



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

**PORTARIA TRT/GP/DGCA N° 692/2011**

Define a Política de Segurança da Informação 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** a observância das recomendações do Tribunal de Contas da União - TCU (Acórdãos TCU - Plenário - n.º 1.603/2008, 2.471/2008 e 663/2009), no que diz respeito à implantação de modelos de governança de Tecnologia da Informação (TI) que incluam planejamento estratégico institucional, planejamento estratégico de TI e comitê diretivo de TI;

**CONSIDERANDO** que compete ao Comitê Técnico Temático de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região (Portaria TRT/GP/DGCA n° 645/2011, de 26 de outubro de 2011, art. 2º), elaborar e aplicar as normas da Política de Segurança da Informação;

**CONSIDERANDO** a necessidade estabelecer os papéis e responsabilidades relacionados ao processo de garantir a integridade, confidencialidade e disponibilidade dos ativos de TI do Tribunal Regional do Trabalho da 24ª Região;

**RESOLVE:**

Definir a Política de Segurança da Informação no âmbito do Tribunal Regional do Trabalho da 24ª Região, nos termos do presente ato.

**CAPÍTULO I**

**DAS DIRETRIZES GERAIS**

Art. 1º A Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região obedecerá às seguintes diretrizes:

- I.** Estabelecer e promover ações para garantir a disponibilidade, integridade, confidencialidade, autenticidade e legalidade das informações em meio computacional;
- II.** Mitigar os riscos associados à dependência da organização em relação ao uso massivo da TI;
- III.** Definir as atribuições e responsabilidades relativas ao processo de estabelecer e promover a aplicação da Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região

Art. 2º A gestão da Política de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região contará com as seguintes instâncias:

- I.** Coordenação de planejamento e gestão;
- II.** Coordenação executiva.



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

**CAPÍTULO II**  
**DAS DEFINIÇÕES**

Art. 3º Para fins deste ato, considera-se:

- I. Ativos de TI:** 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 magistrados e servidores;
- II. Segurança da Informação:** conjunto de medidas que tem como objetivo o estabelecimento dos controles necessários à proteção das informações durante sua criação, aquisição, uso, transporte, guarda e descarte, contra destruição, modificação, comercialização ou divulgação indevidas e acessos não autorizados, acidentais ou intencionais, garantindo a continuidade dos serviços e a preservação de seus aspectos básicos de confidencialidade, integridade, disponibilidade, autenticidade e legalidade;
- III. Usuário de TI:** 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.

### **CAPÍTULO III**

#### **DA COORDENAÇÃO DE PLANEJAMENTO E GESTÃO**

Art. 4º Cabe ao Comitê Técnico Temático de Segurança da Informação do Tribunal Regional do Trabalho da 24ª Região (ctSEG-TRT24):

- I.** Promover as ações necessárias a elaboração, aplicação e revisão das normas da presente política.
- II.** Revisar a Política de Segurança da Informação e seus instrumentos normativos sempre que se fizer necessário, ou, no mínimo, a cada ano, mantendo-se os controles de versões e revisões;
- III.** Acompanhar e fiscalizar a aplicação das normas da Política de Segurança da Informação.

Art. 5º As ações desenvolvidas no âmbito da Política de Segurança da Informação serão norteadas pelos seguintes princípios:

- I.** Clareza: as responsabilidades pela segurança dos ativos de TI do TRT da 24ª Região e pelo cumprimento de processos de segurança devem ser claramente definidas;
- II.** Responsabilidade: os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço devem ter ciência de todas as normas e procedimentos de Segurança da Tecnologia da



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

Informação;

**III. Ética:** todos os direitos e interesses legítimos dos magistrados, servidores, colaboradores, consultores externos, estagiários, prestadores de serviço e visitantes devem ser respeitados sem comprometimento da segurança;

**IV. Proporcionalidade:** o nível, a complexidade e os custos das ações de segurança de TI devem ser apropriados e adequados ao valor e à necessidade de confiança nos ativos do TRT da 24ª Região, considerando os impactos e a probabilidade de ocorrência dos riscos;

**V. Celeridade:** as ações de segurança de TI devem oferecer respostas a incidentes e correções de falhas de segurança o mais rápido possível.

#### **CAPÍTULO IV**

##### **DA COORDENAÇÃO EXECUTIVA**

Art. 6º Cabe a Divisão de Suporte e Segurança da Secretaria de Tecnologia da Informação:

**I.** Promover as ações necessárias para a disponibilização da infraestrutura técnica de segurança e aplicação das normas de segurança;

**II.** Prestar contas da execução da Política de Segurança ao Comitê Técnico Temático de Segurança da Informação (ctSEG-TRT24);

**III.** Promover continuamente iniciativas de capacitação para servidores nos

procedimentos de segurança que envolvam o uso da Tecnologia da Informação, de forma a minimizar ocorrência de problemas de segurança, sem prejuízo das normas internas específicas sobre capacitação;

**IV.** Promover a comunicação e dar publicidade das normas e ações previstas na Política de Segurança da Informação.

## **CAPÍTULO V**

### **DO ÂMBITO E DA APLICAÇÃO**

Art. 7º A Política de Segurança da Informação aplica-se a todos aqueles autorizados a fazerem uso dos ativos de TI, no âmbito das redes de computadores do TRT da 24ª Região, administrados pela Secretaria de Tecnologia da Informação - STI

Parágrafo único. Aplica-se ainda esta política, no que couber, ao relacionamento do TRT da 24ª Região com outros órgãos públicos ou entidades públicas ou privadas.

## **CAPÍTULO VI**

### **DOS INSTRUMENTOS NORMATIVOS**

Art. 8º As ações desenvolvidas no âmbito da Política de Segurança da Informação deverão observar os seguintes instrumentos normativos:

**I. Plano de Uso de Serviços de TI:** define o conjunto de regras uso de serviços e soluções contidas no portfólio de TI;

**II. Plano de Controle de Acessos:** define o conjunto de regras que disciplinam os acessos aos ambientes críticos da área de TI;



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

### **III. Plano de Controle de Software Malicioso**

#### **CAPÍTULO VII**

##### **DAS ATRIBUIÇÕES E RESPONSABILIDADES**

Art. 9º Cabe a todos os usuários de TI do TRT da 24ª Região observar e adotar as ações de Política de Segurança da Informação;

§ 1º. Os usuários de TI devem utilizar os recursos de Tecnologia da Informação, de propriedade do TRT da 24ª Região, somente para fins corporativos, no interesse da administração e para as tarefas a que se destinam.

§ 2º. É considerada imprópria a utilização destes recursos para propósitos particulares ou não autorizados.

#### **CAPÍTULO VIII**

##### **DA CAPACITAÇÃO**

Art. 10º A proposta de capacitação dos servidores envolvidos nos procedimentos de segurança deverá ser anualmente encaminhada ao órgão do Tribunal Regional do Trabalho da 24ª Região responsável pelo programa institucional de capacitação.

Parágrafo único. A capacitação deverá basear-se nas responsabilidades e papéis previstos na Política de Segurança da Informação, sem prejuízo de conteúdos que estejam fora do escopo da norma, mas podem contribuir para sua melhoria.

#### **CAPÍTULO IX**

##### **DA COMUNICAÇÃO**

Art. 11º A Política de Segurança da

Informação, seus normativos, alterações, atualizações e quaisquer ações decorrentes da aplicação das normas previstas serão comunicados aos usuários de TI através das ferramentas de correio eletrônico, Malote Digital e site da STI (STI.TRT24.JUS.BR).

**CAMPO GRANDE-MS, 21.11.2011.**

**MARCIO VASQUES THIBAU DE ALMEIDA**  
**Desembargador Presidente do Tribunal Regional**  
**do Trabalho da 24<sup>a</sup> Região**



## Plano de Uso de Serviços de TI

### 1 DO OBJETIVO

1.1 A Política de Uso de Serviços e Soluções de TI do Tribunal Regional do Trabalho da 24ª Região possui como objetivo orientar os usuários da rede corporativa quanto aos procedimentos básicos a serem adotados para a melhor utilização dos recursos e sistemas existentes.

### 2 DA JUSTIFICATIVA

2.1 O avanço significativo no acesso, manipulação e distribuição da informação através dos diversos setores da Instituição é de fundamental importância para o desempenho funcional dos magistrados e servidores deste Tribunal;

### 3 DOS CONCEITOS

3.1 Consideram-se, para os efeitos deste ato, os seguintes conceitos:

3.1.1 **Ativos de TI:** 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 magistrados e servidores do Tribunal;

3.1.2 **Usuário de TI:** 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;

3.1.3 **Internet:** rede mundial de computadores que permite o tráfego de dados e a comunicação entre si de todos a ela conectados;

3.1.4 **Intranet:** Servidores intranet são computadores que oferecem determinados serviços para usuários da rede de computadores de uma organização. Normalmente utilizados para agrupar funções de alta responsabilidade, servindo como depósito protegido dos arquivos dos usuários, usando todas as facilidades da internet;

3.1.5 **Página:** documento disponibilizado na

internet pelos computadores servidores da rede, com informações que pessoas físicas e jurídicas têm interesse em veicular;

- 3.1.6 **Site:** conjunto de páginas eletrônicas armazenadas em um computador, cujos objetivos primordiais, no caso deste Tribunal, são promover a divulgação da instituição e propiciar aos jurisdicionados o acesso a um número crescente de serviços;
- 3.1.7 **Email** (eletronic mail, correio eletrônico): sistema desenvolvido para a troca de mensagens por meio eletrônico. Também designa a mensagem em si;
- 3.1.8 **CHAT:** aplicação de conversação em tempo real, em grupo ou privada, através da internet;
- 3.1.9 **Conta de usuário de TI:** identificação pessoal e intransferível formada por **login e senha**, criada automaticamente no momento do cadastro no Sistema de Recursos Humanos e que permite acesso à rede de dados, intranet, email, sistemas de informática e demais recursos de TI oferecidos pelo TRT24;
- 3.1.10 **Conta de email pessoal (institucional):** conta de correio eletrônico fornecida pela instituição para cada magistrado e servidor do quadro. Pertence ao usuário e lhe permite enviar e receber mensagens, das quais lhe cabe a responsabilidade;
- 3.1.11 **Conta de email da unidade:** conta do correio eletrônico que permite às diversas unidades do Tribunal enviar e receber mensagens. Pertence à unidade e é de responsabilidade do respectivo titular;
- 3.1.12 **Spam:** a) Mensagem eletrônica contendo propaganda de produtos ou serviços enviada a uma ou mais pessoas sem que essas pessoas tenham solicitado as informações contidas na mensagem. b) Mensagem eletrônica geralmente enviada, indiscriminadamente, a milhares de pessoas, de forma invasiva, intrusiva e abusiva sem que os destinatários a tenham solicitado. c) Mensagem eletrônica, não solicitada pelo destinatário, contendo propaganda comercial, correntes da felicidade, correntes do tipo "solução para os seus problemas financeiros";



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

- 3.1.13 **Assinatura Digital:** método de autenticação de informação digital através de mecanismo de identificação do remetente;
- 3.1.14 **Certificado Digital:** é a tecnologia que provê mecanismos lógicos e matemáticos de assinatura digital, utilizando-se de um arquivo, cartão ou token, onde são armazenadas informações como nome, cpf e chave privada, dentre outras, referentes a uma pessoa, empresa, site ou computador, que fornecem às transações eletrônicas mecanismos de segurança capazes de garantir autenticidade, confidencialidade, integridade e não-repúdio às informações eletrônicas;
- 3.1.15 **Cartão de assinatura digital (smart card):** hardware portátil, semelhante a um cartão magnético, que armazena em seu chip a chave privada do usuário. O acesso às informações nele contidas é feito por meio de uma senha pessoal, determinada pelo titular;
- 3.1.16 **Token de assinatura digital:** hardware portátil, semelhante a um pen-drive, que armazena em seu chip a chave privada do usuário. O acesso às informações nele contidas é feito por meio de uma senha pessoal, determinada pelo titular;
- 3.1.17 **Malote digital:** ferramenta oficial de comunicação eletrônica entre as Unidades Organizacionais da Justiça do Trabalho e demais ramos da justiça nacional;
- 3.1.18 **Rede de Computadores do TRT24:** conjunto de ativos de TI formado pelos equipamentos e serviços de internet, intranet, correio eletrônico, estrutura diretórios e pastas da rede e sistemas corporativos do TRT24.

#### 4 DA APLICAÇÃO

- 4.1 A Política de uso de recursos de TI é parte integrante da Política de Segurança da Informação e aplica-se a todos os usuários de TI autorizados a fazerem uso dos ativos de Tecnologia da Informação - TI, no âmbito das redes de computadores do TRT da 24ª Região, administradas pela Secretaria de Tecnologia da Informação - STI.

## **5 DAS NORMAS GERAIS DE USO DE ATIVOS DE TI**

- 5.1 A responsabilidade pelo acompanhamento da aplicação das normas de uso dos ativos de TI do TRT da 24<sup>a</sup> Região é do Chefe da Divisão de Suporte e Segurança;
- 5.2 A utilização dos recursos de TI destina-se a auxiliar os usuários de TI do TRT da 24<sup>a</sup> Região, em efetivo exercício, na realização de atividades relacionadas estritamente ao serviço, especialmente para discussão de temas jurídicos, institucionais, de repercussão regional, nacional e internacional;
- 5.3 É vedado o uso dos equipamentos e sistemas de informática deste Órgão para veiculação ou armazenamento voluntário de matérias:
  - 5.3.1 Pornográficas;
  - 5.3.2 Político-partidárias ou sindicais;
  - 5.3.3 Ofensivas ao princípio da urbanidade;
  - 5.3.4 Ofensivas ao decoro pessoal;
  - 5.3.5 Que contenham manifestações ofensivas à honra e à dignidade de pessoas, instituições e autoridades;
  - 5.3.6 Que apresentem linguagem incompatível com o decoro da classe;
  - 5.3.7 Que versem assuntos de natureza comercial;
  - 5.3.8 Que provoquem sobrecarga no sistema.
- 5.4 São também vedados:
  - 5.4.1 Participar de ações ilegais ou que de alguma forma caracterizem descumprimento dos deveres para com a Administração;
  - 5.4.2 Participar de qualquer ação que comprometa a segurança da rede de computadores do TRT24;
  - 5.4.3 A utilização de senha alheia;
  - 5.4.4 Revelar ou compartilhar senhas com outros usuários;
  - 5.4.5 A disponibilização a pessoas, Órgãos ou entidades externas de mensagens que possam vir a comprometer a boa imagem da instituição;

## **6 DO ACESSO À REDE DE COMPUTADORES DO TRT24**

- 6.1 Todo usuário de TI receberá conta de usuário para acesso a rede de computadores do TRT24 depois de efetivado o cadastro no Sistema de Recursos Humanos.



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

- 6.1.1 O nome da conta será gerado automaticamente pelo Sistema de Recursos Humanos de acordo com a seguinte regra:
  - 6.1.1.1 O nome da conta será composto pela inicial do 1º nome seguido no último nome. Havendo coincidência com contas já existentes, a nome da conta será composto por combinação das iniciais de todos os nomes seguidos pelo último nome;
  - 6.1.1.2 Modificações no nome da conta só serão realizadas mediante solicitação formal a Secretaria de Tecnologia da Informação.
- 6.1.2 A senha inicial deverá ser alterada pelo usuário através da funcionalidade disponível no site da intranet;
- 6.1.3 Os direitos inicialmente concedidos serão para o acesso básico aos aplicativos e dados correspondentes a lotação do servidor;
  - 6.1.3.1 A concessão de direitos adicionais deverá formalmente solicitada à STI;
- 6.2 As senhas de acesso à rede de computadores, correio eletrônico e sistemas aplicativos são pessoais e intransferíveis, cabendo ao detentor a responsabilidade pelo seu uso indevido;
  - 6.2.1 A responsabilidade por qualquer acesso efetuado que desrespeite a Política de Segurança da Informação é da pessoa que o tenha realizado e, no caso de estagiários e contratados, do servidor responsável;
- 6.3 A alteração da senha de acesso deve ser realizada pelo próprio titular através de funcionalidade disponível no site da intranet ou através de solicitação por telefone a Central de Atendimento da Secretaria de Informática;
  - 6.3.1 No caso de solicitação por telefone o usuário de TI deverá prestar informações cadastrais para fins de confirmação de identidade;
- 6.4 A Diretora do Serviço de Recursos Humanos informará oficialmente a Secretaria de Tecnologia da Informação o desligamento de servidor, do quadro de pessoal deste Tribunal, para a

desativação das contas de usuário;

6.4.1 A revogação de direitos devido à mudança de lotação do servidor será feita automaticamente pelo sistema de Recursos Humanos no momento da alteração do cadastro.

6.5 Ao magistrado/servidor aposentado será facultado o acesso à intranet mediante solicitação formal ao Serviço de Recursos Humanos;

6.6 A inobservância das normas da Política de Segurança da Informação poderá, a qualquer momento, implicar a revogação dos direitos concedidos.

## **7 DO USO DOS DIRETÓRIOS (PASTAS) DA REDE**

7.1 Todo usuário de TI receberá uma pasta pessoal na rede do TRT24 com direitos de leitura, escrita e execução, restrito ao usuário, limitada ao tamanho de 100Mb (cem megabytes);

7.2 Todo usuário de TI receberá o direito de acesso compartilhado a pasta da unidade administrativa em que estiver lotado;

7.3 Todo usuário de TI receberá o direito de acesso a pasta pública e temporária da rede;

7.3.1 O conteúdo da pasta pública é temporário, não possui cópia de segurança e pode ser apagado pela Secretaria de Tecnologia da Informação sem aviso prévio sempre que se fizer necessário liberar espaço de armazenamento.

7.4 É proibida a cópia em qualquer pasta da rede do TRT24 dos seguintes tipos de arquivos contendo:

7.4.1 Material pornográfico, racista, ofensivo, ilegal, preconceituoso ou discriminatório;

7.4.2 Material calunioso ou difamatório;

7.4.3 Propagandas comerciais;

7.4.4 Músicas e filmes de qualquer formato;

7.4.5 Programas ou aplicativos não homologados ou não licenciados;

7.4.6 Programas de conteúdo prejudicial à segurança da rede de computadores do TRT24.

## **8 DO USO DE COMPUTADORES E NOTEBOOKS**

8.1 É expressamente proibido instalar, configurar ou conectar a rede qualquer tipo de equipamento não pertencente ao TRT24 (tais como tablets, notebooks, computadores pessoais, switches, hubs, modems/roteadores wireless, access points) que



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

possam comprometer a segurança da informação, salvo com autorização formal do Comitê de Segurança da Informação;

- 8.2 Os computadores (estações de trabalho) e notebooks fornecidos pelo TRT24 são protegidos por software antivírus e regras de segurança definidas pelo Comitê de Segurança da Informação;
- 8.3 A responsabilidade sobre a inobservância do item 8.1 recai sobre o usuário que a praticar;

**9 DO ENVIO E RECEBIMENTO DE MENSAGENS POR CORREIO ELETRÔNICO**

- 9.1 Para comunicação deverá ser priorizada a utilização do correio eletrônico, evitando-se, tanto quanto possível, a impressão do conteúdo das mensagens;
- 9.2 Cabe a quaisquer dos receptores das mensagens, imagens ou notas indevidas comunicarem o fato a Secretaria de Tecnologia da Informação, para as providências cabíveis;
- 9.3 O uso do correio eletrônico será considerado atividade inadequada e passível de apuração por sindicância se não estiver relacionado à matéria de interesse do Tribunal ou às atribuições do cargo do usuário;
  - 9.3.1 Mesmo se relacionados a matérias de interesse do Tribunal ou às atribuições do cargo do usuário, são consideradas atividades inadequadas o acesso a gravação ou a impressão de textos ou gráficos que excedam o limite dos padrões aceitáveis de ética, bom senso e razoabilidade;
  - 9.3.2 O uso inadequado do correio eletrônico compreende a troca de mensagens contendo:
    - 9.3.2.1 Material pornográfico, racista, ofensivo, ilegal, preconceituoso ou discriminatório;
    - 9.3.2.2 Material calunioso ou difamatório;
    - 9.3.2.3 Propagandas comerciais;
    - 9.3.2.4 Listas de endereços dos usuários do correio eletrônico do TRT24;
    - 9.3.2.5 Entretenimento ou correntes;
    - 9.3.2.6 Músicas e filmes de qualquer formato;
    - 9.3.2.7 SPAM;
    - 9.3.2.8 Aplicativos.
- 9.4 Qualquer mensagem endereçada ao grupo de email

- "TODOS" deverá ser submetida previamente à apreciação da Diretoria-Geral de Coordenação Administrativa;
- 9.5 A Secretaria de Tecnologia da Informação definirá os limites de armazenamento e tamanho de mensagens para a utilização das contas de email pessoal e de unidades;
- 9.6 As unidades judiciais e administrativas que compõem o TRT24 terão contas de correio eletrônico sob responsabilidade dos responsáveis pelas unidades;
- 9.7 Os titulares de conta de email de usuário ou de unidade deverão sempre observar os padrões de envio e recebimento de mensagens estabelecidos pela Secretaria de Tecnologia da Informação;
- 9.8 A leitura das mensagens recebidas deverá ser realizada diariamente, devendo o titular de conta providenciar, se for o caso, a resposta e o respectivo arquivamento, cuidando, em qualquer hipótese, de manter limpa a caixa postal;
- 9.8.1 Nos afastamentos ou impedimentos do titular de conta de unidade, deverá ser designado um responsável pelo acompanhamento das mensagens;
- 9.9 As caixas postais das contas de correio eletrônico sem movimentação por um período de 120 (cento e vinte) dias serão bloqueadas automaticamente;
- 9.10 As caixas postais das contas de correio eletrônico serão limitadas ao tamanho de 40MB (quarenta megabytes);
- 9.11 A Secretaria de Informática, mediante autorização específica do Comitê de Segurança da Informação, poderá acessar contas e monitorar a origem e o destino das mensagens eletrônicas.

## **10 DO USO DA INTERNET E INTRANET**

- 10.1 Por ocasião do acesso a *sites* e páginas da *internet* o usuário deverá:
- 10.1.1 Utilizar os navegadores (*browser*) indicados pela Secretaria de Informática;
- 10.1.2 Manter conduta compatível com a moralidade administrativa, inclusive quando da utilização de serviços de computadores remotos e na transferência de arquivos;
- 10.1.3 Observar os procedimentos ordinários de segurança indicados pela Secretaria de Informática, principalmente antivírus, ficando diretamente responsável pelas consequências decorrentes de práticas



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

contrárias ao recomendado e que danifiquem ou coloquem em risco os sistemas de computadores e os arquivos de dados do Tribunal.

10.2 O acesso à *internet* será considerado atividade inadequada e passível de apuração por sindicância se não estiver relacionado a matérias de interesse do Tribunal ou às atribuições do cargo do usuário;

10.2.1 Mesmo se relacionados a matérias de interesse do Tribunal ou às atribuições do cargo do usuário, são consideradas atividades inadequadas o acesso a gravação ou a impressão de textos ou gráficos que excedam o limite dos padrões aceitáveis de ética, bom senso e razoabilidade;

10.2.2 O uso inadequado do acesso a *internet* compreende:

10.2.2.1 O acesso a websites de conteúdo racista, ofensivo, ilegal ou impróprio;

10.2.2.2 O acesso a serviços do tipo chat, bate-papo e troca de mensagens em tempo real que não tenham sido formalmente autorizados e que apresentem vulnerabilidades ou possam comprometer a integridade da rede de computadores do TRT24;

10.2.2.3 O acesso a serviços de downloads de músicas e filmes de qualquer formato, fotos e material pornográfico, programas não homologados ou licenciados.

10.3 O uso da *internet* poderá ser monitorado pela Secretaria de Tecnologia da Informação, de acordo com a conveniência da administração do Tribunal, mediante o emprego de ferramentas específicas, com a possibilidade de geração de relatórios e estatísticas tais como *sites* visitados, *softwares* e serviços utilizados, frequência e tempo de uso;

10.4 As informações e o conteúdo do monitoramento só serão disponibilizados por determinação do Comitê de Segurança da Informação.

## 11 DA TROCA DE DOCUMENTOS

11.1 Para a troca de documentos, oficiais e de mero expediente, deverá ser priorizada a utilização do

- sistema de Malote Digital;
- 11.2 Os documentos oficiais e de mero expediente encaminhados através do sistema de Malote Digital deverão ser assinados digitalmente;
  - 11.3 As peças processuais encaminhadas através do sistema de Malote Digital ou de outro qualquer deverão ser preferencialmente assinadas digitalmente, cabendo a seu proprietário a guarda do arquivo eletrônico para fins de eventual comprovação de autenticidade;
  - 11.4 Documentos eletrônicos assinados digitalmente serão considerados originais e a impressão dos mesmos será considerada cópia;
  - 11.5 A materialização e juntada de cópias de qualquer tipo de documento eletrônico assinado digitalmente deverá ser acompanhada de certidão, cabendo ao certificador a guarda do arquivo eletrônico para fins de eventual comprovação de autenticidade.

## **12 DO USO DE CERTIFICAÇÃO DIGITAL**

- 12.1 A utilização de certificados digitais tipo A3 (smartcard ou token) para assinatura digital de documentos observará os seguintes critérios:
  - 12.1.1 O certificado de assinatura digital e o hardware portátil (smart card ou token) serão eventualmente fornecidos pelo TRT da 24<sup>a</sup> Região ao magistrado ou servidor de acordo com a conveniência e necessidade para as atividades exercidas;
  - 12.1.2 O uso de certificados de assinatura digital não fornecidos pelo TRT da 24<sup>a</sup> Região fica restrito a certificados digitais emitidos por autoridades certificadoras da cadeia AC-JUS e/ou ICP-Brasil;
  - 12.1.3 A criação e renovação das senhas PIN, PUK, revogação ou quaisquer outras são de inteira responsabilidade do proprietário do certificado;
  - 12.1.4 A renovação da validade do certificado é de inteira responsabilidade do proprietário;
  - 12.1.5 O TRT da 24<sup>a</sup> Região não fornecerá certificados ou hardwares portáteis para reposição em caso de perda, dano ou esquecimento das senhas PINK e PUK.
- 12.2 As aplicações desenvolvidas pela Secretaria de Tecnologia da Informação fornecerão mecanismo de assinatura digital através de certificado tipo A1



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

(usuário e senha);

12.2.1 A renovação da validade do certificado é  
de inteira responsabilidade do  
proprietário;

# Plano de Controle de Acessos

## 1 DO OBJETIVO

- 1.1 Proteger as instalações e equipamentos de TI;
- 1.2 Prevenir perda, dano ou comprometimento dos ativos de TI;
- 1.3 Reduzir as ameaças à continuidade das atividades do negócio.

## 2 DA JUSTIFICATIVA

- 2.1 Os dados corporativos armazenados nas instalações e equipamentos do TRT24 são os ativos mais valiosos da instituição e, eventualmente, podem tornar-se os maiores alvos de ataques e ameaças;
- 2.2 A proteção física dos dados tem papel fundamental na continuidade do negócio;
- 2.3 A dependência da instituição em relação aos recursos de TI exige a prática de controles rígidos sob a exposição dos dados e dos ambientes de armazenamento.

## 3 DOS CONCEITOS

- 3.1 Consideram-se, para os efeitos deste ato, os seguintes conceitos:
  - 3.1.1 **Ativos de TI:** 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 membros e servidores do Tribunal;
  - 3.1.2 **Usuário de TI:** qualquer pessoa física provida da "conta de usuário de TI";
  - 3.1.3 **Acesso físico:** qualquer forma de contato físico entre o usuário de TI e qualquer tipo de equipamento de armazenamento de dados;
  - 3.1.4 **Acesso lógico:** qualquer tipo de contato entre o usuário de TI e as informações armazenadas, seja através do uso de sistemas, aplicativos, ferramentas, SO ou qualquer outro ativo de TI, disponibilizado pelo TRT24 ou não;
  - 3.1.5 **Sala Técnica:** ambiente crítico destinado a abrigar os equipamentos de armazenamento e processamento de dados;

## 4 DA APLICAÇÃO

- 4.1 O Plano de Controle de Acessos é parte integrante



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

da Política de Segurança da Informação e aplica-se a todos os usuários de TI autorizados a fazerem uso dos ativos de TI, no âmbito das redes de computadores do TRT da 24ª Região, administradas pela Secretaria de Tecnologia da Informação;

4.1.1 Aplica-se ainda esta política, no que couber, ao relacionamento do TRT da 24ª Região com outros agentes externos, prestadores de serviços, contratados ou não, que por qualquer razão necessitem acessar os ambientes críticos do TRT da 24ª Região.

## **5 DO CONTROLE DE ACESSO**

5.1 A responsabilidade pelo controle de acesso às salas técnicas do TRT da 24ª Região é do Chefe da Divisão de Suporte e Segurança;

5.2 O acesso às salas técnicas é restrito aos servidores da Secretaria de Tecnologia da Informação autorizados pelo Chefe da Divisão de Suporte e Segurança;

5.2.1 Qualquer acesso de servidor não autorizado somente será permitido mediante identificação e justificativa do propósito e das atividades que serão realizadas no local;

5.2.2 Serviços de terceiros deverão ser agendados previamente, com identificação da pessoa que executará o serviço e o detalhamento da atividade a ser realizada no local;

5.2.3 Qualquer acesso realizado conforme previsto nos itens 5.2.1 e 5.2.2 será acompanhado por servidor designado pelo Chefe da Divisão de Suporte e Segurança.

5.3 O controle de acesso no prédio sede seguirá as seguintes normas:

5.3.1 O acesso a sala técnica será realizado através de cartão eletrônico;

5.3.2 A guarda dos cartões de acesso é de responsabilidade dos servidores proprietários, sendo expressamente proibido o empréstimo para qualquer outra pessoa;

5.3.3 Todas as portas externas a sala técnica deverão permanecer trancadas, mesmo durante horário de expediente;

5.3.4 O acesso ao interior dos cofres modulares será realizado através de identificação

- biométrica e permitido somente aos servidores autorizados pelo Chefe da Divisão de Suporte e Segurança;
- 5.4 O controle de acesso no prédio do Foro Trabalhista seguirá as seguintes normas:
- 5.4.1 O acesso a sala técnica será realizado através fechadura mecânicas do tipo "chave tetra";
- 5.4.2 A guarda das chaves é de responsabilidade dos servidores designados pelo Chefe da Divisão de Suporte e Segurança, sendo expressamente proibido o empréstimo para qualquer outro pessoa;
- 5.4.3 Todas as portas externas a sala técnica deverão permanecer trancadas, mesmo durante horário de expediente;
- 5.4.4 O acesso ao interior dos cofres modulares será realizado através de fechaduras mecânicas e permitido somente aos servidores autorizados pelo Chefe da Divisão de Suporte e Segurança;
- 5.5 Qualquer evento de quebra de segurança associado ao acesso ou a tentativa de acesso não autorizado aos ambientes de TI deve ser imediatamente reportado à área de segurança do TRT24.

## **6 DA INFRAESTRUTURA DO AMBIENTE FÍSICO**

- 6.1 É responsabilidade do Chefe da Divisão de Suporte e Segurança zelar pelo bom funcionamento dos mecanismos de segurança do ambiente das salas técnicas, tais como:
- 6.1.1 Portas
- 6.1.2 Fechaduras e chaves
- 6.1.3 Dispositivos biométricos
- 6.1.4 Câmeras e sensores
- 6.2 Qualquer falha nos mecanismos deve ser imediatamente reportada ao setor responsável para as devidas providências.



## Plano de Controle de Software

### 1 DO OBJETIVO

- 1.1 Prevenir o comprometimento da segurança da informação devido à instalação de softwares maliciosos;
- 1.2 Disciplinar as versões dos softwares utilizados nos computadores e notebooks fornecidos pelo TRT24 através do monitoramento de aplicativos e hardware;
- 1.3 Reduzir as ameaças à continuidade das atividades do negócio.

### 2 DA JUSTIFICATIVA

- 2.1 A dependência da instituição em relação aos softwares instalados nos equipamentos exige a prática de controles rígidos sob instalação e configuração de programas e aplicativos.

### 3 DOS CONCEITOS

- 3.1 Consideram-se, para os efeitos deste ato, os seguintes conceitos:

- 3.1.1 **Ativos de TI:** 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 membros e servidores do Tribunal;

- 3.1.2 **Usuário de TI:** qualquer pessoa física provida da "conta de usuário de TI";

- 3.1.3 **ITIL (Information Technology Infrastructure Library):** Conjunto de boas práticas <[http://pt.wikipedia.org/wiki/Boas\\_práticas](http://pt.wikipedia.org/wiki/Boas_práticas)> a serem aplicadas na infraestrutura, operação e manutenção de serviços de TI para promover a gestão com foco no cliente e na qualidade dos serviços de tecnologia da informação <[http://pt.wikipedia.org/wiki/Tecnologia\\_da\\_informação](http://pt.wikipedia.org/wiki/Tecnologia_da_informação)> (TI).;

- 3.1.4 **COBIT (Control Objectives for Information and related Technology):** guia de boas práticas <[http://pt.wikipedia.org/wiki/Boas\\_práticas](http://pt.wikipedia.org/wiki/Boas_práticas)> dirigido para a gestão de tecnologia de informação <[http://pt.wikipedia.org/wiki/Tecnologia\\_de\\_informação](http://pt.wikipedia.org/wiki/Tecnologia_de_informação)> (TI);

- 3.1.5 **CACIC (Configurador Automático e Coletor de Informações Computacionais):** programa de computador <[http://pt.wikipedia.org/wiki/Programa\\_de\\_computador](http://pt.wikipedia.org/wiki/Programa_de_computador)> do

Governo Federal do Brasil  
<[http://pt.wikipedia.org/wiki/Governo\\_Federal\\_do\\_Brasil](http://pt.wikipedia.org/wiki/Governo_Federal_do_Brasil)>  
destinado a fornecer diagnósticos de parques  
computacionais e informações como o número de  
equipamentos, tipos de software utilizados e licenciados,  
configurações de hardware e outras.

#### **4 DA APLICAÇÃO**

4.1 O Plano de Controle de Software é parte integrante da Política de Segurança da Informação e aplica-se a todos os usuários de TI autorizados a fazerem uso dos ativos de TI, no âmbito das redes de computadores do TRT da 24<sup>a</sup> Região, administradas pela Secretaria de Tecnologia da Informação;

4.1.1 Aplica-se ainda esta política, no que couber, ao relacionamento do TRT da 24<sup>a</sup> Região com outros agentes externos, prestadores de serviços, contratados ou não, que por qualquer razão necessitem acessar os ambientes críticos do TRT da 24<sup>a</sup> Região.

#### **5 DO USO DE PROGRAMAS E APLICATIVOS**

5.1 A instalação e a utilização de programas de computador no TRT24 estão sujeitas aos seguintes requisitos:

5.1.1 Existência de licenças de uso em quantidade suficiente;

5.1.2 Conformidade com a atividade da instituição e com a área de atuação das unidades administrativas;

5.1.3 Compatibilidade com os demais programas utilizados;

5.1.4 Adequação aos recursos computacionais disponíveis; e

5.1.5 Obediência a planejamentos, cronogramas e prioridades existentes.

5.2 A instalação de programa ou aplicativos em equipamentos de informática do TRT24 deve ser realizada exclusivamente pelos técnicos da Secretaria de Tecnologia da Informação;

5.3 É proibida a instalação de programa ou aplicativo de terceiros, sem licença de uso regularmente contratada;

5.4 A cópia de programa ou aplicativo de computador adquirido/contratado pelo TRT24, para uso particular, somente pode ser cedida com a autorização expressa do Comitê de Segurança da Informação, nos termos da licença de uso;



PODER JUDICIÁRIO  
JUSTIÇA DO TRABALHO  
TRIBUNAL REGIONAL DO TRABALHO DA 24ª REGIÃO

- 5.5 É de responsabilidade do usuário a instalação ou a execução não autorizada de programa ou aplicativo recebido como anexo de mensagem de correio eletrônico ou transferido via internet, considerada a possibilidade de dano às instalações de informática do TRT24;
- 5.6 É vedada a utilização de programas ou aplicativo de computador que descaracterizem os propósitos da instituição ou comprometam, de alguma forma, o ambiente instalado, tais como jogos eletrônicos, bate-papo e outros;
- 5.7 As solicitações para instalação de programas ou aplicativos devem ser encaminhadas formalmente, acompanhadas de justificativa à Secretaria de Tecnologia da Informação, que, observados os pressupostos relacionados no item 5.1, efetuará a instalação ou promoverá a contratação, quando não existirem licenças disponíveis;
- 5.8 A listagem com os softwares homologados para a utilização no TRT24 será publicada pela Secretaria de Tecnologia da Informação no site STI.TRT24.JU.BR.
- 5.9 Os softwares provenientes de instalações irregulares serão removidos sem prévio aviso ao usuário.

## **6 DO GERENCIAMENTO DE CONFIGURAÇÃO**

- 6.1 Todos os softwares instalados nos computadores e notebooks do TRT24 estão sujeitos ao Gerenciamento de Configuração definido pelo ctConf-TRT24 (Comitê Técnico Temático de Configuração e Ativos de Serviço) e aplicado pela Divisão de Governança de TI, em alinhamento com a Biblioteca de Infraestrutura de Tecnologia da Informação - ITIL V.3 e processo "DS9 - Gerenciar a Configuração" da Biblioteca Cobit 4.1;
- 6.2 Somente softwares homologados pelo ctConf-TRT24 poderão ser instalados em estações clientes do TRT24, ficando terminantemente proibido a instalação e configuração de softwares não homologados ou versões diversas daquelas homologadas;
- 6.3 Alterações de versões devem ser homologadas pelo ctConf-TRT24;
- 6.4 Cabe a Divisão de Governança de TI, através do agente de inventário - CACIC - e com auxílio da Central de Serviços - HELP DESK - monitorar as configurações e versões instaladas e promover a

padronização do parque computacional do TRT24;

6.5 As solicitações de alteração (Requisição de Mudança), deverão ser feitas ao ctConf-TRT24, via formulário disponibilizado no site da STI - <http://sti.trt24.jus.br/docs/mudanca.odt>, e encaminhadas via sistema de atendimento (SIATE), com chamado aberto para:

- Área Responsável: Help Desk - STI
- Problema: Solicitações STI - Internas
- Descrição do problema: Software a ser mudado/incluído.
- Demais dados do requerente.
- Anexar arquivo: requisição de mudança devidamente preenchida e fundamentada.

6.6 A lista de itens de configuração homologados, bem como as eventuais alterações, será informada aos usuários via mensagem eletrônica e disponibilizada no site STI.TRT24.JUS.BR.