PODER JUDICIÁRIO
TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO

PORTARIA Nº 1.063, DE 04 DE MARÇO DE 2016.

Altera os Anexos 1 e 3 da Portaria nº 4.772/2008, a qual institui a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 4ª Região.

A PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 4ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO a revisão das normas integrantes da Política de Segurança da Informação realizada durante o Projeto de implantação do Sistema de Gestão de Segurança da Informação;

CONSIDERANDO os dados constantes do relatório elaborado pela Secretaria de Tecnologia da Informação e Comunicações quanto ao tráfego de acesso à internet no âmbito deste Regional, no período de 21-07-2015 a 21-10-2015 (processo administrativo eletrônico 0003394-28.2013.5.04.0000);

CONSIDERANDO a necessidade de regulamentar o uso da rede sem fio deste Tribunal, a fim de privilegiar o desempenho das atividades precípuas da Justiça do Trabalho, garantir o uso adequado da rede e a disponibilidade do meio de comunicação para desempenho das atividades diárias,

RESOLVE:

Art. 1º Alterar os Anexos 1 (NSI001 – Controle de Acesso à Internet) e 3 (NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso) da Portaria nº 4.772/2008, que passam a vigorar com as redações constantes no Anexo Único desta Portaria.

Art. 2° Ficam revogadas as disposições em contrário.

Art. 3º Republique-se a Portaria nº 4.772/2008, com as alterações ora efetuadas.

Art. 4º Esta Portaria entra em vigor na data de sua publicação.

BETRIZ RENCK
Presidente do TRT da 4ª Região/RS

ANEXO ÚNICO

ANEXO 1

NSI001 – Controle de Acesso à Internet

1. Objetivos

1.1 Estabelecer diretrizes e padrões para o acesso à internet no âmbito do TRT da 4ª Região.

2. Motivações

2.1 Alinhamento às normas, regulamentações e melhores práticas relacionadas à matéria.

2.2 Proteção do ambiente tecnológico do Tribunal.

2.3 Correto direcionamento e dimensionamento de recursos tecnológicos para prover o serviço de acesso à internet.

3. Referências normativas

3.1 Norma Complementar nº 01/IN01/DSIC/GSIPR, de 15.10.2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.2 Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01), de 15.07.2014, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece diretrizes para a implementação de controles de acesso à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

3.3 Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.4 Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Conceitos e definições

4.1 Arquivo de registro de mensagens (*logs*) - registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

4.2 Código malicioso - termo comumente utilizado para genericamente se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel. Tipos específicos de códigos maliciosos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*.

4.3 *Proxy* - também conhecido por filtro de conteúdo, é o servidor responsável por intermediar o acesso à internet, aplicando regras de controle de acesso e mecanismos de proteção contra códigos maliciosos, previamente configurados, e por controlar a alocação de recursos de rede.

4.4 *Proxy* externo - são servidores não administrados pelo TRT4, responsáveis por intermediar o acesso à internet, que não aplicam as regras de controle de acesso e mecanismos de proteção da mesma forma que o proxy administrado pelo TRT4.

4.5 Sítio - É um conjunto de páginas *web* organizadas a partir de um URL básico, onde fica a página principal, e geralmente são armazenadas numa única pasta ou subpastas relacionadas no mesmo diretório de um servidor.

4.6 Situação de contingência - estado ou condição na qual exista a ocorrência de falha/problema, em um ou mais recursos tecnológicos, que reduzam a capacidade dos sistemas e serviços que suportam a atividade da organização.

5. Diretrizes

5.1 O acesso à internet dar-se-á, exclusivamente, pelos meios autorizados, configurados pela Secretaria de Tecnologia da Informação e Comunicações.

5.1.1 É expressamente proibido o uso de proxies externos ou similares.

5.2 O acesso à internet é disponibilizado pelo TRT4 para uso nas atividades relacionadas ao trabalho, observado o disposto nesta norma.

5.3 Constitui acesso indevido à internet qualquer das seguintes ações:

5.3.1 Acessar páginas de conteúdo considerado ofensivo, ilegal, impróprio ou incompatível com as atividades funcionais ou com

a política de segurança da informação, tais como pornografia, pedofilia, racismo, jogos e páginas de distribuição e de compartilhamento de software.

5.3.2 Utilizar programas de troca de mensagens em tempo real (bate-papo) ou programas para troca de conteúdo via rede ponto-a-ponto (*peer-to-peer*), exceto os definidos como ferramenta de trabalho e homologados pela Secretaria de Tecnologia da Informação e Comunicações.

5.3.3 Utilizar programas e/ou acessar páginas de áudio e vídeo em tempo real, ou sob demanda, exceto as definidas como ferramenta de trabalho.

5.3.4 Acessar sítios que representem ameaça de segurança ou que possam comprometer de alguma forma a integridade da rede de computadores do TRT.

5.3.5 Acessar ou fazer download de arquivos não relacionados ao trabalho, em especial músicas, imagens, vídeos, jogos e programas de qualquer tipo.

5.4 O acesso à internet será controlado, de forma automática, pela ferramenta de proxy (filtro de conteúdo), configurada de acordo com os termos desta norma.

5.4.1 A liberação de acesso a sítios e serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do usuário, dependerá de solicitação, devidamente justificada, do magistrado ou gestor da unidade à Secretaria de Tecnologia da Informação e Comunicações, que a submeterá, quando for o caso, ao Comitê de Segurança da Informação, para deliberação.

5.5 Cabe ao gestor da unidade orientar os usuários sob sua responsabilidade a respeito do uso adequado do recurso de internet, conforme as regras estabelecidas nesta norma, bem como reportar ao Escritório de Segurança da Informação ou Comitê de Segurança da Informação o seu descumprimento.

5.6 A critério da Administração, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet, seja em situações normais de funcionamento, seja em situações de contingência, tais como:

5.6.1 Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços; e

5.6.2 Limitação de banda de tráfego de dados.

5.7 As medidas identificadas no item anterior, sempre que implementadas, serão precedidas de comunicação aos usuários interessados.

6. Monitoramento e Auditorias

6.1 Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pelo Escritório de Segurança da Informação.

6.2 Em caso de indícios de descumprimento das diretrizes previstas nesta norma, a chefia imediata ou superior solicitará, justificadamente, ao Comitê de Segurança da Informação a realização de auditoria extraordinária.

6.3 Os relatórios decorrentes das auditorias ordinárias e extraordinárias realizadas pelo Escritório de Segurança da Informação serão encaminhados ao Comitê de Segurança da Informação, para os devidos fins.

7. Atualização da Norma

7.1 O disposto na presente norma será atualizado sempre que alterados os procedimentos de controle de acesso à internet, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.

ANEXO 3

NSI003 – Uso de Recursos de Tecnologia da Informação e Controle de Acesso

1. Objetivos

1.1. Estabelecer diretrizes e padrões para a utilização dos recursos de tecnologia da informação e para o controle de acesso, no âmbito do Tribunal Regional do Trabalho da 4ª Região (TRT4).

2. Motivações

2.1. Alinhamento às normas, regulamentações e melhores práticas, relacionadas à matéria.

2.2. Garantia de que os acessos aos recursos tecnológicos sejam feitos de forma segura e controlada.

2.3. Necessidade de um processo sistemático para gerenciar o uso de recursos de tecnologia da informação, visando garantir a segurança e continuidade das atividades deste Tribunal.

3. Referências normativas

3.1. Norma Complementar 01/IN01/DSIC/GSIPR, de 15 de outubro de 2008, do Departamento de Segurança da Informação e Comunicações da Presidência da República, que estabelece critérios e procedimentos para elaboração, atualização, alteração, aprovação e publicação de normas complementares sobre a Gestão de Segurança da Informação e Comunicações, no âmbito da Administração Pública Federal, direta e indireta.

3.2. Norma Complementar 07/IN01/DISC/GSIPR, de 06 de maio de 2010, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta.

3.3. Norma Complementar 10/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação nos Aspectos Relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.4. Norma Complementar 12/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes para o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

3.5. Norma Complementar 14/IN01/DSIC/GSIPR, de 30 de janeiro de 2012, que estabelece diretrizes relacionadas à Segurança da Informação e Comunicações para o Uso de Computação em Nuvem nos órgãos e entidades da Administração Pública Federal.

3.6. Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

3.7. Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação.

4. Conceitos e definições

4.1. Arquivo de registro de mensagens (*logs*) - registro de eventos relevantes, utilizados para restaurar um sistema, diagnosticar problemas ou realizar auditorias.

4.2. Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.3. Dispositivo móvel: equipamento portátil dotado de capacidade computacional, que permite conexão à rede cabeada ou à rede sem-fio, podendo acessar recursos de rede e internet. São exemplos: *smartphones*, *notebooks* e *tablets*, dentre outros.

4.4. *Malwares*: programas indesejados, desenvolvidos com a finalidade de executar ações danosas e atividades maliciosas em um computador ou sistema (ex.: *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*).

4.5. Proprietário do ativo de informação: pessoa ou outra entidade que tem a responsabilidade (aprovada pela administração) para qualificar o ciclo de vida de um ativo.

4.6. Rede cabeada: corresponde ao acesso aos recursos tecnológicos e à transmissão de dados através da utilização de meios físicos (ativos de distribuição de dados, cabos e pontos de rede).

4.7. Rede lógica: é a rede de dados utilizada pelo Tribunal, abrangendo serviços e sistemas de tecnologia da informação, rede cabeada, rede sem-fio, ativos de distribuição de dados e equipamentos conectados nessa rede.

4.8. Rede sem-fio: também conhecida como rede *wireless* ou *wi-fi*, corresponde ao acesso aos recursos tecnológicos e à transmissão de dados sem a utilização de meios físicos (cabeamento), através da utilização de pontos de acesso sem-fio.

4.9. Remoção de acesso: processo que tem por finalidade remover/excluir definitivamente ou parcialmente determinado(s) acesso(s).

4.10. Solução baseada em nuvem: modelo computacional que permite acesso por demanda e independente da localização a um conjunto compartilhado de recursos configuráveis de computação (rede de computadores, servidores, armazenamento, aplicativos e serviços), provisionados com esforços mínimos de gestão ou interação com o provedor de serviços;

4.11. Usuários: magistrados e servidores ocupantes de cargo efetivo ou em comissão, requisitados e cedidos, e, desde que previamente autorizados, empregados de empresas prestadoras de serviços terceirizados, consultores, estagiários e outras pessoas que se encontrem a serviço da Justiça do Trabalho, utilizando em caráter temporário os recursos tecnológicos do Tribunal Regional do Trabalho da 4ª Região.

5. Uso de Recursos de Tecnologia da Informação

5.1. Diretrizes gerais

5.1.1. O uso adequado dos recursos de tecnologia da informação visa a garantir a continuidade das atividades desenvolvidas neste Tribunal.

5.1.2. Os recursos de tecnologia da informação disponibilizados pelo Tribunal Regional do Trabalho da 4ª Região aos usuários serão utilizados em atividades relacionadas às funções institucionais, e abrangem os seguintes elementos:

I) os computadores servidores, os computadores para uso individual ou coletivo, de qualquer porte, os equipamentos de armazenamento e distribuição de dados, as impressoras, as copiadoras e os equipamentos multifuncionais, assim como os respectivos suprimentos, periféricos e acessórios;

II) a rede lógica do TRT4 e os respectivos canais e pontos de distribuição;

III) as contas de acesso dos usuários, assim como os certificados digitais;

IV) os sistemas computacionais desenvolvidos com base nos recursos providos pelo TRT4;

V) os sistemas computacionais contratados de terceiros, sob licença ou na forma de *software* livre ou aberto, incluídas as soluções baseadas em nuvem.

5.1.3. O usuário é responsável por:

I) zelar pelos recursos que lhe sejam destinados para o exercício de suas atribuições, especialmente os de utilização pessoal, tais como computadores, impressoras, dispositivos móveis e demais equipamentos;

II) preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados;

III) preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários ou terceiros não autorizados;

IV) atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.

5.1.4. Os procedimentos de instalação, configuração e manutenção de equipamentos e softwares serão realizados pela Secretaria de Tecnologia da Informação e Comunicações ou por terceiros por ela autorizados, sob a supervisão do gestor da unidade, que verificará a adequação do serviço realizado ao atendimento das atividades desenvolvidas pela unidade.

5.1.5. Não será fornecido suporte a equipamentos particulares (computadores, *notebooks*, *smartphones* e *tablets*), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo TRT4, seja quanto às questões relacionadas à conexão à rede sem-fio.

5.1.6. Os equipamentos servidores e os computadores para uso individual ou coletivo, de qualquer porte, serão dotados de mecanismos de proteção contra *malwares*.

5.2. Da Rede Lógica

5.2.1. Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do TRT4 terão seus acessos monitorados por questões de segurança e para fins de auditoria.

5.2.2. A cada ponto de acesso à rede de dados do TRT4 poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da Secretaria de Tecnologia da Informação e Comunicações.

5.2.3. É proibida a conexão de qualquer dispositivo não fornecido pelo TRT4 na rede cabeada do Tribunal, sem a prévia anuência da Secretaria de Tecnologia da Informação e Comunicações.

5.2.3.1. A conexão de qualquer equipamento à rede cabeada do TRT4 será feita pela Secretaria de Tecnologia da Informação e Comunicações, ou por terceiros por ela autorizados.

5.2.4. O Tribunal disponibilizará acesso à rede sem-fio para usuários internos e externos.

5.2.4.1. A conexão, para os usuários internos, será feita por meio da credencial (nome de usuário e senha) utilizada para o acesso à rede, e, para os usuários externos, será feita mediante cadastramento prévio em sistema específico do TRT4.

5.2.4.2. É permitida a conexão de dispositivos móveis particulares nas redes sem-fio administradas pelo TRT4.

5.2.4.3. O acesso à internet por meio das redes sem-fio observará as regras dispostas no Anexo 1 – Controle de Acesso à Internet, da Política de Segurança da Informação.

5.2.4.4. Por questões de segurança tecnológica, regras específicas poderão ser implementadas no acesso à internet via rede sem-fio.

5.2.4.5. Poderão ser bloqueados os acessos à rede sem-fio, temporariamente ou por tempo indeterminado, de dispositivos móveis identificados durante o monitoramento como fonte de ações maliciosas, intencionais ou não, ou em que detectadas vulnerabilidades ou problemas de segurança tecnológica.

5.2.5. Cada unidade do TRT4 terá disponível área de armazenamento em rede para salvaguardar os arquivos relacionados ao trabalho desenvolvido, com garantia de integridade, disponibilidade, controle de acesso e cópia de segurança.

5.2.5.1. Os dados armazenados nas estações de trabalho dos usuários não estão contemplados pelas garantias mencionadas nesse item, cabendo aos usuários providenciar eventual cópia de segurança e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

5.2.5.2. É proibido o armazenamento, em qualquer diretório na rede do Tribunal ou nas soluções baseadas em nuvem, de arquivos não relacionados ao trabalho, os quais ficarão sujeitos à exclusão, sem prévio aviso, pela Secretaria de Tecnologia da Informação e Comunicações, tais como:

a) fotos, músicas e filmes de qualquer formato;

b) programas não homologados ou não licenciados;

c) programas de conteúdo prejudicial à segurança do parque computacional deste Tribunal.

5.3. Nuvem corporativa

5.3.1. Ao armazenamento de arquivos na nuvem corporativa aplicam-se as regras previstas no item 5.2.5.2.

5.3.2. Os arquivos armazenados na nuvem corporativa poderão ser compartilhados exclusivamente com outros usuários do TRT4.

5.3.3. É vedado o armazenamento na nuvem corporativa de arquivos para cuja edição o TRT4 disponibilize sistemas próprios, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas.

5.4. Computadores portáteis fornecidos pelo TRT4

5.4.1. O fornecimento de computadores portáteis a magistrados e servidores está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e Recebimento.

5.4.2. Os computadores portáteis possuem instalação padrão desenvolvida pelo TRT4, composta por *softwares* e aplicativos necessários ao desempenho das funções de trabalho, além de *softwares* para proteção, monitoramento e auditoria do equipamento.

5.4.3. Os problemas de *software* serão solucionados pela reinstalação padrão desenvolvida pelo TRT4, que fica desobrigado de reinstalar e configurar programas que o usuário tenha instalado por iniciativa própria e isento da responsabilidade sobre eventual perda de dados.

5.4.4. A instalação, manutenção e suporte de qualquer *software*/sistema não fornecido pelo Tribunal, bem como o backup de dados locais, é de exclusiva responsabilidade do usuário.

5.4.5. Em caso de exoneração, dispensa da função, cedência, remoção, aposentadoria ou término das atividades que ensejaram o fornecimento, o equipamento deve ser devolvido ao TRT, com todos os acessórios que o acompanharam, no prazo de 20 dias.

5.5. Licenças de *software*

5.5.1. As licenças de *softwares*, de qualquer natureza, contratadas ou adquiridas pelo TRT4 são de uso institucional, privativo deste Tribunal.

5.5.2. O Tribunal utilizará, preferencialmente, em suas atividades, *Software* Livre ou de Código Aberto.

5.5.2.1. Fica definida como padrão a suíte de escritório Libre Office desenvolvida pela Associação Civil sem Fins Lucrativos BrOffice.org Projeto Brasil.

5.5.3. É proibida a instalação de *softwares* não licenciados ou não homologados pela Secretaria de Tecnologia da Informação e Comunicações nos equipamentos conectados à rede do Tribunal.

5.5.3.1. A instalação de *softwares* não homologados poderá ser autorizada excepcionalmente pelo Comitê de Segurança da Informação, desde que demonstrada a necessidade de sua utilização para o desempenho das atribuições funcionais do usuário, observadas as condições de segurança e proteção estabelecidas, bem como a compatibilidade e adequação aos recursos computacionais disponibilizados pelo TRT4.

5.5.3.2. As unidades organizacionais do Tribunal poderão encaminhar à Secretaria de Tecnologia da Informação e Comunicações pedido de homologação de *softwares*, para o uso em suas atividades. Homologado o uso, o *software* passará a integrar o padrão utilizado na configuração dos novos equipamentos. Quando necessário, o pedido, acompanhado de parecer técnico, será submetido ao Comitê de Segurança da Informação.

5.6. Serviço de mensagem instantânea

5.6.1. O serviço de mensagem instantânea disponibilizado pelo TRT4 destina-se às comunicações internas.

5.6.1.1. Se necessário à execução das atividades institucionais, poderá ser solicitada à Secretaria de Tecnologia da Informação e Comunicações, com a devida justificativa, a liberação para comunicação externa.

6. Do controle do acesso

6.1. Do gerenciamento de acessos

6.1.1. O acesso à rede, serviços e aos sistemas computacionais disponibilizados pelo TRT4 serão solicitados à Secretaria de Tecnologia da Informação e Comunicações, por meio do sistema de atendimento, em que definidos os níveis de acesso adequados às atividades desenvolvidas.

6.1.2. Incumbe à chefia imediata solicitar à Secretaria de Tecnologia da Informação e Comunicações:

I) os acessos necessários ao desenvolvimento das atividades dos servidores e estagiários vinculados a sua unidade.

II) a alteração dos níveis de acesso ou a remoção do acesso a sistemas concedidos a servidor ou estagiário da unidade, sempre que necessária sua adequação às atividades desenvolvidas.

III) a remoção dos acessos concedidos ao servidor ou estagiário, imediatamente após o afastamento ou desligamento da unidade.

6.1.2.1. Não solicitada a alteração ou exclusão no momento oportuno, a chefia poderá ser responsabilizada pelo acesso indevido do servidor/estagiário a informações da unidade.

6.1.3. A Secretaria de Apoio aos Magistrados informará à Secretaria de Tecnologia da Informação e Comunicações da nomeação e posse de novos magistrados, a fim de agilizar o primeiro cadastro, e será a responsável pela administração dos acessos de magistrados no sistema PJe.

6.1.4. A Secretaria de Tecnologia da Informação e Comunicações comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a Política de Segurança da Informação, em formato eletrônico, para a caixa postal institucional pessoal do usuário, para ciência.

6.1.5. As novas senhas solicitadas serão fornecidas por meio de comunicação eletrônica para a caixa postal institucional da unidade ou caixa postal institucional pessoal do usuário, proibido o fornecimento de senhas por qualquer outro meio, inclusive telefone.

6.1.5.1. É responsabilidade do usuário a alteração da senha inicial fornecida pela Secretaria de Tecnologia da Informação e Comunicações no primeiro acesso realizado.

6.1.6. A Secretaria de Gestão de Pessoas comunicará à Secretaria de Tecnologia da Informação e Comunicações os casos de falecimento e os afastamentos em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, retorno à origem, ou término do estágio de estudantes, para remoção dos acessos concedidos aos usuários.

6.1.6.1. Os usuários aposentados, cedidos e removidos para outros órgãos, terão acesso aos serviços administrativos via extranet.

6.1.7. As solicitações de acessos de prestadores de serviço aos recursos tecnológicos do TRT4 terão caráter temporário e deverão ser acompanhadas da respectiva justificativa, bem como do prazo previsto para a realização das atividades.

6.1.8. O privilégio de administrador na estação de trabalho é restrito aos técnicos de informática que necessitem de acesso privilegiado para o desempenho das atividades funcionais.

6.1.9. Nos computadores portáteis disponibilizados pelo TRT4, também terão privilégio de administrador os magistrados e servidores destinatários dos equipamentos.

6.2. Da conta de rede e respectiva senha para utilização

6.2.1. Para ter acesso aos recursos de tecnologia da informação disponibilizados pelo TRT4 é necessário que o usuário possua uma conta de rede.

6.2.2. A identificação de usuário será composta pela primeira letra do prenome e o último sobrenome do servidor ou magistrado.

6.2.3. Em situações justificadas, poderá ser utilizado outro prenome ou sobrenome para a composição da identificação.

6.2.4. A cada conta de acesso será associada uma senha, de uso pessoal e intransferível.

6.2.5. Na utilização das credenciais de acesso, compete ao usuário observar os procedimentos a seguir indicados, bem como adotar outras medidas de segurança de caráter pessoal, com vista a impedir o uso não autorizado dos recursos de tecnologia da informação a partir de sua conta de acesso:

I) não compartilhar a senha com outras pessoas;

II) não armazenar senhas em local acessível por terceiros;

III) não utilizar senhas de fácil dedução como as que contém nomes próprios e de familiares, datas festivas e sequências numéricas;

IV) ao ausentar-se de sua estação de trabalho, ainda que temporariamente, o usuário deverá encerrar ou bloquear a sessão.

6.2.6. A senha deverá satisfazer os seguintes requisitos de complexidade:

I) não conter nome da conta do usuário (*login*) ou mais de dois caracteres consecutivos de partes de seu nome completo;

II) ter pelo menos seis caracteres;

III) conter caracteres de, no mínimo, três das quatro categorias a seguir:

a) caracteres maiúsculos (A-Z);

b) caracteres minúsculos (a-z);

c) dígitos de base (0 a 9);

d) caracteres não alfabéticos (como !, $, #, %).

6.2.6.1. Excetuam-se da regra do item 6.2.7 os sistemas atualmente disponibilizados que não permitam o atendimento aos requisitos estabelecidos.

6.2.7. A senha deverá ser alterada com uma periodicidade mínima de 1 (um) dia e máxima de 180 (cento e oitenta) dias desde a última modificação.

6.2.8. A conta do usuário será bloqueada após 10 tentativas consecutivas de acesso não reconhecidas, considerando também as tentativas inválidas de acesso à rede sem-fio.

6.2.9. Em caso de suspeita de comprometimento da senha ou de outro recurso de autenticação, o usuário comunicará imediatamente ao Escritório de Segurança da Informação, que poderá, como medida preventiva, suspender temporariamente o acesso.

7. **Registros (*log*) de Eventos**

7.1. Serão mantidos, por um período mínimo de três (3) meses, os registros dos acessos dos usuários aos recursos tecnológicos disponibilizados pelo TRT4, inclusive para fins de apuração e comprovação de incidentes de segurança.

7.2. Serão registrados os seguintes dados:

I) identificação de usuário de quem efetuou o acesso;

II) data e hora de entrada e saída do sistema;

III) origem do acesso;

IV) erros ou falhas de conexão e acesso;

V) troca de senhas de Serviços de Infraestrutura de TI;

VI) outras informações que venham a ser necessárias para os controles de segurança.

8. Atualização da Norma

8.1. As diretrizes previstas na presente norma serão atualizadas sempre que alterados os procedimentos de uso de recursos de tecnologia da informação e de controle de acesso, observada, ainda, a periodicidade prevista para a revisão da Política de Segurança da Informação.