PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 8ª REGIÃO

PUBLICAÇÃO CONSOLIDADA DA PORTARIA PRESI Nº 353, DE 19 DE ABRIL DE 2018, DETERMINADA PELO ART. 3º DA PORTARIA PRESI Nº 990, DE 16 DE OUTUBRO DE 2019

Estabelece a Política de Controle de Acesso aos Recursos de Tecnologia da Informação 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 seção 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.

RESOLVE:

Art. 1º Regulamentar a política de controle de acesso, 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. 2º Esta Resolução 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. 3º Para o disposto nesse ato, considera-se:

I - Acesso remoto: ingresso, por meio de uma rede, aos dados de um computador fisicamente distante da máquina do usuário. Esse acesso permite a visualização da tela do usuário;

II - Ataque por força bruta: consiste em enumerar todos os possíveis candidatos de uma solução e verificar se cada um satisfaz o problema. Tem como objetivo testar combinações palavras de forma consecutiva, e por meio de tentativa e erro descobrir a senha de acesso;

III - Ativos da informação: qualquer dispositivo de *software* ou *hardware* que agrega valor ao negócio e compõe a infraestrutura de rede de dados do Tribunal, assim como também os locais onde se encontram esses dispositivos, Gestão de Pessoas que a eles têm acesso, além dos processos envolvidos na gestão e operacionalização dos ativos de informação;

IV - Central de Serviços: setor responsável pelo ciclo de vida dos chamados técnicos direcionados à Secretaria de Tecnologia da Informação;

V - Classificação: atribuição, pela autoridade competente, de grau de sigilo a dados, informações, documentos, materiais, áreas ou instalações da instituição;

VI - Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso às informações;

VII - Custodiante: aquele que, de alguma forma, zela pelo armazenamento e preservação de informações que estão sob sua custódia para organização e processamento;

VIII - Perfil básico: acesso exclusivo ao Sistema de Abertura de Chamados disponibilizado pela Secretaria de Tecnologia da Informação do TRT8 (SETIN);

IX - Prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que devem receber credencial especial de acesso;

X - Proprietário da Informação: magistrado ou servidor do TRT8 que tenha a guarda das informações produzidas ou que esteja sob responsabilidade do setor onde estão lotados. São responsabilidades do Proprietário da Informação atribuir os níveis de classificação que uma informação requer, reclassificar esta informação quando necessário e autorizar o acesso à informação aos usuários do TRT8;

XI - Quebra de segurança da informação: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;

XII - Rede de telecomunicações: pode ser composta de várias sub-redes, dependendo do tipo de serviço que é provido ao usuário final. As redes de telecomunicações estão sendo aperfeiçoadas para suportar a transmissão de informações com a introdução de novas tecnologias, tanto do lado dos equipamentos da rede (elementos de rede) quanto dos meios de transmissão (redes de transporte) e dos sistemas de operação para gerenciamento de redes de telecomunicações;

XIII - Segregação de funções: pedido, autorização e administração de acessos realizados por pessoas diferentes;

XIV - Sigilo: segredo de conhecimento restrito a pessoas credenciadas; proteção contra revelação não-autorizada;

XV - Termo de responsabilidade: termo assinado pelo usuário comprometendo-se em guardar segredo acerca de assuntos classificados como sigilosos dos quais tenha tomado conhecimento ou tido acesso em razão de seu ofício no TRT8, zelando pela proteção dos documentos, materiais, áreas e sistemas de informação sob sua responsabilidade, e usando, em estrito interesse e razões de serviço, as máquinas, equipamentos e sistemas colocados à sua disposição para o exercício funcional;

XVI - Usuário: magistrado, servidor, prestador de serviço ou

fornecedor do TRT8 que obteve autorização do Proprietário da Informação pela área interessada para acesso aos Ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade e/ou pedido de concessão de acesso.

CAPÍTULO II
DO CONTROLE DE ACESSO LÓGICO

Art. 4° Todo magistrado, servidor e estagiário 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 pelo setor de Gestão de Pessoas e armazenado de modo seguro.

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

Art. 5° Todos os acessos aos ativos de informação devem ser realizados através de solicitações formais de inclusão, suspensão, alteração de perfil e exclusão de usuários.

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° A criação de uma nova conta de acesso à rede de computadores deve ser autorizada e motivada pelo chefe do setor em que o usuário presta serviço e dar-se-á através do Sistema de Abertura de Chamados disponibilizado pela SETIN do TRT8, contendo:

I - nome completo, CPF, lotação e matrícula do usuário;

II - descrição dos exatos serviços de rede que serão necessários;

III - vigência do contrato, no caso de estagiário ou prestador de serviços terceirizados.

§ 1º As contas de estagiários e prestadores 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 fiscal do contrato no caso do prestador de serviço ou do chefe do setor no caso de estagiário.

§ 2º No ato de criação da conta de acesso à rede para magistrados e servidores, serão criadas também as contas de acesso à intranet, com perfil básico, e de correio eletrônico.

§ 3º O setor de Gestão de Pessoas deve informar à Central de Serviços da SETIN, as aposentadorias, vacâncias, exoneração ou redistribuição de magistrados e servidores, assim como o desligamento de estagiários, para as providências de eliminação das respectivas contas de usuários.

§ 4º No caso de servidores removidos ou cedidos a outros órgãos, os direitos de acesso à conta de usuário de rede e ao correio eletrônico devem ser mantidos.

§ 5º O chefe do setor no qual o prestador de serviços e/ou estagiários desempenham suas atividades deve informar à Central de Serviços da SETIN os casos de desligamento, assim que estes ocorrerem.

§ 6º A Secretaria de Tecnologia da Informação disponibilizará conta no sistema de comunicação eletrônica para magistrados, servidores e ex-servidores voluntários.

§ 7º O magistrado, aposentado pelo Tribunal, terá conta no sistema de comunicação eletrônica do TRT da 8ª Região de forma vitalícia;

§ 8º O servidor, após aposentado, terá excluída sua conta no sistema de comunicação eletrônica do Tribunal, devendo informar uma conta de e-mail pessoal à Secretaria de Gestão de Pessoas para atualização de seus dados cadastrais;

§ 9º Não será permitida a criação de contas genéricas de correio eletrônico para as unidades organizacionais, apenas grupos.

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

§ 11 Aos usuários temporários e externos devem ser aplicadas todas as diretrizes da Política de Segurança da Informação.

§ 12 Servidores cedidos ao TRT8, através de convênios, quando não forem detentores de função de confiança ou cargo comissionado, não terão direito a contas de correio eletrônico.

Art. 7º 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 servidor ou magistrado mantido pelo setor de Gestão de Pessoas. No caso de prestadores de serviço e estagiários a permissão deve ser autorizada pelo Proprietário da Informação, mediante registro no Sistema de Abertura de Chamados disponibilizado pela SETIN, fornecendo todos os dados necessários para a realização do cadastro ou mesmo alteração ou exclusão do acesso, se for o caso.

Art. 8º A permissão ou revogação de acesso aos Sistemas de Informação deve ser autorizada pelo Proprietário da Informação, mediante registro no Sistema de Abertura de Chamados disponibilizado pela SETIN, fornecendo todos os dados necessários para a realização do cadastro ou mesmo alteração ou exclusão do acesso, se for o caso.

Art. 9º São responsabilidades do Proprietário da Informação definir o perfil de acesso a ser atribuído a cada usuário, determinar as mudanças de perfil que se fizerem necessárias e solicitar o cancelamento do acesso quando este não for mais necessário.

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

§ 2º Os usuários criados devem possuir seus perfis definidos no ato do seu cadastramento e tal perfil deve estar de acordo com a função a ser exercida.

§ 3º 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.

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

§ 5º O Proprietário 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 usuário.

Art. 10. O chamado registrado que originou a solicitação de acesso deverá ser respondido, após a conclusão do serviço, com a especificação da liberação do acesso ao ativo da informação, o usuário e a senha de acesso inicial, juntamente com as instruções para a alteração desta após o primeiro acesso.

Art. 11. Os novos sistemas desenvolvidos pela SETIN devem:

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

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. 23 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. 11-A Toda solicitação de publicação de sistema na internet deve ser devidamente motivada e encaminhada à SETIN através do Sistema de Abertura de Chamados.

§ 1º 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.

§ 2º 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. 23 desta política;

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

IV - armazenar dados de usuário e senha apenas em SGBDs.

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

§ 4º A necessidade da publicação do sistema na internet para o negócio será avaliada e apreciada pelo Comitê de Governança de Tecnologia da Informação e Comunicação, que encaminhará um parecer à presidência para deliberação.

Art. 12. Todos os acessos à rede de computadores devem ser registrados para fins de auditoria. Um servidor de *logs* dedicado deve ser implementado pela SETIN.

Art. 13. O *log* de acesso de todos os serviços de TI, deve ser

armazenado por um período de 01 (um) ano e seus registros devem conter, no mínimo:

I - identificação do usuário;

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. 14. As contas de usuário 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 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. 15. As estações de trabalho devem ser configuradas para ter bloqueio automático de tela em casos de períodos de inatividade. Para restaurar a sessão, o usuário deverá ser obrigado a fornecer novamente suas credenciais de acesso.

Art. 16. Não haverá criação de contas genéricas para usuários, 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 usuários.

Art. 17. 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. 18. Os direitos de acesso privilegiados, como acesso de administradores dos recursos de TI, devem ser identificados e registrados.

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

§ 2º O registro de conta de acesso com perfil de administrador somente deve ser concedido a usuários 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. 19. Serão instalados no parque computacional do TRT8 somente os *softwares* homologados pela SETIN.

Art. 20. Apenas servidores e estagiários da SETIN, que possuam conta de acesso com perfil de administrador, estão autorizados a realizar instalações de *softwares* em estações de trabalho do Tribunal.

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

§ 2º O acesso a utilitários de segurança, como editores, compiladores, *softwares* de manutenção, monitoramento e diagnóstico, deve ser restrito a um número mínimo de usuários confiáveis e autorizados.

CAPÍTULO III
DO GERENCIAMENTO DE SENHAS

Art. 21. A senha padrão, que é fornecida após a criação da conta de rede, deverá ser alterada pelo usuário 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. 22. As senhas de acesso à rede, inclusive àquelas 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. 23. 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:!,$,#,%).

CAPÍTULO IV
DO ACESSO REMOTO

Art. 24. A Central de Serviços da SETIN pode ter acesso remoto às estações de trabalho dos usuários para solucionar problemas ou incidentes ocorridos, desde que devidamente autorizada.

§ 1º Para fins de registro e comprovação, a equipe de suporte só poderá realizar acesso remoto, nos casos de chamados técnicos devidamente cadastrados no Sistema de Abertura de Chamados disponibilizado pela SETIN.

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

Art. 25. Magistrados e servidores deste Tribunal podem ter permissão de acesso externo a serviços da rede de computadores, remotamente, quando necessário para o desempenho de suas atribuições.

§ 1º A liberação do acesso remoto terá, obrigatoriamente, duração preestabelecida e só será permitida após avaliação e aprovação da SETIN.

§ 2º 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.

§ 3º Magistrados e servidores 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.

§ 4º O usuário 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.

§ 5º É vedada a utilização do acesso remoto para fins não relacionados às atividades do Tribunal.

§ 6º No caso de evidências de uso irregular dos recursos computacionais, o usuário terá seu acesso remoto bloqueado para averiguação. O usuário infrator será notificado e a ocorrência de transgressão comunicado ao seu superior, estando sujeito a penalidades administrativas e/ou penais, resguardado o direito a ampla defesa.

§ 7º 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.

§ 8º Tanto as solicitações de acesso quanto seus cancelamentos devem ser registrados e encaminhados através do Sistema de Abertura de Chamados disponibilizado pela SETIN, pelo chefe do setor em que o usuário presta serviço.

§ 9º A solicitação do acesso remoto deve conter, no mínimo, as seguintes informações:

I - recursos a serem acessados;

II – justificativa;

III - servidor (es) que realizará (ão) 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.

§ 10. A SETIN deve manter o registro de todos os acessos remotos concedidos visando o acompanhamento e, se for o caso, averiguação.

Art. 26. 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 às máquinas servidoras de rede ou às estações de trabalho de servidores lotados na SETIN, a fim de efetuarem as configurações necessárias na resolução de demandas técnicas.

§ 1º Obrigatoriamente, servidores da SETIN deverão acompanhar todos os procedimentos efetuados pela empresa prestadora do serviço de suporte técnico enquanto durar o acesso remoto.

§ 2º O acesso remoto deverá ser temporário, controlado pelo servidor responsável pelo acompanhamento do serviço, e limitado às necessidades da atividade a ser desempenhada.

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

CAPÍTULO V
DO CONTROLE DE ACESSO FÍSICO

Art. 27. Estão autorizados a acessar as dependências da SETIN:

I - magistrados e servidores do Tribunal;

II - estagiários e prestadores de serviço contratados pelo Tribunal.

§ 1º Pessoas não contempladas nos incisos I e II só poderão ter acesso quando devidamente autorizadas por servidores da SETIN ou estiverem acompanhadas por uma pessoa autorizada.

§ 2º As dependências físicas da SETIN devem contar com:

I - recepção e controle de acessos adequados para restringir a entrada apenas a pessoas devidamente autorizadas;

II - sistema de detecção de intrusos e alarmes que cubram todas as portas externas ou janelas acessíveis;

III - proteção externa para janelas nos casos de dependências situadas no andar térreo;

§ 3º O horário ordinário para o acesso será de 8h00 as 15h00.

§ 4º O acesso em horários fora do estabelecido no § 3º deverá ser autorizado pela Diretoria ou Coordenadorias da SETIN, através de documento formal de acordo com as normas internas do TRT da 8ª Região, ressalvada a possibilidade de acesso sem autorização por motivo de força maior.

Art. 28. Estão autorizados a acessar a Sala Cofre e o *Datacenter Backup* da SETIN, somente:

I - servidores lotados na SETIN;

II - servidores agentes de Segurança Institucional;

III - alta administração do Tribunal.

Parágrafo único. Pessoas não contempladas nos incisos I, II e III só poderão ter acesso se acompanhadas por Servidores da SETIN.

Art. 29. Cópias das chaves para a 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 lotados na Segurança Institucional ou na SETIN podem portar as chaves de entrada ou possuir registro que permita o acesso biométrico.

Art. 30. Sistemas de CFTV devem ser implementados nos perímetros de acesso ao *Datacenter Backup* 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. 31. Todo aquele 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. 32. Aos usuários compete:

I - informar à SETIN a confirmação do recebimento do cadastro da conta de acesso;

II - zelar pelo sigilo de sua senha;

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

IV - fazer a alteração da senha em casos indicativos de

comprometimento desta;

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

Art. 33. Compete à SETIN implementar as diretrizes estabelecidas e comunicar ao Comitê Gestor de Segurança da Informação 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. 34. Os casos de acessos indevidos serão tratados pelo Comitê Gestor de Segurança da Informação do Tribunal Regional do Trabalho da 8ª Região.

Art. 35. Fica revogada a Portaria PRESI nº 755/2016.

Art. 36. Esta Portaria entra em vigor na data de sua publicação no Diário Eletrônico da Justiça do Trabalho.

Publique-se, dê-se ciência e cumpra-se

SUZY ELIZABETH CAVALCANTE KOURY
Desembargadora Presidente