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 - TIC do TRT 18ª Região, visando a adoção de boas práticas em segurança da informação.

2 APLICAÇÃO

Aplica-se a presente a todos os recursos de tecnologia da informação e comunicação do TRT da 18ª Região, 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 ALINHAMENTO

Esta norma está subordinada à Política de Segurança da Informação do TRT 18ª Região.

4 DEFINIÇÕES

4.1 *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;

4.2 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.

4.3 *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;

4.4 *Firewall*: dispositivo de hardware ou software cujo objetivo é limitar, impedir e/ou controlar o acesso a serviços disponibilizados entre redes;

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

4.6 *Gateway*: equipamento destinado a interligar redes distintas;
4.7 *Spam*: mensagem eletrônica não solicitada enviada em massa.

5 CONTEÚDO

5.1 REGRAS GERAIS

5.1.1 Todos os recursos de tecnologia da informação e comunicação do Tribunal são para uso exclusivo no cumprimento de suas atividades institucionais;
5.1.2 Toda e qualquer iniciativa para a contratação (aquisição, locação, convênio etc) de recurso de tecnologia da informação e comunicação deve ser previamente submetida à Secretaria de Tecnologia da Informação para avaliação da oportunidade, compatibilidade com a infraestrutura existente e implicações de segurança da informação, além de verificação da respectiva especificação técnica;
5.1.3 Os serviços e sistemas autenticados serão disponibilizados para os usuários registrados e identificados pelo seu login e senha;
5.1.4 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;
5.1.5 Situações específicas envolvendo a utilização de recursos de tecnologia da informação e comunicação não previstas nesta norma serão encaminhadas ao Comitê 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 Secretaria de Tecnologia da Informação criará padrões de configuração adequados às necessidades de utilização das unidades judiciais e administrativas;
5.2.3 A Secretaria de Tecnologia da Informação 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 Secretaria de Tecnologia da Informação 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 Secretaria de Tecnologia da Informação;

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

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 TRT 18ª Região;

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" (*notebooks*, *netbooks*, *smartphones*, *tablets*, modem e similares) à rede do TRT 18ª Região;

5.3.2 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;

5.3.3 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;

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

5.3.5 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;

5.3.6 A Secretaria de Tecnologia da Informação manterá cópias de segurança do conteúdo dos diretórios compartilhados por um período a ser definido em norma especifica de *backup* e restauração;

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

5.3.8 A Secretaria de Tecnologia da Informação poderá excluir conteúdo que não esteja em conformidade com as normas de segurança da informação do TRT 18ª Região, quando da realização de manutenções periódicas nos diretórios de rede a fim de liberar espaço e otimizar a sua utilização.

5.4 GERENCIAMENTO DE INFRAESTRUTURA

5.4.1 Todos os sistemas e serviços disponibilizados na rede do TRT 18ª Região devem fazer o uso de autenticação de usuário e utilizar mecanismos de criptografia como: *HTTPS, SSL, TLS e VPN*, para o tráfego de nomes de usuários, senhas e de informações sigilosas entre as camadas envolvidas no sistema ou serviço;

5.4.2 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*);

5.4.3 A rede de comunicação de dados do Tribunal deve ser segregada de acordo com a criticidade das informações e das aplicações existentes. A segregação da rede deve ser efetivada por meio de *gateways (firewalls, routers, switches,* etc.) configurados conforme regras definidas pelas áreas competentes da Secretaria de Tecnologia da Informação;

5.4.4 A Secretaria de Tecnologia da Informação deve manter documentação atualizada dos serviços e redes que compõem a infraestrutura de tecnologia da informação e comunicação do TRT 18ª Região.

5.5 COMPUTAÇÃO MÓVEL E TRABALHO REMOTO

5.5.1 Os *notebooks* disponibilizados aos magistrados e servidores do TRT 18ª Região devem ser conectados à rede corporativa pelo menos a cada 10 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;

5.5.2 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 Secretaria de Tecnologia da Informação para as providências;

5.5.3 Documentos sigilosos ou restritos armazenados nos *notebooks* ou em mídias removíveis devem ser criptografados para evitar a sua divulgação indevida em caso de perda ou

furto do equipamento;

5.5.4 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;

5.5.5 A perda ou furto de notebook do TRT 18ª Região deve ser comunicado imediatamente à Secretaria de Tecnologia da Informação, além de tomadas as providências administrativas cabíveis;

5.5.6 O acesso remoto à rede do TRT 18ª Região 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);

5.5.7 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;

5.5.8 É proibido o uso de modems ou conexões via celular em equipamentos conectados à rede corporativa do Tribunal.

5.6 ACESSO À INTERNET E CORREIO ELETRÔNICO

5.6.1 O acesso à Internet pela rede corporativa do Tribunal é de uso exclusivo de seus magistrados, servidores e estagiários, destinando-se a apoiar o cumprimento das suas atribuições institucionais;

5.6.2 A navegação na Internet estará sujeita a filtros de conteúdo e será passível de verificação e auditoria por parte da Secretaria de Tecnologia da Informação, tanto quanto ao conteúdo acessado e volume de dados trafegados;

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

5.6.4 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 TRT 18ª Região. Em caso de uso abusivo o usuário será comunicado e havendo reincidência será enviado um relatório à chefia imediata para as providências cabíveis;

5.6.5 O correio eletrônico corporativo do Tribunal é de uso exclusivo das atividades relativas as funções dos usuários no TRT 18ª Região, podendo ser auditado por determinação da Administração;

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

5.6.7 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;

5.6.8 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;

5.6.9 O tamanho máximo das mensagens de e-mail, incluindo seus anexos, não deve exceder 3 MB;

5.6.10 As pastas Lixeira e Spam serão apagadas periodicamente por rotinas automatizadas e sem aviso prévio.

HISTÓRICO DAS REVISÕES			
Data de vigência	Revisão	Ato normativo	Descrição
20/04/2012	00	**Portaria GP/DG nº 003/2012**	Norma inicial