PORTARIA TRT 18ª Nº 1623/2024

PODER JUDICIÁRIO DA UNIÃO
TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO
SECRETARIA-GERAL DA PRESIDÊNCIA
COORDENADORIA DE SEGURANÇA DA INFORMAÇÃO

Institui requisitos de segurança para a Gestão de Ativos de Informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

O DESEMBARGADOR-PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 18ª REGIÃO, no uso de suas atribuições legais e regimentais, tendo em vista o que consta do Processo Administrativo-Proad nº 6404/2024,

CONSIDERANDO a Resolução Administrativa TRT 18ª nº 145/2019, que institui a Política de Segurança da Informação do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Portaria TRT 18ª SGP/CSIN nº 3358/2022, que disciplina a adoção dos manuais de referência da Estratégia Nacional de Segurança Cibernética no âmbito do Tribunal Regional do Trabalho da 18ª Região;

CONSIDERANDO a Portaria TRT 18ª GP/SGGOVE nº 435/2021, que aprova o processo "Gerenciamento de Processos de Trabalho" do Tribunal Regional do Trabalho da 18ª Região e dá outras providências;

CONSIDERANDO a Portaria TRT 18ª SGP/SGGOVE nº 641/2023, que define os Processos de Gerenciamento de Serviços de Tecnologia da Informação e Comunicações - TIC no âmbito do Tribunal Regional do Trabalho da 18ª Região,

RESOLVE:

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Esta Portaria institui requisitos de segurança para a gestão de ativos de informação no âmbito do Tribunal Regional do Trabalho da 18ª Região.

§1º Aplica-se o disposto nesta Portaria às atividades do processo de Gerenciamento de Configuração e Ativo de Serviço e aos itens de configuração de hardware e software sob gestão deste Regional.

§2º Os requisitos instituidos neste ato fundamentam-se prioritariamente nas medidas de segurança dos controles 01 e 02 contidas nas publicações do *CIS Critical Security Controls version 8 (CIS - Center for Internet Security - cisecurity.org)*, e referenciadas resumidamente na lista do Anexo I à Portaria TRT 18ª SGP/CSIN nº 3358/2022.

Art. 2º Os objetivos específicos dos requisitos aqui explicitados são:

I - Fomentar o aprimoramento da segurança da informação/cibernética da infraestrutura crítica de TIC, por meio da garantia de que o Tribunal tenha o conhecimento preciso da totalidade dos seus ativos corporativos e softwares que precisam ser monitorados e protegidos e, por conseguinte, para que as equipes gestoras técnicas possam tempestivamente identificar e remover ou remediar aqueles ativos que não estejam autorizados a se conectarem ou a serem carregados/executados na infraestrutura de TIC do órgão;

II - Assegurar que informações de qualidade sobre os inventários de ativos corporativos e softwares do TRT da 18ª Região possam suportar outros processos de gestão de segurança da informação, como Riscos, Identidades e Acessos, Incidentes Cibernéticos e Continuidade dos Serviços Essenciais de TIC.

Art. 3º Para os fins desta Portaria, consideram-se as definições constantes do anexo VIII (Glossário) da Portaria CNJ nº 162/2021, das publicações *CIS Critical Security Controls version 8,* no que couber*,* e as seguintes:

I - ativos corporativos: ativos de propriedade ou não do Tribunal que tenham potencial para armazenar ou processar dados e que se conectem à sua infraestrutura de TIC fisicamente, virtualmente e remotamente e aqueles geridos dentro dos ambientes de nuvem, incluindo dispositivos de usuário final (*desktops* e dispositivos portáteis e móveis, como *smartphones*, *tablets* e *notebooks*), dispositivos de rede, dispositivos não computacionais/IoT ("internet das coisas") e servidores;

II - ativos de software ou software: são códigos/programas e outras informações operacionais usadas em um ativo corporativo; eles podem se apresentar na forma de "aplicativos" ou "sistemas operacionais", estes podendo ser compostos por bibliotecas e serviços; softwares podem ser classificados quanto à propriedade, o custo e a permissão para modificar e redistribuir o código;

III - descoberta passiva: técnicas auxiliadas por ferramentas de TIC para identificar ativos de hardware conectados ou que se conectaram à rede, por meio de escuta e análise do tráfego da rede ou pela leitura de registros feitos por servidores que gerenciam a rede.

IV - descoberta ativa: técnicas auxiliadas por ferramentas de TIC para identificar ativos de hardware conectados à rede, por meio de interação com estes ativos ou com dispositivos que gerenciam a rede;

V - dono do processo: unidade responsável por garantir que um processo seja adequado a um propósito. Suas responsabilidades incluem o patrocínio, desenho, melhoria contínua e a prestação de contas sobre sua execução e desempenho final;

VI - gerente do processo: pessoa responsável pelo gerenciamento operacional de um processo, das atividades do processo de trabalho. Suas responsabilidades incluem o planejamento e coordenação de todas as atividades necessárias para executar, monitorar e relatar informações do processo;

VII - gestor técnico de ativos: indivíduo, grupo de trabalho ou unidade designada para custodiar e gerenciar as funcionalidades e a segurança de um ou mais ativos corporativos ou de software;

VIII - software não suportado: software que não recebe mais atualizações, principalmente melhorias e correções nos aspectos de segurança, por ter chegado ao fim do seu ciclo de vida de manutenção por parte de seu fabricante, seja este privado ou sem fins lucrativos, contratado, garantidor ou licenciador a qualquer título.

Art. 4º Devem ser estabelecidos, mantidos e auditados um inventário dos ativos corporativos e outro de ativos de softwares a fim de atingir os objetivos indicados no art 2º, registrando e controlando o ciclo de vida desses ativos desde sua aquisição, "descoberta" e uso até sua desativação/desfazimento.

CAPÍTULO II
DO INVENTÁRIO E CONTROLE DE ATIVOS CORPORATIVOS

Art. 5º O inventário de ativos corporativos deve:

I - registrar todos os ativos corporativos; e

II - registrar para cada ativo os atributos que informem sobre:

a) a identificação única, quando possível associada ao controle patrimonial do órgão;

b) a localização;

c) a responsabilidade pela gestão técnica;

d) a autorização ou não para conectar à infraestrutura crítica de TIC do Tribunal (quem aprovou, quando aprovou e, em caso de exceção, as medidas de mitigação e aceitação dos riscos residuais); e

e) outras informações que se julgue necessárias para apoiar os demais processos de gestão de serviços de TIC e de gestão de segurança da informação.

Art. 6º Recomenda-se que o estabelecimento, a manutenção e a auditoria do inventário considerem informações provenientes:

I - dos controles contratual e patrimonial;

II - de inspeções físicas dos ativos nos ambientes em que deveriam estar instalados, quando apropriado;

III - de sistemas de gestão de tipos específicos de ativos corporativos, como de desktops, pontos de acesso sem fio, servidores e *endpoints* VoIP (voz sobre *Internet Protocol*) etc.;

IV - de registros de *log* dos servidores de DHCP (*Dynamic Host Configuration Protocol*) ou de ferramentas de gestão de endereço *Internet Protocol*;

V - de realização de descobertas ativas e/ou passivas de ativos conectados ou que se conectaram à rede.

Art. 7º Deve-se utilizar ferramentas de descoberta para identificar ativos corporativos conectados à rede e que não estejam inventariados, visando manter atualizado o inventário e tratar tempestivamente os casos de não autorização.

Parágrafo único. Deve-se:

I - realizar descoberta ativa numa frequência diária ou inferior;

II - realizar descoberta passiva numa frequência semanal ou inferior;

III - decidir por autorizar ou não ativos corporativos identificados nas descobertas realizadas, atualizando o inventário e removendo da rede ou quarentenando ativos não autorizados num prazo máximo de uma semana da descoberta.

Art. 8º A auditoria integral e a correção de eventuais desconformidades identificadas no inventário de ativos corporativos devem ser conduzidas e registradas pelo gerente do processo de Configuração e Ativo de Serviço em intervalos não superiores a um ano.

Art. 9º Para efeito de evolução da maturidade no estabelecimento, manutenção e auditoria do inventário de ativos corporativos, ajustes na especificação do seu escopo poderão ser deliberados pelo Comitê de Segurança da Informação e Proteção de Dados Pessoais.

Art. 10. Ativos corporativos que necessitem de manutenção de fornecedores ou que entrem em fim de vida útil (desativação/desfazimento) deverão retornar para a unidade de tecnologia da informação para que eventuais configurações e dados sensíveis e/ou críticos deles sejam previamente copiados e removidos de forma segura.

CAPÍTULO III
DO INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

Art. 11. O inventário de ativos de software deve:

I - catalogar todos os softwares instalados em ativos corporativos geridos pelo Tribunal, especificamente aplicativos, sistemas operacionais e os componentes de software que nestes estejam registrados (exemplo: pacotes de instalação linux e windows); e

II - para cada software catalogado, registrar atributos que informem sobre:

a) título e/ou nomenclatura padronizada do software;

b) a responsabilidade pela gestão técnica, quando apropriado;

c) a autorização ou não para carregar e executar na infraestrutura crítica de TIC do Tribunal, quando apropriado, conforme processo de homologação e controle de ciclo de vida do software (quem aprovou, quando aprovou, objetivo de negócio a ser atendido e, em caso de exceção, as medidas de mitigação e aceitação dos riscos residuais);

d) controles sobre versões, licenças e suporte, quando disponíveis; e

e) outras informações que se julgue necessárias para apoiar os demais processos de gestão de serviços de TIC e de gestão de segurança da informação.

Art. 12. Deve-se utilizar ferramentas para automatizar a descoberta e documentação do software instalado.

Art. 13. Numa frequência mensal, deve-se decidir sobre homologar ou não softwares recém adquiridos e/ou descobertos e assegurar que softwares não autorizados sejam retirados de uso.

Parágrafo único. Software não suportado e/ou não licenciado, que foi recém descoberto ou que já constava do inventário, em regra, não deve ser autorizado.

CAPÍTULO IV
DAS RESPONSABILIDADES

Art. 14. Compete ao dono do processo assegurar que o processo de Gerenciamento de Configuração e Ativo de Serviço, seus respectivos procedimentos e ferramentas de apoio observem os requisitos instituídos nesta Portaria.

Art. 15. Compete aos gestores técnicos de ativos de corporativos e software auxiliar o gerente do processo na realização das atividades previstas no processo de Gerenciamento de Configuração e Ativo de Serviço, especialmente no que se refere à observância dos requisitos instituídos nesta Portaria.

Art. 16. Compete ao gestor de unidade administrativa a realização de inspeções físicas dos ativos corporativos que deveriam estar instalados nos ambientes de sua unidade, mediante demanda do respectivo gestor técnico de ativo, que apresentará as orientações para a realização da inspeção e prazo de conclusão devidamente justificados.

Art. 17. Compete aos usuários custodiantes de ativos corporativos, (em especial os dispositivos portáteis, móveis e outros que estejam sendo usados fora das instalações do órgão):

I - conectar à rede do Tribunal os dispositivos sobre sua responsabilidade em intervalos não superiores a uma semana, para que estes possam receber as atualizações necessárias ao bom funcionamento e à segurança das informações tratadas pelo Regional;

II - notificar tempestivamente a unidade de tecnologia da informação sobre ocorrência de incidente de segurança envolvendo perda, furto ou roubo de dispositivos sob sua responsabilidade, além de tomar as medidas cabíveis conforme regulação específica sobre o caso.

CAPÍTULO V
DAS DISPOSIÇÕES FINAIS

Art. 18. O prazo estabelecido no inciso III do art. 7º deverá ser observado após um ano da publicação desta Portaria.

Art. 19. A presente Portaria substitui o conteúdo referenciado por outros atos normativos como documento “NO03 - GESTÃO DE ATIVOS DE INFORMAÇÃO”.

Art. 20. Esta Portaria entra em vigor na data de sua publicação, revogando-se a Portaria GP/SGGOVE nº 3894/2019.

Publique-se no Diário Eletrônico da Justiça do Trabalho.

(assinado eletronicamente)
GERALDO RODRIGUES DO NASCIMENTO
Desembargador-Presidente
TRT da 18ª Região