Ministério do Trabalho e Emprego
Secretaria-Executiva
Diretoria de Tecnologia da Informação

PORTARIA DTI/MTE Nº 1437, DE 27 DE AGOSTO DE 2025

Estabelece a Norma Operacional de Desenvolvimento Seguro de Softwares no âmbito do Ministério do Trabalho e Emprego - MTE.

O DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DO TRABALHO E EMPREGO , no uso das atribuições que lhe conferem o art. 17, do Decreto nº 11.779, de 13 de novembro de 2023 e na Instrução Normativa nº 1, de 27 de maio de 2020, do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), considerando o disposto na Portaria MTE nº 3.849, de 18 de dezembro de 2023, que institui Sistema de Governança do Ministério do Trabalho e Emprego,

RESOLVE:

Art. 1º Aprovar a Norma Operacional de Desenvolvimento Seguro de Softwares, no âmbito do Ministério do Trabalho e Emprego.

CAPÍTULO I

DO ESCOPO E OBJETIVO

Art. 2º Esta norma tem por objetivo estabelecer diretrizes, diretivas e parâmetros técnicos de segurança no desenvolvimento seguro dos softwares, no âmbito do Ministério do Trabalho e Emprego, conforme princípios e diretrizes da Política de Segurança da Informação do Órgão e na Política Nacional de Segurança da Informação, bem como outras relacionadas ao tema em vigor ou que venham a ser reguladas no ordenamento jurídico para o tema.

Art. 3º Esta norma aplica-se também às unidades da sede e regionais que compõem a infraestrutura de rede, gerenciada pela Diretoria de Tecnologia da Informação - DTI, bem como para servidores públicos, agentes públicos, colaboradores formalmente autorizados pelo Ministério do Trabalho e Emprego -MTE.

Art. 4º As regras gerais para o desenvolvimento seguro de softwares do Órgão estão alinhadas com os princípios e as diretrizes das suas respectivas políticas integrantes do Sistema de Governança, bem como àquelas que venham a ser publicadas que regulem a Administração Pública Federal.

Art. 5º Deverão ser inventariados todos os softwares na rede para que apenas aqueles autorizados sejam instalados e possam ser executados, bem como permita que àqueles não autorizados e não gerenciados sejam encontrados e impedidos de instalação ou execução.

§ 1º Todos os softwares conectados à infraestrutura deverão ser inventariados, com revisões

periódicas desse inventário, de forma a permitir a identificação de qualquer ativo que esteja executando software desnecessário às suas atividades ou que represente potenciais riscos à segurança da plataforma tecnológica do Ministério do Trabalho e Emprego - MTE.

§ 2º Softwares sem suporte devem ser informados neste inventário.

Art. 6º O tratamento destes dados deve estar de acordo com a Lei Geral de Proteção de Dados (LGPD) e demais regulamentações relacionadas, sob pena de responsabilização prevista.

Art. 7º O processo de desenvolvimento de software deverá seguir a metodologia, guias, roteiros de métricas e parâmetros definidos pelo Órgão, bem como SISP e aqueles alinhados aos padrões do Governo Federal.

Parágrafo único. Deverão ser adotadas as medidas de salvaguarda e mitigação de riscos e metodologia para garantir a segurança das informações.

CAPÍTULO II
DAS DEFINIÇÕES

Art. 8º Para os efeitos desta norma, aplicam-se os termos e definições conceituados na Portaria nº 93/GSI/PR, Glossário de Segurança, de 18 de outubro de 2021, na Portaria MTE nº 3.849, de 18 de dezembro de 2023, que institui Sistema de Governança do Ministério do Trabalho e Emprego, bem como outras definições adotadas pela portaria no âmbito do Governo Federal.

I - Apetite ao risco: de acordo com o ISO 73:2009, apetite ao risco é a quantidade e tipo de risco que uma organização está disposta a buscar, manter ou assumir. Refere-se ao grau de exposição a perdas que a organização vê como aceitável, de acordo com seus objetivos e recursos;

II - Tolerância ao risco: define o nível de variação do apetite que a empresa se dispõe a tolerar;

CAPÍTULO III
DOS PRINCÍPIOS

Art. 9º Todos os acessos concedidos aos sistemas do Órgão, bem como outro meio de acesso semelhante serão concedidos obedecendo ao princípio do menor privilégio, conforme disposto em políticas e normas do Sistema de Governança, além das diretrizes do ordenamento jurídico relacionado, em vigor.

Art. 10. Esta norma tem como princípio norteador a garantia da confidencialidade, integridade, disponibilidade, autenticidade e não repúdio dos ativos de informação, bem como da moralidade, ética e da legalidade.

Art. 11. As regras estabelecidas nesta norma estão alinhadas com os princípios e as diretrizes da Política de Segurança da Informação - PSI e Política de Governança de Dados e Sistemas de Informação, ambas do Ministério do Trabalho e Emprego – PGDS, integrantes do seu Sistema de Governança.

CAPÍTULO IV
DA ARQUITETURA E DOS PADRÕES DE DESENVOLVIMENTO DE SISTEMAS

Art. 12. Os sistemas devem ser desenvolvidos unicamente por meio de linguagens de codificação, bibliotecas, frameworks, ferramentas e demais soluções de desenvolvimento previamente aprovadas pela unidade responsável pelas definições de arquitetura de desenvolvimento de software da DTI.

Art. 13. Devem ser adotados repositórios padronizados de armazenamento de dados para o desenvolvimento de sistemas, que permitam minimamente:

I – o controle de versionamento de códigos-fonte e de toda a documentação associada, tais como casos de uso, workflows, casos de testes, diagramas e relatórios; e

II – o versionamento de artefatos de desenvolvimento, tais como arquivos compilados, bibliotecas, contêineres, snapshots, pacotes de instalação, executáveis e binários.

§1º Os repositórios devem ser mantidos de forma centralizada em ambiente controlado, de modo a garantir a confidencialidade, a integridade e a disponibilidade dos códigos e artefatos neles armazenados.

§2º Devem ser mantidos acordos de confidencialidade para desenvolvedores ou demais interessados que necessitem acessar os códigos desenvolvidos ou sob custódia do MTE, mesmo que de forma temporária.

Art. 14. A criação e a aprovação dos modelos de dados para o desenvolvimento dos sistemas, sob incumbência da unidade responsável pela modelagem de dados da DTI, devem contemplar controles efetivos com o intuito de conferir segurança na disponibilização e no processamento dos dados.

Art. 15. Devem ser utilizados recursos de criptografia no desenvolvimento e na implantação de sistemas de informação para assegurar, entre outros:

§1º A confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas em bases de dados ou sistemas de arquivo ou que sejam objeto de transmissão eletrônica.

§2º O não repúdio, como forma de comprovar a ocorrência de um evento ou ação e sua associação à entidade originária.

Art. 16. A identificação da necessidade da utilização de recursos criptográficos deverá ser resultado da análise dos requisitos de segurança da aplicação associada à análise de ameaças.

Parágrafo único. A transmissão eletrônica de credenciais de acesso aos sistemas de informação deverá sempre ser realizada de forma criptografada.

Art. 17. O MTE publicará um procedimento de uso de recursos criptográficos indicando quais são os recursos de criptografia aprovados para utilização, contemplando, ao menos, algoritmos para criptografia simétrica, assimétrica e cálculo de resumos criptográficos (hashes).

§1º Os sistemas podem adotar padrões de criptografia específicos, também previstos no procedimento a que se refere o caput deste, de acordo com as peculiaridades necessárias ao seu processo de desenvolvimento ou por força de legislação que assim o requeira.

§2º O procedimento será revisado anualmente ou quando houver modificação relevante nas tecnologias de criptografia.

Art. 18. Devem ser estabelecidas arquiteturas de referência para as diferentes linguagens de desenvolvimento de sistemas, que incluam os controles mínimos de segurança aplicáveis.

CAPÍTULO V

DOS AMBIENTES DE EXECUÇÃO DOS SISTEMAS

Art. 19. Os sistemas do MTE devem contar com ambientes de execução diferenciados para desenvolvimento, homologação e produção dos sistemas.

Parágrafo único. Sistemas fornecidos por terceiros, com ou sem ônus para o MTE, deverão contar obrigatoriamente com os ambientes de desenvolvimento, homologação e produção.

Art. 20. Os ambientes de desenvolvimento e homologação devem buscar o mais fielmente

possível o ambiente de produção, para fins de redução de vulnerabilidades de segurança, com exceção das características de dimensionamento dos ambientes.

Art. 21. Cabe exclusivamente à unidade responsável pela infraestrutura de TI da DTI o controle sobre o dimensionamento e o acesso aos ambientes de execução dos sistemas de Bancos de Dados de Produção, não devem ser acessados diretamente pela equipe de desenvolvimento.

Art. 22. Os sistemas devem ser devidamente testados e homologados em seus ambientes de execução apropriados, antes da sua liberação para a produção, de acordo com o processo de liberação de sistemas definido pela DTI.

Art. 23. A infraestrutura dos ambientes de execução dos sistemas deve possuir mecanismos que garantam o acesso seguro, observando-se, no mínimo, os seguintes controles:

I – Somente a unidade responsável pela infraestrutura dos ambientes de produção da DTI deve possuir acesso direto aos ambientes de produção dos sistemas, exceto por determinação da DTI, após análise e aprovação de justificativa fundamentada;

II – O acesso aos ambientes de desenvolvimento, testes e homologação é permitido somente à equipe de infraestrutura e à equipe de desenvolvimento do sistema que esteja sendo construído ou testado; e

III – A unidade responsável pela infraestrutura de TI da DTI poderá, após análise, conceder o direito de acesso remoto aos ambientes de desenvolvimento, teste e homologação do sistema aos seus desenvolvedores ou interessados, desde que seja solicitado com as devidas justificativas.

Parágrafo único. Toda e qualquer concessão de permissões de acesso aos ambientes deve ser precedida de assinatura do Termo de Responsabilidade.

CAPÍTULO VI

DO PROJETO DE SISTEMAS

Art. 24. Devem ser especificados os requisitos de segurança relativos ao sistema a ser desenvolvido, quanto a confidencialidade, integridade, disponibilidade, autenticidade, não-repúdio e privacidade dos dados por ele tratados.

§1º Todos os requisitos e especificações devem ser analisados e revisados quanto ao aspecto da segurança da informação, antes e durante a codificação, de acordo com as definições de desenvolvimento seguro aprovadas para cada tecnologia de codificação empregada.

§2º A análise de segurança dos requisitos e especificações do sistema deve direcionar as ações de verificação e testes de segurança necessárias ao longo do processo de desenvolvimento do sistema.

Art. 25. Os sistemas sob responsabilidade do MTE classificados como de criticidade alta devem ser submetidos à análise de riscos, observado o disposto na Portaria, devendo também considerar:

a) O apetite ao risco do MTE;

b) O perfil de risco do MTE;

c) A realização de análise de ameaças; e

d) A avaliação e revisão periódica dos riscos das aplicações.

Art. 26. Os sistemas desenvolvidos por terceiros, em decorrência de demanda formalizada pelo MTE, bem como seus respectivos artefatos e documentações, deverão ser submetidos à verificação de segurança, de acordo com critérios definidos pela unidade responsável pela segurança da informação do MTE.

CAPÍTULO VII

DA CODIFICAÇÃO DOS SISTEMAS

Art. 27. O processo de desenvolvimento de sistemas no âmbito do MTE deverá observar os procedimentos de desenvolvimento seguro, definidos em conjunto pela unidade responsável pela segurança da informação e pelas coordenadorias de desenvolvimento, conforme as tecnologias utilizadas, visando à garantia da confidencialidade, integridade e disponibilidade dos sistemas e de seus dados.

Parágrafo único. Os procedimentos de desenvolvimento seguro serão formalizados e disponibilizados em guias técnicos especializados, publicados pela unidade responsável pela segurança da informação do MTE.

Art. 28. Os procedimentos de codificação segura dos sistemas devem considerar, no mínimo, os seguintes controles de segurança:

I – O desenvolvimento deve ser auxiliado por interfaces, ferramentas ou procedimentos que garantam a codificação segura do sistema;

II – O sistema deve utilizar camada de persistência segura para acesso ao banco de dados, de modo a evitar ataques contra a integridade, a confidencialidade e a disponibilidade dos dados;

III – Os dados de entrada do sistema devem ser submetidos a validação ou sanitização antes da sua inserção na base de dados;

IV – Os dados de saída do sistema devem ser codificados de forma a garantir a integridade e a confidencialidade das informações, quando seus requisitos assim o requererem;

V – A ocorrência de exceções e erros na execução dos sistemas em ambiente de produção deve ser tratada com a apresentação de mensagens de erro na tela dos usuários que não apresentem códigos ou textos que revelem detalhes técnicos sobre os erros. Tais detalhes devem ser apresentados exclusivamente no registro do evento no log do sistema; e

VI – Os sistemas não devem conter senhas, chaves de criptografia, credenciais, endereços de IP ou informações pessoais como CPF, nome, e-mail, título de eleitor ou outros dados sensíveis diretamente escritos em seus códigos fonte.

CAPÍTULO VIII

DO AMBIENTE DE COMPILAÇÃO E IMPLANTAÇÃO DE SOFTWARE

Art. 29. Devem ser definidos e documentados procedimentos de compilação de software de acordo com as linguagens de programação utilizadas.

§1º A definição do processo de compilação deve ser disponibilizada em um local centralizado e acessível às ferramentas e profissionais envolvidos com o processo de desenvolvimento.

§2º As ferramentas utilizadas no processo de compilação devem contar com manutenção ativa de seus fabricantes ou comunidades de desenvolvimento, devem ser configuradas segundo as boas práticas de segurança por eles recomendadas e devem ser submetidas a um processo periódico de aplicação de correções de segurança disponibilizadas, como patches, hotfixes, entre outros métodos.

§3º As ferramentas utilizadas no processo de compilação devem prover mecanismos de verificação de integridade dos artefatos gerados (tais como hashes ou assinaturas).

§4º Verificações de segurança automatizadas devem ser integradas ao processo de implantação de software, tais como a Análise Estática de Código-Fonte (Static Application Security Testing - SAST).

§5º Os resultados das verificações de segurança automatizadas deverão compor os critérios de aceitação para a implantação dos sistemas em ambiente de produção.

Art. 30. Todos os componentes e bibliotecas de terceiros utilizados no desenvolvimento de sistemas do MTE devem ser mantidos em repositório centralizado.

§ 1 º Os componentes e bibliotecas de terceiros devem ser submetidos à verificação de vulnerabilidade periodicamente ou sempre que necessária sua avaliação, de preferência de forma automatizada.

§2º Nos casos em que o componente a ser verificado integra sistema classificado como de alta criticidade, a verificação deve incluir uma análise manual detalhada, para a garantia de uma maior eficácia na realização dos testes.

§3º O processo de desenvolvimento de sistemas deve considerar preferencialmente o uso de bibliotecas já existentes e disponíveis no repositório, com o intuito de se reduzir a ocorrência de possíveis riscos no uso de bibliotecas de terceiros que estejam vulneráveis a ataques.

Art. 31. Devem ser definidos e documentados procedimentos de implantação de software nos ambientes de desenvolvimento, homologação e produção.

§1º A definição do processo de implantação deve ser disponibilizada em um local centralizado e acessível a ferramentas e profissionais envolvidos com o processo de desenvolvimento.

§2º As ferramentas utilizadas no processo de implantação devem contar com manutenção ativa de seus fabricantes ou comunidades de desenvolvimento, devem ser configuradas segundo as boas práticas de segurança recomendadas e devem ser submetidas a um processo periódico de aplicação de correções de segurança para ela disponibilizadas como patches, hotfixes, entre outros métodos.

§3º Os procedimentos de implantação devem ser automatizados em todos os estágios, a fim de eliminar falhas decorrentes de execução manual.

Art. 32. É obrigatória a realização de testes dinâmicos em aplicações (Dynamic Application Security Testing - DAST), bem como de testes de intrusão, observando-se a classificação dos sistemas, de acordo com procedimento definido pela unidade responsável pela segurança da informação do MTE, considerando também os critérios de grau de sigilo, a criticidade das informações tratadas e o processo de modelagem de ameaças adotado pelo MTE, com apoio de ferramentas especializadas e deve contemplar os seguintes controles:

I – Todas as falhas encontradas, bem como as correções e evidências dos testes, devem ser registradas de forma centralizada e reportadas às equipes responsáveis pelo projeto de desenvolvimento e correção;

II – Preferencialmente, deve ser realizada análise de riscos sobre as falhas encontradas e não corrigidas;

III – Adicionalmente, na verificação de segurança de aplicações classificadas como críticas, devem ser realizados testes complementares com técnicas exploratórias sobre os controles de segurança da aplicação, como autenticação, criptografia utilizada, controle de acessos e demais mecanismos de proteção.

CAPÍTULO IX

DA GESTÃO DE IDENTIDADES, AUTENTICAÇÃO E CERTIFICAÇÃO DIGITAL

Art. 33. A autenticação de usuários nos sistemas do MTE deverá ser realizada por meio de soluções padronizadas de gestão de identidades e autenticação, homologadas pela unidade responsável pelas definições de arquitetura de desenvolvimento de software da DTI. É vedado o armazenamento de credenciais oriundas de soluções de autenticação não homologadas. Devem ser obrigatoriamente observadas as disposições da versão mais atualizada da Portaria MTE nº 3.849/2023, quanto às bases de identificação de usuários e aos níveis de autenticação exigidos.

§1º As soluções de gestão de identidades e autenticação devem considerar a implementação de controles de segurança, tais como:

I – uso de autenticação multifator (MFA);

II – suporte a certificação digital e tokens;

III – mecanismos de verificação de robôs (ex: captcha);

IV – gestão de políticas de senhas;

V – gestão de perfis e direitos de acesso;

VI – registro de logs de criação, modificação, exclusão de credenciais e autenticações.

§2º As funcionalidades de autorização de acesso dos usuários aos sistemas devem ser implementadas, preferencialmente, com base em perfis de direitos de acesso, evitando-se atribuições individualizadas.

§3º Os sistemas que demandem acesso externo ao MTE devem contar com controles de segurança adicionais, que complementem o uso de credenciais baseadas em usuário e senha, como a autenticação multifator (MFA) obrigatória ou o uso de certificação digital.

§4º O MTE publicará procedimento contendo a relação das soluções homologadas de gestão de identidades e autenticação, com a indicação dos cenários de uso recomendados.

§5º O procedimento mencionado no parágrafo anterior será revisado anualmente ou sempre que houver atualizações relevantes que justifiquem sua revisão.

§6º As credenciais de acesso aos bancos de dados e aos sistemas devem possuir o menor conjunto de permissões necessário para o desempenho das suas funções, conforme o princípio do menor privilégio.

Art. 34. Os sistemas expostos externamente ao MTE devem ser disponibilizados por meio de mecanismos que garantam a identidade do sistema, assim como a criptografia do tráfego de informações entre o ambiente do MTE e os clientes desses sistemas.

Parágrafo único. Quando utilizados certificados digitais, suas informações devem ser mantidas em repositório seguro controlado, de preferência por meio do uso de solução de gerenciamento centralizada, para fim de gestão de seus ciclos de vida.

CAPÍTULO X

DOS REGISTROS DE LOG DOS SISTEMAS

Art. 35. Os registros de log dos sistemas deverão atender às diretrizes estabelecidas no normativo publicado pelo MTE.

Art. 36. Os projetos de desenvolvimento de sistemas devem prever mecanismos para geração, armazenamento e replicação de logs, conforme definições da unidade responsável pela segurança da informação do MTE. O sistema deverá manter uma base de logs local, com replicação obrigatória para uma base centralizada, observando os critérios estabelecidos pelas áreas técnicas competentes.

Art. 37. Os sistemas desenvolvidos pelo MTE devem gerar registros sobre sua utilização, com especificação de data e hora da ocorrência em milissegundos, tais como:

I – autenticação de usuários, com sucesso ou falha;

II – alteração de perfil do usuário;

III – erros e exceções sem tratamento nos sistemas;

IV – acesso a dados sensíveis para alteração;

V – acesso a dados sensíveis para leitura;

VI – negação de acesso a páginas ou funções;

VII – usuário autenticado executando a ação;

VIII – nome do servidor do sistema (se aplicável);

IX – IP e número da porta de origem da máquina cliente do sistema (se aplicável);

X – tipo da ação; e

XI – tipo de erro.

CAPÍTULO XI
DO CICLO DE VIDA DOS SISTEMAS

Art. 38. Deve ser observado o procedimento para manutenção do ciclo de vida dos sistemas desenvolvidos ou de propriedade do MTE, envolvendo a inclusão de regras para o descarte, descontinuação e transição segura de sistemas e base de dados previstas na Política de Segurança da Informação.

§1º Para fins de transparência e obediência à Política de Gestão da Informação do MTE, o descarte deverá estar previsto na Tabela de Temporalidade, seguindo os trâmites internos de gestão documental para o descarte seguro dos dados e documentos, com registro no Sistema Eletrônico de Informações – SEI e publicação de edital de descarte no portal do MTE.

§2º Qualquer informação orgânica/arquivística armazenada em sistemas, bancos e bases de dados deverá ser avaliada e autorizada pela Comissão Permanente de Avaliação Documental (CPAD) antes do descarte, conforme a Política de Gestão da Informação e de Documentos.

Art. 39. O procedimento para manutenção do ciclo de vida dos sistemas deverá considerar, no mínimo, os seguintes controles:

I – sistemas e respectivas bases de dados que tenham sido substituídos ou classificados como legados deverão ser retirados do ambiente de produção e preservados por meio de procedimento de armazenamento, conforme regras definidas pela DTI na Norma de Gerenciamento de Backup e Restauração de Dados, salvo por motivação legal ou por determinação da Diretoria de Tecnologia da Informação;

II – bases de dados de sistemas legados que não realizem mais transações, mas que ainda exijam disponibilização para consulta, deverão, preferencialmente, ser acessadas por meio de soluções de descoberta e publicação de dados;

III – os ambientes de desenvolvimento e homologação deverão ser desativados quando não houver mais evolução no sistema, quando o sistema for retirado do ambiente de produção, ou mediante solicitação formal do gestor responsável;

IV – as unidades gestoras dos sistemas deverão ser consultadas periodicamente quanto à necessidade de manutenção dos sistemas em produção.

CAPÍTULO XII
DO INVENTÁRIO DE SISTEMAS

Art. 40. Todos os sistemas desenvolvidos internamente ou de propriedade do MTE devem ser claramente identificados e inventariados, contendo informações relevantes para o gerenciamento e manutenção da segurança dos dados institucionais.

§1º. A responsabilidade pela elaboração e atualização do inventário de sistemas é da Coordenação-Geral de Soluções Digitais (CGSOL).

§2º. Compete à Coordenação-Geral de Infraestrutura (CGINFRA) complementar o inventário com os dados técnicos necessários ao seu detalhamento.

Art. 41. Todas as informações sobre os ativos de sistema devem ser reunidas de forma integrada, preferencialmente por meio de base de gerência de ativos centralizada.

Art. 42. O detalhamento de informações no inventário sobre cada ativo de sistema deve contemplar, no mínimo e quando aplicável, os seguintes conjuntos de dados:

I – nome do sistema;

II – classificação do sistema;

III – versão atual do sistema;

IV – abrangência de uso;

V – unidade gestora responsável;

VI – unidade técnica responsável;

VII – data inicial de entrada em produção;

VIII – data de desativação;

IX – endereço de acesso ao sistema nos diversos ambientes (desenvolvimento, homologação e produção);

X – arquitetura de referência;

XI – linguagem de codificação utilizada;

XII – integrações com outros sistemas;

XIII – bases de dados utilizadas; e

XIV – servidores e instâncias hospedeiras.

Parágrafo único. O gerenciamento dos ativos de sistemas deve considerar o disposto no processo de gerenciamento de configuração instituído no MTE, em acordo com Portaria MTE nº 3.849/23.

CAPÍTULO XIII

DISPOSIÇÕES FINAIS

Art. 43. Os casos omissos serão resolvidos pela Diretoria de Tecnologia da Informação.

Art. 44. Esta norma deverá ser periodicamente revisada e atualizada, a cada 12 meses ou sempre que se fizer necessária ou conveniente para o MTE.

Parágrafo único. Os procedimentos técnicos complementares desta norma poderão ser atualizados, sempre que necessário, pela Diretoria de Tecnologia da Informação.

Art. 45. O descumprimento desta portaria deve ser imediatamente registrado como incidente de segurança e comunicado Gestor de Segurança da Informação para apuração e consequente adoção das providências cabíveis.

Art. 46. Esta portaria entra em vigor na data de sua publicação e sua implementação se fará de acordo com os níveis de maturidade acordados com Divisão de Segurança, da Coordenação Geral de Infraestrutura, a contar dessa data.

Art. 47. Ficam revogadas disposições em contrário a esta norma.

Documento assinado eletronicamente

HEBER FIALHO MAIA JUNIOR

Diretor de Tecnologia da Informação

Documento assinado eletronicamente por **Heber Fialho Maia Junior**, **Diretor(a)**, em 27/08/2025, às 16:09, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://processoeletronico.trabalho.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=3&cv=6460119&crc=E25128BE, informando o código verificador **6460119** e o código CRC **E25128BE**.

Referência: Processo nº 19958.206241/2024-65. SEI nº 6460119