UTILIZAÇÃO DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC

1 OBJETIVO

Estabelecer regras e condições para a utilização dos recursos de tecnologia da informação e comunicação do TRT 18ª Região (TRT18), visando a adoção de boas práticas em segurança da informação.

2 APLICAÇÃO

Aplica-se a presente norma a todos os recursos de tecnologia da informação e comunicação do TRT18, assim compreendidos as estações de trabalho, serviços de rede, *link* de internet, correio eletrônico corporativo, aplicativos, sistemas, armazenamento em rede, *notebooks*, *modems*, mídias removíveis, entre outros.

3 REFERÊNCIA NORMATIVA

3.1 Portaria TRT18 GP/NGTIC nº 001/2016 e anexo "**PO01**", que aprova a revisão 1.1 das diretrizes da Política de Segurança da Informação e Comunicação do TRT18.

3.2 Portaria TRT18 GP/NGTIC nº 002/2016 e anexo "**PO02**", que aprova a revisão 0.1 das diretrizes da Política de Controle de Acesso do TRT18.

3.3 Portaria TRT18 GP/NGTIC nº 004/2016 e anexo "**NO02**", que aprova a revisão 0.1 das regras de Controle de Acesso à Rede do TRT18.

4 DEFINIÇÕES

Para efeito desta norma, serão adotadas as definições descritas nesta seção e no documento PO02.

4.1 Domínio: conjunto de estações de trabalho e servidores com gerenciamento centralizado em um banco de dados central de credenciais e diretivas de acesso.

4.2 *Firewall:* dispositivo de hardware ou software cujo objetivo é limitar, impedir e/ou

controlar o acesso a serviços disponibilizados entre redes.

4.3 *Gateway*: equipamento destinado a interligar redes distintas.

4.4 *Logoff*: é a operação que termina uma sessão autenticada (uso de usuário e senha) de uma aplicação ou sistema operacional, no caso do sistema operacional o *logoff* irá também fechar todos os aplicativos em uso.

4.5 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, disquetes, *Flash Drive*, *Pen Drive,* entre outros.

4.6 *Proxy*: dispositivo de hardware ou software capaz de inspecionar dados trafegados entre a rede local e a Internet e efetuar bloqueio de acesso a conteúdo de acordo com políticas preestabelecidas.

4.7 *Spam*: mensagem eletrônica não solicitada enviada em massa.

4.8 VPN: *Virtual Private Network*. Rede privada construída sobre uma infraestrutura de rede pública, com recursos para proteção dos dados transmitidos contra interceptações e capturas.

5 CONTEÚDO

5.1 REGRAS GERAIS

5.1.1 Todos os recursos de tecnologia da informação e comunicação do TRT18 são para uso exclusivo no cumprimento de suas atividades institucionais.

5.1.2 Os serviços e sistemas autenticados serão disponibilizados para os usuários registrados e identificados pelo seu login e senha.

5.1.3 As credenciais de identificação são de uso pessoal e intransferível. O usuário deve zelar pela confidencialidade de sua senha de acesso, podendo ser responsabilizado pelas operações realizadas com a utilização de suas credenciais.

5.1.4 Situações específicas envolvendo a utilização de recursos de tecnologia da informação e comunicação não previstas nesta norma serão encaminhadas à Comissão de Segurança da Informação para deliberação.

5.2 ESTAÇÕES DE TRABALHO

5.2.1 As estações de trabalho serão instaladas e configuradas pela Secretaria de Tecnologia da Informação (STI).

5.2.2 A STI criará padrões de configuração adequados às necessidades de utilização das unidades judiciais e administrativas.

5.2.3 A STI deverá estabelecer um procedimento de homologação de softwares e

hardwares passíveis de serem instalados e utilizados nas estações de trabalho.

5.2.4 Não é permitida a instalação de softwares não homologados, mesmo que de livre utilização.

5.2.5 A instalação de softwares dependerá da disponibilidade de licença de uso.

5.2.6 A equipe técnica da STI poderá instalar softwares para testes, avaliação e homologação, entretanto a utilização em ambiente de produção deve ser precedida do respectivo licenciamento e homologação.

5.2.7 Não é permitido ao usuário a abertura dos gabinetes, a instalação ou remoção de qualquer componente de software ou hardware nas estações de trabalho, bem como a desabilitação ou alteração de configurações em serviços relacionados à segurança da informação, como antivírus, proxy e firewall, devendo essas tarefas, quando necessárias, serem executadas pela equipe técnica da STI.

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

5.2.9 É proibido o consumo de alimentos sólidos ou líquidos próximo aos equipamentos de informática.

5.2.10 A conexão de dispositivos removíveis de armazenamento como *pen drives*, discos rígidos externos, cartões de memória e outros só poderá ser efetuada mediante autorização da chefia imediata.

5.2.11 O usuário deve executar a cada uso varreduras à procura de vírus em *pen drives* ou outros dispositivos removíveis de armazenamento que estejam autorizados para o uso nos equipamentos do TRT18.

5.2.12 O usuário deve bloquear o sistema operacional de sua estação de trabalho quando se ausentar da frente do equipamento mesmo por curtos intervalos. No caso de ausência prolongada deverá fechar todas as suas aplicações em uso e realizar o *logoff* da estação de trabalho.

5.2.13 Ao acessar dados sigilosos ou sensíveis, o usuário deve certificar-se de que o posicionamento físico de seu monitor não permita a visualização das informações por terceiros.

5.3 USO DA REDE LOCAL (DOMÍNIO TRT18)

5.3.1 É proibida a conexão de equipamentos “pessoais” (estações de trabalho, *notebooks*, *netbooks*, *smartphones*, *tablets*, *modems* e similares) à rede do TRT18 sem a devida autorização expressa da STI, exceto para a situação indicada no item 5.4.3.

5.3.2 A STI estabelecerá condições e procedimentos para a requisição, análise e eventual autorização de conexão de equipamento pessoal à rede do TRT18, observadas as diretrizes da Política de Controle de Acesso, documento PO02.

5.3.3 Serão fornecidos diretórios compartilhados de rede para armazenamento de arquivos de trabalho. É proibida a utilização desta área para o armazenamento de arquivos pessoais ou sem relação com as atividades institucionais do Tribunal.

5.3.4 Será oferecida área pública (J:) temporária para transferência de arquivos, cujo esvaziamento se dará semanalmente por meio de rotina automatizada. A referida área não deverá ser utilizada para gravação de arquivos que devam ser mantidos por mais de um dia.

5.3.5 Cada unidade administrativa ou judicial terá um diretório compartilhado (G:) para os usuários lotados na respectiva área, com acesso de leitura e gravação.

5.3.6 Cada unidade administrativa ou judicial terá um diretório compartilhado (X:) para publicação de arquivos de interesse de outras áreas, com acesso de escrita para os usuários lotados na respectiva área e acesso de leitura para os demais usuários.

5.3.7 A STI manterá cópias de segurança do conteúdo dos diretórios compartilhados por um período a ser definido em norma especifica de *backup* e restauração.

5.3.8 O usuário deve, periodicamente, fazer a eliminação de arquivos desnecessários e evitar a manutenção de mais de uma cópia do mesmo arquivo.

5.3.9 A STI poderá excluir conteúdo que não esteja em conformidade com as normas de segurança da informação do TRT18, quando da realização de manutenções periódicas nos diretórios de rede a fim de liberar espaço e otimizar a sua utilização.

5.3.10 A área pública (J:), a área compartilhada (X:) e outras de natureza similar devem ser utilizadas para armazenar apenas informações de interesse geral, não devendo, portanto, ser repositório para o armazenamento de arquivos que contenham assuntos sigilosos, restritos ou de natureza específica.

5.4 USO DA REDE SEM FIO

5.4.1 Serão disponibilizadas na Sede, e futuramente em localidades remotas, ao menos duas redes sem fio: uma para uso privado e outra para uso público. Ambas estarão integradas de modo seguro à infraestrutura de redes do TRT18.

5.4.2 A rede sem fio privada dará acesso a quase totalidade dos serviços normalmente disponibilizados através de conexão cabeada de rede local, enquanto

a rede sem fio pública permitirá acesso apenas a alguns serviços disponibilizados no portal do TRT18, como Processo Judicial Eletrônico. Não será disponibilizado acesso à internet a partir da rede sem fio pública.

5.4.3 A rede sem fio pública poderá ser acessada por qualquer pessoa, sem necessidade de credenciamento prévio do indivíduo e do equipamento.

5.4.4 A rede sem fio privada será destinada aos usuários internos do TRT18 e somente poderá ser acessada mediante fornecimento das respectivas credenciais de acesso à rede local.

5.4.5 Poderá ser permitido o uso da rede privada por usuários temporários e externos.

5.4.6 A STI estabelecerá condições e procedimentos para a requisição, análise e autorização de acesso à rede sem fio privada por usuários temporários e externos, observadas as diretrizes da Política de Controle de Acesso, documento PO02.

5.5 GERENCIAMENTO DE INFRAESTRUTURA

5.5.1 Todo equipamento servidor de serviços de tecnologia da informação e comunicação deve implementar dispositivos de segurança para proteger suas portas de acesso remoto (*Firewall* no *Host*).

5.5.2 A rede de comunicação de dados do Tribunal deve ser protegida por equipamento de detecção e prevenção de intrusão (IPS) e segmentada de acordo com a criticidade das informações e das aplicações existentes. A segmentação da rede deve ser efetivada por meio de *gateways* (*firewalls*, *routers*, *switches* de camada 3, etc.) configurados conforme regras definidas pelas áreas competentes da STI.

5.5.3 A STI deve manter documentação atualizada dos serviços e redes que compõem a infraestrutura de tecnologia da informação e comunicação do TRT18.

5.6 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

5.6.1 Os *notebooks* disponibilizados aos magistrados e servidores do TRT18 devem ser conectados à rede corporativa pelo menos a cada 30 dias para que recebam as atualizações de segurança e políticas necessárias, devendo ser utilizados apenas pelos usuários autorizados, sendo proibido o seu empréstimo a terceiros.

5.6.2 É responsabilidade do usuário manter o antivírus do seu *notebook* atualizado. Na hipótese de inexequibilidade da atualização pelo usuário, o aparelho deve ser encaminhado à STI para as providências.

5.6.3 Os *notebooks* disponibilizados pelo Tribunal deverão estar configurados para

acionar a proteção de tela após um período de inatividade com exigência de senha para desbloqueio.

5.6.4 A perda ou furto de *notebook* do TRT18 deve ser comunicado imediatamente à STI, além de tomadas as providências administrativas cabíveis.

5.6.5 O acesso remoto à rede do TRT18 realizado por servidores e magistrados com a utilização da *VPN* e do Gabinete Virtual desta Corte não deve ser realizado a partir de computadores de uso público (*lan houses*, quiosques de internet, etc.).

5.6.6 O usuário quando utilizar o acesso remoto (Gabinete Virtual, *VPN*) fora das dependências do Tribunal deve permanecer conectado apenas enquanto estiver efetivamente utilizando os serviços disponibilizados, tomando o cuidado de desconectar-se nas interrupções e no término do trabalho. Deve cuidar ainda para que informações sigilosas não sejam capturadas por terceiros que estejam próximos ao equipamento.

5.6.7 A STI estabelecerá condições e procedimentos para a requisição, análise e autorização de acesso à *VPN* e ao Gabinete Virtual por usuários registrados, observadas as diretrizes da Política de Controle de Acesso, documento PO02.

5.6.8 É expressamente proibido:

a) acessar a internet a partir de equipamento simultaneamente conectado à rede local física do TRT18 e à rede de dados celular, seja via *modems* portáteis ou *smartphones*.
b) conectar à rede do TRT ponto de acesso de rede sem fio sem autorização expressa da STI.

5.7 ACESSO À INTRANET E INTERNET

5.7.1 O acesso à Intranet e Internet pela rede corporativa do Tribunal é de uso exclusivo de seus usuários autorizados e destina-se a apoiar o cumprimento das suas atribuições institucionais.

5.7.2 A autorização a que se refere o item 5.7.1 segue as regras da norma de Controle de Acesso à Rede, documento NO02.

5.7.3 A navegação na Internet estará sujeita a filtros de conteúdo e será passível de verificação e auditoria por parte da STI, tanto quanto ao conteúdo acessado quanto ao volume de dados trafegados.

5.7.4 As requisições de liberação ou bloqueio de conteúdos deverão ser encaminhadas por magistrado ou chefe de unidade à Central de Serviços do Núcleo de Atendimento ao Usuário de TIC, acompanhadas da devida justificativa e em

conformidade com os procedimentos estabelecidos pela STI.

5.7.5 Os conteúdos a serem filtrados são determinados precariamente pela STI e levados à deliberação da Comissão de Segurança da Informação.

5.7.6 As regras de filtragem são compostas, dentre outros recursos, pela combinação entre grupos de usuários, categorias de sítios, tipos de arquivos e ação de bloqueio ou liberação. Elas devem ser mantidas mais genéricas e em menor número possível.

5.7.7 É proibida a utilização de qualquer tipo de mecanismo ou recurso para burlar os controles de acesso à Internet implementados.

5.7.8 O acesso à Internet deve ser realizado de forma responsável e comedida, evitando o comprometimento da rede corporativa, dos links de comunicação de dados e da disponibilidade dos serviços do TRT18. Em caso de uso abusivo o usuário será comunicado e havendo reincidência será enviado um relatório à chefia imediata para as providências cabíveis.

5.8 ACESSO AO COMUNICADOR INSTANTÂNEO E AO CORREIO ELETRÔNICO

5.8.1 O Comunicador Instantâneo e o correio eletrônico corporativo do Tribunal são de uso exclusivo nas atividades relativas às funções dos usuários autorizados do TRT18, podendo ser auditados por determinação da Administração.

5.8.2 A autorização a que se refere o item 5.8.1 segue as regras da norma de Controle de Acesso à Rede, documento NO02.

5.8.3 O tráfego de mensagens eletrônicas estará sujeito a filtros de conteúdo visando reduzir mensagens *spam*, inapropriadas ou maliciosas.

5.8.4 É proibido o uso do correio eletrônico corporativo para o envio de mensagens em massa que não tenham relação com as atividades do Tribunal.

5.8.5 O usuário do e-mail deve sempre utilizar o campo “Cópia Oculta” no envio de mensagens para muitos usuários, a fim de preservar os endereços dos destinatários.

5.8.6 As caixas postais possuem espaço limitado, devendo ser realizada manutenção periódica pelos seus usuários (apagando e-mails antigos e desnecessários), evitando assim a interrupção do recebimento de mensagens por insuficiência de espaço.

5.8.7 A capacidade das caixas postais, assim como o tamanho máximo das mensagens de e-mail, incluindo seus anexos, serão determinados e divulgados pela STI.

5.8.8 As pastas Lixeira e *Spam* serão apagadas periodicamente por rotinas

automatizadas e sem aviso prévio.

Este texto não substitui o publicado no DEJT de 11/02/2016.