CONTROLE DE ACESSO À REDE

1 OBJETIVO

Estabelecer regras de controle de acesso à rede de computadores do TRT 18ª Região.

2 APLICAÇÃO

Esta norma de segurança da informação se aplica no âmbito do TRT 18ª Região (TRT18).

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.

4 DEFINIÇÕES

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

5 DISPOSIÇÕES INICIAIS

5.1 A rede de computadores do TRT18 é formada por segmentos físicos e lógicos interligados por subsistemas de comunicação de longa distância, de rede metropolitana e de redes locais cabeadas e sem fio.

5.2 Os serviços primários da rede de computadores do TRT18 abrangem: diretório compartilhado de pastas e arquivos digitais; comunicador instantâneo (Spark); correio eletrônico institucional interno e externo utilizando o domínio "@trt18.jus.br";

intranet; internet.

5.3 Os perfis de acesso padrão aos serviços de rede são representados pelos seguintes níveis:

a) 1: nenhum acesso;
b) 2: acesso à intranet e ao correio institucional interno;
c) 3: “nível 2” e comunicador instantâneo;
d) 4: “nível 3” e correio institucional externo;
e) 5: “nível 4”, diretório compartilhado e internet.

5.4 O controle de acesso à rede do TRT18 adota as diretrizes da Política de Controle de Acessos, documento PO02, quanto ao credenciamento (identificação, autenticação e autorização), à política de senhas (proteção das senhas e complexidade das senhas), ao monitoramento (registro de eventos e análise crítica) e ao acesso privilegiado.

5.5 A concessão de senhas para autenticação na rede segue os procedimentos indicados no documento PC02 – Gerenciamento da Concessão de Senhas de Rede.

6 CADASTRAMENTO E AUTORIZAÇÃO DE USUÁRIOS

6.1 A cada usuário interno ou temporário deve ser atribuído um código de identificação (*login*) único formado por uma letra e seis dígitos numéricos, sendo a letra:

a) “m” para magistrados;
b) “s” para servidores;
c) “e” para estagiários;
d) “a” para menores trabalhadores/aprendizes;
e) “t” para terceirizados.

6.2 Os seis dígitos numéricos são fornecidos pelos Gestores de Pessoal aos usuários, após o processo de admissão. O controle dessa numeração é acordada entre Gestores de Pessoal e Secretaria de Tecnologia da Informação e Comunicação (STI).

6.3 O *login* de usuário externo é formado pela letra “x” seguida do respectivo CPF.

6.4 O *login* para usuários especiais será formatado a critério da Coordenadoria de Infraestrutura e Comunicação.

6.5 Compete aos Gestores de Pessoal solicitar tempestiva e formalmente à Central de Serviços, do Núcleo de Atendimento ao Usuário de TIC, o cadastramento e as

alterações cadastrais de usuários internos e temporários.

6.6 Compete à Central de Serviços encaminhar as solicitações de cadastramento e alterações de cadastro aos Gestores de Acesso, para que estes efetivem o cadastramento e mantenham atualizada a situação cadastral dos usuários internos e temporários de rede.

6.7 Compete à Coordenadoria de Infraestrutura e Comunicação, no papel de Gestor de Ativo de Informação, analisar, aprovar ou reprovar solicitações de cadastramento e cadastrar, manter e monitorar contas de acesso para usuários externos e especiais, assim como credenciar Gestores de Acesso à rede.

6.8 As contas de acesso de usuários temporários e externos serão automaticamente bloqueadas, expirado o tempo de acesso previsto em contratos ou em outros documentos que justifiquem as respectivas credenciais.

6.9 Observadas as regras de uso de correio eletrônico, de internet e de diretórios compartilhados da norma NO01, as permissões padrão para acesso aos serviços de rede compreendem:

a) nível 5 para usuários internos;
b) nível 4 para usuários especiais do tipo “unidade organizacional”;
c) nível 3 para usuários temporários;
d) nível 2 para usuários em situação cadastral “inativo”;
e) nível 1 para usuários externos, usuários especiais e demais usuários em situação cadastral “bloqueado” ou “desligado”.

6.10 Permissão de acesso adicional pode ser solicitada, desde que devidamente justificada quanto ao interesse do serviço e ao baixo risco à segurança das informações. Do mesmo modo, a redução de permissão de acesso pode ser solicitada pelo gestor do usuário.

6.11 Compete ao gestor do usuário solicitar ao gestor de ativo de informação, através da central de serviços, liberação ou restrição de acessos a usuários sob sua responsabilidade.

6.12 Deve ser evitado o uso de correio eletrônico institucional externo por usuários temporários e usuários externos.

6.13 É proibido:

a) o uso de conta de unidade organizacional para acessar internet e diretórios compartilhados;
b) o uso de contas privilegiadas e contas de serviço nas atividades normais de

negócio.

7 DISPOSIÇÕES GERAIS

7.1 Quando necessários, procedimentos sobre cadastramento, alteração cadastral, solicitação e aprovação de direitos de acesso serão detalhados, implantados, comunicados e mantidos pela STI.

7.2 A Secretaria de Tecnologia da Informação e Comunicação terá o prazo de 180 dias para realizar as adequações tecnológicas necessárias à implantação desta norma.

7.3 Esta norma deverá ser revisada anualmente.

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