



**PODER JUDICIÁRIO**  
**Tribunal Regional do Trabalho da 9ª Região**

**POLÍTICA nº 17 DE 13 DE DEZEMBRO DE 2017.**

*Institui a Política de Acesso Físico aos Ambientes de TIC no âmbito do Tribunal Regional do Trabalho da 9ª Região.*

**O DIRETOR DA SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO DO TRIBUNAL REGIONAL DO TRABALHO DA 9ª REGIÃO**, usando de suas atribuições legais e regimentais,

**CONSIDERANDO:**

- a Política de Segurança da Informação (PSI) deste Tribunal;
- o Ato 190/2017 da Presidência, que normatiza a Instituição de Políticas de TIC;
- a instituição, por meio da Política nº 10/2017, da Política de Gerenciamento de Processos de trabalho no âmbito do Tribunal;

**RESOLVE:**

**CAPÍTULO I**  
**DAS DISPOSIÇÕES INICIAIS**

**Art. 1º** Instituir a POLÍTICA DE ACESSO FÍSICO AOS AMBIENTES DE TIC, no âmbito deste Tribunal.

**Art. 2º** Esta política integra a Política de Segurança da Informação do Tribunal (PSI) e tem como objetivo assegurar o acesso físico de pessoal autorizado aos dispositivos de armazenamento e de provimento de serviços e prevenir acessos não autorizados, modificação, destruição ou interferência, dos ativos de Tecnologia de Informação e Comunicação (TIC) do Tribunal Regional do Trabalho da 9ª Região por meio de instrumentos mecânicos e/ou tecnológicos em instalações de caráter restrito.



**PODER JUDICIÁRIO**  
**Tribunal Regional do Trabalho da 9ª Região**

**CAPÍTULO II**  
**DOS CONCEITOS E DEFINIÇÕES**

**Art. 3º** Para os efeitos desta Política, aplicam-se as seguintes definições e conceitos:

I - AMBIENTES RESTRITOS DE TIC: locais, elencados em instrumento próprio pelo Diretor da STI, em que se encontram instalados equipamentos servidores e/ou equipamentos de rede e comunicação;

II - AMBIENTES CRÍTICOS DE TIC: ambientes restritos de TIC em que se encontram instalados equipamentos servidores e/ou equipamentos de rede e comunicação, que por sua importância para a continuidade dos serviços de TIC prestados, devem possuir controles de acesso mais rígidos;

III - AMBIENTES DE TIC: refere-se ao conjunto de ambientes restritos e ambientes críticos de TIC;

IV - DATA CENTER: ambiente crítico de TIC projetado para abrigar servidores e outros componentes como sistemas de armazenamento de dados (*storages*) e ativos de rede (*switches, roteadores*);

V - EQUIPAMENTOS CRÍTICOS DE TIC: equipamentos de Tecnologia da Informação e Comunicação, tais como servidores, sistemas de armazenamento de dados (*storages*) e ativos de rede, que operam em regime 24x7x365 (24 Horas por dia, 7 dias por semana, 365 dias por ano) e cuja indisponibilidade impacta um número grande de usuários;

VI - LEITOR BIOMÉTRICO: dispositivo que lê e analisa as características físicas únicas de um indivíduo a fim de identificá-lo, podendo informar o resultado da verificação a um sistema de provisionamento de acesso. Exemplo: leitor de impressão digital;

VII - UNIDADE DE SEGURANÇA PATRIMONIAL: responsável pela segurança física das instalações do Tribunal.

**Parágrafo único.** Outras definições e conceitos específicos encontram-se definidos no GLOSSÁRIO, disponível em sítio na Intranet ou Internet mantidos por este Tribunal.

**CAPÍTULO III**  
**DOS PAPÉIS E RESPONSABILIDADES**

**Art. 4º** Cabe à Unidade de Segurança Patrimonial a gerência e o controle dos meios e procedimentos de acesso às áreas do Tribunal que contenham os perímetros de segurança física dos ambientes restritos de TIC.

**Art. 5º** Cabe à STI a gerência e o controle dos meios e procedimentos de acesso aos locais restritos de TIC, especificamente.



**PODER JUDICIÁRIO**  
**Tribunal Regional do Trabalho da 9ª Região**

**CAPÍTULO IV**  
**DAS DIRETRIZES DE ACESSO FÍSICO AOS AMBIENTES RESTRITOS DE TIC**

**Art. 6º** O acesso aos ambientes restritos de TIC do Tribunal é franqueado exclusivamente aos Servidores lotados na STI, ou a outras pessoas, mediante autorização e acompanhamento presencial de um servidor do quadro da STI.

**§1º** O Diretor da STI pode, caso a caso, autorizar previamente a visita de funcionários externos ou prestadores de serviços autorizados, para a realização de manutenções preventivas e corretivas, mediante solicitação formal e apresentação de documentos de identificação.

**§2º** Procedimentos específicos para o fornecimento de autorização de acesso aos ambientes restritos de TIC devem ser elaborados e executados de forma rigorosa, sendo que os funcionários de vigilância devem estar instruídos a sempre proibir a entrada de visitantes sem identificação.

**Art. 7º** Funcionários externos, prestadores de serviços autorizados ou visitantes, autorizados pelo Diretor da STI, devem utilizar um meio de identificação com foto, com validade nacional, para obter acesso ao ambiente.

**Art. 8º** A entrada de pessoas no ambiente deve sempre ser precedida de uma verificação do motivo de suas visitas e do preenchimento de controles/registros de acesso ao local.

**Parágrafo Único.** A STI deve ser informada com antecedência sobre qualquer visita quando esta estiver sendo conduzida ou acompanhada por outra unidade do Tribunal.

**Art. 9º** Ambientes restritos de TIC localizados em unidades do interior do estado deverão ser acondicionados em sala específica, devidamente isolada e exclusiva, com dispositivo de controle de acesso preferencialmente com leitor biométrico.

**Parágrafo único.** Na impossibilidade de instalação do sistema de controle de acesso descrito no *caput* deste artigo, o controle de acesso deve ser delegado ao responsável administrativo da unidade judiciária, devendo ele, e somente ele, controlar o acesso ao ambiente através de meios, no mínimo, mecânicos, e manter registro dos acessos.

**CAPÍTULO V**  
**DAS DIRETRIZES DE ACESSO FÍSICO AOS AMBIENTES CRÍTICOS DE TIC**

**Art. 10.** Para acesso aos ambientes críticos de TIC aplicam-se as mesmas disposições do acesso aos ambientes restritos de TIC.

**§1º** A STI, em conjunto com outras áreas competentes, deve definir um perímetro de segurança física no entorno dos ambientes críticos de TIC, com controle de entrada e saída e franquia de acesso apenas a pessoal autorizado.

**§2º** O acesso aos ambientes críticos deve ser controlado por meio de leitores biométricos. Em situação de falha do leitor biométrico, o acesso deve ser realizado por meio de senha, digitada pelo responsável pelo ambiente na interface do dispositivo de controle eletrônico de acesso.



**PODER JUDICIÁRIO**  
**Tribunal Regional do Trabalho da 9ª Região**

§3º Acessos aos ambientes críticos de TIC fora do horário de expediente oficial do Tribunal deve ser autorizado previamente, e estarem os funcionários da vigilância patrimonial e controle de acesso informados com nome e local de trabalho dos envolvidos.

§4º Em casos emergenciais, deve-se estar disponível aos funcionários da vigilância patrimonial e controle de acesso os números de telefones, ou outra forma de contato, dos superiores, conforme o caso, do(s) técnico(s) que precisarão ter acesso ao ambiente crítico de TIC em horário não convencional.

**Art. 11.** A entrega ou retirada de equipamentos e a carga e descarga de materiais destinadas a ambientes críticos deve acontecer em uma área de recepção implantada especificamente para esse fim, sendo seu acesso monitorado por alarmes e câmeras.

**Parágrafo único.** As movimentações devem ser registradas, indicando o maior número de informações possível do respectivo equipamento ou material e o nome e o local de trabalho do(s) agente(s) atuante(s) nesse processo.

**Art. 12.** Quadrimestralmente deve ser realizada análise de conformidade técnica dos acessos físicos com requisitos e padrões de segurança do *Data Center*, conforme definido em procedimento específico.

**CAPÍTULO V**  
**DO CONTROLE E MONITORAMENTO**

**Art. 13.** O monitoramento das áreas de acesso aos ambientes críticos de TIC e de suas áreas internas deve ser realizado por câmeras de segurança estrategicamente posicionadas e deverá ser controlado e gerenciado pela Unidade de Segurança Patrimonial.

**Art. 14.** O detalhamento dos controles e do monitoramento dos acessos aos ambientes de TIC está definido no Processo de Acesso físico aos ambientes de TIC.

**CAPÍTULO VI**  
**DAS SANÇÕES**

**Art. 15.** O descumprimento das determinações contidas nesta política poderá acarretar as sanções previstas na PSI.

**CAPÍTULO VII**  
**DA PRESTAÇÃO DE CONTAS E TRANSPARÊNCIA**

**Art. 16.** A STI deve apresentar aos membros da Comissão de Segurança da Informação (CSI) ou aos demais órgãos Colegiados de TIC que as requererem, informações acerca do cumprimento da presente política.

**Art. 17.** A Política, as listas de ambientes críticos e ambientes restritos de TIC, o detalhamento dos processos, entre outros documentos relacionados serão publicados pela STI na *intranet* ou em sítio específico na *Internet* mantido por este Tribunal, devendo

A



**PODER JUDICIÁRIO**  
**Tribunal Regional do Trabalho da 9ª Região**

também ser inseridas, classificadas e relacionadas no Sistema de Apoio à Governança e Gestão vigente.

**CAPÍTULO VIII**  
**DAS DISPOSIÇÕES FINAIS E TRANSITÓRIAS**

**Art. 18.** Em consonância com o Ato 190/2017 da Presidência e a Política nº 10/2017, o dono do **Processo de Acesso Físico aos ambientes de TIC** é o(a) Diretor(a) da STI.

**Art. 19.** Os casos omissos serão resolvidos pela instância instituidora dessa política e persistindo dúvidas, estas devem ser encaminhadas à(s) instância(s) imediatamente superior(es).

**Art. 20.** Esta Política entra em vigor na data de sua publicação.

*Luciano Kuehne*

**LUCIANO KUEHNE**

Diretor Substituto da Secretaria de Tecnologia da Informação

PUBLICADO NO BOLETIM  
DE SERVIÇO N.º 1  
DE 09/11/18.

*Adriane Gesser*

**Adriane Gesser**  
Técnica Judiciária