PODER JUDICIÁRIO FEDERAL
TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO

ATO TRT7.GP Nº 65/2020

Institui a Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 7ª REGIÃO, no uso de suas atribuições legais e regimentais,

CONSIDERANDO as boas práticas para seleção e implementação de controles de segurança da informação, especialmente a Norma ABNT NBR ISO/IEC 27002;

CONSIDERANDO a necessidade de disciplinar o controle de acesso e a utilização dos recursos de Tecnologia da Informação, visando prevenir o comprometimento de equipamentos, sistemas de informação, dados e a interrupção das atividades do TRT da 7ª Região;

CONSIDERANDO que o Ato n. 195/2011 desta Corte instituiu a norma de segurança dos recursos de tecnologia da informação, no âmbito do Tribunal Regional do Trabalho da 7ª Região;

CONSIDERANDO que o Ato n. 228/2013 desta Corte aprovou a norma complementar 02/NC/STI, que dispõe sobre a utilização dos recursos de tecnologia da informação no âmbito do Tribunal Regional do Trabalho da 7ª Região;

CONSIDERANDO que o Ato n. 231/2013 desta Corte aprovou a norma complementar 05/NC/STI, que dispõe sobre o controle de acesso aos recursos de tecnologia da informação no âmbito do Tribunal Regional do Trabalho da 7ª Região;

CONSIDERANDO que esses normativos possuem forte interdependência;

CONSIDERANDO a necessidade de revisão periódica das normas de segurança, nos termos do Art. 24 do Ato n. 195/2011 em conjunto com o Art. 21 da Resolução TRT7 n. 278/2017,

Fonte: Diário Eletrônico da Justiça do Trabalho, Brasília, DF, n. 2989, 08 jun. 2020. Caderno Administrativo do Tribunal Regional do Trabalho da 7ª Região, p.1.

RESOLVE:

Art. 1º Instituir Norma de Controle de Acesso e Utilização dos Recursos de Tecnologia da Informação e Comunicação, na forma do anexo, para observância e aplicação em todo o Regional.

Art. 2º Revogar os Atos nºs 195/2011, 228/2013 e 231/2013.

Art. 3º Este ato entra em vigor na data de sua publicação.

Fortaleza, 04 de junho de 2020.
Plauto Carneiro Porto
Presidente do Tribunal

ANEXO

1 OBJETIVO

1.1 Disciplinar o acesso e utilização dos recursos de Tecnologia da Informação, visando prevenir o comprometimento de equipamentos, sistemas de informação, dados e a interrupção das atividades do TRT da 7ª Região.

2 OBJETIVOS ESPECÍFICOS

2.1 Estabelecer a política de uso aceitável de equipamentos de informática, da rede corporativa, do correio eletrônico, do serviço de comunicação instantânea, da nuvem corporativa, dos sistemas de informação e programas de computador, do acesso à *internet*, do acesso remoto, dos dispositivos móveis, de mídias removíveis e das redes sociais.

2.2 Prevenir danos potenciais decorrentes da instalação ou uso de programas inadequados e reduzir o risco de disseminação de programas nocivos de computador a partir das estações de trabalho e de dispositivos móveis.

2.3 Limitar o acesso aos recursos computacionais, bem como prevenir as perdas, danos, furto, roubo ou comprometimento dos recursos computacionais e a interrupção das atividades do Tribunal Regional do Trabalho da 7ª Região.

2.4 Disciplinar o uso de equipamentos pessoais no âmbito da rede corporativa do TRT da 7ª Região, inclusive quanto ao teletrabalho.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

3.1 Resolução Administrativa TRT7 n. 278/2017, Art. 6º, Inciso VIII, que determina como diretriz a expedição de norma complementar para uso de recursos de TIC e controle de acesso.

3.2 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.

3.3 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.

3.4 Norma Complementar 15/IN01/DSIC/GSIPR, de 11 de junho de 2012, que estabelece diretrizes para o uso seguro das redes sociais na Administração Pública Federal.

3.5 Cobit 5 – Gerenciar Serviços de Segurança (DSS05): proteger contra *malware*, gerenciar segurança de rede e conectividade, segurança de endpoints, gerenciar identidade e acesso lógico dos usuários, gerenciar acesso físico a ativos de TI, gerenciar documentos e dispositivos de saída sensíveis, monitorar infraestrutura quanto a eventos relacionados a segurança.

3.6 ABNT NBR ISO/IEC 27002:2013, Código de prática para a gestão de segurança de informação, que estabelece:

3.6.1 “Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios.” (capítulo 9).

3.6.2 Uso aceitável dos ativos (tópico 8.1.3).

3.6.3 Dispositivos móveis e teletrabalho (tópico 6.2).

3.6.4 Restrições sobre o uso e instalação de *software* (tópico 12.6.2).

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições, em adição aos presentes na Resolução TRT7 n. 278/2017:

4.1 Usuários: Magistrados e Servidores ocupantes de cargo efetivo ou em comissão deste Regional, servidores cedidos ou permutados para o TRT7 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 os recursos tecnológicos deste Regional em caráter temporário.

4.2 Acesso – ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de TI do Tribunal.

4.3 Controle de acesso – conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou excluir acesso aos recursos de TIC.

4.4 Necessidade de conhecer – condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de TI.

4.5 Perfil de acesso – conjunto de atributos de cada usuário, definidos previamente como necessários para credencial de acesso.

4.6 Credenciamento – processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

4.7 Credenciais ou contas de acesso – permissões, concedidas por autoridade competente após o processo de credenciamento, que habilita determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário (*login*) e senha.

4.8 Autorização: processo realizado mediante credencial de acesso que garante o acesso ao recurso.

4.9 *Login*: identificador único de usuário para acesso a sistemas computacionais, exprimindo-se pela matrícula, nome ou combinação dos dados dos usuários.

4.10 Mecanismo de Autenticação: ocorre quando as credenciais de acesso de um determinado usuário são validadas por um sistema, sendo possível a utilização de combinação de credenciais.

4.11 Assinatura digital: método de autenticação de informação digital, legalmente considerada como análoga à assinatura física em papel, constituído de código criado com o uso de certificado digital, de modo que a pessoa ou entidade destinatária da mensagem contendo este código possa identificar o remetente e verificar a integridade da mensagem.

4.12 Certificado digital: credencial emitida por autoridade certificadora, que no país é a ICP-Brasil, responsável pela emissão de certificados digitais com validade legal, pode ser armazenado em computador ou mídia eletrônica, contendo dados pessoais e/ou institucionais, sendo utilizado como assinatura digital para comprovação de identidade e verificação de integridade de mensagens ou transações virtuais.

4.13 Consumíveis: Cartuchos de tonalizador, unidades fusoras e cilindros de imagem para impressoras a laser, cartuchos para impressoras a jato de tinta, fitas magnéticas de *backup*, mídias CD/DVD, bobinas para impressoras térmicas e laser, baterias.

4.14 Comunicação Instantânea: serviço de mensagens instantâneas que possibilita comunicação em tempo real entre usuários.

4.15 Dispositivos móveis: equipamentos e periféricos que possam ser transportados com conteúdo e acessíveis em qualquer lugar, como *notebooks*, celulares com acesso a redes de computadores e dispositivos de armazenamento portáteis, *smartphones*, câmeras digitais, *pendrives*, tocadores de MP3.

4.16 Diretório Funcional: local de armazenamento dos documentos da unidade organizacional localizado no servidor de arquivos do Tribunal.

4.17 Equipamentos de informática: servidores de rede e de bancos de dados, concentradores de rede com ou sem fio, roteadores, *racks*, bastidores (distribuidores ou armários repetidores), sistemas de armazenamento e de *backup*, appliances de computador (*firewall*, filtro de conteúdo, IPS/IDS, outros), projetores multimídia, equipamentos de videoconferência, câmeras IP, computadores de mesa, *notebooks*, monitores, scanners, impressoras e multifuncionais.

4.18 *Intranet*: ambiente de rede de computadores composta pelo conjunto de redes locais e recursos computacionais utilizados para sua formação.

4.19 Incidente de segurança: qualquer fato hostil, confirmado ou sob suspeita, relacionado à política de segurança.

4.20 Licença de uso: cessão onerosa ou não de direito de uso de programa de computador, outorgada pelo detentor dos direitos autorais e da propriedade intelectual, por prazo determinado ou indeterminado.

4.21 Programa de computador: conjunto de instruções em linguagem natural ou codificada executado por computador, dispositivo ou periférico de modo a fazê-los funcionar para fins determinados.

4.22 Serviço de *e-mail* Institucional: ferramenta de trabalho que provê serviço de correio eletrônico para comunicação interna e externa, possuindo o sufixo@trt7.jus.br.

4.23 Serviço de Diretório: é um conjunto de atributos sobre recursos e serviços existentes na Rede de Computadores, de modo a controlar o acesso aos mesmos, de forma centralizada, para reforço da segurança e proteção dos recursos computacionais.

4.24 Serviço de Armazenamento de Arquivos em Rede (pastas de rede): provê espaço de armazenamento dos arquivos produzidos pelos usuários em suas atividades laborais com garantia de disponibilidade, controle de acesso e cópia de segurança.

4.25 *Backup*: cópia de segurança para os arquivos.

4.26 Rede Corporativa: conjunto de ativos de Tecnologia disponível no âmbito do TRT da 7ª Região e suas unidades, que permite a comunicação via rede aos diversos serviços de tecnologia da informação.

4.27 Nuvem Corporativa: é conjunto de serviços de TI, mantida internamente ou em outro ente da APF ou ainda contratada de terceiros, acessível pela rede corporativa ou via *Internet*.

4.28 *Spam*: termo usado para se referir a mensagens eletrônicas não solicitadas, originadas do envio indiscriminado a um grande número de pessoas.

4.29 Códigos maliciosos: termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em computadores, tais como: a obtenção de vantagens financeiras (compras em nome do usuário, por exemplo), furto de identidade, coleta e exposição de informações confidenciais, exclusão de dados, publicação de mensagens ideológicas, desejo de autopromoção e o vandalismo. Além disto, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam*.

4.30 Quebra de segurança – ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e comunicações.

4.31 Mídia removível: é um tipo de memória que pode ser removida do seu aparelho de leitura, conferindo portabilidade para os dados que carrega, como exemplos temos: CDs e DVDs graváveis, cartão de memória, Flash Drive, Pen Drive, entre outros.

5 DA COMPETÊNCIA

5.1 Compete ao Comitê Gestor de Segurança da Informação (CGSI), definir as diretrizes e garantir os recursos para implementação desta norma, segundo os objetivos, os princípios e as diretrizes estabelecidos pela Política de Segurança da Informação e Comunicações.

5.2 Compete ao Núcleo de Apoio a Gestão de TIC e Segurança da Informação orientar e monitorar a implementação desta norma, fornecendo ao CGSI relatórios periódicos.

5.3 Compete à Secretaria de Tecnologia da Informação e Comunicação (SETIC):

5.3.1 Implantar os mecanismos necessários que garantam a aplicação desta norma.

5.3.2 O controle do uso, a instalação, a configuração, a manutenção, a monitoração e a auditoria dos Recursos de TIC referidos nesta Norma Complementar.

5.4 Compete, solidariamente, às demais unidades organizacionais do Tribunal Regional do Trabalho da 7ª Região verificar o uso adequado dos recursos computacionais e a observância das regras contidas na presente Norma Complementar.

5.5 Compete aos dirigentes e às chefias imediatas:

5.5.1 adotar as providências para que o pessoal sob sua responsabilidade conheça integralmente as medidas de segurança estabelecidas no âmbito do TRT da 7ª Região, zelando por seu fiel cumprimento.

5.5.2 requerer a concessão, alteração ou exclusão de direitos de acesso aos recursos de TIC para o pessoal sob sua responsabilidade, via Central de Serviços de TIC.

5.6 Compete aos gestores das áreas de negócio:

5.6.1 A gestão do acesso, ou seja, efetivar o cadastro, a alteração ou a revogação do acesso dos usuários aos sistemas e/ou dados sob sua responsabilidade.

5.6.2 Excepcionalmente, compete à SETIC efetivar as concessões, alterações ou revogações de acesso, no prazo definido no acordo de nível de serviço aplicável, quando não for possível tecnicamente que a própria área de negócio realize a gestão do acesso.

5.7 Compete aos usuários:

5.7.1 conhecer e cumprir integralmente as normas de controle de acesso e utilização dos recursos de TIC do TRT da 7ª Região.

5.7.2 reportar, por meio da Central de Serviços de TI, suspeita ou ocorrência de violações desta norma.

5.8 Observadas as diretrizes desta norma, a adoção de regras adicionais para a gestão de acesso (regras de concessão de papéis em um sistema de informação, por exemplo) está condicionada à formalização por parte do gestor do recurso de TIC envolvido, preferencialmente na concepção/implantação do recurso, e subsequentes adequações no ambiente, processos de trabalho, ferramentas e divulgação. Tais regras adicionais serão incorporadas à documentação técnica-operacional do recurso de TIC.

5.9 Compete à Secretaria de Gestão de Pessoas:

5.9.1 Requerer à SETIC, por meio da Central de Serviços, a criação da conta e *e-mail* corporativos para os novos usuários, como parte do processo de admissão.

5.9.2 Comunicar mensalmente à SETIC os casos de afastamentos do exercício da função no Tribunal, tais como aqueles em decorrência de exoneração, redistribuição, aposentadoria, remoção e cedência a outro órgão, ou retorno à origem, os falecimentos e desligamento dos estagiários.

5.10 Poderá ser concedido acesso temporário a funcionários de empresas prestadoras de serviços, quando necessário para desenvolver atividade para este Tribunal.

5.10.1 Compete ao Gestor do Contrato a requisição da liberação deste acesso, informando o perfil necessário, bem como a solicitação de exclusão imediatamente após o desligamento dos terceirizados.

5.10.2 Compete ao Fiscal Técnico do Contrato supervisionar o uso dos recursos de TIC liberados para os terceirizados.

5.11 Poderá ser concedido acesso temporário a servidores pertencentes a outros Órgãos Públicos, quando em atividade de interesse deste Tribunal, sendo de competência do Gestor da Unidade a requisição da liberação de acesso, informando o perfil necessário, bem como a solicitação de bloqueio imediatamente após o término das atividades.

6 DO CREDENCIAMENTO

6.1 O acesso aos ativos de TI será disponibilizado para usuários autorizados com a utilização de identificador único (*login*) e senha concedidos pela SETIC.

6.1.1 A SETIC comunicará à unidade respectiva sobre a efetivação do cadastro, fornecendo as informações necessárias ao acesso, e encaminhará a POSIC, em formato eletrônico, para a caixa postal institucional pessoal do usuário, para ciência.

6.1.2 Norma específica definirá as regras para obtenção e uso de certificados digitais pessoais de uso corporativo, aplicando-se ainda, no que couber, as diretrizes desta norma.

6.2 A SETIC manterá uma base de dados única e centralizada, apoiada em serviço de diretório na rede corporativa para armazenamento das contas de acesso aos ativos de TI.

6.3 Cada usuário deve possuir uma única conta de acesso às informações e ativos de TI do TRT.

6.3.1 Excepcionalmente, quando previamente autorizada pela SETIC, poderá ser criada conta adicional em sistema de informação, quando for tecnicamente inviável a integração com o credenciamento e autenticação da rede corporativa.

6.4 Deve ser concedido aos usuários do TRT7 o acesso às informações e aos recursos de TIC limitado ao mínimo que atenda à necessidade de conhecer e aos requisitos previstos em lei, acordos, contratos e regulamentos específicos.

6.5 Os direitos de acesso devem estar consistentes com a norma de classificação da informação.

6.6 Deve-se atribuir permissões ao usuário por meio da inclusão da sua conta em grupo previamente cadastrado e com as permissões já parametrizadas e testadas, evitando-se, sempre que possível, a concessão de permissão diretamente à credencial do usuário.

6.7 Contas de acesso de estagiários e terceirizados aos recursos de TIC, devem ter, como padrão, caráter temporário equivalente ao período de serviço previsto em contrato, podendo ter seu acesso renovado mediante novo contrato.

6.8 Aos membros do Ministério Público do Trabalho será concedida credencial de acesso aos recursos de TIC necessários para o desempenho de suas funções, em especial para participação nas Sessões do Tribunal Pleno e Turmas.

6.9 Na utilização das credenciais de acesso, compete ao usuário adotar medidas de segurança de caráter pessoal com vista a impedir o uso não autorizado dos recursos de TIC a partir de sua conta de acesso, tais como: não compartilhar senhas ou anotá-las em local visível.

7 DA IDENTIFICAÇÃO DO USUÁRIO

7.1 A credencial (*login* e senha) do usuário é pessoal e intransferível.

7.2 É vedada a criação de identificação genérica e/ou compartilhada.

7.2.1 Excepcionalmente, é permitido o uso de identificação compartilhada para promover o acesso do recurso de TIC à rede do TRT, previamente autorizado pela SETIC, nos casos de uso compartilhado para acesso específico e limitado, tais como os microcomputadores destinados ao público externo nas salas de audiência e totens para o registro de ponto eletrônicos dos servidores.

7.3 O identificador do usuário é utilizado para associá-lo aos respectivos direitos de acesso e ao histórico de ações realizadas enquanto perdurar tais direitos.

7.4 A formatação da credencial seguirá o padrão de formatação de endereços de correio eletrônico e caixas postais individuais especificado no ePING, inclusive quanto às regras de exceção.

7.4.1 A credencial da rede corporativa, em qualquer hipótese, será criada e fornecida pela SETIC, após solicitação, via Central de Serviços.

7.5 A credencial de acesso, para os recursos de TIC que não possuam autenticação integrada à rede corporativa, poderá ser criada pelo respectivo gestor, mediante autorização prévia da SETIC, e, sempre que possível, a identificação deve ser a mesma usada na rede corporativa.

7.6 Excepcionalmente, caso o usuário necessite alterar a sua identificação, deverá encaminhar solicitação à SETIC, devidamente justificada, via Central de Serviços, que, se aprovada, promoverá a adequação.

7.6.1 A nova identificação, sempre que possível, deverá seguir a padronização a que se refere o item 7.4.

8 DAS SENHAS

8.1 A senha utilizada no acesso às informações e ativos de TI do TRT deve possuir tamanho maior ou igual a 8 (oito) caracteres.

8.2 As senhas devem conter ao menos 3 (três) tipos de caracteres dentre maiúsculas, minúsculas, números e caracteres especiais.

8.3 As senhas não devem ser de fácil dedução como as que contém nomes próprios e de familiares, datas festivas ou de aniversário, sequências alfanuméricas, palavras encontradas em dicionários, placas de automóvel, dados pessoais como RG ou CPF, entre outras.

8.4 A senha deverá ser alterada pelo usuário com uma periodicidade máxima de 180 dias desde a última modificação, sendo impedido o uso das últimas 10 senhas anteriormente utilizadas.

8.4.1 A senha não poderá ser alterada novamente em menos de 48 horas após a última modificação.

8.4.2 Se viável tecnicamente a SETIC deverá implementar mecanismos automatizados que garantam a vigência máxima e mínima da senha.

8.5 Em caso de bloqueio permanente ou perda da senha por parte do usuário, a sua recuperação somente dar-se-á mediante requisição feita à Central de Serviços da SETIC.

8.6 A SETIC encaminhará a senha provisória aos usuários:

8.6.1 No credenciamento inicial.

8.6.2 Nos casos de bloqueios, perda ou esquecimento de senhas.

8.6.3 Em caso de suspeita de violação da confidencialidade da senha.

8.6.4 Na ocasião da instalação de equipamentos ou *softwares* com senha "padrão de fábrica".

8.7 As senhas provisórias serão fornecidas preferencialmente por meio de comunicação eletrônica para a caixa postal institucional pessoal do usuário.

8.7.1 Excepcionalmente, caso a caixa postal esteja indisponível, a senha temporária poderá ser informada por telefone.

8.8 As senhas enviadas pela SETIC aos usuários, em qualquer hipótese, têm caráter temporário e devem ser imediatamente alteradas pelo usuário.

8.8.1 A SETIC deverá, sempre que viável tecnicamente, implementar mecanismo que obrigue a alteração das senhas provisórias.

8.8.2 Caso o usuário suspeite de violação da confidencialidade da senha é de sua responsabilidade alterá-la imediatamente.

8.9 É vedado a qualquer unidade organizacional, inclusive à SETIC, solicitar aos usuários, por qualquer meio, o envio de senhas.

8.10 Os usuários não devem:

8.10.1 anotar sua senha de acesso aos sistemas do Tribunal em lembrete visível no ambiente de trabalho do Tribunal ou mesmo no teletrabalho.

8.10.2 armazenar a senha em qualquer *software* que possua recurso de "memorização de senhas" (navegador web, por exemplo).

8.10.3 compartilhar a senha com outras pessoas.

8.10.4 armazenar a senha em local acessível por terceiros (computadores próprios, pastas de rede, ambiente de colaboração, etc).

8.10.5 cadastrar a mesma senha utilizada na sua conta institucional do TRT em qualquer serviço externo ao TRT7, mesmo que relacionado ao serviço.

9 DA AUTENTICAÇÃO

9.1 Recursos de TI devem, sempre que possível tecnicamente, conter mecanismos de autenticação que exijam a confirmação da identidade do usuário.

9.2 A autenticação deve ser realizada minimamente por meio do fornecimento de *login* e senha.

9.3 Pode ser exigida a autenticação de multifatores, como por exemplo o uso simultâneo do *login* e senha ou certificado digital com código de validação em dispositivo móvel, a depender dos requisitos de segurança identificados para cada recurso de TI.

9.4 Quando tecnicamente viável, os mecanismos de autenticação devem:

9.4.1 Forçar a utilização de senhas que estejam em conformidade com a política de senhas.

9.4.2 Não exibir a senha digitada.

9.4.3 Não exibir o *login* do último usuário que acessou o recurso de TI.

9.4.4 Não sugerir o armazenamento da senha com finalidade de agilizar acessos futuros.

9.4.5 Criptografar o tráfego rede que contém a identificação do usuário (*login* e senha), durante o processo de autenticação.

9.5 Durante um processo mal sucedido de autenticação, o mecanismo de autenticação não deve revelar qual parte dos dados está incorreta, se *login* ou senha, mas ambos os campos como incorretos.

9.6 O acesso às informações (classificadas ou não) e aos recursos computacionais deve ser obrigatoriamente por meio de contas de acesso, com exceção para as informações públicas disponibilizadas nos portais institucionais.

9.7 Os mecanismos de autenticação, quando tecnicamente viável, devem ser configurados de modo a bloquear temporariamente o acesso do usuário após um determinado número de tentativas de autenticação consecutivas sem sucesso.

9.7.1 O desbloqueio deverá ocorrer automaticamente, sempre que possível tecnicamente, decorrido o tempo pré-configurado para bloqueio.

9.8 Devem ser implementados, quando tecnicamente viável, mecanismos de desconexão automática após determinado período de ausência de atividade.

9.9 O número de tentativas de acesso mal sucedidas, o tempo de bloqueio automático e o tempo para desconexão automática por inatividade são determinados em função dos requisitos de segurança de cada recurso de TIC que necessite de controle de acesso.

10 DOS RECURSOS DE TIC

10.1 O acesso aos recursos de Tecnologia da Informação será concedido a todos aqueles que exercem atividades relacionadas ao TRT da 7ª Região, segundo as necessidades indispensáveis e inerentes ao cumprimento do dever funcional.

10.2 A identificação, a autorização, a autenticação e a necessidade de conhecer são condicionantes prévias para concessão de acesso aos recursos de Tecnologia da Informação do TRT7.

10.3 Cada usuário, a critério da Administração e de acordo com a necessidade de serviço, credenciado consoante diretrizes e procedimentos estabelecidos nesta norma, poderá ter acesso aos seguintes tipos de recursos de TIC:

10.3.1 Centros de dados (Data Center).

10.3.2 Equipamentos de informática.

10.3.3 Rede corporativa.

10.3.4 Correio eletrônico.

10.3.5 Comunicadores instantâneos.

10.3.6. Nuvem corporativa.

10.3.7 Sistemas de informação e programas de computador.

10.3.8 *Internet*.

10.3.9 Dispositivos móveis.

10.3.10 Mídias removíveis.

10.3.11 Redes sociais.

10.4 Os usuários são responsáveis pelo uso adequado dos recursos de tecnologia da informação, conforme às diretrizes desta e demais normas que constituem a Política de Segurança da Informação do Tribunal Regional do Trabalho da 7ª Região.

10.5 São proibidos o acesso, uso, armazenamento e o encaminhamento por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região de:

10.5.1 Material não ético, discriminatório, malicioso, ofensivo, obsceno ou ilegal.

10.5.2 Fotos, imagens, músicas, sons e vídeos, que não sejam do interesse do Tribunal.

10.5.3 Jogos de qualquer natureza, entretenimentos e "correntes".

10.5.4 Material protegido por lei de propriedade intelectual, para os quais o usuário não possua o devido direito.

10.5.5 Propagandas com objetivo comercial.

10.5.6 Material de natureza político-partidária.

10.5.7 Material de cunho religioso.

10.5.8 É tolerado o envio de mensagens de natureza associativa ou sindical provenientes do sindicato ou associação de servidores e magistrados, apenas de caráter informativo, sendo vedado o uso do *e-mail* corporativo para fóruns de discussão e propaganda eleitoral das chapas.

10.5.9 Vírus de computador ou qualquer tipo de programa malicioso que possa ser considerado nocivo aos recursos de TIC.

10.5.10 Programas de computador não enquadrados no item "Do Uso dos Sistemas de Tecnologia da Informação e Programas de Computador".

10.5.11 Trabalhos particulares ou atividades alheias às funções jurisdicionais e administrativas deste Regional.

10.6 É proibido o encaminhamento de informações privilegiadas, confidenciais e/ou de propriedade do Tribunal para destinatários não autorizados, por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região.

10.7 É proibida aos usuários a divulgação da lista de endereços eletrônicos deste Regional ou de outro órgão público, por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região.

10.8 É proibida a utilização, por pessoas não classificadas nesta Norma Complementar, de quaisquer recursos de TIC deste Regional.

10.9 É proibido o armazenamento e encaminhamento de dados criptografados, por intermédio de quaisquer dos meios e recursos de tecnologia da informação disponibilizados pelo TRT da 7ª Região, exceto se usando funcionalidade de criptografia presente em sistemas ou serviços homologados e/ou disponibilizados pelo Tribunal.

10.10 Para implementar os controles de acesso aos recursos é fundamental a elaboração de processos de trabalho, bem como programas periódicos de sensibilização e conscientização em conformidade com a POSIC e normas complementares.

11 ACESSO PRIVILEGIADO OU ADMINISTRATIVO

11.1 O acesso local ou remoto aos computadores deste Regional com privilégios de Administrador de Sistema é exclusivo da Secretaria de Tecnologia da Informação, podendo ser atribuído tal privilégio, temporariamente, a usuários de outras unidades organizacionais, unicamente para fins de manutenção emergencial de equipamentos.

11.2 A concessão de acesso privilegiado deve atender à necessidade de conhecer e ser restrita a um número mínimo de pessoas da SETIC.

11.3 O credenciamento, a política de senhas e o monitoramento de contas de acesso privilegiadas seguem as mesmas diretrizes para as contas de acesso normais.

11.4 O uso de contas com privilégios administrativos é restrito às atividades exclusivas de administração e configuração dos ativos de TI, sendo proibido o uso para desempenho de atividades de negócio.

11.5 A SETIC deverá, sempre que possível, evitar o uso das contas administrativas genéricas, mantendo-as desativadas.

11.6 Aos servidores da SETIC e demais pessoas formalmente envolvidas em novos projetos de TIC são permitidos a instalação e uso de *softwares* não homologados e mudança na configuração padrão das estações de trabalho, durante a duração do projeto para viabilizar a execução de provas de conceito, prospecção de novas tecnologias, testes de funcionamento e homologação de soluções, vedada a execução de testes nos ambientes de produção.

12 DO ACESSO AOS CENTROS DE DADOS

12.1 O acesso físico aos centros de dados e aos demais espaços destinados aos equipamentos, computadores servidores, bastidores ou *racks* de equipamentos de rede lógica e comunicação deste Tribunal é restrito ao pessoal da Divisão de Infraestrutura de Tecnologia da Informação e Comunicação (DITIC), da SETIC.

12.2 O acesso às áreas referidas neste Item por pessoas estranhas à DITIC somente poderá ser feito com a necessária autorização, ser agendado previamente, com identificação da pessoa que executará o serviço, o detalhamento das atividades a serem realizadas no local, e mediante designação de acompanhante da DITIC. Deverá ser mantido registro de todos os acessos.

12.3 Será permitido acesso de terceiros para execução de serviços não previamente agendados nos centros de dados para manutenção emergencial, desde que acompanhados por servidor da DITIC, que providenciará registro após a intervenção.

12.4 É responsabilidade de todos que tenham acesso às salas técnicas, aos Depósitos de *Hardware* e às Bibliotecas de *Software* zelar pelo bom funcionamento dos mecanismos de segurança: portas, fechaduras e chaves, dispositivos biométricos, câmeras, sensores, entre outros.

12.4.1 Qualquer falha nos mecanismos referenciados neste item deve ser imediatamente reportada ao responsável pelo ambiente e, por este, ao responsável pela manutenção dos mecanismos, para que sejam tomadas as devidas providências.

12.5 O acesso lógico (pela rede corporativa ou remotamente), para suporte e manutenção corretiva ou preventiva, aos servidores de rede e demais equipamentos e *softwares* presentes nos Centros de Dados deste Tribunal é restrito ao pessoal da DITIC, podendo ser estendido a outras unidades da SETIC, conforme a necessidade, mediante autorização e controle de acessos pela DITIC.

12.6 Quando da manutenção de equipamentos e *softwares* por prestadores de serviço do TRT, o acesso remoto, quando concedido, será feito exclusivamente conforme as regras definidas pela DITIC.

12.6.1 Ao ser identificada a necessidade de acesso remoto por prestador de serviço, é necessário que a diretoria de infraestrutura esteja antecipadamente ciente da data, hora e duração da manutenção a ser feita para que possa ser concedido o acesso temporário.

13 DO USO DE EQUIPAMENTOS DE INFORMÁTICA

13.1 Relativamente ao uso dos equipamentos de informática, são atividades proibidas aos usuários:

13.1.1 instalar nos computadores qualquer tipo de dispositivo de conectividade com ou sem fio à Rede de Computadores deste Tribunal, tais como modems de acesso móvel à *internet* e roteadores *wireless*.

13.1.2 a instalação de *softwares* de qualquer natureza nos computadores do Tribunal.

13.1.3 a abertura dos equipamentos, a instalação ou remoção de qualquer componente de *software* ou *hardware*.

13.1.4 a alteração das configurações de funcionamento do sistema operacional e dos sistemas de informação e *softwares* aplicativos existentes nos computadores da rede corporativa.

13.1.5 desabilitar ou alterar configurações em serviços relacionados à segurança da informação, tais como antivírus, proxy e *firewall*.

13.1.6 Essas tarefas devem, quando necessárias, ser executadas pela equipe técnica da SETIC, ou, em caráter excepcional, pelos usuários quando solicitado pela SETIC e sob supervisão deste.

13.2 A SETIC criará padrões de configuração adequados às necessidades de utilização das unidades judiciais e administrativas.

13.3 Os equipamentos de informática, como por exemplo computadores, impressoras, multifuncionais e scanners, serão instalados e configurados pela SETIC ou por equipe por ela autorizada, com respectiva atualização do inventário de bens. Cabe ao responsável pelo setor a que se destina o equipamento o imediato recebimento do bem no sistema de controle de bens patrimoniais assim que instalado.

13.4 É de responsabilidade do usuário:

13.4.1 Desligar ou bloquear a tela e teclado do dispositivo - controlados por senha, token ou mecanismo de autenticação similar - quando sem monitoração ou uso.

13.4.2 Encerrar as sessões ativas, ou protegê-las por bloqueio, nos sistemas de informação.

13.4.3 Substituir os consumíveis (papel, toner, outros).

13.5 A SETIC poderá implementar mecanismos de bloqueio automático nos computadores da rede corporativa para o encerramento de sessões abertas nos sistemas quando sem uso.

13.6 O usuário deve zelar pela conservação, segurança e utilização adequada dos equipamentos, evitando obstruir suas entradas e saídas de ar.

13.7 Não será fornecido suporte remoto a equipamentos particulares (computadores, *notebooks*, *smartphones* e *tablets*), seja quanto à instalação e configuração de sistemas ou aplicativos, ainda que disponibilizados pelo TRT7 (certificado digital, por exemplo), seja quanto às questões relacionadas à conexão à rede sem-fio.

13.7.1 O suporte de TI prestado aos usuários externos pela Central de Serviços da SETIC, bem como aos usuários internos em teletrabalho, sobre os equipamentos particulares limitar-se-á ao fornecimento de orientação técnica, por telefone, *e-mail* ou *site* institucional.

13.7.2 Excepcionalmente, a Central de Serviços de TI poderá prestar suporte presencial (em sua sede) aos usuários externos e servidores em teletrabalho na configuração de equipamentos particulares para uso dos serviços de TI do Tribunal, mediante autorização da chefia da unidade e acompanhamento pelo usuário, vedada a guarda de equipamento pela Central de Serviços.

13.8 Em caso de teletrabalho obrigatório, os titulares das unidades administrativas e judiciárias poderão ceder, a título de empréstimo, aos Servidores e Magistrados computador, monitor, webcam e headset exclusivamente para o exercício das atividades em teletrabalho.

13.8.1 Os equipamentos só poderão se retirados após assinatura de termo de autorização de saída, no qual deverá constar a descrição detalhada dos bens e a identificação patrimonial.

13.8.2 O Servidor ou Magistrado assumirá a responsabilidade integral do bem emprestado.

13.8.3 O Servidor ou Magistrado deverá devolver o bem no prazo de 5(cinco) dias úteis, a contar do encerramento do teletrabalho ou a qualquer tempo a pedido do Tribunal.

14 DO USO DE DISPOSITIVOS MÓVEIS

14.1 Quando da concessão de dispositivos móveis do Tribunal ao usuário, é necessário que esses sejam previamente homologados e configurados pela SETIC, atendendo aos requisitos de segurança, incluindo a instalação de *software* de segurança de endpoint do Tribunal.

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

14.3 O *backup* de dados locais (armazenado no dispositivo) é de exclusiva responsabilidade do usuário.

14.4 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 5 (cinco) dias úteis.

14.5 O uso de dispositivos móveis ou portáteis (*smartphone, tablets, notebooks*) particulares, independente da natureza do vínculo do usuário com o Tribunal, deve ser restrito somente às redes destinadas para usuários externos ou visitantes.

14.6 Os dispositivos móveis disponibilizados pelo TRT não terão privilégio de administrador para os destinatários dos equipamentos, aplicando-se as mesmas regras de segurança das estações de trabalho, no que couber.

14.7 A perda ou furto de equipamentos de TI do TRT7 deve ser comunicado imediatamente à SETIC, além de tomadas as providências administrativas cabíveis.

15 DO USO DE MÍDIAS REMOVÍVEIS

15.1 É de responsabilidade do usuário o armazenamento físico seguro de mídias removíveis que contenham informações do Tribunal, não os mantendo na mesa ou no próprio equipamento quando não em uso.

15.2 Não haverá cópia de segurança de dados armazenados em mídias removíveis.

15.3 Os arquivos do Tribunal não devem ser copiados ou armazenados em mídias removíveis, devendo permanecer no dispositivo apenas durante o tempo necessário para conclusão da atividade quando necessário, arquivando-os nos sistemas de informação apropriados, nuvem corporativa ou na pasta de rede da respectiva área, conforme o caso.

15.3.1 Não é permitido copiar para dispositivos removíveis, base de dados inteiras, a título, por exemplo, de armazenamento ou transporte de material de referência.

16 DO USO DOS SISTEMAS DE TECNOLOGIA DA INFORMAÇÃO E PROGRAMAS DE COMPUTADOR

16.1 Os sistemas de tecnologia da informação deste Tribunal são constituídos de programas de computador desenvolvidos pela Justiça do Trabalho ou de terceiros, para uso das unidades organizacionais, cabendo à SETIC a manutenção e melhoria tecnológica.

16.2 Nos sistemas de tecnologia da informação é obrigatória a utilização dos mecanismos de autenticação eletrônica.

16.2.1 A autenticação eletrônica substitui a assinatura dos usuários para prática dos atos de ofício.

16.3 A criação de novos sistemas de tecnologia da informação, bem como a alteração dos existentes, somente poderá ser realizada pela SETIC ou por terceiros por ela autorizados.

16.4 As unidades organizacionais do TRT7 serão responsáveis pela alimentação e atualização das informações que lhes competirem nos sistemas de tecnologia da informação, devendo manter a precisão e a correção dos dados informados.

16.5 Nos casos de alteração ou remoção de informação existente na base de dados, a SETIC deverá preservar os dados anteriores, mediante a criação de cópia de segurança para fins de auditoria, segundo as especificações da política de *backup*.

16.6 A SETIC verificará a compatibilidade com os demais programas utilizados e adequação aos recursos computacionais disponíveis.

16.7 Relativamente ao uso dos sistemas de tecnologia da informação e programas de computador deste Regional, são atividades proibidas:

16.7.1 instalação de programas de computador, de qualquer natureza, sem a autorização da SETIC e que não estejam homologados e/ou que não possuam licença de uso contratada.

16.7.2 alteração das configurações padronizadas, definidas pela SETIC.

16.7.3 retirada dos programas-padrão instalados pela Secretaria de Tecnologia da Informação, assim entendidos aqueles específicos do sistema operacional, aplicativos de acesso a banco de dados, programas de edição de texto, apresentações e planilhas, antivírus, programas de segurança e manutenção remota e programas específicos das diversas unidades organizacionais deste Regional.

16.7.4 verificada a infração ao disposto nos subitens anteriores, a SETIC deverá promover a imediata adequação e encaminhar ao Comitê Gestor de Segurança da Informação relatório circunstanciado sobre o fato.

16.8 As unidades organizacionais do Tribunal Regional do Trabalho da 7ª Região poderão submeter pedido de homologação de programa de computador à Secretaria de Tecnologia da Informação para uso em suas atividades, que poderá homologá-lo ou, se entender necessário, elaborar parecer técnico e submetê-lo à apreciação do Comitê Gestor de Segurança da Informação e/ou do Comitê de Governança de TI.

16.9 A Secretaria de Tecnologia da Informação publicará, na *Intranet*, a listagem de programas homologados, onde constarão os nomes, a versão, a unidade organizacional autorizada a utilizá-los e o tipo de licença de uso.

16.10 Os sistemas e serviços de TIC do TRT7 quando disponíveis para acesso via *internet* devem ser protegidos com o uso de mecanismos de criptografia.

16.11 Os sistemas de TIC elegíveis ao acesso remoto (a partir da *internet*, como por exemplo para servidores em teletrabalho) são os disponíveis no Portal de Colaboração, Extranet e Portal de Serviços do Tribunal disponibilizados por meio da *internet*.

16.11.1 Se econômica e tecnicamente viável, poderá ser concedido acesso remoto para servidores e magistrados aos demais serviços não disponíveis nas plataformas citadas

acima, quando indispensável ao teletrabalho, por meio de soluções homologadas e mantidas pela SETIC, tais como VPN e/ou soluções de virtualização.

17 DO USO DO CORREIO ELETRÔNICO

17.1 REGRAS GERAIS

17.1.1 A utilização do correio eletrônico (*e-mail* institucional) é meio oficial aos servidores do Tribunal para comunicação interna feita de acordo com as regras adiante estabelecidas.

17.1.2 Os magistrados e servidores ativos deverão possuir conta de *e-mail* para fins de recebimento e envio de documentos decorrentes de suas funções de trabalho no Tribunal Regional do Trabalho da 7ª Região, adotando-se as regras do Governo Federal (ePING) para padronização da formação de endereços de correio eletrônico, acrescido do sufixo@trt7.jus.br.

17.1.2.1 É vedado o fornecimento de caixa postal institucional para magistrados e servidores inativos, bem como para pensionistas.

17.1.3 Cabe a SETIC administrar os recursos de TIC envolvidos e os limites de utilização das caixas postais de cada usuário.

17.1.4 A SETIC providenciará que as informações que trafegam em mensagens eletrônicas sejam protegidas por protocolo seguro de comunicação, quando no perímetro corporativo.

17.1.5 O acesso ao correio eletrônico, a partir de estações de trabalho fornecidas pelo Tribunal, será feito apenas a partir do navegador de *internet*.

17.1.6 Serão registrados os dados de envio e recebimento de mensagens eletrônicas no âmbito deste Regional, especificamente para fins de auditoria, garantida a confidencialidade do seu conteúdo, os quais deverão ser arquivados segundo a política de *backup* do Tribunal.

17.1.7 São proibidos, no desempenho das atribuições institucionais, o envio e recebimento de mensagens eletrônicas mediante a utilização de serviços de *e-mail* pertencentes a entidades estranhas ao TRT7.

17.1.8 O uso do correio eletrônico será monitorado por meio de ferramentas com o objetivo de evitar o recebimento de *spam*, *hoax*, *phishing*, mensagens contendo *malware* e outros arquivos que coloquem em risco a segurança do Tribunal ou que contenham conteúdo impróprio.

17.1.9 Havendo suspeitas de que alguma mensagem de *e-mail* possa ocasionar falha de segurança, hostilidades decorrentes da ação de *crackers* (erroneamente conhecidos como *hackers*), transmissão de códigos maliciosos ou violação de quaisquer das veda-

ções constantes desta Norma Complementar, a Secretaria de Tecnologia da Informação adotará medidas imediatas para a apuração e solução do Incidente de Segurança.

17.2 CAIXAS POSTAIS DE ESTAGIÁRIOS E TERCEIRIZADOS

17.2.1 Poderá ser solicitada à SETIC a criação de conta de *e-mail* para uso por estagiário ou empregado terceirizado, desde que devidamente justificada pelo requerente, acrescendo-se ao identificador do usuário a expressão ".estag", no caso de estagiário, e ".terc", quando empregado terceirizado.

17.2.2 A quantidade de caixas postais disponíveis para estagiários e terceirizados deverá ser previamente autorizada pelo Comitê de Governança de TIC, sempre que se tratar de serviço contratado.

17.3 CAIXAS POSTAIS DE UNIDADES ORGANIZACIONAIS

17.3.1 Poderá ser criada conta de *e-mail* para unidades organizacionais, apenas se houver recurso técnico para delegação da conta.

17.3.2 É vedado o compartilhamento de senhas para acesso à caixa postal.

17.3.3 O endereço eletrônico será composto pela sigla da unidade, usualmente utilizada neste Tribunal, e pelo sufixo@trt7.jus.br.

17.3.4 A conta deverá ser delegada ao titular da unidade e servidores autorizados a operá-la.

17.4 LISTAS DE DISTRIBUIÇÃO

17.4.1 É permitida a criação de lista de distribuição, com o objetivo de facilitar e otimizar a troca de informações sobre assuntos de interesse do Tribunal.

17.4.2 A criação de lista de distribuição pode ser solicitada pelo gestor da unidade a qual se destina. A solicitação deve ser encaminhada à SETIC e, quando destinada à atividade temporária, do período de sua duração.

17.4.3 Cada lista de distribuição terá um gestor, a quem incumbe:

17.4.3.1 manter permanentemente atualizado o rol de integrantes da lista de distribuição.

17.4.3.2 solicitar exclusão como gestor e indicar, simultaneamente, o novo responsável pela lista de distribuição.

17.4.3.3 solicitar exclusão da lista de distribuição, quando esta não for mais necessária.

17.4.4 A lista de distribuição será composta exclusivamente por endereços eletrônicos do Tribunal.

17.4.4.1 Excepcionalmente, poderão ser incluídos em listas de distribuição de grupos ou comissão de trabalho do Tribunal os endereços eletrônicos de representantes de outras entidades (OAB, por exemplo), desde que formalmente designados pela Diretoria-Geral ou Presidência do Tribunal como integrantes do respectivo grupo/comissão.

17.4.4.2 A SETIC, poderá, por solicitação do gestor da lista ou sempre que necessário para o controle de segurança (*spam*, por exemplo) bloquear as listas de distribuição para o recebimento de mensagens eletrônicas enviadas apenas pelo público interno.

17.4.5 A SETIC deve manter permanentemente na *intranet* tabela atualizada com as listas de distribuição do Tribunal e seus respectivos gestores.

17.5 RESPONSABILIDADES DOS USUÁRIOS DO SERVIÇO DE *E-MAIL*

17.5.1 verificação diária das caixas postais eletrônicas.

17.5.2 manter espaço disponível para recebimento de novas mensagens.

17.5.3 excluir mensagens que não sejam de interesse da Administração.

17.5.4 não permitir o acesso de terceiros ao seu *e-mail*.

17.5.5 encaminhar as comunicações oficiais à caixa postal das unidades organizacionais.

17.5.6 utilizar o seguinte texto para rodapé de *e-mails* do Tribunal enviados a destinatários externos:

“AVISO LEGAL: O emitente desta mensagem é responsável por seu conteúdo e endereçamento. Cabe ao destinatário cuidar quanto ao tratamento adequado. Sem a devida autorização é proibida a divulgação, reprodução ou distribuição das informações aqui dispostas. Se você não for o destinatário ou a pessoa autorizada a receber esta mensagem, não deve usar, copiar ou divulgar as informações nela contida ou tomar qualquer ação baseada nessas informações. Este ambiente está sujeito a monitoramento.”

17.5.7 Notificar a SETIC, via Central de Serviços, quando do recebimento de mensagens com conteúdo suspeito.

17.5.8 Evitar acessar hiperlinks inseridos em mensagens de correio eletrônico (páginas de *internet*) quando recebidas de origem desconhecida, pois esses podem iniciar a instalação de *softwares* maliciosos ou direcionar o usuário da rede para um sítio falso, possibilitando a captura de informações.

17.5.9 Levar em conta o sigilo da informação a ser encaminhada, devendo consultar seu superior hierárquico em caso de dúvida.

18 DO USO DOS SERVIÇOS DE COMUNICAÇÃO INSTANTÂNEA

18.1 O serviço de mensagem instantânea disponibilizado pelo TRT7 é de uso facultativo e destina-se às comunicações internas.

18.2 O responsável por unidade organizacional poderá solicitar à SETIC liberação de acesso para uso por estagiário ou empregado terceirizado, desde que devidamente justificada pelo requerente.

18.3 É vedado é uso de IM (*Instant Messenger*) não homologado ou não autorizado.

18.4 magistrados e servidores poderão acessar o serviço de comunicação instantânea via *internet*.

18.5 Se necessário à execução das atividades institucionais, poderá ser solicitada à SETIC, com a devida justificativa, a liberação para comunicação externa.

19 DO USO DA NUVEM CORPORATIVA

19.1 O acesso via *internet* deverá ser exclusivamente por meio de protocolos seguros de comunicação, cabendo à SETIC a implementação transparente deste recurso.

19.2 Informações e documentos específicos armazenados na nuvem corporativa poderão ser compartilhados temporariamente com usuários externos (como por exemplo, servidores de outros órgãos ou empregados de empresas contratadas), quando necessários ao desenvolvimento das atividades, previamente autorizado pelo responsável da unidade e mediante, quando for o caso, assinatura de termo de confidencialidade.

19.3 A nuvem nuvem corporativa poderá ser utilizada para salvaguardar os arquivos provenientes, exclusivamente, das atividades laborais, com garantia de disponibilidade, controle de acesso e durabilidade.

19.3.1 As responsabilidades pela disponibilidade, controle de acesso e cópia de segurança são da prestadora de serviço e estabelecidas em contrato. A periodicidade e retenção mínima dos *backups* deverão estar de acordo com a política de cópia de segurança do Tribunal.

19.4 Cabe ao chefe de unidade organizacional organizar as pastas de trabalho no ambiente virtual, orientando seus subordinados quanto ao uso (inclusão, alteração, organização e remoção de arquivos), bem como a concessão e revogação de compartilhamento.

19.5 Os arquivos mantidos pelos usuários na nuvem corporativa devem estar acessíveis, ao menos, pelo proprietário e, se houver, seu substituto e ainda pelo chefe da unidade.

20 DO USO DA REDE CORPORATIVA

20.1 A SETIC poderá bloquear, pelo tempo necessário para diagnóstico e solução, qualquer dispositivo conectado à rede que esteja gerando problemas de desempenho, tráfego suspeito ou quaisquer formas de violações à política de segurança da informação, visando preservar a segurança e a disponibilidade dos recursos computacionais do Tribunal.

20.2 Todos os equipamentos e dispositivos móveis conectados à rede lógica de dados do TRT7 terão seus acessos monitorados por questões de segurança e para fins de auditoria.

20.3 A cada ponto de acesso físico à rede de dados do TRT7 poderá ser conectado apenas um equipamento, vedada a utilização de dispositivos multiplicadores de acesso, salvo mediante expressa autorização da SETIC para atendimentos de situações excepcionais e temporárias.

20.4 A conexão de qualquer equipamento à rede cabeada do TRT7 só pode ser realizada pela SETIC, ou por terceiros por ela autorizados.

20.5 A SETIC manterá área de armazenamento em rede (pasta de rede) para salvaguardar os arquivos provenientes, exclusivamente, das atividades laborais das unidades administrativas, com garantia de disponibilidade, controle de acesso e cópia de segurança.

20.6 Cada unidade administrativa, conforme o organograma do Tribunal, terá disponível 1 (uma) área de armazenamento em rede.

20.7 Não haverá área de armazenamento dedicada a usuário ou grupos específicos.

20.8 A SETIC definirá os diretórios e as regras de acesso para aplicação padronizada em todas as unidades administrativas e judiciárias.

20.9 Cabe ao Gestor da Unidade a criação e organização das pastas no diretório.

20.10 Os usuários devem, periodicamente, fazer a eliminação de arquivos desnecessários e evitar a manutenção de mais de uma cópia do mesmo arquivo.

20.11 A SETIC poderá excluir conteúdo que não esteja em conformidade com as normas de segurança da informação do TRT7, quando da realização de manutenções periódicas nos diretórios de rede a fim de liberar espaço e otimizar a sua utilização.

20.12 Os dados armazenados nas estações de trabalho dos usuários do Tribunal não estão contemplados pelas garantias de disponibilidade, controle de acesso e cópia de segurança, cabendo aos usuários providenciar cópia para os repositórios oficiais (pastas na rede, sistemas de informação ou colaboração) e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.

20.13 É vedado o armazenamento de documentos em locais distintos daqueles para cuja edição e armazenamento o TRT7 disponibilize sistemas próprios, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas.

21 DO USO DA REDE SEM FIO

21.1 O Tribunal disponibilizará acesso a uma rede sem fio para equipamentos de propriedade do Tribunal, destinado para magistrados, servidores, entre outros e uma outra rede para equipamentos particulares (de magistrados, servidores, advogados, procuradores, visitantes, outros).

21.2 As redes sem fio deverão estar integradas de modo seguro à infraestrutura de redes do TRT7.

21.3 A rede sem fio destinada aos equipamentos do Tribunal poderá ser utilizada para acesso à *internet* e aos recursos de TIC disponibilizados pelo TRT7 na *intranet* e portal institucional, com filtragem de conteúdo e manutenção dos registros de acessos.

21.4 A rede sem fio disponibilizada pelo TRT7 para dispositivos particulares permitirá acesso apenas para alguns serviços informatizados, tais como *site* institucional e portal de serviços e ao Processo Judicial Eletrônico.

21.5 Poderá ser disponibilizado acesso a *internet* por meio da rede sem fio destinada aos equipamentos particulares em locais específicos, adotando-se limite de utilização, filtragem de conteúdo e, sempre que possível, manutenção dos registros de acessos.

21.6 A abrangência das redes sem fio será definida pelo Comitê de Governança de TIC, conforme a disponibilidade orçamentária para aquisição e manutenção.

22 DO USO DA *INTERNET*

22.1 Cada usuário, a critério da Administração, de acordo com a necessidade de serviço, poderá ter acesso à *internet*, identificado pela sua credencial, de uso pessoal e intransferível.

22.2 As contas de usuários deverão ter níveis de acessos distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela SETIC.

22.3 Cabe à SETIC implementar o controle de acesso e os mecanismos de monitoramento e auditoria, bem como restringir o teor do conteúdo da rede mundial de computadores acessível a partir da rede corporativa desta Corte.

22.3.1 Norma complementar de cópia de segurança definirá o prazo de retenção dos registros de monitoramento.

22.4 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 SETIC.

22.4.1 A SETIC poderá negar o pedido caso o *site* represente ameaça de segurança ou possa comprometer de alguma forma o desempenho ou disponibilidade da rede de computadores do TRT.

22.4.2 A SETIC manterá histórico dos sítios liberados, por solicitação dos gestores, para conhecimento do CGSI.

22.5 A SETIC poderá bloquear ou limitar transmissão contínua (streaming de áudio e vídeo) com o propósito de garantir a disponibilidade de recursos dos circuitos de comunicação de dados ou dos equipamentos servidores de rede aos serviços essenciais.

22.6 É proibido o acesso à *internet* usando os recursos de TIC disponibilizados pelo TRT7:

22.6.1 Por meio do uso de provedores de acesso externos ou de qualquer outra forma de conexão à *internet* não autorizada expressamente pela SETIC.

22.6.2 Uso de proxy anônimo.

22.6.3 Utilização de *softwares* de compartilhamento de conteúdos na modalidade peer-to-peer (P2P).

22.7 O acesso a *internet* somente poderá ser efetuado por navegadores homologados pela SETIC.

23 DO USO DE REDES SOCIAIS

23.1 O acesso às redes sociais utilizando a infraestrutura de rede corporativa do Tribunal é restrito a usuários autorizados e às atividades institucionais ou de comprovada necessidade de serviço.

23.1.1 O pedido de acesso será avaliado pelo Comitê Gestor de Segurança da Informação.

23.1.2 Será concedido acesso aos usuários internos para visualizarem as publicações do TRT7 nas redes sociais, sempre que a tecnologia permitir restringir o acesso apenas ao respectivo perfil.

23.2 Não é permitido aos Magistrados e Servidores criar perfis de unidades (administrativas e judiciárias) nas redes sociais, exceto se formalmente autorizados.

23.3 Não são permitidas aos Magistrados e Servidores postagens nas redes sociais em nome do Tribunal, exceto se formalmente autorizados.

23.4 À Divisão de Comunicação Social é atribuída a função de agente responsável pela administração de cada perfil institucional nas redes sociais.

23.5 A publicação de conteúdo nas redes sociais utilizando os perfis institucionais deve estar vinculada à missão institucional do Tribunal e à observância do interesse público, evitando-se a promoção de indivíduos ou agentes públicos, e destina-se a divulgar campanhas promovidas pela Justiça do Trabalho ou Poder Judiciário como um todo, informações administrativas sobre o funcionamento da Justiça do Trabalho no Estado e informações úteis aos jurisdicionados e à sociedade em geral. Decisões da Corte Trabalhista, divulgação de eventos abertos ao público, mensagens institucionais e informações úteis são exemplos de publicações a serem feitas pelo TRT7 nas redes sociais.

23.6 Nos perfis institucionais é proibida a publicação de conteúdo com emissão de opinião de caráter pessoal, político-partidário, ofensivo, discriminatório ou jocoso.

23.7 As senhas dos perfis institucionais devem ser diferentes das senhas utilizadas na rede corporativa.

23.8 Devem ser utilizadas senhas distintas para cada perfil institucional criado.

23.9 É permitido a participação de servidores e magistrados em fóruns de discussões na *internet* utilizando a identificação pessoal institucional (nome, email, cargo), quando necessária às atividades institucionais, de comprovada necessidade de serviço ou de propósito de aprimoramento técnico, seguindo, no que couber, as regras dispostas neste tópico.

24 DAS DISPOSIÇÕES FINAIS

24.1 Será permitida a manutenção preventiva e corretiva dos recursos de TIC por preposto de empresa responsável por garantia técnica, na forma prevista no respectivo contrato, mediante autorização e agendamentos prévio com a SETIC.

24.2 Cabe ao Setor de Manutenção da Divisão de Engenharia o controle do uso, a instalação e a manutenção dos equipamentos de fornecimento de energia elétrica para a área de tecnologia da informação.

24.3 A utilização dos Recursos de Tecnologia da Informação deverá ser monitorada com a finalidade de identificar divergências entre as normas que integram a POSIC e os registros de eventos monitorados, fornecendo evidências, no caso de incidentes de segurança, para que sejam tomadas as devidas providências.

24.4 O Comitê Gestor de Segurança da Informação, em conjunto com as demais unidades da estrutura organizacional do TRT da 7ª Região, promoverá a comunicação e a ampla divulgação desta, para que todos a conheçam e a cumpram no âmbito de suas atividades e atribuições.

24.5 A SETIC deverá promover verificação anual, quanto a eficiência dos controles implementados para aferir o correto cumprimento desta Norma Complementar.

24.6 Configurado o descumprimento das normas estabelecidas, a SETIC encaminhará comunicado ao CGSI para análise.

24.7 Situações específicas envolvendo a utilização de recursos de tecnologia da informação e comunicação não previstas nesta norma serão resolvidos pela SETIC.

25. DA VIGÊNCIA E REVISÃO

25.1 Esta norma deverá ser revisada e atualizada periodicamente, no máximo, a cada três anos.

25.2. Esta Norma Complementar entra em vigor na data de sua publicação.