Tribunal Regional do Trabalho da 18ª Região Comissão de Segurança da Informação Núcleo de Governança Corporativa de TIC Setor de Segurança da Informação	Código: **PO02** Revisão: **0.1** Vigência: **(DATA DE PUBLICAÇÃO)** Classificação: **PÚBLICO** Ato normativo: **Portaria TRT 18ª GP/NGTIC Nº 002/2016**

POLÍTICA DE CONTROLE DE ACESSO

1 OBJETIVO

Estabelecer diretrizes para gerenciar credenciais de usuários e restringir o acesso aos ativos de informação, com vistas a preservar a confidencialidade, integridade, disponibilidade e autenticidade das informações sob a responsabilidade do Tribunal.

2 APLICAÇÃO

Este documento integra a Política de Segurança da Informação e Comunicação e aplica-se 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 Norma Complementar nº 07/IN01/DSIC/GSIPR, Revisão 01, de 15/07/2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal (APF).

3.3 Seção 9 da norma ABNT ISO/IEC 27002:2013 (código de prática para controles de segurança da Informação).

4 DEFINIÇÕES

Para efeito desta política, serão adotadas as definições descritas nesta seção e no documento PO01.

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

4.2 Ativos de informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso.

4.3 Autenticação de multifatores: utilização de dois ou mais fatores de autenticação para concessão de acesso a um sistema. Os fatores de autenticação se dividem em: algo que o usuário conhece (senhas, frases de segurança, PIN, dentre outros); algo que o usuário possui (certificado digital, *tokens*, códigos enviados por SMS, dentre outros); algo que o usuário é (aferível por meios biométricos, tais como digitais, padrões de retina, reconhecimento facial, dentre outros).

4.4 Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.

4.5 Biometria: é a verificação da identidade de um indivíduo por meio de uma característica física ou comportamental única, através de métodos automatizados.

4.6 Bloqueio de acesso: processo que tem por finalidade suspender temporariamente o acesso.

4.7 Contas de Acesso: permissões, concedidas por gestor competente após o processo de credenciamento, que habilitam determinada pessoa, sistema ou organização ao acesso. A credencial pode ser física como crachá, cartão e selo ou lógica como identificação de usuário e senha.

4.8 Contas de Serviço: contas de acesso à rede corporativa de computadores necessárias a um procedimento automático (aplicação, script, etc.) sem qualquer intervenção humana no seu uso.

4.9 Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso.

4.10 Credenciamento: processo pelo qual o usuário recebe credenciais que concederão o acesso, incluindo a identificação, a autenticação, o cadastramento de código de identificação e definição de perfil de acesso em função de autorização prévia e da necessidade de conhecer.

4.11 Credenciais*:* mesmo que contas de acesso.

4.12 Exclusão de acesso: processo que tem por finalidade suspender definitivamente o acesso, incluindo o cancelamento do código de identificação e do perfil de acesso.

4.13 Gestão de Riscos de Segurança da Informação e Comunicação: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos.

4.14 Gestor de Ativo de Informação: proprietário ou custodiante de ativo de informação, responsável por definir perfis de acesso e por aprovar ou reprovar solicitações de credenciais de acesso aos ativos sob sua gestão.

4.15 Gestor de Acesso: Gestor de Ativo de Informação, ou servidor por ele delegado mediante Termo de Responsabilidade de Gestão de Acesso, responsável por executar, mediante aprovação prévia, tarefas de credenciamento, bloqueio ou exclusão de acessos de usuários associados ao ativo em questão.

4.16 Gestor de Usuário: chefe de unidade de lotação de servidor, terceirizado, estagiário ou menor trabalhador/aprendiz; chefe de unidade responsável por coordenar assuntos de magistrados e de usuários externos; gestor de contrato de prestação de serviços. Compete a ele solicitar aos gestores de ativos de informação as credenciais de acesso para os usuários sob sua gestão.

4.17 Gestor de pessoal: Gestor de contrato de terceirização de mão de obra ou servidor da Secretaria de Gestão de Pessoas responsáveil por cadastar e atualizar a situação funcional de magistrados, servidores, estagiários e menores trabalhadores/aprendizes.

4.18 Necessidade de conhecer: condição pessoal, inerente ao efetivo exercício de cargo, função, emprego ou atividade, indispensável para o usuário ter acesso à informação, especialmente se for sigilosa, bem como o acesso aos ativos de informação.

4.19 Perfil de acesso: conjunto de permissões de acesso a ativo específico, que pode ser atribuído a usuário ou grupo de usuários com necessidade de conhecer em comum.

4.20 Prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderá receber credencial especial de acesso.

4.21 Proprietário de ativo de informação: refere-se à parte interessada da unidade da organização, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação.

4.22 Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta

no comprometimento da segurança da informação e comunicação.

4.23 Situação cadastral: estado em que se encontra determinado usuário em relação ao seu vínculo e execício no TRT18, podendo ser:

a) **ativo**;
b) **inativo** (aposentado; pensionista; afastado; em licença; em exercício em outro órgão);
c) **bloqueado**, a pedido de gestor competente;
d) **desligado**.

4.24 Termo de Responsabilidade: termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações e ativos de informação a que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso (Modelo - Anexo A).

4.25 Termo de Responsabilidade de Gestão de Acesso: termo assinado pelo gestor de acesso concordando com o uso adequado dos direitos para credenciamento de usuários, bem como assumindo as responsabilidades decorrentes de tais direitos (Modelo - Anexo B).

4.26 Usuário: pessoa que obteve autorização para acesso a Ativos de Informação do TRT18 mediante a assinatura de Termo de Responsabilidade, podendo pertencer a uma das seguintes classes:

4.26.1 Usuário interno: magistrados e servidores;

4.26.2 Usuário temporário: terceirizados, estagiários e menores trabalhadores/aprendizes;

4.26.3 Usuário externo: público em geral (advogados, partes, arrematantes etc.), prestadores de serviços (peritos, leiloeiros, ténicos em geral etc.) e agentes de outros órgãos (magistrados, procuradores etc.);

4.26.4 Usuário especial: contas de serviço, contas privilegiadas e contas de unidades organizacionais.

5 DISPOSIÇÕES INICIAIS

5.1 O objetivo do controle é sistematizar a concessão de acesso, físico ou lógico, a fim de evitar quebra de segurança, mediante a proteção dos ativos de informação contra indisponibilidade, perda, alteração indevida, acesso, transmissão e divulgação não autorizados.

5.2 A identificação, a autenticação, a autorização, a necessidade de conhecer são

condicionantes prévios para a concessão de acesso.

5.3 O gerenciamento de riscos de segurança da informação pode determinar a necessidade de implementação de novos controles de acesso, assim como de ajustes em controles já existentes.

5.4 Observada a legislação vigente e as diretrizes desta política, a implementação de novos controles de acesso está condicionada à elaboração de regras específicas por parte do proprietário do ativo de informação, sua aprovação prévia pela administração do TRT18 e subsequente adequações no ambiente: processos de trabalho, ferramentas e divulgação.

5.5 Cada conjunto de regras específicas a que se refere o item anterior, regulamentando o controle de acesso a um ou mais ativos de informação, deve ser formalizado em uma norma de segurança da informação cujo título deve ser iniciado por “CONTROLE DE ACESSO”.

5.6 Deve ser concedido aos usuários do TRT18 o acesso às informações e aos recursos de Tecnologia da Informação limitado ao mínimo que atenda à necessidade de conhecer e aos requisitos previstos em Lei, acordos, contratos e regulamentos específicos.

5.7 O acesso lógico aos recursos de tecnologia da informação do TRT18 se dá:

5.7.1 Preferencialmente por meio de contas de acesso;

5.7.2 Obrigatoriamente por meio de contas de acesso, no caso de ativos associados às informações classificadas em grau diferente de “público”.

5.8 O acesso ao código-fonte e dicionário de dados dos sistemas de informação deve ser controlado, de forma a permitir acesso de leitura e gravação somente por usuários autorizados.

6 CREDENCIAMENTO

6.1 O credenciamento de usuários para acesso a ativos de informação deve ser efetivado pelos respectivos gestores de acesso, incumbidos também pelo arquivamento de Termos de Responsabilidade.

6.2 Após o credenciamento, o usuário deverá assinar um Termo de Responsabilidade pelo uso das contas de acesso e dos ativos de informação, conforme modelo do anexo A.

6.3 Sempre que possível, deve-se utilizar uma base de dados única e centralizada, apoiada em serviço de diretório, para armazenamento das contas de acesso aos

ativos de informação.

6.4 A obtenção, a renovação ou a revogação de Certificados Digitais válidos no âmbito da ICP-Brasil seguem as regras estabelecidas pelas Autoridades Certificadoras e de Registros a ela subordinadas.

6.5 Os recursos providos e controlados por terceiros, disponibilizados para uso do TRT18, seguem regras próprias de registro, obtenção e manutenção de identidade, autenticação e autorização de acesso.

6.6 O credenciamento para acesso físico às instalações e recursos do TRT18 segue regulamentação própria, observadas as regras de segurança da informação específicas para acesso aos locais e instalações de ativos críticos de Tecnologia da Informação e Comunicação.

6.7 Identificação

6.7.1 A cada usuário deve ser fornecido um único código de identificação (código de usuário ou *login*), de caráter pessoal e intransferível, por ativo de informação a ser acessado.

6.7.2 O código de usuário é utilizado para associá-lo aos respectivos direitos de acesso e ao histórico de ações realizadas enquanto perduram tais direitos.

6.7.3 Sempre que possível, o código de identificação dos usuários deve utilizar formato padronizado pela STIC e ser único para todos os ativos de informação a que tiver direito de acesso.

6.7.4 O *login* de usuários internos e temporários será criado e fornecido pelos gestores de pessoal do TRT18 durante o processo admissional.

6.7.5 Os *logins* para usuários externos e especiais serão criados e fornecidos ao usuário pelos respectivos gestores de ativos de informação.

6.7.6 Esses mesmos gestores devem manter a situação cadastral de cada usuário, procedendo com a atualização imediata a cada mudança de estado: ativo; desligado; etc.

6.8 Autenticação

6.8.1 Ativos de informação podem conter mecanismos de autenticação que exijam a confirmação da identidade do usuário.

6.8.2 Essa autenticação deve ser realizada minimamente por meio do fornecimento de *login* e de um fator de autenticação representado por uma informação secreta (senha), de uso pessoal e intransferível.

6.8.3 Pode ser exigida a autenticação de multifatores (cartão com certificado digital e

PIN – *personal identification number;* senha e biometria etc.) a depender dos requisitos de segurança identificados para cada ativo de informação.

6.8.4 Deverá ser estabelecido no mínimo um processo formal de gerenciamento da concessão de senhas contendo procedimentos seguros para a manipulação das informações secretas de autenticação de usuários.

6.8.5 Os mecanismos de autenticação devem:

a) forçar o uso de senhas de qualidade, conforme a política de senhas;
b) não exibir a senha digitada;
c) sempre que possível:
   - não exibir o *login* do último usuário que acessou o ativo de informação;
   - não sugerir o armazenamento local da senha com finalidade de agilizar acessos futuros.

6.8.6 O *login* e senha do usuário devem ser autenticados simultaneamente.

6.8.7 Durante um processo malsucedido de autenticação, o mecanismo de autenticação não deve revelar qual parte dos dados está incorreta, se *login* ou senha.

6.8.8 Quando possível, os mecanismos de autenticação devem ser configurados de modo a bloquear temporariamente o acesso do usuário após um determinado número de tentativas de autenticação consecutivas sem sucesso, desbloqueando automaticamente tal acesso decorrido o tempo pré-configurado para bloqueio.

6.8.9 No caso de bloqueio temporário, na forma do item anterior, a liberação antecipada pode ser solicitada pelo usuário à unidade responsável pela gerência de acessos ao ativo de informação em questão.

6.8.10 Quando aplicável, devem ser implementados mecanismos de desconexão automática de sessão após decorrido um período de inatividade.

6.8.11 O número de tentativas de acesso malsucedidas, o tempo de bloqueio automático e o tempo para desconexão automática por inatividade são determinados em função dos requisitos de segurança de cada ativo de informação que necessite de controle de acesso.

6.9 Autorização

6.9.1 Para cada ativo de informação que necessite de controle de acesso, os respectivos gestores devem criar e nomear perfis de acesso padrão, que representam papéis ou grupos de usuários com necessidades de conhecer comuns.

6.9.2 A cada perfil de acesso deve ser associado um ou mais direitos de acesso

sobre o ativo e suas informações relacionadas: entrar, usar, ler, assinar, copiar, imprimir, apagar, modificar etc.

6.9.3 A autorização para um usuário ter acesso a determinado ativo de informação depende de solicitação formal, a ser realizada pelo respectivo gestor de usuário, endereçada ao gestor do ativo em questão.

6.9.4 A exclusão de acesso deve seguir a mesma formalidade do item anterior.

6.9.5 Concluído o processo de solicitação e aprovação pelos gestores competentes, a autorização deve ser efetivada pelo gestor de acesso mediante a associação do código do usuário a um ou mais perfis de acesso do ativo de informação.

6.9.6 É permitida a criação de perfis específicos para determinados usuários, a depender da necessidade de conhecer e dos requisitos de segurança do ativo de informação.

6.9.7 Os direitos de acesso devem estar consistentes com a norma de classificação da informação.

7 POLÍTICA DE SENHAS

7.1 Proteção das Senhas

7.1.1 Durante o processo de credenciamento, o usuário tem a oportunidade de cadastrar ou de obter uma senha provisória, com validade de até um dia.

7.1.2 O usuário deve zelar pela confidencialidade de sua senha, preservando o caráter pessoal e intransferível da mesma.

7.1.3 As senhas, assim como as informações biométricas, devem ser transmitidas e armazenadas em meios seguros, protegidas por criptografia compatível com as regras de classificação da informação e de uso de controles criptográficos.

7.1.4 As senhas devem ser trocadas:

a) imediatamente:
   - na ocasião do primeiro acesso do usuário com senha provisória;
   - em caso de suspeita de violação da confidencialidade da senha;
   - na ocasião da instalação de equipamentos ou softwares com senha “padrão de fábrica”;

b) periodicamente, em intervalo não superior ao que for deliberado e comunicado pela Comissão de Segurança da Informação.

7.1.5 As senhas podem ser trocadas a qualquer momento, por iniciativa do usuário.

7.2 Complexidade das Senhas

As diretrizes sobre complexidade aplicam-se às senhas, provisórias ou não, utilizadas para acessar os serviços de rede e os sistemas aplicativos desenvolvidos pela STIC.

7.2.1 As senhas devem ter obrigatoriamente:

a) tamanho mínimo de 8 (oito) caracteres;
b) no mínimo 1 (uma) letra minúscula;
c) no mínimo 1 (uma) letra maiúscula;
d) no mínimo 1 (um) dígito numérico;
e) ausência de três ou mais caracteres sequenciais (“234”, “5432”, “cdefg” etc.).

7.2.2 Elas devem preferencialmente:

a) não conter palavras de dicionário, em qualquer língua, ou termos de fácil dedução (número de RG ou CPF, placas de automóveis, datas, nomes próprios, *login* etc.);
b) não serem reutilizadas nas sucessivas trocas de senha.

8 MONITORAMENTO

8.1 Registro de Eventos

8.1.1 Os eventos (*logs*) de gerenciamento e uso de credenciais devem ser registrados em base de dados centralizada, que permita rastreabilidade e auditoria.

Os dados a serem registrados (como tipo do evento, endereço IP de origem, data, hora, *login* do gestor de acesso, *login* do usuário etc.), assim como o tempo de retenção dos mesmos, são determinados pela Comissão de Segurança da Informação, observadas as exigências legais e os recursos disponíveis para proteção, armazenamento, transmissão e processamento de tais informações.

8.2 Análise Crítica

8.2.1 As autorizações de acesso concedidas aos usuários devem ser mantidas em base de dados centralizada, de modo a permitir aos envolvidos (usuário, gestor de usuário, gestor de ativo de informação) a consulta das permissões de acesso vigentes.

8.2.2 Mudanças de lotação, de atribuições ou mudanças de estado de atividade (remoção para outro órgão, aposentadoria etc.), dentre outras, podem provocar inconformidades caso não sejam imediatamente comunicadas aos gestores de acesso.

8.2.3 Os gestores de ativos de informação devem analisar criticamente, em

intervalos não superiores a três meses, as autorizações de acesso concedidas visando identificar não conformidades e providenciar as adequações necessárias.

8.2.4 Os gestores de usuários devem informar imediatamente aos gestores de ativos de informação as mudanças nos perfis de acesso dos usuários sobre suas responsabilidades.

8.2.5 O período a que se refere o item 8.2.3 não ultrapassará um mês nos casos de autorizações de acesso privilegiado.

9 ACESSO PRIVILEGIADO

9.1 O acesso privilegiado a equipamentos de comunicação, sistemas operacionais, sistemas de gerenciamento de banco de dados, ambiente de desenvolvimento e demais recursos de TIC críticos deve ocorrer através de contas de acesso associadas a perfil de administrador ou a contas de serviço.

9.2 A concessão de acesso privilegiado deve atender à necessidade de conhecer e ser restrita a um número mínimo de pessoas da STIC.

9.3 O credenciamento, a política de senhas e o monitoramento de contas de acesso privilegiadas seguem as mesmas diretrizes para as contas de acesso normais, observada a necessidade de criação de código de usuário distinto do *login* utilizado nas atividades normais de negócio.

9.4 É proibido o uso de contas de acesso privilegiadas para o desempenho de atividades de negócio.

9.5 Deve ser evitado o uso de código de usuário genérico com perfil de administrador.

9.6 Devem ser restritas ao mínimo, em quantidade e usuários, e devidamente controladas as ferramentas que tenham potencial para contornar os mecanismos de controle de acesso tradicionais.

10 DISPOSIÇÕES GERAIS

10.1 Esta política deverá ser revisada periodicamente, em intervalos de até um ano.

ANEXO A – Modelo de Termo de Responsabilidade

Tribunal Regional do Trabalho da 18ª Região
TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____, CPF_____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ deste Tribunal Regional do Trabalho 18ª Região (TRT18), DECLARO, sob pena das sanções cabíveis nos termos da legislação vigente, que assumo a responsabilidade por:

I) tratar o(s) ativos de informação a que tiver acesso como patrimônio do TRT18;

II) utilizar as informações, em qualquer suporte e sob minha custódia, exclusivamente no interesse do serviço do TRT18;

III) contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Política de Segurança da Informação e Comunicação do TRT18, anexa à Portaria GP/NGTIC nº 001/2016, publicada no DEJT em 28/01/2016;

IV) utilizar as credenciais (contas de acesso) e os ativos de informações em conformidade com a legislação vigente e normas específicas do TRT18;

V) responder, perante o TRT18, pelo uso indevido das minhas credencias e dos ativos de informação.

Local e data: _____, ____ de _____ de _____.

_____

Assinatura

Nome do usuário e unidade de lotação

_____

Assinatura

Nome do gestor responsável pela autorização do acesso

ANEXO B – Modelo de Termo de Responsabilidade

Tribunal Regional do Trabalho da 18ª Região
TERMO DE RESPONSABILIDADE DE GESTÃO DE ACESSO

Pelo presente instrumento, eu _____, CPF_____, identidade _____, expedida pelo _____, em _____, e lotado no(a) _____ deste Tribunal Regional do Trabalho 18ª Região (TRT18), DECLARO, sob pena das sanções cabíveis nos termos da legislação vigente, que assumo a responsabilidade por:

I) utilizar os direitos de credenciamento de usuários apenas mediante devida solicitação realizada pelos respectivos gestores de usuários e devida aprovação por parte dos gestores de ativos de informação envolvidos na referida solicitação;

II) utilizar os meios seguros disponibilizados pelo Tribunal para a entrega de senha provisória de usuário;

III) revelar a senha provisória somente ao usuário solicitante;

IV) responder, perante o TRT18, pelo uso indevido das minhas credencias e dos ativos de informação.

Local e data: _____, ____ de _____ de _____.

_____

Assinatura

Nome do usuário e unidade de lotação

_____

Assinatura

Nome do gestor responsável pela autorização do acesso