodos e práticas aprovadas pelo Tribunal para desenvolvimento, homologação e implantação de soluções.

3.6. Homologação funcional – etapa do processo de desenvolvimento na qual a unidade demandante verifica se a solução atende integralmente aos requisitos de negócio, regras institucionais, usabilidade e fluxos operacionais previamente definidos. A homologação funcional tem por finalidade assegurar que o produto entregue corresponde às necessidades institucionais antes de sua entrada em produção, podendo resultar em aprovação, solicitação de ajustes ou reprovação.

3.7. Homologação Explícita - É o processo formal de validação e aceite de um software, solução ou funcionalidade realizado de maneira documentada e expressa pelo usuário responsável, área requisitante ou equipe de negócio.

3.8. Homologação Implícita - É o aceite tácito, considerado automaticamente quando o usuário responsável ou área demandante não se manifesta dentro do prazo estabelecido após a disponibilização do software ou funcionalidade para homologação.

4. Diretrizes gerais

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

4.1. Todo desenvolvimento de software ou aplicação deverá ser iniciado e conduzido exclusivamente pela CDSA, utilizando obrigatoriamente as metodologias, ferramentas e processos previstos no Processo de Desenvolvimento de Software do Tribunal.

4.2. Nenhuma solução poderá ser implantada sem:

4.2.1. Desenvolvimento pela CDSA, ou justificativa formal para exceção aprovada pela SETIC;

4.2.2. Avaliação de segurança realizada pela Divisão de Segurança da Informação;

4.2.3. Homologação funcional, seja implícita ou explícita, pela unidade demandante;

4.2.4. Aprovação formal da SETIC e do CGTIC para entrada em produção.

4.3. A implantação de softwares externos, adquiridos ou produzidos por terceiros, deverá seguir os mesmos requisitos de avaliação de segurança e homologação, quando possível.

5. Da avaliação de segurança

5.1. Nenhum software ou aplicação poderá entrar em produção sem avaliação técnica da Divisão de Segurança da Informação (DSI).

5.2. A avaliação de segurança compreenderá, no mínimo:

5.2.1. Análise de código-fonte (quando aplicável);

5.2.2. Verificação de dinâmica de vulnerabilidades;

5.2.3. Validação de requisitos mínimos de segurança;

5.3. A DSI poderá solicitar correções obrigatórias antes da liberação da solução.

5.4. Em casos de soluções contratadas ou de terceiros, a unidade responsável deverá fornecer toda documentação técnica necessária para a análise.

6. Da implantação e entrada em produção

6.1. A autorização para entrada em produção será emitida pela SETIC após:

PODER JUDICIÁRIO
JUSTIÇA DO TRABALHO
TRIBUNAL REGIONAL DO TRABALHO DA 14ª REGIÃO
Gabinete da Presidência

PORTARIA GP N.º 0152, DE 19 DE FEVEREIRO DE 2026.

6.1.1. parecer favorável da DSI;

6.1.2. validação técnica de infraestrutura pela Divisão de Infraestrutura e Serviços;

6.2. Qualquer alteração relevante em solução já implantada deverá ser submetida ao mesmo fluxo de avaliação, homologação e aprovação.

7. Da responsabilidade por incidentes de segurança

7.1. Caso a solução não tenha sido produzida diretamente pela CDSA, a Secretaria de Tecnologia da Informação e Comunicação (SETIC):

7.1.1. fica eximida de responsabilidade sobre incidentes de segurança decorrentes do uso da solução;

7.1.2. poderá recomendar a não implantação da solução;

7.1.3. comunicará formalmente aos gestores responsáveis os riscos associados.

7.2. Caberá à unidade demandante assumir as responsabilidades pelos riscos decorrentes da implantação sem avaliação de segurança ou sem participação da CDSA.

8. Da revisão

8.1. Esta norma será revisada sempre que necessário, ou durante o ciclo de revisão da Política de Segurança da Informação.

8.2. As atualizações deverão ser aprovadas pelo Comitê de Segurança da Informação (CSI), conforme previsto na PSI.