MARCUS AUGUSTO LOSADA MAIA

PORTARIA PRESI N.º 686, DE 27 DE JUNHO DE 2023

Estabelece a Política de Controle de Acesso aos Recursos de Tecnologia da Informação e Comunicação do Tribunal Regional do Trabalho da 8ª Região.

O DESEMBARGADOR PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA OITAVA REGIÃO, no uso de suas atribuições legais e regimentais, e

CONSIDERANDO a dependência crescente dos sistemas de informação nas atividades judiciais e administrativas da Justiça do Trabalho no Pará e Amapá;

CONSIDERANDO a necessidade de garantir a segurança das informações armazenadas nos servidores do Tribunal Regional do Trabalho da 8ª Região;

CONSIDERANDO a necessidade de gerenciar os dados a fim de manter a completude, a precisão, a disponibilidade e a proteção das informações;

CONSIDERANDO que a perda de informações eletrônicas podem significar graves dificuldades administrativas e de prestação jurisdicional ocasionando a paralisação de atividades essenciais do Tribunal;

CONSIDERANDO a Resolução CNJ N.º 370 de 28/01/2021, que estabeleceu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

CONSIDERANDO a Resolução CNJ N.º 396 de 07/06/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ N.º 162 de 10/06/2021, que aprovou Protocolos e Manuais criados pela Resolução CNJ n.º 396/2021;

CONSIDERANDO as seções 9 e 11 da norma ABNT-NBR 27.002/2013, que estabelece diretrizes para definição de Controles de Acesso lógico e físico aos recursos computacionais, com o intuito de proteger o negócio contra perda de dados;

CONSIDERANDO ainda o que consta do PROAD n.º 467/2022,

RESOLVE:

Art. 1.º Estabelecer a Política de Controle de Acesso aos Recursos de Tecnologia da Informação e Comunicação, no âmbito do Tribunal Regional do Trabalho da 8ª Região (TRT8), com o objetivo de estabelecer controles de segurança, resguardando e gerenciando o acesso aos recursos de Tecnologia da Informação.

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 2.º Esta Portaria aplica-se a toda Justiça do Trabalho da 8ª Região e faz parte de um conjunto de normas que atendem a Política de Segurança da Informação deste Tribunal.

Art. 3.º Para o disposto nesta Portaria, consideram-se as definições de termos descritas no Glossário de Segurança da Informação, aprovado pela portaria PRESI N.º 685 de 27/06/2023.

CAPÍTULO II
DO CONTROLE DE ACESSO LÓGICO

Art. 4.º Todo(a) magistrado(a), servidor(a), estagiário(a), menor aprendiz e voluntário(a) que ingressar no TRT8, deve assinar um termo de responsabilidade para ter direito ao acesso às informações e aos recursos de Tecnologia da Informação. Este termo deve ser mantido pela Secretaria de Gestão de Pessoas e armazenado de modo seguro.

Parágrafo único. No caso de prestador(a) de serviço ou fornecedor(a), que necessite acesso às informações ou recursos de Tecnologia da Informação, o(a) gestor(a) do contrato ficará responsável por recolher a assinatura no termo de responsabilidade, a ser arquivado no respectivo processo de contratação.

Art. 5.º Todos os acessos aos ativos de informação devem ser realizados através de registros formais, de inclusão, suspensão, alteração de perfil e exclusão de usuários(as).

Parágrafo único. O controle de acesso lógico deve se basear na segregação de funções seguindo a premissa de que tudo é proibido a menos que expressamente permitido. As permissões devem considerar os princípios da “necessidade de conhecer” e “necessidade de uso”, visando sempre o bom andamento das atividades jurisdicionais.

Art. 6.º A criação de uma nova conta de usuário(a) na rede interna de computadores ocorrerá de forma automática, a partir do registro do vínculo funcional no Sistema de Gestão de Pessoas do Tribunal, e conterá o nome completo, CPF, data de nascimento, lotação, matrícula, cargo, função, foto e e-mail pessoal do(a) usuário(a).

§ 1.º As contas de estagiários(as), menores aprendizes, voluntários(as) e prestadores(as) de serviço devem ficar vinculadas a um grupo específico, controladas e facilmente identificáveis, sendo configuradas para expiração automática a cada 06 (seis) meses. A renovação, se necessária, dar-se-á através da autorização do(a) fiscal do contrato, no caso do(a) prestador(a) de serviço, ou do(a) chefe do setor no caso de estagiário(a), menor aprendiz ou voluntário(a).

§ 2.º Poderá ser permitido o uso da rede local por usuários(as) temporários(as) e externos, com as permissões suficientes e necessárias às execuções de suas atividades, resguardada a segurança das informações acessadas.

§ 3.º No caso de prestador(a) de serviço, a criação da conta de acesso à rede interna de computadores a que se refere o caput do artigo deve ocorrer de forma manual, sob demanda, sendo autorizada e motivada pelo(a) chefe do setor em que o serviço é prestado, a partir de chamado na Central de Serviços.

§ 4.º Aos(As) usuários(as) temporários e externos devem ser aplicadas todas as diretrizes da Política de Segurança da Informação.

Art. 7.º No ato de criação da conta de acesso à rede para magistrados(as), servidores(as), estagiários(as), menores aprendizes e voluntários(as), serão criadas também as contas de acesso ao correio eletrônico e à *intranet*.

§ 1.º Contas de correio eletrônico serão criadas para estagiários(as), menores aprendizes e voluntários(as), visando somente a comunicação interna, com restrição de envio de mensagens a endereços de e-mail que não façam parte do domínio do TRT8.

§ 2.º Não será permitida a criação de contas genéricas de correio eletrônico para as unidades organizacionais, apenas grupos.

Art. 8.º A exclusão da conta de usuário(a) da rede interna de computadores e de correio eletrônico ocorrerá de forma automática a partir do registro do término do vínculo funcional, no

Sistema de Gestão de Pessoas do Tribunal, observada a carência mínima de 30 dias com relação à exclusão dos arquivos de trabalho, armazenados em nuvem e diretamente vinculados ao endereço de e-mail a ser excluído.

§ 1.º No caso de servidores(as) removidos(as) ou cedidos(as) a outros órgãos, os direitos de acesso à conta de usuário(a) de rede e ao correio eletrônico devem ser mantidos.

§ 2.º O(A) magistrado(a), aposentado(a) pelo Tribunal, terá conta no correio eletrônico do TRT da 8ª Região de forma vitalícia.

§ 3.º O(A) servidor(a), após aposentado(a), terá excluída sua conta no correio eletrônico do Tribunal, devendo informar uma conta de e-mail pessoal à Secretaria de Gestão de Pessoas para atualização de seus dados cadastrais, observada a carência mínima de 30 dias com relação à exclusão dos arquivos de trabalho, armazenados em nuvem e diretamente vinculados ao endereço de e-mail a ser excluído.

§ 4.º O(A) chefe do setor no qual prestadores(as) de serviço e voluntários(as) desempenham suas atividades, deve informar à Central de Serviços da SETIN os casos de desligamento, assim que estes ocorrerem.

Art. 9.º A permissão ou revogação de acesso aos documentos do servidor de arquivos ocorrerá de forma automatizada, através de procedimento implementado pela SETIN, de acordo com o cadastro da lotação do(a) usuário(a) mantido pelo setor de Gestão de Pessoas.

Parágrafo único. O acesso de estagiários(as) e menores aprendizes será restrito a uma pasta exclusiva no caso de unidades organizacionais judiciárias e nas demais unidades o acesso é idêntico ao dos(as) demais usuários(as).

Art. 10. A permissão ou revogação de acesso aos Sistemas de Informação deve ser autorizada pelo(a) Proprietário(a) da Informação, mediante registro na Central de Serviços do TRT8, fornecendo todos os dados necessários para a realização do cadastro ou mesmo alteração ou exclusão do acesso, se for o caso.

Art. 11. São responsabilidades do(a) Proprietário(a) da Informação definir o perfil de acesso a ser atribuído a cada usuário(a), determinar as mudanças de perfil que se fizerem necessárias e solicitar o cancelamento do acesso quando este não for mais necessário.

§ 1.º Qualquer autorização de acesso deverá estar de acordo com a Política de Classificação da Informação do Tribunal.

§ 2.º Os(As) usuários(as) criados(as) devem possuir seus perfis definidos no ato do seu cadastramento e tais perfis devem estar de acordo com a função a ser exercida.

§ 3.º Deve ser informado à Central de Serviços o encerramento de atividades, contratos ou acordos para que os direitos de acesso às informações e aos recursos de Tecnologia da Informação sejam removidos.

§ 4.º Caso o Sistema de Informação possua módulo específico para a manutenção e criação de contas, habilitado para uso do(a) Proprietário(a) da Informação, a responsabilidade pela criação e manutenção de contas será deste, devendo zelar pela base de usuários(as) de forma que somente pessoas autorizadas tenham acesso ao sistema.

§ 5.º O(A) Proprietário(a) da Informação deve revisar a cada 06 (seis) meses os direitos de acesso concedidos, ajustando os perfis de acordo com a necessidade de conhecer do(a) usuário(a).

Art. 12. O chamado registrado que originou a solicitação de acesso deverá ser respondido após à conclusão do serviço, com a especificação da liberação do acesso ao ativo da informação, o identificador do(a) usuário(a) e a senha de acesso inicial, juntamente com as instruções para a alteração desta após o primeiro acesso.

Art. 13. Os novos sistemas desenvolvidos pela SETIN devem:

I - possuir log com o registro de acesso dos(as) usuários(as);

II - ser acessados, preferencialmente, via certificado digital. Caso contrário, devem:

a) impedir a transmissão de senhas em texto claro pela rede e armazená-las com criptografia;

b) forçar a utilização de senhas de qualidade, conforme o padrão definido no Art. 24 desta política;

c) forçar a alteração da senha no primeiro acesso ao sistema;

d) forçar mudanças de senha a cada 06 (seis) meses;

e) impedir a repetição das últimas 03 (três) senhas utilizadas.

III - exibir as seguintes informações quando o procedimento de entrada (*logon*) ocorrer com sucesso:

a) data e hora do último *logon* com sucesso;

b) detalhes de qualquer tentativa de *logon* sem sucesso, desde o último procedimento realizado com sucesso.

Art. 14. O desenvolvimento de sistemas e o acesso a IDEs e Frameworks é de competência da Secretaria de Tecnologia da Informação. Qualquer desenvolvimento ou customização de sistema a ser realizado por usuário(a) que não esteja lotado(a) na SETIN deverá seguir o padrão tecnológico do TRT8, ter suas informações armazenadas nos Servidores de Bancos de Dados da SETIN e ser analisado e autorizado por esta Secretaria, a partir de encaminhamento de solicitação formal à Central de Serviços.

Art. 15. Toda solicitação de publicação de sistema na *Internet* deve ser devidamente motivada e encaminhada à SETIN através da Central de Serviços.

§ 1.º Serão considerados aptos para publicação na *Internet* apenas os sistemas que atendam aos requisitos mínimos de segurança da informação e que sejam realmente necessários para o negócio do Tribunal.

§ 2.º Para atender aos requisitos mínimos de segurança da informação o sistema deve:

I - permitir a atualização de segurança das versões das bibliotecas, do servidor *web*, do servidor de aplicação, do SGBD, do sistema operacional, do java e dos navegadores, em casos de vulnerabilidades descobertas;

II - ser acessado via certificado digital de autoridade certificadora válida ou a partir da utilização de senhas de qualidade, conforme o padrão definido no art. 24 desta política;

III - implementar o protocolo HTTPS e regras de autenticação e autorização criptografadas, impedindo o tráfego e o armazenamento de senhas em texto claro;

IV - armazenar dados de identificação do(a) usuário(a) e senha apenas em SGBDs.

V - ter os ativos de informação que o suportam, submetidos à varredura de vulnerabilidades, supervisionada pela Divisão de Riscos e Segurança da Informação.

§ 3.º A SETIN realizará análise sobre a aderência do sistema aos requisitos mínimos de segurança da informação e encaminhará um parecer ao Comitê de Tecnologia da Informação e Comunicação para deliberação e autorização de publicação.

Art. 16. Todos os acessos à rede interna de computadores devem ser registrados para fins de auditoria. Um servidor de *logs* dedicado deve ser implementado pela SETIN.

Art. 17. O *log* de acesso de todos os sistemas desenvolvidos pela SETIN, deve ser armazenado por um período de 01 (um) ano e seus registros devem conter, no mínimo:

I - identificação do(a) usuário(a);

II - datas e horários de entrada (*logon*) e saída do sistema (*logoff*);

III - identificação da estação de trabalho que originou o acesso;

IV - registros das tentativas de acesso (aceitas e rejeitadas) ao sistema;

V - quando for o caso, as informações acerca dos recursos computacionais, aplicativos, arquivos de dados e utilitários utilizados e que tipos de operações foram efetuadas.

Art. 18. As contas de usuário(a) de rede devem:

I - ser bloqueadas ou desativadas caso não sejam utilizadas por um período maior que 06 (seis) meses ou ainda em caso de identificação de comprometimento da segurança da informação;

II - ter uma limitação de 05 (cinco) tentativas de *logon* sem sucesso. Após a quinta tentativa mal sucedida, o sistema deve forçar um tempo de espera de 30 minutos antes de permitir novas tentativas;

II – ter restrição de 3 (três) sessões concorrentes, permitindo que um usuário possa acessar a rede a partir de, no máximo, 3 (três) computadores simultaneamente.

Art. 19. As estações de trabalho devem ser configuradas para ter bloqueio automático de tela em casos de períodos de inatividade iguais ou superiores a 15 minutos. Para restaurar a sessão,

o(a) usuário(a) deverá ser obrigado(a) a fornecer novamente suas credenciais de acesso.

Art. 20. Não haverá criação de contas genéricas para usuários(as), excetuando-se os casos de necessidade justificada e acompanhada de parecer da SETIN acerca da possibilidade de aceitação dos riscos associados.

Parágrafo único. Não devem existir contas duplicadas de acesso para os(as) usuários(as).

Art. 21. As contas de serviço, que fornecem uma solução de identidade única para serviços executados por computadores servidores e/ou sistemas, serão tratadas de forma especial, podendo estar associadas há várias sessões concorrentes e tendo seus prazos de expiração de senha a serem definidos internamente pela SETIN.

Art. 22. Os direitos de acesso privilegiados, como acesso de administradores(as) dos recursos de TI, devem ser identificados e registrados.

§ 1.º O perfil de administrador(a) deve ser concedido à conta específica do(a) usuário(a). Não deve existir uma conta genérica compartilhada de administrador(a).

§ 2.º O registro de conta de acesso com perfil de administrador(a) somente deve ser concedido a usuários(as) da SETIN que necessitem deste perfil no desempenho de suas tarefas na administração dos recursos de TI, excetuando-se os casos de necessidade justificada e acompanhada de parecer da SETIN acerca da possibilidade de aceitação dos riscos associados.

Art. 23. Apenas servidores(as) e estagiários(as) da SETIN, que possuam conta de acesso com perfil de administrador(a), estão autorizados a realizar instalações de *softwares* homologados pela SETIN nas estações de trabalho do Tribunal.

§ 1.º As contas de acesso que não sejam privilegiadas devem ser configuradas de forma que o(a) usuário(a) não consiga realizar instalação de nenhum tipo de *software*.

§ 2.º Deve ser restrito a um número mínimo de usuários(as), confiáveis e autorizados(as), o acesso a editores de desenvolvimento de *software*, compiladores, *softwares* de manutenção, monitoramento e diagnóstico, assim como programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações.

CAPÍTULO III
DO GERENCIAMENTO DE SENHAS

Art. 24. A senha padrão, que é fornecida após a criação da conta de rede, deverá ser alterada pelo(a) usuário(a) no primeiro acesso ao sistema.

Parágrafo único. A senha padrão deve ser única para uma pessoa e não deve ser fácil de ser quebrada por tentativas ou força bruta.

Art. 25. As senhas de acesso à rede, inclusive aquelas relacionadas a acessos privilegiados, devem ter sua validade expirada a cada 06 (seis) meses. Ao final desse prazo o sistema deve solicitar automaticamente a alteração destas, sendo impedido o uso de senhas iguais as 03 (três) últimas utilizadas.

Art. 26. As senhas de acesso à rede e sistemas devem, obrigatoriamente, possuir o mínimo de 08 (oito) caracteres, contendo, pelo menos, três das quatro categorias a seguir:

I - Letras maiúsculas (A-Z);

II - Letras minúsculas (a-z);

III - Números (0-9);

IV - Caracteres não alfabéticos (exemplos:!,$,#,%).

Art. 27. O duplo fator de autenticação deve ser ativado nos sistemas em uso no Tribunal que permitam tal funcionalidade e deve ser requisito exigido na aquisição ou desenvolvimento de novos sistemas.

CAPÍTULO IV
DO ACESSO REMOTO

Art. 28. A Central de Serviços da SETIN pode ter acesso remoto às estações de trabalho dos(as) usuários(as), através de uma conexão à área de trabalho, para solucionar problemas ou incidentes ocorridos, desde que devidamente autorizada.

§ 1.º Para fins de registro e comprovação, a equipe de suporte só poderá realizar acesso remoto, nos casos de chamados técnicos devidamente cadastrados na Central de Serviços da

SETIN.

§ 2.º Antes da realização de qualquer acesso remoto, a Central de Serviços da SETIN deverá entrar em contato com o(a) usuário(a) para comunicar que sua máquina será acessada. Caso não seja possível estabelecer uma comunicação com o(a) usuário(a), o acesso remoto ficará proibido.

Art. 29. Empresas que possuam vínculo contratual com o Tribunal para a prestação de serviços de suporte técnico a sistemas e infraestrutura de Tecnologia da Informação poderão realizar acessos remotos, momentâneos e monitorados, através de uma conexão específica à área de trabalho de máquina servidora de rede ou de estação de trabalho de servidor(a) lotado na SETIN, a fim de efetuarem as configurações necessárias na resolução de demandas técnicas.

§ 1.º Obrigatoriamente, deve ser designado pelo menos um(a) servidor(a) da SETIN a fim de acompanhar todos os procedimentos efetuados pela empresa prestadora do serviço de suporte técnico enquanto durar o acesso remoto.

§ 2.º O acesso remoto deverá ser temporário, controlado pelo(a) servidor(a) responsável pelo acompanhamento do serviço e limitado às necessidades das atividades a serem desempenhadas.

§ 3.º As máquinas servidoras e as estações de trabalho disponibilizadas para o acesso remoto devem estar com seus sistemas operacionais, programas e ferramentas de antivírus atualizados, ficando o(a) servidor(a) designado(a) para o acompanhamento do serviço responsável por observar e garantir estes requisitos.

Art. 30. Magistrados(as), servidores(as), estagiários(as), menores aprendizes e voluntários(as) podem acessar, externamente, máquina servidora de área de trabalho remoto com serviços específicos do TRT8, a partir de acesso, via navegador, à aplicação *web* dedicada, com conexão criptografada e realização de controle de acesso com base na autenticação e autorização dos(as) usuários(as).

Art. 31. O acesso externo à rede de computadores do TRT8 deve ocorrer através de configuração de rede privada virtual e será autorizada somente para servidores(as) da SETIN, e para servidores(as) que necessitem de acesso a sistemas internos, cujo o acesso seja devidamente autorizado pela SETIN, sendo esse acesso restrito aos ativos de informação

constantes na autorização.

§ 1.º O acesso remoto só poderá ocorrer mediante procedimento de autenticação, sendo que as senhas e as informações que trafegam entre uma estação remota externa e a rede do tribunal devem estar criptografadas.

§ 2.º Prestadores(as) de serviço de suporte técnico em tecnologia da informação poderão ter acesso remoto com duração preestabelecida e só será permitido após avaliação e aprovação da SETIN.

§ 3.º O acesso remoto, de que trata o §2º, tanto em suas solicitações quanto em seus cancelamentos, deve ser registrado e encaminhado pelo(a) chefe do setor em que o(a) usuário(a) presta serviço, através da Central de Serviços do Tribunal.

§ 4.º A solicitação do acesso remoto para prestadores(as) de serviços deve conter, no mínimo, as seguintes informações:

I - recursos a serem acessados;

II – justificativa;

III - nome completo, CPF e e-mail profissional de quem realizará o acesso remoto;

IV - identificação da origem do acesso;

V - horário de conexão que o acesso remoto deverá estar disponibilizado;

VI - tempo de validade do acesso remoto.

§ 5.º Terminada a necessidade de utilização do serviço que motivou a solicitação de acesso, a SETIN deve ser imediatamente e formalmente comunicada para que proceda com o cancelamento da respectiva credencial, desabilitando sistemas, portas e recursos utilizados no acesso remoto.

Art. 32. A SETIN deve manter o registro de todos os acessos remotos realizados visando o monitoramento e, se for o caso, averiguação.

§ 1.º É vedada a utilização do acesso remoto para fins não relacionados às atividades do Tribunal.

§ 2.º No caso de evidências de uso irregular dos recursos computacionais, o(a) usuário(a) terá seu acesso remoto bloqueado para averiguação. O(A) usuário(a) infrator(a) será notificado(a) e a ocorrência de transgressão comunicada ao(à) seu(sua) superior(a), estando sujeito a penalidades administrativas e/ou penais, resguardado o direito à ampla defesa.

§ 3.º Os(As) usuários(as) devem manter suas credenciais de acesso remoto em sigilo absoluto sendo responsáveis pela salvaguarda destas, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas.

Art. 33. O(A) usuário(a) que possuir autorização de acesso remoto deve comunicar imediatamente à SETIN qualquer incidente relacionado ao comprometimento da respectiva credencial ou ainda qualquer vulnerabilidade no sistema de acesso.

CAPÍTULO V
DO CONTROLE DE ACESSO FÍSICO

Art. 34. Cópias das chaves das portas de entrada nas dependências da SETIN poderão ficar sob a guarda da segurança institucional do TRT8 para ser usada em casos especiais, motivo de força maior, quando não houver tempo hábil para solicitar acesso à diretoria da SETIN.

Parágrafo único. Somente servidores(as) lotados(as) na Segurança Institucional ou na SETIN podem portar as chaves das portas de entrada.

Art. 35. Estão autorizados a acessar as áreas técnicas (Sala Cofre e *Datacenter)* da SETIN, somente:

I - servidores(as) lotados(as) na SETIN;

II - servidores(as) agentes de segurança institucional;

III - alta administração do Tribunal;

IV - Servidores(as) das unidades organizacionais de manutenção elétrica e predial do Tribunal e prestadores(as) de serviço técnico das empresas mantenedoras dos ambientes.

§ 1.º Pessoas não contempladas nos incisos I, II , III e IV deste artigo só poderão ter acesso se acompanhadas por Servidores(as) da SETIN.

§ 2.º A Sala Cofre deve ter seu acesso físico resguardado com controle por biometria, sendo necessário o registro biométrico prévio do autorizado.

Art. 36. Sistemas de CFTV devem ser implementados nos perímetros de acesso ao *Datacenter* e à Sala Cofre.

Parágrafo único. O tempo de retenção das imagens gravadas pelos sistemas de CFTV deve ser de, no mínimo, 03 (três) meses.

CAPÍTULO VI
DAS RESPONSABILIDADES

Art. 37. Todo(a) aquele(a) que assinar o Termo de Responsabilidade deve:

I - guardar segredo acerca de assuntos classificados como sigilosos dos quais tenha tomado conhecimento;

II - zelar pela proteção dos documentos, materiais, áreas e sistemas de informação sob sua responsabilidade;

III - usar, em estrito interesse e razões de serviço, as máquinas, equipamentos e sistemas colocados à sua disposição para o exercício funcional.

Art. 38. Aos(Às) usuários(as) compete:

I - zelar pelo sigilo de sua senha;

II - zelar pela segurança das informações, fechando as sessões ativas dos sistemas e bloqueando as telas de equipamentos de TI, quando não os estiver utilizando;

III - fazer a alteração da senha em casos indicativos de comprometimento desta;

IV - comunicar imediatamente à SETIN qualquer suspeita de que estejam sendo executados atos em seu nome, por meio de suas credenciais de acesso.

Art. 39. Compete à SETIN implementar as diretrizes estabelecidas e comunicar ao Comitê de Segurança da Informação e Proteção de Dados os incidentes de segurança da informação quando da ocorrência, mediante ao não cumprimento das normas de controle de acesso.

CAPÍTULO VII

DAS DISPOSIÇÕES FINAIS

Art. 40. Os casos de acessos indevidos serão tratados pelo Comitê de Segurança da Informação e Proteção de Dados do Tribunal Regional do Trabalho da 8ª Região.

Art. 41. Fica revogada a Portaria PRESI N.º 353/2018.

Art. 42. Esta Portaria entra em vigor na data de sua publicação no Diário Eletrônico da Justiça do Trabalho.

MARCUS AUGUSTO LOSADA MAIA

Desembargador Presidente