ATO TRT7.GP Nº 340, DE 17 DE NOVEMBRO DE 2023

Atualiza a Norma de Controle de Acesso e a Utilização dos Recursos de Tecnologia da Informação e Comunicação no âmbito do Tribunal Regional do Trabalho da 7ª Região (TRT-7).

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-7;

CONSIDERANDO a necessidade de revisão periódica das normas de segurança da informação, nos termos da Política de Segurança da Informação deste Tribunal;

CONSIDERANDO o Ato CSJT.SG.SETIC.NUGOV n° 1, de 23 de março de 2022, que oficializa a segunda versão do Guia Referencial de Segurança da Informação da Justiça do Trabalho;

CONSIDERANDO a Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO a Portaria CNJ nº 162, de 10 de junho de 2021, que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a ENSEC-PJ;

RESOLVE:

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

Art. 2º Esta norma deverá ser revisada periodicamente, no máximo, a cada três anos.

Art. 3º Fica revogado o Ato TRT7.GP nº 65, de 4 de junho de 2020.

Art. 4º Este ato entra em vigor na data de sua publicação.

PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.

Fortaleza, 17 de novembro de 2023.

DURVAL CÉSAR DE VASCONCELOS MAIA

Presidente do Tribunal

ANEXO

1. DO OBJETIVO

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

2. DOS OBJETIVOS ESPECÍFICOS

2.1 Estabelecer a política de uso aceitável de equipamentos de TIC, 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.

2.5 Disciplinar o credenciamento dos(as) usuários(as), a concessão de acessos e o uso de senhas.

3. DO FUNDAMENTO LEGAL

3.1 A Resolução Normativa nº 5, de 3 de março de 2023, que institui a Política de Segurança da Informação e Comunicação do TRT-7 (POSIC), estabelece no art. 10, inciso I, diretriz para expedição de norma de controle de acesso e uso dos recursos de TIC.

3.2 A Instrução Normativa GSIPR Nº 5, 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal.

3.3 A Instrução Normativa GSIPR Nº 6, de 23 de dezembro de 2021, que estabelece diretrizes de segurança da informação para o uso seguro de mídias sociais nos órgãos e nas entidades da administração pública federal.

3.4 A 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 A Norma Complementar 07/IN01/DSIC/GSIPR, de 15 de julho de 2014, 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.

3.6 A ABNT NBR ISO/IEC 27002:2013, Código de Prática para a Gestão de Segurança de Informação, que estabelece:

“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);

- Uso aceitável dos ativos (tópico 8.1.3);
- Dispositivos móveis e teletrabalho (tópico 6.2);
- Restrições sobre o uso e instalação de software (tópico 12.6.2);”

4. DOS CONCEITOS E DAS DEFINIÇÕES

Para os efeitos desta Norma são estabelecidos os seguintes conceitos e definições, em adição aos presentes na POSIC do TRT-7:

4.1 Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de

TIC do Tribunal.
4.2 Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder, bloquear ou excluir acesso aos recursos de TIC.
4.3 Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o(a) usuário(a) ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de TIC.
4.4 Perfil de acesso: conjunto de atributos de cada usuário(a), definidos previamente como necessários para credencial de acesso.
4.5 Credenciamento: processo pelo qual o(a) usuário(a) recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e a definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.
4.6 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(a) (login) e senha.
4.7 Autorização: processo realizado mediante credencial de acesso que garante o acesso ao recurso.
4.8 Login: identificador único de usuário(a) para acesso a sistemas computacionais, exprimindo-se pela matrícula, nome ou combinação dos dados dos(as) usuários(as).
4.9 Mecanismo de Autenticação: ocorre quando as credenciais de acesso de um(a) determinado(a) usuário(a) são validadas por um sistema, sendo possível a utilização de combinação de credenciais.
4.10 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 a entidade destinatária da mensagem contendo este código possa identificar o(a) remetente e verificar a integridade da mensagem.
4.11 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.
4.12 Comunicação Instantânea: serviço de mensagens instantâneas que possibilita comunicação em tempo real entre usuários (as).
4.13 Dispositivos móveis: equipamentos e periféricos que possam ser transportados com conteúdo e acessíveis em qualquer lugar, tais como notebooks, tablets, smartphones, pendrives e unidades de armazenamento externo.
4.14 Equipamentos de TIC: equipamentos tais como, 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, appliances de computador (firewall, filtro de conteúdo, IPS/IDS, outros), equipamentos de videoconferência, câmeras IP, computadores de mesa e notebooks, monitores, scanners, impressoras e multifuncionais.
4.15 Intranet: é o portal institucional com informações, serviços e sistemas de TIC voltados exclusivamente aos(às) usuários (as) internos(as).
4.16 Extranet: é o portal institucional com informações, serviços e sistemas de TIC voltados exclusivamente aos(às) usuários (as) internos(as), mas que podem ser acessados remotamente, via internet, mediante autenticação do(a) usuário(a). Geralmente é uma extensão ou subconjunto da intranet.
4.17 Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, intencional ou acidental, relacionado à segurança dos sistemas de computação ou das redes de computadores.
4.17.1 É permitido a manutenção de contas de acesso à extranet para servidores(as) e magistrados(as) inativos(as), com permissão apenas aos serviços estritamente necessários, como por exemplo, acesso ao contracheque.
4.18 Licença de uso: cessão onerosa ou não de direito de uso de programa de computador, outorgada pelo(a) detentor(a) dos direitos autorais e da propriedade intelectual, por prazo determinado ou indeterminado.
4.19 Programa de computador: conjunto de instruções executado por computador, dispositivo ou periférico de modo a fazê-los funcionar para fins determinados.
4.20 Serviço de Armazenamento de Arquivos (pastas de rede): provê espaço de armazenamento para os arquivos produzidos pelos(as) usuários(as) em suas atividades laborais, com garantia de disponibilidade e controle de acesso, utilizando infraestrutura de TIC própria e/ou de terceiros (nuvem corporativa).
4.21 Rede Corporativa: conjunto de ativos de TIC disponível no âmbito do TRT-7 e suas unidades, que permite aos(às) usuários(as) internos(as) acessarem os serviços de TIC internos e externos.
4.22 Nuvem Corporativa: é um conjunto de serviços de TIC mantido em outro ente da Administração Pública Federal (APF) ou ainda contratado de terceiros(as), acessível pela rede corporativa ou via Internet.
4.23 Spam: termo usado para se referir a mensagens eletrônicas não solicitadas, originadas do envio indiscriminado a um grande número de pessoas.
4.24 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(a) usuário (a), 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 disso, os códigos maliciosos são muitas vezes usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam.
4.25 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: cartões de memória, discos externos, flash drive, pen drives, entre outros.
4.26 Solução de segurança de endpoints: solução de software para instalação nos equipamentos dos(as) usuários(as) finais, tais como computadores, notebooks e smartphones, cuja finalidade é proteger o equipamento e principalmente as informações das ameaças cibernéticas, tais como roubo de senhas, aplicação de golpes virtuais ou comprometimento das informações do Tribunal.
5. DA COMPETÊNCIA

5.1 Compete ao Comitê de Segurança da Informação e Proteção de Dados (CSIPD) 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 Comunicação.
5.2. Compete à Coordenadoria de Segurança da Informação (CSI) orientar e monitorar a implementação desta norma, fornecendo ao CSIPD 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.
5.4 Compete, solidariamente, às demais unidades organizacionais do TRT-7 verificar o uso adequado dos recursos computacionais e a observância das regras contidas nesta norma.
5.5 Compete aos(às) 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-7, zelando por seu fiel cumprimento.
5.5.2 Requerer a concessão, alteração ou a 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(às) gestores(as) das áreas de negócio:
5.6.1 A gestão do acesso, ou seja, efetivar o cadastro, a alteração ou a revogação do acesso dos(as) usuários(as) aos sistemas e /ou aos dados sob sua responsabilidade;
5.6.2 Excepcionalmente, compete à SETIC efetivar as concessões, alterações ou as 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 O(A) usuário(a) é responsável por:
5.7.1 Conhecer e cumprir integralmente as normas de controle de acesso e utilização dos recursos de TIC do TRT-7.
5.7.2 Reportar, por meio da Central de Serviços de TIC, suspeita ou ocorrência de violações desta norma.
5.7.3 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.
5.7.4 Preservar o sigilo de sua senha ou outro mecanismo de autenticação que venha a ser utilizado para acesso aos recursos tecnológicos disponibilizados.
5.7.5 Preservar o sigilo das informações a que tiver acesso, sendo vedada sua revelação a usuários(as) ou terceiros(as) não autorizados(as).
5.7.6 Atos praticados e acessos realizados aos recursos de tecnologia por meio de sua credencial de acesso.
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(a) gestor(a) 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 do e-mail corporativos para os(as) novos(as) usuários(as), 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, de falecimentos e de desligamento dos(as) estagiários(as).
5.9.3 Comunicar mensalmente à SETIC os casos de mudanças de lotação, de uma unidade gestora para outra no Tribunal.
5.10 Poderá ser concedido acesso temporário a funcionários(as) de empresas prestadoras de serviços, quando necessário para desenvolver atividade para este Tribunal.
5.10.1 Compete ao(à) gestor(a) do contrato a requisição da liberação deste acesso, informando o perfil necessário, bem como a solicitação de exclusão imediatamente após o desligamento dos(as) terceirizados(as);
5.10.2 Compete ao(à) fiscal técnico(a) do contrato supervisionar o uso dos recursos de TIC liberados para os(as) terceirizados (as);
5.11 Poderá ser concedido acesso temporário a servidores(as) pertencentes a outros órgãos públicos, quando em atividade de interesse deste Tribunal, sendo de competência do(a) gestor(a) 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 TIC será disponibilizado para usuários(as) autorizados(as) 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 Resolução Normativa TRT7 nº 5/2023, que dispõe sobre a POSIC), bem como a presente norma, em formato eletrônico, para a caixa postal institucional pessoal do(a) usuário(a), 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 para armazenamento das contas de acesso aos ativos de TIC, de modo a controlar o acesso aos mesmos para reforço da segurança e da proteção dos recursos computacionais.
6.3 Cada usuário(a) deve possuir uma única conta de acesso às informações e ativos de TIC do TRT.
6.3.1 Excepcionalmente, quando previamente autorizado 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(às) usuários(as) do TRT-7 o acesso às informações e aos recursos de TIC limitado ao mínimo que atenda à necessidade de conhecer (princípio do menor privilégio) e aos requisitos previstos em lei, acordos, contratos e

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

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(à) usuário(a) 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(a) usuário(a);
6.7 Contas de acesso de estagiários(as) e de terceirizados(as) 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 Especializadas, Tribunal Pleno e nas Turmas.
6.9 Na utilização das credenciais de acesso, compete ao(à) usuário(a) 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.
6.10 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade pública será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.
6.11 Os eventos de acesso, alteração, exclusão, compartilhamento ou qualquer outra forma de tratamento das informações serão registrados, sempre que possível, para rastreamento da data/hora, origem dos acessos e autoria das ações.
6.12 O TRT-7 poderá suspender, integralmente ou parcialmente, o acesso aos recursos de TIC para servidores(as) ou magistrados(as) que estejam de licença de longa duração, por deliberação da Presidência, em cada caso concreto.
6.13 O TRT-7 deverá suspender o acesso aos recursos de TIC para servidores(as) que estejam cedidos(as) a outros órgãos, mantendo o mínimo de recursos necessários para comunicação institucional com o(a) servidor(a) e seu acesso aos comprovantes de renda.
7. DA IDENTIFICAÇÃO DO(A) USUÁRIO(A)
7.1 A credencial (login e senha) do(a) usuário(a) 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-7, previamente autorizado pela SETIC, nos casos de uso compartilhado para acesso específico e limitado, tais como os microcomputadores destinados:
a) ao público externo nas salas de audiência;
b) aos totens de registro de ponto eletrônico dos(as) servidores(as);
c) às salas de treinamento;
d) às sessões de julgamento.
7.3 O identificador do(a) usuário(a) é utilizado para associá-lo(a) aos respectivos direitos de acesso e ao histórico de ações realizadas enquanto perdurar tais direitos.
7.4 A formatação da credencial deverá seguir, no que couber, o padrão de formatação de endereços de correio eletrônico e de caixas postais individuais especificado no ePING, inclusive quanto às regras de exceção.
7.5 A credencial da rede corporativa, em qualquer hipótese, será criada e fornecida pela SETIC, após solicitação, via Central de Serviços.
7.6 A credencial de acesso, para os recursos de TIC que não possuam autenticação integrada à rede corporativa, poderá ser criada pelo(a) respectivo(a) gestor(a), mediante autorização prévia da SETIC, e, sempre que possível, a identificação deve ser a mesma usada na rede corporativa.
7.7 Excepcionalmente, caso o(a) usuário(a) necessite alterar a sua identificação, deverá encaminhar solicitação à SETIC, devidamente justificada, via Central de Serviços de TIC, que, se aprovada, promoverá a adequação.
7.7.1 A nova identificação, sempre que possível, deverá seguir a padronização a que se refere o item 7.4.
8. DAS SENHAS DOS ATIVOS DE TIC DO TRT-7
8.1 A senha utilizada no acesso às informações e ativos de TIC do TRT deve possuir tamanho maior ou igual a 12 (doze) caracteres, contendo ao menos 3 (três) dos seguintes tipos: letras maiúsculas, minúsculas, números e caracteres especiais.
8.2 No caso de sistemas legados, quando inviável sua melhoria, admitir-se-ão senhas com no mínimo 8 caracteres, sendo ao menos 1 caractere alfabético e 1 caractere numérico.
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(a) usuário(a) com uma periodicidade máxima de 180 (cento e oitenta) 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 3 dias 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(a) usuário(a), a sua recuperação somente dar-se-á mediante requisição feita à Central de Serviços de TIC.
8.6 A SETIC encaminhará a senha provisória aos(às) usuários(as):
8.6.1 No credenciamento inicial.
8.6.2 Nos casos de bloqueios, perda ou de 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(a) usuário(a).
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(às) usuários(as), em qualquer hipótese, têm caráter temporário e devem ser

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

imediatamente alteradas pelo(a) usuário(a);
8.8.1 A SETIC deverá, sempre que viável tecnicamente, implementar mecanismo que obrigue a alteração das senhas provisórias.
8.9 Caso o(a) usuário(a) suspeite de violação da confidencialidade da senha, é de sua responsabilidade alterá-la imediatamente.
8.10 É vedado a qualquer unidade organizacional, inclusive à SETIC, solicitar aos(às) usuários(as), por qualquer meio, o envio de senhas.
8.11 É permitido o uso pelos(as) usuários(as) internos(as) de software de gerenciamento de senhas (cofre de senhas) quando armazenadas em local seguro e com criptografia e, ainda, previamente homologado pela SETIC.
8.12. Os(As) usuários(as) não devem:
8.12.1 Anotar sua senha de acesso aos sistemas do Tribunal em lembrete visível no ambiente de trabalho do Tribunal ou mesmo no teletrabalho.
8.12.2 Armazenar a senha em qualquer software que possua recurso de "memorização de senhas" (navegador web, por exemplo), exceto quando utilizando a solução de cofre de senhas homologada pela SETIC.
8.12.3 Compartilhar a senha com outras pessoas.
8.12.4 Armazenar a senha em local acessível a terceiros(as), tais como: computadores próprios, ambiente de colaboração, etc.
8.12.5 Cadastrar a mesma senha utilizada na sua conta institucional do TRT em qualquer serviço externo ao TRT-7, mesmo que relacionado ao serviço.
8.13 O cadastramento de senhas em serviços externos e necessários às atividades deve seguir, no que couber, as disposições desta norma.
8.13.1 Não é permitido o compartilhamento de usuário(a) e senha dos serviços externos, exceto se não estiver disponível a individualização dos acessos.
9. DA AUTENTICAÇÃO
9.1 Recursos de TIC devem, sempre que possível tecnicamente, conter mecanismos de autenticação que exijam a confirmação da identidade do(a) usuário(a).
9.2 A autenticação deve ser realizada minimamente por meio do fornecimento de login e senha.
9.3 Dar-se-á preferência pela exigência da autenticação de multifatores para o controle de acesso lógico, a fim de autenticar a identidade de um(a) usuário(a) e vinculá-lo(a) a uma conta de acesso a ativos de informação, como por exemplo o uso simultâneo do login e senha com código de validação em dispositivo móvel, a depender dos requisitos de segurança identificados para cada recurso de TIC.
9.3.1 Sempre que possível, deverá ser implementado múltiplo fator de autenticação para soluções de acesso remoto, como VPN e Remote Desktop, e para privilégios administrativos, como acessos a redes de controle ou gerência, interfaces de administração de soluções, entre outros.
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(a) último(a) usuário(a) que acessou o recurso de TIC.
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(a) usuário(a) (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.
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(a) usuário(a) 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(as) aqueles(as) que exerçam 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 TIC do TRT-7.
10.3 Cada usuário(a), a critério da Administração e de acordo com a necessidade de serviço, credenciado(a) 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 TIC.
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.

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

10.3.8 Internet.
10.3.9 Dispositivos móveis.
10.3.10 Mídias removíveis.
10.3.11 Redes sociais.
10.4 Os(As) usuários(as) são responsáveis pelo uso adequado dos recursos de tecnologia da informação, conforme as diretrizes desta norma e das demais que constituem a Política de Segurança da Informação e Comunicação 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 TIC disponibilizados pelo TRT-7 de:
10.5.1 Material não ético, discriminatório, malicioso, ofensivo, obsceno ou ilegal.
10.5.2 Jogos de qualquer natureza e "correntes".
10.5.3 Material protegido por lei de propriedade intelectual, sobre os(as) quais os(as) usuários(as) não possuam o devido direito.
10.5.4 Propagandas com objetivo comercial.
10.5.5 Material de natureza político-partidária.
10.5.6 Material de cunho religioso.
10.5.7 Vírus de computador ou qualquer tipo de programa malicioso que possa ser considerado nocivo aos recursos de TIC.
10.5.8 Trabalhos particulares.
10.5.9 Materiais online ou offline (armazenados nos dispositivos) voltados ao entretenimento, tais como filmes, livros, sons, textos, redes sociais pessoais, canais de TV digital, galerias de imagens ou vídeos.
10.5.10 É tolerado a reprodução habitual de músicas, desde que os conteúdos não contrariem os itens de 10.5.1 a 10.5.9 deste ato, por meio de acesso online via internet ou ainda arquivos de áudios armazenados no desktop do(a) próprio(a) usuário(a) e para uso individual, preferencialmente com uso de fones de ouvido. Alternativamente, poderá ser utilizado o dispositivo de som do desktop, quando não cause perturbação ao ambiente de trabalho, a juízo do(a) gestor(a) da unidade.
10.6 É vedado instalar nas estações de trabalho programas de computador não enquadrados no item "Do Uso dos Sistemas de Tecnologia da Informação e Programas de Computador".
10.7 É tolerado o envio de mensagens de natureza associativa ou sindical provenientes do sindicato ou da associação de servidores(as) e de magistrados(as), apenas de caráter informativo, sendo vedado o uso do e-mail corporativo para fóruns de discussão e propaganda eleitoral das chapas.
10.8 É proibido o encaminhamento de informações privilegiadas, confidenciais e/ou de propriedade do Tribunal para destinatários(as) não autorizados(as), por intermédio de quaisquer dos meios e de recursos de tecnologia da informação e comunicação disponibilizados pelo TRT da 7ª Região.
10.9 É proibida aos(às) usuários(as) 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 e comunicação disponibilizados pelo TRT da 7ª Região, exceto nos casos em que a atividade funcional demande tal ação.
10.10 É proibida a utilização, por pessoas não classificadas nesta norma, de quaisquer recursos de TIC deste Regional.
10.11 É proibido o armazenamento e o encaminhamento de dados criptografados, por intermédio de quaisquer dos meios e recursos de tecnologia da informação e comunicação disponibilizados pelo TRT da 7ª Região, exceto se usando funcionalidade de criptografia presente em sistemas ou serviços homologados e/ou disponibilizados pelo Tribunal.
10.12 É proibido aos(às) usuários(as) criarem contas em serviços externos, tais como serviços de e-mail, redes sociais, aplicativos de mensagens ou quaisquer outros utilizando o nome ou a sigla do Tribunal da 7ª Região ou de suas unidades organizacionais, exceto quando justificados e previamente autorizados pela Presidência. Exemplos de proibições: e-mails tais como fulanodetal.TRT-7@gmail.com, trtce.secretariaX@outlook.com; contas em redes sociais tais como varadotrabalho-trtce ou trtce-setorx.
10.12.1 É permitida a criação de contas/listas/grupos de servidores(as) ou de magistrados(as) em redes sociais que contenham o nome ou a sigla do Tribunal ou de suas unidades organizacionais, desde que destinadas exclusivamente para comunicação interna e integração destes, vedada a prestação de serviços ou publicação de informações, dados ou documentos em nome do Tribunal.
10.13 É vedado o armazenamento de informações em dispositivos (nuvem, e-mail, rede, entre outros) para cuja edição e armazenamento o TRT-7 disponibilize ambientes ou sistemas próprios para aquele tipo de informação, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas e informações pessoais.
10.14 Para implementar os controles de acesso aos recursos de TIC é fundamental a elaboração de processos de trabalho, bem como programas periódicos de sensibilização e de conscientização em conformidade com a POSIC e com as normas complementares.
10.15 Não é permitido utilizar os serviços e os sistemas de TIC do Tribunal utilizando microcomputadores de uso compartilhado em estabelecimentos tais como cibercafés ou hotéis.
10.16 Não é permitido o uso habitual dos serviços e dos sistemas de TIC do Tribunal utilizando redes públicas, tais como as disponibilizadas em hotéis, restaurantes, aeroportos ou prefeituras.
10.16.1 Quando necessário, o(a) usuário(a) deverá dar preferência pelo acesso utilizando sua rede de dados móveis, ou nesta impossibilidade, deverá se certificar que está se comunicando com criptografia de ponta a ponta (por exemplo, sites que aparecem um símbolo de cadeado fechado em seu endereço/URL).
11. DO ACESSO PRIVILEGIADO OU ADMINISTRATIVO
11.1 O acesso local ou remoto aos computadores deste Regional com privilégios de Administrador(a) de Sistema é exclusivo da SETIC, podendo ser atribuído tal privilégio, temporariamente, a usuários(as) 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

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

diretrizes para as contas de acesso normais.
11.4 O uso de contas com privilégios administrativos é restrito às atividades exclusivas de administração e de configuração dos ativos de TIC, sendo proibido o uso para desempenho de atividades de negócio.
11.5 A SETIC deverá, sempre que a tecnologia suportar o uso de contas individuais, evitar o uso das contas administrativas genéricas, mantendo-as desativadas.
11.6 É permitida a criação de contas de serviços ou de sistemas, quando estritamente necessários à operacionalização ou à integração destes, cuja senha poderá ser de conhecimento apenas das pessoas envolvidas na implantação e na sustentação destes serviços.
11.7 Aos(Às) servidores(as) da SETIC e às demais pessoas formalmente envolvidas em novos projetos de TIC são permitidos a instalação e o uso de softwares não homologados e a mudança na configuração padrão das estações de trabalho, durante o 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.
11.7.1 É de responsabilidade dos(as) das pessoas mencionadas no item 11.7 executar, ou abrir chamado na Central de Serviço de TIC, para remoção dos softwares utilizados durante o projeto, bem como para a restauração das configurações padronizadas.
11.8 A SETIC deverá adotar solução informatizada para gerenciamento de acesso privilegiado, destinado principalmente às contas dos(as) administradores(as) de sistemas de informação e de recursos de TIC (redes, bancos de dados, sistemas operacionais, armazenamento, entre outros), bem como para proteção de contas não humanas, como por exemplo, contas de sistemas de informação para acesso e/ou integração com outros recursos.
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 Coordenadoria de Infraestrutura de Tecnologia da Informação e Comunicação (CITIC), da SETIC.
12.2 O acesso às áreas referidas neste item por pessoas estranhas à CITIC 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 CITIC.
12.2.1 Deverá ser mantido registro de todos os acessos.
12.3 Será permitido acesso de terceiros(as) para execução de serviços não previamente agendados nos centros de dados para manutenção emergencial, desde que acompanhados(as) por servidor(a) da CITIC, que providenciará registro após a intervenção.
12.4 É responsabilidade de todos(as) 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(à) responsável pelo ambiente e, por este(a), ao(à) 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 aos demais equipamentos e softwares presentes nos Centros de Dados deste Tribunal é restrito ao pessoal da CITIC, podendo ser estendido a outras unidades da SETIC, conforme a necessidade, mediante autorização e controle de acessos pela CITIC.
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 CITIC.
12.6.1 Ao ser identificada a necessidade de acesso remoto por prestador de serviço, é necessário que a Coordenadoria de Infraestrutura de TIC esteja antecipadamente ciente da data, hora e da duração da manutenção a ser feita para que possa ser concedido o acesso temporário.
13. DO USO DE EQUIPAMENTOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
13.1 Relativamente ao uso dos equipamentos de TIC, 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 a 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 As atividades descritas nos subitens 13.1.1 a 13.1.5 devem, quando necessárias, ser executadas pela equipe técnica da SETIC, ou, em caráter excepcional, pelos(as) usuários(as), quando solicitado pela SETIC e sob supervisão desta.
13.2 A SETIC criará padrões de configuração adequados às necessidades de utilização das unidades judiciais e administrativas.
13.3 Os equipamentos de TIC, 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.
13.3.1 Cabe ao responsável pela unidade a que se destina o equipamento o imediato recebimento do bem no Sistema de Controle de Material e Património (SCMP) assim que instalado.
13.4 É de responsabilidade do(a) usuário(a):
13.4.1 Desligar ou bloquear a tela e o 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 bens de consumo, tais como cartuchos de tonalizador, unidades fusoras e cilindros de imagem para impressoras a laser, cartuchos para impressoras a jato de tinta, fitas magnéticas, mídias removíveis, tokens para certificados

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

digitais, bobinas para impressoras térmicas e laser, baterias.
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(A) usuário(a) 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 à configuração de sistemas ou aplicativos, ainda que disponibilizados pelo TRT-7 (certificado digital, por exemplo), seja quanto às questões relacionadas à conexão à rede sem fio.
13.8 Os computadores para uso individual ou coletivo serão dotados de solução de proteção de endpoints.
14. DO USO DE DISPOSITIVOS MÓVEIS
14.1 Quando da concessão de dispositivos móveis do Tribunal ao(à) usuário(a), é necessário que esses sejam previamente homologados e configurados pela SETIC, atendendo aos requisitos de segurança, incluindo a instalação de software de segurança de endpoints do Tribunal.
14.2 O fornecimento de computadores portáteis a magistrados(as) e a servidores(as) está condicionado às necessidades de trabalho e à assinatura do Termo de Responsabilidade e Recebimento.
14.3 A cópia de segurança de dados locais (armazenados no dispositivo) é de exclusiva responsabilidade do(a) usuário(a).
14.4 Em caso de exoneração, dispensa da função, cedência, remoção, aposentadoria ou de término das atividades que ensejaram o fornecimento, o equipamento deverá ser devolvido ao TRT-7, 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(a) usuário(a) com o Tribunal, deve ser restrito somente às redes sem fio destinadas para essa finalidade.
14.6 Os dispositivos móveis disponibilizados pelo TRT não terão privilégio de administrador(a) para os(as) destinatários(as) dos equipamentos, aplicando-se as mesmas regras de segurança das estações de trabalho, no que couber.
14.7 A perda ou o furto de equipamentos de TIC do TRT-7 devem ser comunicados imediatamente à SETIC, além de tomadas as providências administrativas cabíveis.
15. DO USO DE MÍDIAS REMOVÍVEIS
15.1 É de responsabilidade do(a) usuário(a) 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(as) usuários(as) para prática dos atos de ofício.
16.2.2 Sempre que possível, dar-se-á preferência pela utilização de assinatura eletrônica por meio de certificado digital emitido por autoridade certificadora pertencente à cadeia de confiança de certificação digital ICP-Brasil ou outro mecanismo seguro com pelo menos dois fatores de autenticação.
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(as) por ela autorizados(as).
16.4 As unidades organizacionais do TRT-7 serão responsáveis pela alimentação e pela atualização das informações que lhes competirem nos sistemas de tecnologia da informação e comunicação, devendo manter a precisão e a correção dos dados informados.
16.5 Nos casos de alteração ou de 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 cópia de segurança.
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 comunicação e dos 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 SETIC, 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.
16.8 As unidades organizacionais do Tribunal Regional do Trabalho da 7ª Região poderão submeter pedido de homologação de programa de computador à SETIC para uso em suas atividades, que poderá homologá-lo ou, se entender necessário, elaborar parecer técnico e submetê-lo à apreciação do CSIPD.
16.9 A SETIC publicará, na Intranet/Extranet, 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 os serviços de TIC do TRT-7, quando disponíveis para acesso via internet, devem ser protegidos com o uso de mecanismos de criptografia.

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(às) magistrados(as) e (às)servidores(as) do Tribunal para comunicação interna feita de acordo com as regras adiante estabelecidas.
17.1.2 Os(As) magistrados(as) e os(as) servidores(as) ativos(as) deverão possuir conta de e-mail para fins de recebimento e de 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 @TRT-7.jus.br.
17.1.2.1 É vedado o fornecimento de caixa postal institucional para magistrados(as) e para servidores(as) inativos(as), bem como para pensionistas.
17.1.3 Cabe à SETIC administrar os recursos de TIC envolvidos e os limites de utilização das caixas postais de cada usuário (as).
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 será feito do navegador de internet, não sendo permitida a utilização de softwares cliente de e-mail para baixar e gerenciar mensagens diretamente no microcomputador, tais como Mozilla Thunderbird, Mailbird e Opera Mail.
17.1.5.1 É permitida a utilização do e-mail institucional no smartphone pessoal do titular da conta, sendo vedada a utilização da mesma para sincronização das cópias de segurança dos dados pessoais presentes no dispositivo, tais como fotos e vídeos.
17.1.6 Serão registrados os dados de envio e de 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 cópia de segurança do Tribunal.
17.1.7 São proibidos, no desempenho das atribuições institucionais, o envio e o recebimento de mensagens eletrônicas mediante a utilização de serviços de e-mail pertencentes a entidades estranhas ao TRT-7.
17.1.8 O uso do correio eletrônico será monitorado por meio de ferramentas com o objetivo de evitar o recebimento de mensagens que coloquem em risco a segurança das informações 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 vedações constantes desta norma, a SETIC adotará medidas imediatas para a apuração e solução do Incidente de Segurança.
17.1.10 As mensagens de e-mail permanecerão na lixeira pelo período de 30 (trinta) dias após a exclusão, sendo excluídas automaticamente após esse período ou também poderão ser excluídas da lixeira pelo(a) usuário(a), não sendo possível a recuperação nessas hipóteses.
17.1.11 Em nenhuma hipótese, será realizada pela SETIC transferência, cópia de segurança ou download de e-mails recebidos ou enviados.
17.1.12 A caixa postal institucional pessoal de magistrados(as) e/ou de servidores(as) será excluída definitivamente nos casos de falecimento, exoneração, demissão, redistribuição, aposentadoria, remoção, permuta, vacância por posse em outro cargo inacumulável e cedência a outro órgão ou retorno à origem.
17.1.12.1 Não ocorrerá a exclusão da caixa postal institucional pessoal nos casos de licenças.
17.1.12.2 A exclusão da caixa postal será realizada pela SETIC após comunicada pela Secretaria de Gestão de Pessoas, ou, independente de aviso, se constatada no sistema de gestão de pessoas o término do vínculo com o TRT-7, resguardado o disposto nos itens 20.7 a 20.10.
17.1.13 A SETIC poderá definir, ouvido o Comitê de Segurança da Informação e Proteção de Dados, capacidade mínima e máxima das caixas postais e tamanho máximo de cada e-mail.
17.2 DAS CAIXAS POSTAIS DE ESTAGIÁRIOS(AS) E DE TERCEIRIZADOS(AS)
17.2.1 Poderá ser solicitada à SETIC a criação de conta de e-mail para uso por estagiário(a) ou por empregado(a) terceirizado (a), desde que devidamente justificada pelo(a) requerente, acrescendo-se como prefixo ao identificador do(a) usuário(a) a expressão “estagio.”, no caso de estagiário(a), e de “terceirizado(a)”, quando empregado(a) terceirizado(a).
17.2.2 A quantidade de caixas postais disponíveis para estagiários(as) e para terceirizados(as) deverá ser previamente autorizada pelo Comitê de Governança de TIC, sempre que se tratar de serviço contratado.
17.2.3 O envio de mensagens por estagiários(as) ou por terceirizados(as) será restrito a endereços eletrônicos mantidos pelo TRT-7.
17.2.3.1 Quando for expressamente solicitado, com a devida justificativa pelo(a) gestor(a) da unidade a que vinculados(as), será permitido o envio a endereços externos.
17.3 DAS CAIXAS POSTAIS DE UNIDADES ORGANIZACIONAIS
17.3.1 Poderá ser criada conta de e-mail para unidades organizacionais, de qualquer nível organizacional, apenas se houver recurso técnico para delegação, limitada a uma conta por unidade.
17.3.2 É vedado o compartilhamento de senhas para acesso à caixa posta.
17.3.3 O endereço eletrônico será composto pela sigla da unidade, usualmente utilizada neste Tribunal, e pelo sufixo @TRT-7.jus.br.
17.3.4 A conta deverá ser delegada ao(à) titular da unidade e a servidores(as) autorizados(as) a operá-la.
17.4. DAS CAIXAS POSTAIS DE SISTEMA
17.4.1 A caixa postal de sistema será criada quando houver essa necessidade para o funcionamento de um sistema informatizado.
17.4.2 O(A) gestor(a) da unidade responsável pelo desenvolvimento ou manutenção do sistema informatizado será também o (a) gestor(a) da respectiva caixa postal, competindo-lhe:
17.4.2.1 Solicitar a criação, alteração e a exclusão da caixa postal de sistema.
17.4.2.2 Autorizar o acesso de outros(as) servidores(as), mediante delegação no sistema de correio eletrônico, bem como

excluir esse acesso.
17.4.2.3 O identificador do endereço de correio eletrônico será formado pela denominação ou sigla que permita a identificação do respectivo sistema informatizado.
17.5 DAS LISTAS DE DISTRIBUIÇÃO PARA UNIDADES, COMISSÕES OU PARA GRUPOS DE TRABALHO
17.5.1 É permitida a criação de lista de distribuição com o objetivo de facilitar e de otimizar a troca de informações sobre assuntos de interesse do Tribunal.
17.5.2 A criação de lista de distribuição pode ser solicitada pelo(a) gestor(a) da unidade a qual se destina, pela Presidência ou ainda por coordenadores(as) de comissões ou de grupos de trabalho.
17.5.3 A solicitação deve ser encaminhada à SETIC acompanhada de informações sobre a finalidade da lista, nome do(a) gestor(a) da lista, e, quando destinada à atividade temporária, do período de sua duração.
17.5.4 O identificador do endereço eletrônico será formado pela denominação ou pela sigla, que permita, de forma clara, a identificação de sua finalidade, ou do grupo de endereços eletrônicos nela reunidos.
17.5.5 É responsabilidade do(a) gestor(a) da lista:
17.5.5.1 Manter permanentemente atualizado o rol de integrantes da lista de distribuição.
17.5.5.2 Solicitar exclusão como gestor(a) e indicar, simultaneamente, o(a) novo(a) responsável pela lista de distribuição.
17.5.5.3 Solicitar exclusão da lista de distribuição, quando esta não for mais necessária.
17.5.6 A lista de distribuição será composta exclusivamente por endereços eletrônicos do Tribunal.
17.5.6.1 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 pela Presidência do Tribunal como integrantes do respectivo grupo/comissão.
17.5.6.2 A SETIC poderá, por solicitação do(a) gestor(a) 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.
17.5.7 O envio de mensagem eletrônica para lista de distribuição que englobe elevado número de endereços eletrônicos é permitido em caráter excepcional ou a unidades administrativas, autorizado pela Presidência.
17.5.8 O TRT-7 poderá disponibilizar lista de distribuição contendo todos(as) os(as) usuários(as) internos(as), desde que exista bloqueio para o recebimento de mensagens eletrônicas enviadas apenas pelo público interno.
17.6 DAS LISTAS DE DISTRIBUIÇÃO PARA PÚBLICO EXTERNO
17.6.1 Compete à Coordenadoria de Comunicação Social do TRT-7 a criação, gerenciamento e o uso de listas de distribuição destinadas ou público externo, como imprensa, advogados(as) e instituições parceiras, entre outros.
17.6.1.1 Excepcionalmente, outras unidades poderão criar listas de distribuição para o público externo, desde que formalmente autorizadas pela Presidência do Tribunal.
17.7. DAS RESPONSABILIDADES DOS(AS) USUÁRIOS(AS) DO SERVIÇO DE E-MAIL
17.7.1 Rotina diária de verificação das caixas postais eletrônicas realizada pelos(as) servidores(as).
17.7.2 Manter espaço disponível para recebimento de novas mensagens.
17.7.3 Excluir mensagens que não sejam de interesse da Administração.
17.7.4 Não permitir o acesso de terceiros(as) ao seu e-mail.
17.7.5 Encaminhar as comunicações oficiais à caixa postal das unidades organizacionais.
17.7.6 Utilizar o seguinte texto para rodapé de e-mails do Tribunal enviados a destinatários(as) externos(as):
"AVISO LEGAL: O(A) emitente desta mensagem é responsável por seu conteúdo e endereçamento. Cabe ao(à) destinatário (a) cuidar quanto ao tratamento adequado. Sem a devida autorização é proibida a divulgação, reprodução ou a distribuição das informações aqui dispostas. Se você não for o(a) destinatário(a) 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."
17.7.7 Notificar a SETIC, via Central de Serviços de TIC, quando do recebimento de mensagens com conteúdo suspeito.
17.7.8 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(a) usuário(a) da rede para um sítio falso, possibilitando a captura de informações.
17.7.9 Levar em conta o sigilo da informação a ser encaminhada, devendo consultar seu(sua) superior hierárquico(a) em caso de dúvida.
18. DO USO DOS SERVIÇOS DE COMUNICAÇÃO INSTANTÂNEA
18.1 O serviço de mensagem instantânea disponibilizado pelo TRT-7 é de uso facultativo e destina-se às comunicações internas.
18.2 O(A) responsável por unidade organizacional poderá solicitar à SETIC liberação de acesso para uso por estagiário(a) ou por empregado(a) terceirizado(a), desde que devidamente justificada pelo(a) requerente.
18.3 É vedado o uso de IM (Instant Messenger) não homologado ou não autorizado;
18.4 Os(As) magistrados(as) e os(as) servidores(as) 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 ARMAZENAMENTO DE ARQUIVOS
19.1 Cada unidade organizacional, conforme o organograma do Tribunal, terá disponível 1 (uma) área de armazenamento, em rede própria ou em nuvem contratada para salvaguardar os arquivos provenientes, exclusivamente, das atividades laborais das unidades administrativas, com garantia de controle de acesso.
19.2 A SETIC definirá as regras de acesso para aplicação padronizada em todas as unidades administrativas e judiciárias.
19.3 Cabe ao(à) Gestor(a) da Unidade a criação e a organização de pastas dos documentos dentro da área de armazenamento;
19.4 Os(As) usuários(as) devem, periodicamente, fazer a eliminação de arquivos desnecessários e evitar a manutenção de mais de uma cópia do mesmo arquivo.
19.5 A SETIC poderá excluir conteúdo que não esteja em conformidade com as normas de segurança da informação do TRT-

7, quando da realização de manutenções periódicas nas áreas de armazenamento de arquivos a fim de liberar espaço e de otimizar a sua utilização.
19.6 As regras de cópias de segurança para as áreas de armazenamento serão disciplinadas em ato próprio.
19.7 Os dados armazenados nas estações de trabalho dos(as) usuários(as) do Tribunal não estão contemplados pelas garantias de controle de acesso e cópia de segurança, cabendo aos(às) usuários(as) providenciar cópia para os repositórios oficiais (pastas de armazenamento, sistemas de informação ou colaboração) e a eliminação periódica dos arquivos armazenados nos discos rígidos locais.
19.8 É vedado o armazenamento de documentos em locais distintos daqueles para cuja edição e armazenamento o TRT-7 disponibiliza sistemas próprios, tais como minutas de despachos, sentenças, acórdãos e outras decisões judiciais ou administrativas.
19.9 Sempre que possível, a SETIC deverá registrar as operações realizadas pelos(as) usuários(as) nas áreas de armazenamento, tais como leitura, alteração ou exclusão de pastas e arquivos, de forma a permitir a rastreabilidade e a identificação do(a) usuário(a), mantendo-os pelo período mínimo de 6 (seis) meses.
20. DO USO DA NUVEM CORPORATIVA
20.1 O acesso via internet deverá ser exclusivamente por meio de protocolos seguros de comunicação, cabendo à SETIC a implementação transparente deste recurso.
20.2 Informações e documentos específicos armazenados na nuvem corporativa poderão ser compartilhados temporariamente com usuários(as) externos(as) (como servidores(as) de outros órgãos ou empregados(as) de empresas contratadas), quando necessários ao desenvolvimento das atividades, previamente autorizado pelo(a) responsável da unidade e mediante, quando for o caso, assinatura de termo de confidencialidade.
20.3 Cabe ao(à) chefe de unidade organizacional a orientação dos(as) seus(suas) subordinados(as) quanto à concessão e à revogação de compartilhamento.
20.4 Os arquivos mantidos pelos(as) usuários(as) na nuvem corporativa devem estar acessíveis, ao menos, ao(à) proprietário (a) e, se houver, a seu(sua) substituto(a) e aindaao(à) chefe(a) da unidade.
20.5 Os arquivos armazenados na nuvem corporativa permanecerão na lixeira pelo período de 30 (trinta) dias em caso de exclusão, sendo excluídos automaticamente após esse período, ou também poderão ser excluídos da lixeira pelo(a) usuário (a), não sendo possível a recuperação nessas hipóteses.
20.6 Os arquivos armazenados na nuvem corporativa deverão ser vinculados (ter como proprietário(a)) à conta institucional da unidade, quando existente, ou outra designada pelo(a) gestor(a) da unidade para tal fim.
20.7 Nos casos de mudanças de lotação ou de desligamento de servidor(a) ou de estagiário(a) (casos de exclusão da conta da nuvem corporativa), o(a) gestor(a) da unidade deverá solicitar ao(à) servidor(a) ou ao(à) estagiário(a), de forma antecipada, sempre que possível, a verificação da existência de arquivos que digam respeito às atividades da unidade e que permaneçam na propriedade do(a) servidor(a)/estagiário(a), para que sejam transferidos para a conta da unidade ou para outra designada pelo(a) gestor(a).
20.7.1 Caso persistam arquivos vinculados à conta do(a) servidor(a)/estagiário(a) quando de sua exclusão, eles serão transferidos para a conta da última unidade de lotação, com a finalidade exclusiva de manter o acesso aos arquivos compartilhados.
20.7.2 Caso não seja possível identificar a última unidade de lotação ou, ainda, se ela não possuir uma conta, os arquivos serão movimentados para a conta da Secretaria de Gestão de Pessoas.
20.8 Nos casos de desligamento de magistrados(as) (casos de exclusão da conta da nuvem corporativa), a Presidência decidirá, de ofício ou por provocação, de forma antecipada, sempre que possível, sobre a necessidade de transferência ou de download dos arquivos armazenados na nuvem, com a finalidade exclusiva de manter o acesso aos arquivos compartilhados, quando necessário.
20.9 Nos casos de exclusão da caixa postal institucional de unidade, os arquivos serão transferidos para a conta da unidade designada como nova responsável pelas atividades ou para servidor(a) designado para tal fim.
20.10 Em nenhuma hipótese será realizado pela SETIC, transferência, cópia de segurança ou download dos registros de eventos em agendas e históricos de conversas nos espaços de chat.
20.10.1 Os itens de 20.7 à 20.9 referem-se exclusivamente aos arquivos presentes nos espaços de armazenamento da conta.
20.11 A SETIC poderá excluir conteúdo que não esteja em conformidade com as normas de segurança da informação do TRT-7, quando da realização de manutenções periódicas nas pastas de armazenamento de arquivos a fim de liberar espaço e de otimizar a sua utilização.
21. DO USO DA REDE CORPORATIVA
21.1 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 e Comunicação, visando preservar a segurança e a disponibilidade dos recursos computacionais do Tribunal.
21.2 Todos os equipamentos e os dispositivos móveis conectados à rede lógica de dados do TRT-7 terão seus acessos monitorados por questões de segurança e para fins de auditoria.
21.3 A cada ponto de acesso físico à rede de dados do TRT-7, 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.
21.4 A conexão de qualquer equipamento à rede cabeada do TRT-7 só pode ser realizada pela SETIC, ou por terceiros(as) por ela autorizados(as).
21.5 A SETIC deverá utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.
21.6 Os acessos à rede corporativa de computadores serão registrados de forma a permitir a rastreabilidade e a identificação do(a) usuário(a), mantendo-os pelo período mínimo de 6 (seis) meses.
21.6.1 Sempre que possível, deve-se registrar, ao menos, a identificação do(a) usuário(a) e do equipamento utilizado (número IP), data/hora de login e data/hora de logout ou desligamento.

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

21.6.2 Para implementação deste controle, caso necessário, pode-se adotar o arquivamento dos registros em mídia de backup offline, mantendo em ambiente de produção somente os registros mais recentes.

22. DO USO DA REDE SEM FIO

22.1 O Tribunal disponibilizará 02 (duas) redes sem fio, sendo uma para usuários(as) internos(as) e outra para eventos ou para visitantes.

22.2 A abrangência das redes sem fio será definida pelo Comitê de Tecnologia da Informação e Comunicação, conforme a disponibilidade orçamentária para aquisição e para manutenção.

22.3 As redes sem fio deverão, necessariamente, estar separadas de modo seguro da infraestrutura de redes do TRT-7.

22.4 A rede sem fio disponibilizada para os(as) usuários(as) internos(as) dará acesso autenticado à internet, com filtragem de conteúdo e manutenção dos registros de acessos.

22.5 A rede sem fio disponibilizada para eventos ou para visitantes dará acesso à internet, com filtragem de conteúdo e, sempre que possível, manutenção dos registros de acessos.

22.6 A critério da SETIC, poderão ser adotadas medidas visando a manutenção da disponibilidade e da qualidade do acesso à internet disponibilizada aos serviços essenciais, como por exemplo, a limitação de banda de tráfego de dados para as redes sem fio.

23. DO USO DA INTERNET

23.1 Cada usuário(a), a critério da Administração, de acordo com a necessidade de serviço, poderá ter acesso à internet, identificado(a) pela sua credencial, de uso pessoal e intransferível, ressalvado o disposto no item 7.2.1.

23.2 As contas de usuários(as) deverão ter níveis de acessos distintos, conforme a necessidade dos serviços, de acordo com os perfis definidos pela SETIC;

23.3 O acesso a internet somente poderá ser efetuado por navegadores homologados pela SETIC;

23.4 Por motivos de segurança, todo acesso à internet será monitorado, e os registros serão mantidos pela SETIC.

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

23.5 Todo tráfego de internet será controlado, de forma automática, e poderá ser inspecionado, pela ferramenta de proxy web (filtro de conteúdo), configurada de acordo com os limites estabelecidos por esta norma ou definidos pela Administração do Tribunal.

23.5.1 A liberação de acesso a sítios e a serviços bloqueados, mas necessários ao desempenho das atribuições funcionais do (a) usuário(a), dependerá de solicitação, devidamente justificada, do(a) magistrado(a) ou do(a) gestor(a) da unidade à SETIC.

23.5.2 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.

23.6 Equipamentos do TRT-7 que estão fora das dependências (ex.: teletrabalho, home office, etc) da Justiça do Trabalho poderão ser configurados para utilizar os mecanismos de controle de acesso à internet estabelecidos nesta norma.

23.7 A utilização da Internet para acesso a informações e a serviços de caráter pessoal é permitida, desde que a frequência do uso e a quantidade de dados transmitidos considerem a disponibilidade dos canais de acesso, observadas as restrições presentes no item 10.5.

23.8 Constitui acesso indevido à internet qualquer das seguintes ações, exceto quando homologadas pelo TRT-7 ou autorizadas pelo Comitê de Segurança da Informação e Proteção de Dados:

23.8.1 Utilizar softwares para troca de conteúdo via rede ponto-a-ponto (peer-to-peer).

23.8.2 Uso de provedores de acesso externos.

23.8.3 Uso de proxy anônimo.

23.9 A comunicação entre a rede corporativa dos Tribunais e a Internet priorizará a prestação jurisdicional acima de outras necessidades.

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

23.10.1 Bloqueios totais ou parciais e/ou priorização de acessos a determinados sítios e serviços.

23.10.2 Limitação de banda de tráfego de dados.

23.11 As medidas identificadas no item 23.10, quando implementadas, serão comunicadas à Central de Serviços de TIC, para possibilitar o repasse de informações aos(às) usuários(as) interessados(as).

23.12 Os(As) usuários(as) devem evitar acessar links ou baixar arquivos de origem desconhecida.

24. DO USO DE REDES SOCIAIS

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

24.1.1 O pedido de acesso será avaliado pelo CSIPD.

24.1.2 Será concedido acesso aos(às) usuários(as) internos(as) para visualizarem as publicações do TRT-7 nas redes sociais, sempre que a tecnologia permitir restringir o acesso apenas ao respectivo perfil.

24.2 Exceto se formalmente autorizado, não é permitido aos(às) magistrados(as) e aos(às) servidores(as) criarem perfis de unidades (administrativas e judiciárias) nas redes sociais, bem como realizar postagens em quaisquer perfis de rede sociais em nome do Tribunal.

24.2.1 A solicitação deve ser encaminhada à Presidência, contendo a justificativa e o nome do(a) servidor(a) que será o(a) responsável pela conta.

24.3 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 de agentes públicos, e destina-se a divulgar campanhas promovidas pela Justiça do Trabalho ou pelo 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.

24.3.1 Decisões da Corte Trabalhista, divulgação de eventos abertos ao público, mensagens institucionais e informações úteis são exemplos de publicações a serem feitas pelo TRT-7 nas redes sociais.

24.4 Nos perfis institucionais, é proibida a publicação de conteúdo com emissão de opinião de caráter pessoal, político-

partidário, ofensivo, discriminatório ou jocoso.
24.5 As senhas dos perfis institucionais devem ser diferentes das senhas utilizadas na rede corporativa.
24.6 Devem ser utilizadas senhas distintas para cada perfil institucional criado.
24.7 É permitida a participação de servidores(as) e de magistrados(as) em fóruns de discussões na internet utilizando a identificação pessoal institucional (nome, e-mail, 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.
24.8 A Coordenadoria de Comunicação Social (CCS) é a unidade responsável pela administração e pelo gerenciamento dos perfis institucionais nas redes sociais.
24.9 Compete à equipe de administração e gerenciamento de perfis institucionais em mídias sociais:
24.9.1 Criar, alterar, excluir e controlar os perfis institucionais em mídias sociais do órgão ou da entidade.
24.9.2 Remover, tão logo tome conhecimento, postagens que atentem contra a segurança da informação.
24.9.3 Elaborar relatório semestral sobre a utilização de mídias sociais sob sua administração e apresentar ao CSIPD, contendo, ao menos, total de contas criadas e excluídas, total de seguidores(as) registrados(as), quantidade de postagens realizadas e removidas, e, se for o caso, descrição dos incidentes de segurança ocorridos e as medidas de correção adotadas.
24.9.4 Gerenciar, acompanhar e analisar, de forma contínua, as práticas de uso seguro de mídias sociais, com relação aos aspectos de segurança da informação.
24.9.5 Verificar se este ato normativo sobre o uso seguro de mídias sociais está sendo seguido de forma adequada e se há necessidade de revisão.
24.9.6 Implementar a cultura de uso seguro de mídias sociais e realizar as ações de segurança da informação cabíveis nesse contexto.
25. DO TELETRABALHO
25.1 Os sistemas de TIC elegíveis ao acesso ao teletrabalho são os disponíveis no Sítio Institucional do Tribunal, Extranet, Portal de Trabalho Remoto e Portal de Serviços do Tribunal disponibilizados por meio da internet.
25.2 Se econômica e tecnicamente viável, poderá ser concedido acesso remoto para servidores(as) e para magistrados(as) aos demais serviços não disponíveis nas plataformas citadas no item 25.1, quando indispensável ao teletrabalho, por meio de soluções homologadas e mantidas pela SETIC, tais como VPN e/ou soluções de virtualização.
25.3 O suporte de TIC prestado pela Central de Serviços de TIC aos(às) servidores(as) em teletrabalho, sobre os equipamentos particulares, limitar-se-á ao fornecimento de orientação técnica, por telefone, e-mail ou site institucional.
25.3.1 Excepcionalmente, a Central de Serviços de TIC poderá prestar suporte presencial (em sua sede) aos(às) teletrabalhadores(as) na configuração de equipamentos particulares para uso dos serviços de TIC do Tribunal, mediante autorização da chefia da unidade e acompanhamento pelo(a) usuário(a), vedada a guarda de equipamento pela Central de Serviços de TIC.
25.4 Em caso de teletrabalho obrigatório, os(as) titulares das unidades administrativas e judiciárias poderão ceder, a título de empréstimo, aos(ás) servidores(as) e aos(ás) magistrados(as) computador, monitor, webcam e headset exclusivamente para o exercício das atividades em teletrabalho.
25.4.1 Os equipamentos só poderão ser retirados após assinatura de termo de autorização de saída, no qual deverá constar a descrição detalhada dos bens e a identificação patrimonial.
25.4.2 O(A) servidor(a) ou o (a) Magistrado(a) assumirá a responsabilidade integral do bem emprestado.
25.4.3 O(A) servidor(a) ou o(a) magistrado(a) 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.
25.5 Quanto aos equipamento particulares, o(a) servidor(a) em teletrabalho deverá:
25.5.1 Assegurar a proteção do equipamento utilizado, por meio de software antivirus atualizado.
25.5.2 Manter o sistema operacional atualizado para a versão mais recente.
25.5.3 Garantir a compatibilidade do equipamento utilizado com o ambiente computacional padrão do Tribunal, como, por exemplo, o navegador para Internet e o software de gerenciamento do certificado digital.
25.5.4 Armazenar as informações e os documentos nos sistemas, na rede corporativa ou no ambiente de colaboração do Tribunal, conforme a natureza dos dados.
25.5.4.1 As informações e os documentos só poderão ser mantidos no computador pessoal durante a manipulação dos mesmos, devendo ser excluídos assim que armazenados no ambiente corporativo.
25.5.5 Utilizar somente softwares originais.
25.6 É vedado ao(à) servidor(a) em teletrabalho:
25.6.1 Utilizar o acesso remoto para fim diverso da atividade desenvolvida.
25.6.2 Obter cópias de pastas de trabalhos ou base de dados inteiras, protegidos ou não, sem autorização da SETIC.
25.6.3 Obter cópias de programas licenciados pelo Tribunal, para instalação em equipamentos particulares.
25.7 A autenticação dos acessos dos(as) servidores(as) em teletrabalho dar-se-á, necessariamente, por meio da utilização de duplo fator de autenticação.
25.7.1 A dispensa do previsto no caput poderá ser realizada pela Presidência ou pelo Comitê de Segurança da Informação e Proteção de Dados, em sistemas ou ambientes específicos, quando não for tecnicamente e/ou economicamente viável tal implementação.
26. DO SUPORTE AOS(ÀS) USUÁRIOS(AS) EXTERNOS(AS)
26.1 O suporte de TIC prestado aos(às) advogados(as), partes, procuradores e aos(às) demais usuários(as) externos(as) pela Central de Serviços da SETIC, limitar-se-á ao fornecimento de orientação técnica, por telefone, e-mail ou site institucional.
26.1.1 Excepcionalmente, a Central de Serviços de TIC poderá prestar suporte presencial (em sua sede) aos(às) usuários(as) externos(as) na configuração de equipamentos particulares para uso dos serviços de TIC do Tribunal, mediante autorização da chefia da unidade e acompanhamento pelo(a) usuário(a), vedada a guarda de equipamento pela Central de Serviços de TIC.
27. DAS DISPOSIÇÕES FINAIS
27.1 Será permitida a manutenção preventiva e corretiva dos recursos de TIC por preposto(a) de empresa responsável por garantia técnica, na forma prevista no respectivo contrato, mediante autorização e agendamento prévio na SETIC.

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml

27.2 Cabe à Coordenadoria de Manutenção e Projetos o controle do uso, a instalação e a manutenção de toda infraestrutura de fornecimento ininterrupto de energia elétrica para a área de tecnologia da informação e comunicação.
27.3 A utilização dos Recursos de Tecnologia da Informação e Comunicação 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.
27.4 A Coordenadoria 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 norma, para que todos(as) a conheçam e a cumpram no âmbito de suas atividades e atribuições.
27.5 A SETIC deverá promover verificação anual, quanto à eficiência dos controles implementados, para aferir o correto cumprimento desta norma.
27.6 Configurado o descumprimento das normas estabelecidas, a SETIC deverá promover a imediata adequação e encaminhar ao CSIPD relatório sobre o fato.
27.7 Situações específicas envolvendo a utilização de recursos de tecnologia da informação e comunicação não previstas nesta norma serão resolvidos pelo CSIPD ou, em última instância, pela Presidência.
27.8 Os registros dos acessos (logs) aos sistemas de informações, serviços de TIC, dados, informações, rede e equipamentos do TRT-7, realizados pelos(as) usuários(as) internos(as) ou externos(as) são de propriedade do TRT-7 e podem ser recuperados (lidos) pela SETIC, de ofício, a qualquer momento, sem aviso prévio, e encaminhados à Secretaria Geral da Presidência ou à Corregedoria Regional, conforme o caso, quando justificado ou mediante requerimento da Secretaria Geral da Presidência ou da Corregedoria Regional em qualquer caso.
27.8.1 Sempre que a tecnologia permitir, deverão ser gravados nos registros de acesso, pelo menos, a data/hora do acesso, a identificação do(a) usuário(a) e o endereço de rede de origem (endereço IP).

PROAD 7793/2023. DOC 4. Para verificar a autenticidade desta cópia,
acesse o seguinte endereço eletrônico e informe o código 2023.KWNP.YGBY:
https://proad.trt7.jus.br/proad/pages/consultadocumento.xhtml