

**INSTRUÇÃO NORMATIVA Nº 298, DE 09 DE JULHO DE 2024**

*Dispõe sobre o uso aceitável de recursos de tecnologia da informação do Supremo Tribunal Federal.*

**O DIRETOR-GERAL DA SECRETARIA DO SUPREMO TRIBUNAL FEDERAL**, no uso das atribuições que lhe confere o art. 41, inciso X, alínea b, do Regulamento da Secretaria de 2024, e tendo em vista o que consta do Processo Administrativo eletrônico 003015/2023;

**CONSIDERANDO** a Norma Complementar 7 - DSIC/GSI/PR, de 15 de julho de 2014, que estabelece diretrizes para implementação de controles de acesso relativos à Segurança da Informação e das Comunicações nos órgãos e entidades da Administração Pública Federal;

**CONSIDERANDO** a Resolução 749/2021, que estabelece o Modelo de Gestão Operacional do STF e regulamenta as modalidades de trabalho;

**CONSIDERANDO** a Resolução 773/2022, que institui a Política de Segurança da Informação do STF (PSI/STF);

**CONSIDERANDO** o direito fundamental à autodeterminação informativa (art. 5º, LXXIX, da Constituição de 1988) e a entrada em vigor da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);

**CONSIDERANDO** que a LGPD estabelece as condições sob as quais os dados pessoais podem ser tratados, define um conjunto de direitos para os titulares dos dados e impõe obrigações específicas aos controladores dos dados;

**CONSIDERANDO** a Resolução 759/2021, que institui a Política de Privacidade e de Proteção de Dados;

**R E S O L V E:**

Art. 1º Este normativo estabelece as diretrizes para o uso aceitável dos recursos de tecnologia da informação (TI) do Supremo Tribunal Federal (STF), visando garantir a segurança das informações e dos dados pessoais dos titulares, bem como preservar a reputação e os recursos da instituição.

**CAPÍTULO I****DOS CONCEITOS E DEFINIÇÕES**

Art. 2º Para os efeitos desta instrução normativa, será aplicado o glossário de termos de segurança da informação, definido e publicado no Repositório Digital do STF (<https://bibliotecadigital.stf.jus.br/xmlui/>).

**CAPÍTULO II****DOS PRINCÍPIOS**

Art. 3º O uso aceitável dos recursos de TI se alinha às estratégias do STF, de sua Política de Segurança da Informação e de sua Política de Privacidade e de Proteção de Dados, tendo como premissas:

I – responsabilidade: a obrigação dos usuários dos recursos de TI em utilizá-los de forma adequada e responsável;

II – capacitação: a necessidade de treinamento e conscientização dos usuários dos recursos de TI, para que possam compreender as normas e diretrizes estabelecidas e aplicá-las adequadamente em seu trabalho.

**CAPÍTULO III****DO USO NÃO ACEITÁVEL DE RECURSOS DE TECNOLOGIA DA INFORMAÇÃO**

Art. 4º Considera-se o uso não aceitável dos equipamentos de TI:

I – o uso para atividades ilegais, impróprias, ofensivas, discriminatórias, assédio ou qualquer outra forma de violação de direitos individuais ou coletivos;

II – o uso de forma a compartilhar informações sigilosas ou de carácter restrito com pessoas ou organizações de forma não autorizada;

III – o uso para fins pessoais, incluindo entre estes o comércio, venda de produtos ou engajamento em atividades comerciais de qualquer natureza;

IV – o uso de forma a difundir por meio de recursos de TI trotes, boatos, pornografia, propaganda comercial, religiosa ou político-partidária;

V – o armazenamento nas estações de trabalho de arquivos que possam violar direitos autorais, como fotos, filmes e músicas;

*VI – o compartilhamento de senhas ou a utilização de senhas de outras pessoas para acessar os recursos de TI;*

*VII – o uso dos recursos de TI para acessar, copiar, modificar ou excluir informações ou dados sem a devida autorização ou consentimento;*

*VIII – o uso dos recursos de TI para a propagação de vírus, worms, cavalos de troia, spyware ou qualquer outra forma de software malicioso;*

*IX – o uso dos recursos de TI para realizar tentativas de ataques ou intrusão a sistemas informatizados do STF ou de terceiros;*

*X – conectar, sem a autorização da STI, equipamentos à rede de dados do STF;*

*XI – alterar a configuração do software e do hardware fornecido pela STI;*

*XII – manter o computador desbloqueado ou sob o cuidado de terceiros sem o seu monitoramento direto.*

## **CAPÍTULO IV**

### **DO USO DE EQUIPAMENTOS EM REGIME DE TRABALHO HÍBRIDO OU REMOTO**

*Art. 5º Os servidores que realizarem atividades de trabalho em regime remoto ou híbrido deverão seguir as mesmas normas e diretrizes estabelecidas neste normativo em relação ao uso dos recursos de TI, além de:*

*I – garantir que o local de trabalho remoto esteja devidamente equipado e com as ferramentas tecnológicas necessárias para o desempenho das atividades;*

*II – manter a confidencialidade e a privacidade dos dados e informações do STF;*

*III – garantir a segurança da conexão com a rede do STF, utilizando sistemas operacionais licenciados e atualizados, com antivírus instalado, e evitando acessar sites ou aplicativos que possam comprometer a segurança das informações e dos sistemas;*

*IV – providenciar para que os arquivos de interesse do STF sejam armazenados e manipulados no sistemas desenvolvidos internamente pelo Tribunal ou nos serviços de armazenamento centralizado (rede interna ou nuvem);*

*V – providenciar equipamentos e programas que atendam às orientações da STI, especialmente nos requisitos de segurança.*

*Art. 6º No momento da conexão remota, ferramentas de segurança do STF poderão avaliar as configurações do equipamento do usuário com relação aos requisitos de segurança definidos, impedindo a conexão em caso de não conformidade.*

*Parágrafo único. O disposto neste artigo deverá constar expressamente em termo de compromisso a ser assinado por servidor em trabalho remoto ou híbrido.*

## **CAPÍTULO V**

### **DO USO DA REDE SEM FIO E DISPOSITIVOS MÓVEIS**

*Art. 7º O uso da rede sem fio é destinado a complementar a rede cabeada, possibilitando o acesso diferenciado para os usuários internos e externos aos recursos de TI do STF.*

*Art. 8º A STI segmentará a rede sem fio de forma a separar o tráfego originado de dispositivos móveis fornecidos pelo próprio Tribunal, o uso da rede por dispositivos móveis de colaboradores e o uso da rede por dispositivos móveis por visitantes.*

*Parágrafo único. A STI aplicará regras de segurança e monitoramento de acordo com as características de cada rede sem fio.*

*Art. 9º O uso da rede sem fio por visitantes será permitida mediante cadastro prévio operacionalizado pela STI, desde que o usuário:*

*I – forneça seus dados de identificação e concorde com as normas e diretrizes estabelecidas neste normativo antes de receber a autorização para acessar a rede sem fio;*

*II – utilize a rede sem fio apenas para atividades relacionadas às suas visitas, sendo vedado o acesso a sites ou serviços que não sejam relacionados ao trabalho ou aos interesses do STF.*

*Parágrafo único. A STI monitorará o uso da rede sem fio pelos visitantes e manterá o registro dos acessos realizados pelo período definido no processo de gestão e monitoramento dos registros de atividades (logs).*

## **CAPÍTULO VI**

### **DO USO ACEITÁVEL DE E-MAIL CORPORATIVO**

*Art. 10. O uso do e-mail corporativo é considerado um recurso crítico de TI, e seu emprego deve ser pautado por práticas responsáveis e alinhadas às políticas de segurança estabelecidas pelo STF.*

*Art. 11. O e-mail corporativo é sujeito a monitoramento e deve ser utilizado exclusivamente para fins profissionais, relacionados às atividades institucionais e no cumprimento de suas atribuições.*

*Art. 12. Os anexos de e-mails devem ser utilizados de maneira criteriosa, evitando o envio de arquivos que possam conter vírus, malware ou que violem direitos autorais.*

## **CAPÍTULO VII**

### **DO USO DE RECURSOS DE TI PARA TRATAMENTO DE INFORMAÇÕES SIGILOSAS**

*Art. 13. As portas USB e demais conexões em estações de trabalho que tratam informações sigilosas poderão ser desabilitadas por pedido do titular da respectiva unidade, a fim de evitar a possibilidade de vazamento de informações ou o uso indevido de dispositivos externos.*

## **CAPÍTULO VIII**

### **DO MONITORAMENTO E FISCALIZAÇÃO**

*Art. 14. O STF monitorará, por meio de registros de logs, o uso dos recursos de TI pelos servidores e visitantes, estes últimos no uso da rede sem fio, a fim de garantir o cumprimento das normas e diretrizes estabelecidas neste normativo.*

*§ 1º O monitoramento e fiscalização dos recursos de TI pode incluir a gravação de dados e a interceptação de comunicações, em conformidade com a legislação aplicável e realizado por ferramentas automatizadas.*

*§ 2º A gestão dos arquivos de log será versada por normativo específico para esse fim.*

## **CAPÍTULO IX**

### **DA CONSCIENTIZAÇÃO DO USO ACEITÁVEL DOS RECURSOS DE TECNOLOGIA DA INFORMAÇÃO**

*Art. 15. O STF deve promover programas de conscientização e treinamento sobre o uso aceitável dos recursos de TI, visando garantir que os servidores compreendam e cumpram as normas e diretrizes estabelecidas no presente normativo.*

*Parágrafo único. A STI deverá implementar e conduzir os programas de conscientização e treinamento.*

*Art. 16. De acordo com o artigo 6º da Resolução 773/2022 (PSI/STF), a nível operacional, poderão ser elaborados procedimentos de segurança da informação que contemplem regras operacionais e roteiros técnicos para o uso adequado de recursos específicos, como serviços de e-mail e armazenamento local e na nuvem.*

*Art. 17. Fica revogada a Instrução Normativa 81, de 26 de março de 2009.*

*Art. 18. Esta instrução normativa entra em vigor na data de sua publicação.*

**EDUARDO S. TOLEDO**

Publicado no DJE/STF em 10/7/2024.

**Este texto não substitui a publicação oficial.**