

## Política de Utilização de Recursos de TI

PÚBLICO ALVO: AGENTES PÚBLICOS	EMIÇÃO:	CODIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

## Política de Utilização de Recursos de TI

### 1. Apresentação

Esta política norteará a implementação de medidas para regular a utilização dos recursos de Tecnologia da Informação (TI) utilizados pelos usuários do Tribunal Regional Federal da 5ª Região (TRF5) de forma a minimizarem os riscos à segurança das informações da corte.

Suas orientações devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos, para que o maior patrimônio da instituição, a informação, tenha o grau de confidencialidade, integridade, disponibilidade e autenticidade exigidos.

As suas definições e orientações estão de acordo com as exigidas pelo item 9.3.2 – Política de Utilização de Recursos de TI – do Anexo I da Resolução N° 6, de 7 de abril de 2008 do Conselho da Justiça Federal que definiu a Política de Segurança da Informação (**PSI**) no âmbito do Conselho e da Justiça Federal de primeiro e Segundo graus.

### 2. Escopo

O escopo desta Política de Segurança da Informação abrange o Tribunal Regional Federal da 5ª Região.

### 3. Público Alvo

Esta Política de Controle de Acesso Lógico se aplica aos agentes públicos do Tribunal Regional Federal da 5ª Região e ainda a estagiários, aprendizes, clientes, parceiros e empresas e/ou pessoas contratadas com a administração.

### 4. Termos e Definições

**Arquivo** – agrupamento de registros que, geralmente, seguem uma regra estrutural, e que contém informações (dados)

**Confidencialidade** – sigilo. Preservar a confidencialidade de uma informação significa garantir que apenas as pessoas que devem ter conhecimento a seu respeito poderão acessá-las

**Criptografia** – arte e ciência de esconder o significado de uma informação de receptores não desejados

## Política de Utilização de Recursos de TI

PÚBLICO ALVO: AGENTES PÚBLICOS	EMISSÃO:	CODIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

**Disponibilidade** – uma informação disponível é aquela que pode ser acessada por aqueles que dela necessitam, no momento em que precisam

**Integridade** – a preservação da integridade envolve proteger as informações contra alterações, intencionais ou acidentais, em seu estado original.

**Smartphone** – Telefone móvel, dotado de grande capacidade computacional, cumprindo funções de telefone celular, agenda e sistema informático de escritório elementar, com possibilidade de interconexão com um computador pessoal e redes de computação.

**Privilégio Mínimo** – conceito que define que uma pessoa só precisa acessar os sistemas e recursos mínimos necessários para realizar suas atividades.

**Programa** – uma coleção de instruções que descrevem uma tarefa a ser realizada por um computador.

**Recursos de TI** – Recursos de Tecnologia da Informação. Softwares e hardwares que geram, processam, recebem ou transmitem informações como desktops, notebooks, sistemas operacionais, processadores de texto, *smartphone*, *pendrive*, etc.

### 5. Dos Recursos de TI

5.1 Todos os recursos de TI disponibilizados pelo TRF5 são de propriedade do mesmo.

5.2 Todas as informações geradas, recebidas, processadas ou armazenadas utilizando os recursos de TI do TRF5 são passíveis de auditoria.

5.3 A utilização dos recursos de TI devem ser realizadas respeitando-se os princípios da legalidade, moralidade, economicidade e eficiência.

5.4 Os agentes públicos, estagiários, aprendizes, clientes, parceiros e contratados, doravante denominados de forma geral como usuários, devem ter acesso unicamente àqueles recursos de tecnologia da informação que forem indispensáveis à realização de suas atividades, obedecendo ao princípio do privilégio mínimo.

## **Política de Utilização de Recursos de TI**

PÚBLICO ALVO: AGENTES PÚBLICOS	EMISSÃO:	CODIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

5.5 Os recursos de TI disponibilizados nas diversas áreas do Tribunal destinam-se, exclusivamente, ao atendimento das necessidades do serviço público, sendo vedada a utilização dos mesmos para fins particulares.

5.6 Os usuários são responsáveis pelos recursos de TI por eles utilizados, devendo contribuir para seu funcionamento e segurança.

5.7 As paralisações programadas de quaisquer serviços disponibilizados pelo TRF5 deve ser comunicada com antecedência aos usuários, indicando os períodos de indisponibilidade dos serviços.

5.8 É vedada a utilização de recursos de TI particulares, no ambiente de TI do TRF5, sem prévia solicitação formal justificando a necessidade de utilização do recurso e autorização da Diretoria Geral mediante parecer técnico emitido pela Subsecretaria de Informática (SI).

5.9 Os parâmetros de configuração de hardwares e softwares dos recursos de TI serão definidos pela SI, tendo em vista os requisitos de segurança, estabilidade, confiabilidade e padronização do ambiente computacional do Tribunal.

5.10 A SI deverá manter lista atualizada de hardwares e softwares homologados que poderão ser utilizados no ambiente de TI do TRF5 obedecendo ao princípio de privilégio mínimo.

5.11 É vedada a utilização de hardwares e softwares que não estejam previamente licenciados e homologados.

5.12 A SI poderá proceder à desinstalação sumária dos softwares e hardwares que estejam em desacordo com os itens 5.10 e 5.11 deste documento.

5.13 A SI deverá prover mecanismos que proíbam o acesso à rede corporativa e recursos de TI do TRF5 de dispositivos que não estejam em conformidade com os padrões de segurança definidos.

5.14 O deslocamento de qualquer recurso de TI, dentro de uma unidade ou entre unidades diferentes, devem ser comunicados a SI, a fim de que seja registrada a ocorrência pela SI.

## **6. Das Estações de Trabalho**

## Política de Utilização de Recursos de TI

PÚBLICO ALVO: AGENTES PÚBLICOS	EMISSÃO:	CODIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

6.1 As estações de trabalho fornecidas possuirão configurações de hardware e software padronizadas, de acordo com a necessidade de utilização dos usuários.

6.2 Nas estações de trabalho somente devem ser instalados softwares homologados e licenciados pela SI e necessários para execução das atividades dos usuários.

6.3 A SI deverá realizar o lacre das estações de trabalho a fim de evitar modificações por usuários não autorizados.

6.4 É vedado ao usuário abrir o gabinete das estações de trabalho e modificar a configuração do hardware e/ou software.

6.5 O usuário deve informar à SI quando identificar violação da integridade física do equipamento por ele utilizado.

## 7. Computação Móvel

7.1 A utilização de dispositivos móveis como, mas não se limitando a, notebook, smartphone e pendrive, devem ser utilizados obedecendo o princípio do privilégio mínimo.

7.2 Aplicam-se, quando pertinentes, aos dispositivos móveis as mesmas regras de utilização das estações de trabalho.

7.3 A SI deverá prover sistemas que efetuem o bloqueio de utilização de dispositivos móveis, sem autorização, nos recursos de TI, a fim de evitar a fuga de informações confidenciais.

7.4 Os equipamentos portáteis, particulares ou do TRF5, quando não estiverem sendo utilizados, devem ser guardados em local seguro.

7.5 O usuário, ao solicitar o empréstimo de equipamentos portáteis do TRF5, deve fazê-lo ao gestor da área, tornando formal a solicitação por meio de documento oficial.

7.6 Na devolução do equipamento portátil, o usuário que o utilizou deve retirar todos os arquivos gravados e manipulados, durante sua utilização, além de todos os objetos pessoais, como disquetes, cd's, dentre outros.

## Política de Utilização de Recursos de TI

PÚBLICO ALVO: AGENTES PÚBLICOS	EMISSÃO:	CODIGO PCAS
DATA DA REVISÃO: 00/00/0000	REVISÃO N°00	VERSÃO N° 01

7.7 Os arquivos armazenados nos equipamentos portáteis devem ser, sempre que possível, protegidos por senhas de acesso e/ou criptografia.

### 8. Armazenamento de Dados

8.1 Todas as informações corporativas devem ser armazenadas nos servidores de dados corporativos do TRF5.

8.2 A SI deverá prover os mecanismos necessários para a proteção das informações armazenadas nos servidores corporativos do TRF5 visando a garantir a integridade, disponibilidade e confidencialidade das informações e obedecendo sempre ao princípio do privilégio mínimo.

8.3 A SI deverá efetuar backup periódico dos sistemas e das informações corporativas armazenadas nos servidores do TRF5.

8.4 A SI não é responsável pela salvaguarda das informações armazenadas nas estações de trabalho e dispositivos móveis.

8.5 É vedado o compartilhamento de pastas nas estações de trabalho dos usuários, salvo solicitação justificada, a qual a SI procederá com a realização do compartilhamento e efetuará as configurações de permissão visando o princípio do privilégio mínimo.

8.6 A SI deverá prover mecanismos de descarte seguro de informação armazenada em meio digital, de forma a preservar a confidencialidade dos dados do TRF5.

### 9. Periodicidade de Revisão

9.1 Esta política deverá ser revista, anualmente, pelo Comitê Local de Segurança da Informação, com vistas a adequar a mesma às necessidades atuais.

9.2 O acontecimento de fatos supervenientes, relevantes para a segurança da informação, autorizam o Comitê Local de Segurança da Informação a rever esta política a qualquer tempo.