PORTARIA TRT/GP/DG Nº 375/2023

Define a Política de Controle de Acessos do Tribunal Regional do Trabalho da 24ª Região.

O PRESIDENTE DO TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO, no uso de suas atribuições regimentais,

CONSIDERANDO que o controle de acesso relativo à segurança da informação fornece maior garantia para o alcance dos objetivos institucionais;

CONSIDERANDO a observância e adoção das recomendações do framework de governança de TIC COBIT 5.0;

CONSIDERANDO as normas da série ISO 27000, que tratam da definição de requisitos para um sistema de segurança da informação, notadamente no referente aos controles de acesso e a segurança em recursos humanos;

CONSIDERANDO o Anexo VI da Portaria CNJ 162/2021, de 10 de junho de 2021, relativo ao Manual de Referência para Gestão de Identidade e de Controle de Acessos,

RESOLVE:

REVOGAR a Portaria TRT/GP/DGCA nº 52/2016, de 06 de maio de 2016, e **DEFINIR** a Política de Controle de Acessos no âmbito do Tribunal Regional do Trabalho da 24ª, nos termos da presente Portaria.

CAPÍTULO I
DAS DEFINIÇÕES

Art. 1º. Para fins desta Portaria, considera-se:

I. **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação do TRT24;

II. **Acesso físico:** qualquer forma de contato físico entre um usuário de TIC ou um prestador de serviços a qualquer tipo de equipamento de armazenamento ou processamento de dados;

III. **Acesso lógico:** qualquer tipo de contato entre o usuário de TIC e as informações armazenadas ou processadas em sistemas, aplicativos, ferramentas, sistema operacional ou outros ativos de TIC do TRT da 24ª Região;

IV. **Ativos de TIC** - qualquer mecanismo ou dispositivo de software ou hardware que compõem a infraestrutura da rede de dados do TRT24 e que é utilizado como ferramenta de trabalho para o desempenho funcional dos colaboradores do Tribunal;

V. **Chamado**: solicitação de atendimento à Central de Serviços por parte de algum usuário de TIC;

VI. **Conta de usuário de TIC:** identificação pessoal e intransferível formada por login, senha e, sempre que possível, por um segundo fator de autenticação criados automaticamente no momento do cadastro no Sistema de Recursos Humanos e que permitam

acesso à rede de dados, intranet, e-mail, sistemas de informática e demais recursos de TIC oferecidos pelo TRT24;

VII. **Controle de acesso:** conjunto de procedimentos, recursos e meios utilizados com a finalidade de solicitar, conceder, verificar e bloquear acessos;

VIII. **Manual de Controle de Acessos:** documento integrante da Política de Controle de Acessos que descreve os aspectos técnicos relativos ao controle de acessos lógicos e físicos;

IX. **Perímetro crítico:** ambiente destinado a armazenar ativos de TIC, cuja interrupção não programada do funcionamento ou a indisponibilidade comprometam significativamente as atividades do TRT24;

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

XI. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulte no comprometimento da segurança da informação e comunicações;

XII. **Termo de Adesão à Política de Segurança da Informação:** documento onde o usuário de TIC declara conhecer e aderir às normas estabelecidas pela Política de Segurança da Informação do TRT24;

XIII. **Usuário de TIC**: todos aqueles que exerçam, ainda que transitoriamente e sem

remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública em qualquer unidade organizacional do TRT da 24ª Região;

XIV. **VPN (Virtual Private Network)**: Rede privada virtual baseada em um mecanismo seguro que faz a criação de um túnel criptografado para acesso externo ao ambiente privado do TRT24;

XV. **Segregação de funções**: separação de funções de autorização, aprovação, execução, controle e contabilização das operações, evitando o acúmulo de funções por parte de um mesmo colaborador;

XVI. **Princípio do privilégio mínimo**: estratégia de segurança que se baseia na atribuição das permissões mínimas necessárias ao desempenho de uma atividade específica, evitando privilégios desnecessários;

XVII. **Gestor de sistemas**: colaborador técnico ou negocial, com vínculo estatutário, responsável por gerenciar os acessos lógicos em determinado sistema do TRT24, seguindo os princípios da segregação de função e privilégios mínimos.

CAPÍTULO II
DAS DIRETRIZES GERAIS

Art. 2º. A Política de Controle de Acessos é parte integrante da Política de Segurança da Informação e obedecerá às seguintes diretrizes:

I. Estabelecer os processos de trabalho para garantir que a identificação, autorização, autenticação e o interesse do serviço são condicionantes prévios para concessão de acesso aos ativos de TIC do TRT da 24ª Região, sob responsabilidade da unidade de Tecnologia da Informação e Comunicações;

II. Definir as atribuições e responsabilidades relativas ao processo de trabalho **Gerenciar Controle de Acessos**.

CAPÍTULO III
DOS PROCESSOS DE TRABALHO

Art. 3º. As atividades executadas no âmbito da Política de Controle de Acessos deverão observar os procedimentos descritos no processo de trabalho **Gerenciar Controle de Acessos**, disponível no site do Portal de Governança de TIC do TRT24, item “Políticas e Processos de Trabalho”.

CAPÍTULO IV
DOS RESPONSÁVEIS E DAS RESPONSABILIDADES

Art. 4º. Os responsáveis e as responsabilidades no âmbito da presente Política serão definidos de acordo com os papéis estabelecidos no processo de trabalho **Gerenciar Controle de Acessos**:

I. cabe ao Secretário de Tecnologia da Informação e Comunicações exercer o papel de “**Dono do Processo**” e observar as seguintes responsabilidades:

a. assegurar que todos os envolvidos na execução do processo sejam informados das mudanças e suporte efetuados;
b. aprovar as atualizações do processo;
c. buscar a qualidade e eficiência gerais do processo.

II. cabe ao Chefe da Divisão de Proteção de Dados e Segurança da Informação exercer os papéis de **"Gerente do Processo"** e de **"Gerente de Segurança"** e observar as seguintes responsabilidades:

a. buscar a eficiência e a efetividade do processo;
b. manter o desenho e indicadores do processo atualizados, garantindo que estejam adequados aos propósitos da organização;
c. produzir informações gerenciais (indicadores);
d. promover a execução das atividades do processo;
e. definir e manter atualizados os perímetros críticos;
f. garantir que os mecanismos automatizados de concessão/revogação de direitos estejam em funcionamento adequadamente;
g. oferecer suporte aos gestores de sistemas para garantir que os direitos de acessos estejam alinhados a atribuição atual dos usuários de TIC;
h. promover a assinatura dos Termos de Adesão;
i. registrar solicitações de acessos;
j. registrar agendamento de acessos;

k. realizar ou promover continuamente testes de segurança nos dispositivos de segurança dos perímetros críticos;
l. reportar ao Comitê de Segurança da Informação e Proteção de Dados os eventos relacionados a quebras de segurança ou desconformidades;
m. tomar as providências cabíveis em casos de ocorrência de incidentes de segurança da informação.

III. cabe ao Chefe do Setor de Gerenciamento da Central de Serviços exercer o papel de "**Central de Serviços**" e observar as seguintes responsabilidades:
a. auxiliar os usuários nas tarefas de criação/alteração de senhas e certificados;
b. promover a assinatura do Termo de Adesão à Política de Segurança da Informação.

IV. cabe aos servidores designados como responsáveis pelos perímetros exercerem o papel de "**Responsável pelo perímetro**" e observarem as seguintes responsabilidades:
a. autenticar acessos físicos;
b. comunicar acessos físicos ao Setor de Segurança da Informação;
c. negar / interromper acessos físicos;
d. permitir acessos físicos.

V. cabe aos servidores designados como membros da equipe de monitoramento exercerem o papel de "**Equipe de Monitoramento**" e observarem a seguinte responsabilidade:
a. verificar constantemente os sistemas de monitoramento em busca de eventos que

comprometem ou podem comprometer a segurança física.

VI. cabe aos servidores designados como gestores de sistemas exercerem o papel de "**Gestor de Sistemas**" e observarem as seguintes responsabilidades:

a. conceder/revogar direitos de acessos a sistemas do qual seja gestor;

b. zelar pela aplicabilidade dos princípios de segregação de função e privilégio mínimo.

VII. cabe aos servidores da Divisão de Infraestrutura de TIC exercerem o papel de "**Infraestrutura**" e observarem as seguintes responsabilidades:

a. cadastrar novo usuário terceirizado;

b. conceder novos acessos à rede.

Parágrafo único. A designação dos servidores responsáveis pelos perímetros, dos membros da Equipe de Monitoramento e dos gestores dos sistemas será feita pelo **Secretário de Tecnologia da Informação e Comunicações** através de portaria, registrada no processo administrativo eletrônico relativo ao processo Gerenciar Controle de Acessos, ou através de ordem de serviço para integrantes da unidade de Tecnologia da Informação.

CAPÍTULO V
DO ÂMBITO E DA APLICAÇÃO

Art. 5º. A Política de Controle de Acessos aplica-se a todos os usuários de TIC do TRT da 24ª da Região e também, no que couber, a eventuais agentes externos, prestadores de serviços, contratados ou não, que por qualquer

razão necessitem acessar os ativos de TIC do TRT da 24ª Região.

CAPÍTULO VI
DO CONTROLE DE ACESSOS LÓGICOS DE CONTAS DE USUÁRIOS

Art. 6º. Todo usuário de TIC receberá uma conta de usuário para acesso a rede de computadores do TRT da 24ª Região, depois de efetivado o cadastro no Sistema de Recursos Humanos.

§1º O nome da conta será composto pela inicial do primeiro nome seguido do último nome.

§2º Havendo coincidência com contas já existentes, o nome da conta será composto pela combinação das iniciais de todos os nomes seguidos do último nome.

§3º Modificações no nome da conta somente poderão ser realizadas mediante solicitação formal a unidade de Tecnologia da Informação.

Art. 7º. Uma senha de acesso provisória será criada juntamente com a conta de usuário.

Parágrafo único. A senha inicial dará direito de acesso:

I. À Intranet do TRT da 24ª Região;

II. Ao sistema AssineWeb.

Art. 8º. A senha provisória deverá ser alterada pelo usuário por meio de funcionalidade disponível na Intranet.

§1º As senhas criadas pelos usuários deverão satisfazer os seguintes requisitos de complexidade:

I. Devem possuir tamanho mínimo de 12 caracteres;

II. Devem conter letras e números não sequenciais;

III. Devem conter pelo menos uma das letras maiúscula ou uma das letras minúscula;

IV. Não devem conter informações pessoais (CPF, RG, matrícula, data de aniversário, nome ou login da rede);

V. Não devem ser reproduções das últimas duas senhas cadastradas pelo usuário;

VI. Devem ser periodicamente trocadas, no mínimo, a cada 1 dia e no máximo a cada 180 dias (6 meses);

VII. As contas de usuário serão bloqueadas após 10 tentativas consecutivas de acesso não reconhecidas.

§2º Alterações adicionais da senha de acesso podem ser realizadas pelo titular através da funcionalidade mencionada no caput.

§3º Sempre que uma senha de rede for alterada, haverá o envio automático de e-mail com remetente "naoresponda@trt24.jus.br", apenas relatando o evento, sem solicitação de qualquer tipo de informações pessoais nem redirecionamentos para links externos.

§4º Em caso de esquecimento da senha, deverá ser utilizada a funcionalidade de recuperação de senhas presente na área restrita do Portal, o qual solicitará informações pessoais para o envio de uma nova senha em e-mail externo previamente cadastro pela área de recursos humanos do Tribunal. Caso o e-mail externo não esteja cadastrado na base de informações pessoais do TRT24, o colaborador deverá comparecer pessoalmente ao setor de RH para solicitar este cadastro.

§5º As senhas das contas de e-mails setoriais ficarão sob a responsabilidade dos gestores de área e observarão todas as regras mencionadas no caput.

Art. 9º. As senhas de acesso são pessoais e intransferíveis, cabendo ao detentor:

I. A responsabilidade pelo seu uso indevido;

II. Não compartilhar a senha com outras pessoas;

III. Não anotar a senha em papel ou em qualquer outro meio eletrônico, inclusive dispositivos de uso pessoal, como celulares e tablets;

IV. Não utilizar senhas de fácil dedução, como as que contenham informações pessoais (data de aniversário, CPF, RG, login, etc);

V. Ao ausentar-se, ainda que temporariamente, efetuar o bloqueio ou encerramento da sua sessão nos sistemas e recursos do TRT24;

VI. Comunicar imediatamente à unidade de Segurança da Informação, através da Central de Atendimento de TIC, eventuais suspeitas de comprometimento da senha para a adoção das medidas cabíveis;

VII. Não utilizar as mesmas senhas dos sistemas do Tribunal em contas de redes sociais ou quaisquer serviços não relacionados ao TRT24;

VIII. Utilizar os privilégios concedidos em sua senha exclusivamente para as finalidades relacionadas a atribuição do cargo/função.

Art. 10. Após a criação de uma senha personalizada, o novo usuário de TIC deverá criar as

assinaturas eletrônicas necessárias nos diversos sistemas eletrônicos do TRT24, conforme for concedido o acesso ao usuário.

Art. 11. O novo usuário de TIC deverá conhecer e assinar o Termo de Adesão definido no âmbito da Política de Segurança da Informação.

§1º A assinatura do Termo de Adesão é condição necessária para a concessão de direitos de acesso adicionais.

§2º A assinatura do Termo de Adesão poderá ser exigida dos usuários antigos a qualquer momento, caso verificada a ausência da mesma.

Art. 12. Após a assinatura do Termo de Adesão o responsável pela unidade de lotação do usuário de TIC deverá formalmente solicitar à Central de Atendimento de TIC a concessão de direitos de acesso aos sistemas, aplicações e às pastas de uso compartilhado da unidade.

§1º A concessão de direitos de acessos a sistemas e aplicações seguirá as definições de cada serviço e aplicação existente, seguindo se o princípio do privilégio mínimo e segregação de funções sempre que possível;

§2º Alterações nos direitos de acesso deverão ser solicitados formalmente à Central de Atendimento da TIC pelos gestores das unidades.

Art. 13. Em caso de fechamento de provimento, término do vínculo ou mudança de lotação do usuário, a alteração/exclusão dos acessos será feita pelos gestores dos sistemas.

§1º Os responsáveis pelas unidades deverão abrir chamado para encerramento dos acessos de magistrados, servidores e colaboradores com lotação alterada ou desligados

do Tribunal, em caso de ausência de automatização ou de permissão para exclusão em algum serviço ou aplicação.

§2º A unidade de Segurança da Informação confeccionará relatório de possíveis acessos não encerrados, no mínimo semestralmente, enviando notificação aos gestores dos sistemas para as devidas providências ou manifestações.

Art. 14. O uso compartilhado de credenciais de acesso somente será permitido onde forem estritamente necessários por razões operacionais ou de negócios e deve ser aprovado pelo Comitê de Segurança da Informação e Proteção de Dados.

Parágrafo único. As contas de uso compartilhado deverão estar associadas exclusivamente aos ativos para os quais foram definidos.

Art. 15. A inobservância das normas da Política de Controle de Acessos do TRT da 24ª Região poderá, mediante autorização do Comitê de Segurança da Informação e Proteção de Dados, implicar na revogação dos diretos concedidos a qualquer tempo.

CAPÍTULO VII
DO CONTROLE DE ACESSOS LÓGICOS DE CONTAS PRIVILEGIADAS

Art. 16. Os servidores da unidade de tecnologia da informação, em razão de suas atividades técnicas, poderão ter acessos especiais ou totais aos ativos e sistemas de TIC, observando se os princípios do privilégio mínimo e da segregação de funções.

§1º Os privilégios especiais deverão ser atribuídos a uma conta distinta daquela utilizada diariamente para acesso a rede de dados, e-mails, internet e VPN;

§2º O acesso a uma conta privilegiadas deverá, sempre que possível tecnicamente, ser feita a partir de uma estação de trabalho ou servidor de rede exclusivo para este fim, com restrições na navegação da Internet;

§3º Contas privilegiadas deverão ser utilizadas apenas para execução dos comandos estritamente necessários ao desempenho de tarefa específica, sem que seja necessário o "login" no domínio de rede do Tribunal;

§4º Contas com acessos especiais jamais poderão ser utilizadas de modo compartilhado e deverão ser atribuídas única e exclusivamente a um único colaborador técnico.

Art. 17. O uso de senhas em códigos fontes de programas, "scripts", macros, arquivos de configurações e documentações só será permitido caso seja empregado mecanismos de criptografia adequados bem como usuários com permissões específicas e mínimas para execução da funcionalidade, observando se o princípio do privilégio mínimo e segregação de funções em todas as situações.

Parágrafo único. A utilização das senhas mencionadas neste artigo será temporária, quando possível tecnicamente, e poderão ser revogadas a qualquer momento caso se constate vulnerabilidades relacionadas à Segurança da Informação.

CAPÍTULO VIII
DOS CONTROLES DE ACESSOS LÓGICOS - REQUISITOS TÉCNICOS GERAIS

Art. 18. Os acessos lógicos aos sistemas e serviços do TRT24 deverão ter registros mínimos de acessos armazenados em "log" para possibilitar rastreabilidade, caso necessário.

Art. 19. Senhas em trânsito, seja pela rede interna ou rede pública, deverão sempre ser transportadas de forma segura, utilizando sistemas de criptografia fortes e atualizadas.

Art. 20. Sempre que possível, os serviços críticos bem como os novos sistemas desenvolvidos internamente ou por contratação/convênio, deverão considerar:

I. Autenticação e autorização via base de dados única de usuários (Active Directory) ou que no mínimo seja passível de integração via “scripts” auxiliares;

II. Uso de duplo fator de autenticação, de preferência baseado em certificados digitais e biometria ou, não sendo possível as alternativas preferenciais, aplicativos para geração de códigos OTP no celular (Google Authenticator, Microsoft Authenticator, etc);

III. Criptografia dos dados e informações em trânsito/repouso, conforme a sua criticidade.

Art. 21. Acessos remotos (protocolos SSH, RDP, SFTP, etc) aos ativos e utilitários de gerenciamentos dos serviços de TIC deverão ser realizados, sempre que possível tecnicamente, por meio de ferramenta centralizada que implemente mecanismos de criptografia, auditoria e duplo fator de autenticação.

CAPÍTULO IX
DO CONTROLES DE ACESSOS LÓGICOS EM CONEXÕES EXTERNAS

Art. 22. O acesso externo de usuários via VPN (Virtual Private Networks ou Rede Virtual Privada) deverá ser devidamente autorizado pela administração do Tribunal e só será permitido aos colaboradores que possuam permissão explícita para tal fim.

Art. 23. Deverão ser garantidos no mínimo os seguintes requisitos de segurança para que uma conexão VPN seja permitida:

I. Criptografia da comunicação, através do estabelecimento de um túnel encriptado;

II. Autenticação multifator;

III. Software antivírus atualizado e ativo;

IV. Sistema Operacional atualizado.

Art. 24. A conta de acesso à VPN será a mesma utilizada para acesso à rede interna do Tribunal, sendo de inteira responsabilidade do seu proprietário todas as atividades executadas com essa conta.

Art. 25. Toda solicitação de acesso externo por empresas terceirizadas, seja via VPN ou outro método, deverá passar pela análise de riscos e vulnerabilidades da unidade de Segurança da Informação.

CAPÍTULO X
DA SEGURANÇA EM RECURSOS HUMANOS E CONTROLE DE ACESSOS FÍSICOS

Art. 26. As listas de perfis de acesso e perímetros críticos para a segurança física da informação do TRT da 24ª Região, os dispositivos de segurança e os detalhes técnicos relativos as execuções das tarefas serão descritas no Manual de Controle de Acessos, observando-se os seguintes critérios:

I. Por questão de segurança, o documento deverá ser mantido sob sigilo e disponível apenas aos responsáveis pelas tarefas;

II. O documento deverá ser atualizado no mínimo 1 (uma) vez por ano ou sempre que houver demanda para revisão.

Art. 27. O acesso aos perímetros críticos é restrito às equipes das unidades de Infraestrutura de TIC, Segurança da Informação e ao(s) servidor(es) designado(s).

Art. 28. Todos os acessos aos perímetros críticos deverão ser previamente agendados e autorizados pelas unidades de Segurança da Informação e Infraestrutura de TIC mediante identificação da(s) pessoa(s) que entrarão no perímetro e a justificativa do propósito e das atividades que serão realizadas no local.

Art. 29. O controle de acesso aos perímetros críticos seguirá as seguintes diretrizes:

I. O acesso será realizado por meio de senha, controle biométrico, cartão eletrônico ou chave mecânica;

II. A guarda dos cartões de acesso e/ou chaves mecânicas é de responsabilidade dos servidores designados, sendo expressamente

proibido o empréstimo para qualquer outra pessoa;

III. Todas as portas de acesso aos perímetros críticos deverão permanecer trancadas, mesmo durante o horário de expediente.

Art. 30. Qualquer evento de quebra de segurança associado ao acesso ou a tentativa de acesso não autorizado aos perímetros críticos deve ser imediatamente reportado à área de segurança do TRT da 24ª Região.

Art. 31. É vedado o uso do espaço interno dos perímetros críticos para o armazenamento de quaisquer tipos de equipamentos ou itens de consumo que não estejam em utilização.

Art. 32. O monitoramento das condições ambientais dos perímetros críticos será realizado pela Equipe de Monitoramento.

Art. 33. Esta portaria entra em vigor na data de sua publicação.

João Marcelo Balsanelli
Desembargador Presidente