Política de Controle de Acesso do SIGEP-JT (PCA-SIGEP-JT)

Outubro de 2023

Versão 1.0

Art. 1º A Política de Controle de Acesso do SIGEP-JT (PCA-SIGEP-JT) será disciplinada nos termos da presente Resolução.

§ 1º A PCA-SIGEP-JT estabelece diretrizes e procedimentos que visam garantir o acesso apropriado e seguro aos módulos do SIGEP-JT, a fim de minimizar os riscos de acesso não autorizado, de vazamento de informações e de comprometimento da integridade dos recursos de informação do SIGEP-JT.

§ 2º A PCA-SIGEP-JT foi elaborada com base na norma ISO/IEC 27002 e na Lei Geral de Proteção de Dados Pessoais (LGPD).

§ 3º A Política de Controle de Acesso do SIGEP-JT será revisada periodicamente para garantir que continue alinhada com as necessidades de negócios e os requisitos de segurança, em constante mudança.

CAPÍTULO I
APLICAÇÃO E ABRANGÊNCIA

Art. 2º Esta política se aplica a todos(as) os(as) usuários(as) autorizados(as) que acessam os módulos do SIGEP-JT, incluindo magistrados(as) e servidores(as) ocupantes de cargo efetivo ou em comissão, requisitados(as) e cedidos(as), empregados(as) de empresas prestadoras de serviços terceirizados, consultores(as), estagiários(as), auditores(as) e outras pessoas que, devidamente autorizadas, utilizem o sistema para processos relacionados aos órgãos da Justiça do Trabalho (JT).

Art. 3º A PCA-SIGEP-JT não substitui as políticas de segurança da informação e de controle de acesso existentes nos órgãos da JT, devendo ser aplicada em consonância com esses dispositivos.

CAPÍTULO II
TERMOS E DEFINIÇÕES

Art. 4º Termos utilizados nesta norma:

I. **Categorias de Usuários -** Agrupamentos lógicos de usuários por critérios configuráveis e pré-definidos, possibilitando a definição automática de pertencimento de um usuário a uma categoria, com base em seus dados cadastrais no Módulo Principal do SIGEP-JT.

II. **Gestor de Controle de Acesso** - Usuário responsável pela decisão e operacionalização da concessão e/ou remoção de direitos em um determinado módulo/submódulo do SIGEP-JT.

III. **Single Sign-On** - É um método de autenticação e autorização que permite que usuários acessem múltiplas aplicações com apenas um único login.

IV. **Mudança na Condição do Usuário** - Considera-se mudança na condição do usuário as seguintes situações:
- mudança de lotação;
- mudança de cargo;
- aposentadoria;
- exoneração/Demissão;
- falecimento;
- término de prestação de serviço;
- alteração de dados cadastrais que impactem em categorias pré-existentes de usuários.

CAPÍTULO III
PRINCÍPIOS GERAIS

Art. 5º Menor Privilégio - Qualquer tipo de acesso configurado será realizado da forma mais restritiva possível, garantindo que o acesso seja concedido apenas:

I. às pessoas necessárias;
II. pelo tempo necessário;
III. aos recursos necessários;
IV. aos perfis necessários.

Art. 6º Necessidade de Acesso - O acesso aos módulos do SIGEP-JT será concedido com base no princípio do menor privilégio. Os usuários terão acesso somente às funcionalidades e informações necessárias para desempenhar suas funções relacionadas ao sistema.

Art. 7º Identificação e Autenticação - Todos os usuários devem ser devidamente identificados e autenticados antes de acessar os módulos do SIGEP-JT. A autenticação será realizada por meio de métodos seguros, como senhas fortes, autenticação de dois fatores ou outras tecnologias aprovadas pelo CSJT.

Art. 8º Acesso Autorizado - O acesso aos módulos do SIGEP-JT será concedido com base nas autorizações pré-definidas para os perfis do sistema descritas no Mapa de Perfil de Acesso, anexo a esta resolução.

Art. 9º Monitoramento e Auditoria - Todas as atividades de acesso aos módulos do SIGEP-JT serão registradas e monitoradas. Auditorias regulares serão realizadas para verificar a conformidade com esta política e identificar atividades suspeitas ou não autorizadas.

Art. 10º Encerramento de Acesso - O acesso aos módulos do SIGEP-JT será encerrado imediatamente após a cessação do vínculo com o tribunal ou da

necessidade de acesso. Procedimentos claros serão seguidos para garantir o encerramento adequado do acesso.

Art. 11º Segregação de Funções - As funções e responsabilidades dentro do SIGEP-JT serão segregadas para evitar conflitos de interesse e garantir a supervisão adequada das atividades de acesso.

Art. 12º Uso Adequado - Os usuários são responsáveis por utilizar o acesso concedido aos módulos do SIGEP-JT de maneira apropriada e somente para os fins autorizados. O acesso não deve ser compartilhado, emprestado ou divulgado a terceiros sem autorização explícita.

CAPÍTULO IV
RESPONSABILIDADES

Art. 13º Cada TRM (Tribunal Responsável pelo Módulo) é responsável por implementar e manter as medidas de controle de acesso para seu respectivo módulo do SIGEP-JT.

Art. 14º Os gestores de cada área dos tribunais são responsáveis por identificar as necessidades de acesso aos módulos do SIGEP-JT dos membros de sua equipe e garantir que apenas as permissões necessárias sejam concedidas.

Art. 15º Os usuários são responsáveis por proteger suas credenciais de acesso aos módulos do SIGEP-JT e relatar qualquer suspeita de acesso não autorizado.

CAPÍTULO V
PROVISIONAMENTO PARA ACESSO DE USUÁRIO

Art. 16º É considerado provisionamento para acesso de usuário o processo que visa conceder ou revogar os direitos de acesso do usuário para todos os tipos de acesso em todos os sistemas e serviços.

Art. 17º Para concessão e a revogação de acesso de usuário a um módulo do SIGEP-JT, os tribunais seguirão o documento Procedimentos e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT.

Parágrafo único. O perfil do usuário será configurado de acordo com o Mapa de Perfil de Acesso do módulo.

Art. 18º Quando for necessária a realização de auditoria, o órgão auditor deverá solicitar ao tribunal que será auditado a habilitação de acesso nos módulos do SIGEP-JT que serão usados na auditoria.

§ 1º O acesso será concedido conforme descrito no documento Procedimentos e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT, anexo a esta resolução, e no Mapa de Perfil de Acesso dos módulos. Caso um módulo não possua o perfil próprio de Auditor, então o tribunal indicará qual perfil será atribuído aos membros da equipe de auditoria.

§ 2º Ao fim da rotina de auditoria, caberá ao tribunal auditado revogar todos os acessos concedidos para aquele fim específico.

CAPÍTULO VI
GERENCIAMENTO DE DIREITOS DE ACESSO PRIVILEGIADOS

Art. 19º São considerados direitos de acesso privilegiado os que se referem a perfis com recursos elevados que vão além dos usuários normais. Essas contas podem ser usadas para realizar tarefas administrativas, como instalar software, fazer alterações no sistema ou acessar dados confidenciais.

Parágrafo único. No SIGEP-JT, são considerados perfis com acesso privilegiado os de administrador negocial, administrador de TI, gestor de controle de acesso e auditor, por seu potencial acesso a informações sensíveis.

Art. 20º Define-se como concessão de acesso privilegiado a vinculação a um usuário específico de qualquer perfil com acesso privilegiado.

Art. 21º Os TRMs deverão:

I. identificar nos documentos Procedimentos e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT” e Mapa de Perfis de Acesso os perfis considerados como “perfil com acesso privilegiado”;
II. para módulos que permitem a customização de perfis pelos administradores, identificar as funcionalidades que , quando atribuídas a um perfil, o transformam em um “perfil com acesso privilegiado”.

Art. 22º O perfil com acesso privilegiado será concedido observando os requisitos estabelecidos no documento Procedimentos e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT.

§ 1º A concessão de acesso privilegiado será realizada obrigatoriamente por processo de autorização formal e rastreável, estabelecido pelo tribunal, registrando a lista de privilégios concedidos e/ou o perfil atribuído, os dados de quem os recebeu e o(s) módulo(s) do SIGEP-JT afetado(s) e a duração do acesso.

§ 2º Por padrão, todos os acessos privilegiados deverão ter a duração máxima estabelecida no Procedimento e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT, após a qual, automaticamente, serão revogados.

§ 3º Os direitos de acesso só poderão ser concedidos após a finalização do processo de autorização formal, com seu respectivo deferimento.

§ 4º O processo de autorização formal deverá prever as situações nas quais o direito de acesso privilegiado será revogado, podendo incluir, mas não se limitando a:

I. lapso temporal;
II. morte;
III. desligamento do órgão ou mudança na situação fática do portador do acesso;
IV. mudança na situação fática do órgão ou interesse da administração.

Art. 23º O módulo de controle de acesso do SIGEP-JT deverá identificar mudanças ocorridas na condição do usuário, revogando seus acessos imediatamente, de maneira que o acesso aos demais módulos seja, por consequência, interrompido.

Parágrafo único. Sistemas que não utilizem o módulo de controle de acesso do SIGEP-JT deverão, preferencialmente, realizar a mesma verificação diretamente nos dados funcionais do usuário.

Art. 24º Caberá aos gestores de acesso do SIGEP-JT nos tribunais analisar, a cada período máximo estabelecido no documento Procedimentos e Critérios para Concessão de Acesso aos Módulos do SIGEP-JT ou na data de finalização do tempo de acesso privilegiado concedido, as competências dos usuários com direitos de acesso privilegiado, para verificar se eles estão alinhados com as suas obrigações, realizando as alterações necessárias no respectivo módulo.

Art. 25º Não serão admitidos login genérico e/ou usuários compartilhados - como “admin” - nos módulos do SIGEP-JT.

Art. 26º Os usuários que possuam perfis com acesso privilegiado e que necessitem acessar o sistema para realizar outras operações negociais não vinculadas com o referido acesso privilegiado devem fazê-lo por meio de perfil sem acesso privilegiado.

§ 1º Para realizar login com o perfil com acesso privilegiado, o usuário deve escolher expressamente, no momento do login ou após ter sido logado com perfil sem acesso privilegiado, por padrão.

§ 2º Alternativamente ao que se preconiza no caput e no parágrafo primeiro, o usuário que necessite de um perfil com acesso privilegiado concomitante a outros sem acesso privilegiado poderá ter logins de usuário distintos e independentes entre si para cada perfil.

Art. 27º Não será permitido aos usuários acessarem o sistema utilizando mais de um perfil ao mesmo tempo.

CAPÍTULO VII
GERENCIAMENTO DA INFORMAÇÃO DE AUTENTICAÇÃO SECRETA DE USUÁRIOS

Art. 28º A gestão da informação de autenticação secreta de usuários é fundamental para garantir a segurança da informação e a integridade dos sistemas. Esta prática tem o objetivo de assegurar que a autenticação dos usuários em sistemas sensíveis ocorra de forma segura e controlada.

Art. 29º Para a gestão da informação de autenticação secreta de usuários, as seguintes ações deverão ser implementadas pelos tribunais conforme sua própria Política Institucional de Segurança da Informação:

I. **Declaração de Confidencialidade -** Instituir a obrigatoriedade da assinatura de uma declaração por parte dos usuários, comprometendo-se a manter a confidencialidade da informação de autenticação secreta. Integrar essa declaração aos termos e condições de contratação dos usuários;

II. Autenticação Temporária - Estabelecer um protocolo onde os usuários, ao receberem suas informações de autenticação, inicialmente obtenham uma senha temporária que deve ser alterada no primeiro acesso;

III. Verificação de Identidade - Implementar procedimentos rigorosos para verificar a identidade do usuário antes de conceder ou redefinir qualquer informação de autenticação secreta;

IV. Fornecimento Seguro - Assegurar que as informações de autenticação secretas temporárias sejam enviadas aos usuários por métodos seguros, evitando o uso de e-mails de terceiros ou mensagens não criptografadas;

V. Unicidade e Complexidade - Garantir que cada informação de autenticação secreta temporária seja única e não seja facilmente dedutível;

VI. Alteração Pós-Instalação - Assegurar que qualquer senha ou informação de autenticação padrão, fornecida por sistemas ou softwares recém-instalados, seja alterada imediatamente após a instalação;

VII. Tipos de Informações de Autenticação Secreta - Embora as senhas sejam o método mais comum de autenticação, os tribunais devem

considerar o uso de outras formas de autenticação secreta, como chaves criptográficas e tokens (por exemplo, smart cards), que fornecem códigos de autenticação.

CAPÍTULO VIII
RETIRADA OU AJUSTE DE DIREITOS DE ACESSO

Art. 30º Quando houver mudança na condição do usuário, que lhe permitiu ter o nível de acesso atual, os direitos de acesso aos módulos/submódulos que compõem o SIGEP-JT devem ser ajustados.

Parágrafo único. Considera-se mudança na condição do usuário as seguintes situações:

I. mudança de lotação;
II. mudança de cargo;
III. aposentadoria;
IV. exoneração/demissão;
V. falecimento;
VI. término de prestação de serviço;
VII. alteração de dados cadastrais que impactem em categorias pré-existentes de usuários.

Art. 31º A mudança na condição do usuário deve refletir em seus direitos de acesso aos módulos/submódulos do SIGEP-JT de imediato, tão logo a nova condição do usuário seja formalizada.

§ 1º Direitos concedidos por lotação devem ser ajustados automaticamente para refletir a mudança de lotação do usuário, removendo os direitos associados à lotação anterior e concedendo os direitos associados à nova lotação.

§ 2º Direitos concedidos por cargo devem ser ajustados automaticamente para refletir a mudança de cargo do usuário, removendo os direitos associados ao cargo anterior e concedendo os direitos associados ao novo cargo.

§ 3º Direitos concedidos por categoria devem ser ajustados automaticamente para refletir o enquadramento do usuário em uma nova categoria ou a remoção do usuário de uma categoria pré-existente.

§ 4º Direitos concedidos individualmente devem ser ajustados, pelo Gestor de Controle de Acesso do módulo/submódulo afetado, para refletir a mudança na condição do usuário.

Art. 32º Sem prejuízo dos ajustes imediatos de direitos, previstos no artigo anterior, em função das eventuais mudanças nas condições dos usuários, deve o

Gestor de Controle de Acesso, periodicamente, verificar se todos os usuários que possuem direitos tem justificativa para tal e, em caso negativo, tratar de imediato a mudança.

Art. 33º Caso os ajustes nos direitos do usuário acarretem a remoção de todos os seus direitos, esse usuário terá seu acesso ao SIGEP-JT revogado.

CAPÍTULO VIII
RESPONSABILIDADES DOS USUÁRIOS

Art. 34º São deveres do usuário:

I. zelar pelo sigilo de sua senha, garantindo o não compartilhamento com outras pessoas;
II. não anotar a senha em papel ou em qualquer outro meio eletrônico não aprovado (sistema de gerenciamento de senha), inclusive dispositivos de uso pessoal, como celulares e tablets;
III. ao ausentar-se, ainda que temporariamente, efetuar o bloqueio ou encerramento da sua sessão nos sistemas e recursos do SIGEP-JT;
IV. fazer a alteração da senha em casos indicativos de comprometimento desta;
V. comunicar imediatamente à unidade de Segurança da Informação eventuais suspeitas de comprometimento da senha para a adoção das medidas cabíveis;
VI. não utilizar senhas de fácil dedução, como as que contenham informações pessoais (data de aniversário, CPF, RG, login, nomes próprios), sequência numérica (123...) ou alfabética (abc...);
VII. alterar a senha no primeiro acesso nos casos em que a senha não tenha sido criada pelo usuário (senha temporária);
VIII. não utilizar as mesmas senhas dos sistemas do SIGEP-JT em contas pessoais, sejam redes sociais ou quaisquer outros serviços não relacionados ao SIGEP-JT.

CAPÍTULO IX
PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA (LOGON)

Art. 35º À exceção de informações e funcionalidades consideradas de uso público, todos os módulos do SIGEP-JT deverão exigir autenticação dos usuários, ao realizar a entrada no sistema (logon).

§ 1º A técnica de autenticação deverá ser uniformizada entre todos os módulos do SIGEP-JT e adequada para validar a identificação alegada de um usuário.

§ 2º É vedada a utilização de técnica considerada menos segura do que a estabelecida como padrão, no parágrafo primeiro.

§ 3º A critério do CSJT e do Tribunal Responsável pelo Módulo (TRM), justificadamente, poder-se-á optar por técnica de autenticação considerada mais segura do que a estabelecida como padrão para todos os módulos do SIGEP-JT.

Art. 36º Sempre que possível, o procedimento para entrada nos módulos do SIGEP-JT será configurado para minimizar a oportunidade de acessos não autorizados.

Art. 37º No procedimento de entrada (logon), é vedada a revelação de informações sobre o sistema, ou sobre o usuário em questão, em especial na tentativa mal sucedida de acesso.

Art. 38º O procedimento de entrada no sistema (logon):

I. não deverá mostrar identificadores de sistema até que o processo tenha sido concluído com sucesso;
II. poderá mostrar um aviso geral informando que o sistema deve ser acessado somente por usuários autorizados;
III. não deverá fornecer mensagens de ajuda que possam auxiliar um usuário não autorizado;
IV. deverá validar informações de acesso somente quando todos os dados de entrada forem fornecidos, sem indicar qual parte do dado de entrada está correta ou incorreta, em caso de condição de erro;
V. deverá, obrigatoriamente, registrar todas as tentativas de acesso, sejam bem ou mal sucedidas;
VI. não deverá mostrar a senha que está sendo informada;
VII. não deverá transmitir senhas em texto claro, sem criptografia, pela rede.

Art. 39º Sessões inativas após um período definido de inatividade deverão ser encerradas automaticamente.

Parágrafo único. Mediante justificativa, o tempo de conexão máximo poderá ser restringido, a critério do CSJT ou do TRM, para fornecer segurança adicional nas aplicações de alto risco e reduzir a janela de oportunidade para acessos não autorizados.

CAPÍTULO X
SISTEMA DE GERENCIAMENTO DE SENHA

Art. 40º Os tribunais devem instituir sua própria Política Institucional de Segurança da Informação, que deve tratar da utilização e seguridade de logins e senhas.

Art. 41º No âmbito do SIGEP-JT, a autenticação dos usuários é feita por Single Sign ON (SSO), ou seja, as credenciais são geradas no próprio tribunal e utilizadas em todos os módulos/submódulos do SIGEP-JT. Por isso, é esperado que os tribunais, em suas políticas institucionais de segurança da informação, sigam as recomendações da norma ISO/IEC 27002:

I. obrigue o uso individual de ID de usuário e senha para manter responsabilidades;
II. permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros;
III. obrigue a escolha de senhas de qualidade;
IV. obrigue os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema;
V. force as mudanças de senha em intervalos regulares;
VI. mantenha um registro das senhas anteriores utilizadas e bloqueie a reutilização;
VII. não mostre as senhas na tela quando forem digitadas;
VIII. armazene os arquivos de senha separadamente dos dados do sistema da aplicação;
IX. armazene e transmita as senhas de forma protegida.

CAPÍTULO XI
USO DE APLICAÇÃO PRIVILEGIADA

Art. 42º O uso de aplicação capaz de sobrepor os controles de segurança deve ser restrito e controlado. Sua utilização requer autorização, devendo seguir as diretrizes para uso:

I. procedimentos de identificação, autenticação e autorização para o uso da aplicação;
II. segregação da aplicação em módulo específico;
III. registro do uso da aplicação;
IV. definição e documentação dos níveis de autorização para a aplicação;
V. remoção ou desabilitação da aplicação após o seu uso;
VI. não deixar habilitado para usuários com acesso às aplicações onde a segregação de funções é requerida.