

 <p>Poder Judiciário da União Tribunal Regional do Trabalho da 18ª Região</p>	Código: NO01
	Revisão: 1.5
	Vigência: (DATA DE PUBLICAÇÃO)
	Classificação: PÚBLICO
	Ato normativo: (Portaria TRT 18ª GP/SSGOVE nº ____/2019)

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

A presente norma integra a Política de Segurança da Informação do TRT18 e aplica-se a todos os recursos de tecnologia da informação e comunicação do Tribunal, 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** PO01 – Política de Segurança da Informação e Comunicação do TRT18.
3.2 PO02 – Política de Controle de Acesso do TRT18.
3.3 NO02 – 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

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 1/11
--------------	--------------	---------------------------------------	--------------

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.

4.9 Usuário administrador local de TI: usuários não lotados na STI do Tribunal que são autorizados para prestação de suporte técnico e atendimento ao usuário.

4.10 Unidade de rede: diretório ou pasta digital localizado na infraestrutura tecnológica, acessível pelo computador do usuário cujo mapeamento (atalho para a unidade de rede a partir do *Windows Explorer*) é feito de forma automática.

5 CONTEÚDO

5.1 REGRAS GERAIS

5.1.1 Os recursos de tecnologia da informação e comunicação do TRT18 são para uso diretamente relacionado às atribuições funcionais do usuário. Solicitações de utilização de recursos de TIC sem a devida justificativa relacionada às atribuições funcionais deverão ser autorizadas pela Comissão de Segurança da Informação.

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

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 2/11
--------------	--------------	--------------------------------	--------------

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 e Comunicação (STI) ou por usuário administrador local de TI, com assinatura de termo de responsabilidade.

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, exceto aqueles disponibilizados na *STI Store*, 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 ou por usuário administrador local de TI.

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 A conexão de dispositivos removíveis de armazenamento como *pen drives*, discos rígidos externos, cartões de memória e outros poderá ser efetuada por qualquer servidor, desde que certifique a origem confiável dos mesmos e observe o procedimento indicado no item 5.2.10, sob pena de responsabilização por possíveis incidentes de segurança da informação.

5.2.10 O usuário deve executar a cada uso varreduras à procura de vírus em

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 3/11
--------------	--------------	--------------------------------	--------------

pen drives ou outros dispositivos removíveis de armazenamento que estejam autorizados para o uso nos equipamentos do TRT18.

5.2.11 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.

5.2.12 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 cabeada do TRT18.

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

5.3.3 Serão fornecidas unidades 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 uma unidade de rede (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 de lotação terá uma unidade de rede (G:) para os usuários lotados na respectiva área, com acesso de leitura e gravação.

- a) A inclusão de acesso será realizada automaticamente quando houver novo usuário na unidade de lotação;
- b) A exclusão de acesso **não** será realizada automaticamente quando houver saída de usuário da unidade de lotação;
- c) Periodicamente, o gestor de unidade de lotação deverá revisar o cadastro de usuários com permissão de acesso, devendo solicitar à STI as exclusões pertinentes;

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 4/11
--------------	--------------	--------------------------------	--------------

- d) Quando necessário, o gestor de unidade de lotação deverá solicitar à STI a inclusão de acesso para usuários lotados em outras unidades;
- e) Excetuados os servidores lotados em unidades CJ-4, os demais lotados em unidades superiores terão acesso aos diretórios das unidades de lotação subordinadas.

5.3.6 Cada unidade de lotação terá uma única unidade de rede compartilhada (X:) para publicação de arquivos de interesse de outras áreas, ou para criação de pastas de armazenamento de documentos restritos a grupo de usuários que tenham necessidade de acessar e conhecer tais documentos, cabendo ao gestor desta unidade ou substituto controlar as permissões de acesso.

5.3.7 Cada usuário interno terá uma unidade de rede privada (H:) com limite de 20GB para armazenamento de arquivos de uso exclusivo do usuário para fins de trabalho, não sendo possível compartilhar seu conteúdo com outros usuários ou unidades de lotação.

5.3.8 A STI poderá criar outras unidades de rede para atender demandas específicas, devendo para isso expor a justificativa e a finalidade, bem como regulamentar em Procedimento próprio regras de uso, papéis e responsabilidades.

5.3.9 A STI manterá cópias de segurança do conteúdo das unidades de rede compartilhada (X:), de lotação (G:) e privada (H:) por um período a ser definido em norma específica de *backup* e restauração.

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

5.3.11 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.

5.3.12 A unidade de rede (J:) 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.

5.3.13 O armazenamento de arquivos executáveis nas unidades de rede será permitido apenas a membro da equipe técnica da STI e a usuário administrador local

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 5/11
--------------	--------------	--------------------------------	--------------

de TIC.

5.4 USO DA REDE SEM FIO

O uso da rede sem fio do TRT18 é regulamentado em normativo próprio.

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 inexecuibilidade 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 equipamentos de TI 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.*).

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 6/11
--------------	--------------	--------------------------------	--------------

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) o acesso à Internet em equipamento do Tribunal do tipo *desktop* via rede de dados de celular, exceto para manutenção pela STI.
- 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 da área 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 pela STI mediante análise de riscos devidamente fundamentada. A critério do solicitante, casos de indeferimento serão levados à deliberação da Comissão de Segurança da Informação juntos às respectivas análises de riscos.

5.7.6 As regras de filtragem são compostas, dentre outros recursos, pela

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 7/11
--------------	--------------	--------------------------------	--------------

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

O acesso e a utilização do comunicador instantâneo e do correio eletrônico corporativo do Tribunal são regulamentados em normativo próprio.

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 8/11
--------------	--------------	--------------------------------	--------------

HISTÓRICO DAS REVISÕES				
Data de vigência	Revisão	Ato normativo	Descrição	Responsável
20/04/2012	0.0	Portaria GP/SGP nº 034/2012	Norma inicial	Comitê de Segurança da Informação
06/08/2015	1.0	Portaria GP/DG nº 319/2015	Alteração de layout Inclusão dos itens 3.2 e 3.3 Inclusão de preâmbulo no item 4 Inclusão do item 4.8 Exclusão do item 5.1.2 Alteração dos itens 5.3.1 Inclusão do item 5.3.2 Inclusão da seção 5.4 Exclusão do item 5.4.1 Exclusão do item 5.5.3 Inclusão do item 5.6.7 Alteração do item 5.6.8 Alteração da seção 5.7, com divisão na seção 5.8 Inclusão dos itens 5.7.2, 5.7.4, 5.7.5, 5.7.6, 5.8.2 e 5.8.3 Alteração dos itens 5.8.1 e 5.8.7	Comitê de Segurança da Informação
12/02/2016	1.1	Portaria TRT 18ª GP/NGTIC nº 004/2016	Alteração da identificação da estrutura hierárquica no topo da primeira página Alteração do item 5.7.4 Inclusão do item 5.3.10	Comissão de Segurança da Informação

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 9/11
--------------	--------------	--------------------------------	--------------

17/05/2017	1.2	Portaria TRT 18ª GP/NGTIC nº 1109/2017	Alteração do item 2, sobre “integrar a PSI do TRT”; Modificações, confirme ata de reunião CSegInfo de 24/03/17: Inclusão do item 4.9; Alteração dos itens 5.1.1, 5.2.1, 5.2.7, 5.2.10, 5.3.6, 5.4.5, 5.4.6, 5.4.7, 5.6.4, 5.6.8 e 5.7.5. Exclusão do item 5.2.9 e respectiva numeração dos antigos itens 5.2.10 a 5.2.13 para 5.2.9 a 5.2.12.	Comissão de Segurança da Informação
25/04/2018	1.3	Portaria TRT 18ª GP/DGOV nº 1184/2018	Inclusão do item 4.10; Alteração dos antigos itens 5.3.3 a 5.3.7, 5.3.9 e 5.3.10; Alteração da numeração dos antigos itens 5.3.7 a 5.3.10 devido à inserção dos novos itens 5.3.7 e 5.3.8; Inclusão do item 5.3.13; Exclusão dos itens 5.8.1 a 5.8.8; Inclusão do novo item 5.8.1.	Comissão de Segurança da Informação
13/01/2018	1.4	Portaria TRT 18ª GP/DGOV nº 3673/2018	Alteração dos itens 5.3.1, 5.3.2 e 5.4	Comissão de Segurança da Informação

	1.5		Alteração dos itens 5.3.6, 5.3.12 e 5.3.13.	Comissão de Segurança da Informação
--	-----	--	---	-------------------------------------

Código: NO01	Revisão: 1.5	Vigência: (DATA DE PUBLICAÇÃO)	Página: 11/11
--------------	--------------	--------------------------------	---------------