



**PREFEITURA MUNICIPAL DE SÃO MATEUS
ESTADO DO ESPÍRITO SANTO
GABINETE DO PREFEITO**

DECRETO Nº. 18.229/2025

APROVA VERSÃO 01 DA INSTRUÇÃO NORMATIVA
STI Nº 004/2025 – DISPÕE SOBRE O USO DE
ACESSO REMOTO VIA VPN À REDE INTERNA DA
PREFEITURA MUNICIPAL POR MEIO DE
EQUIPAMENTOS PESSOAIS (BYOD) E DÁ OUTRAS
PROVIDÊNCIAS

Considerando o Processo Administrativo nº. 25909/2025 de 16/10/2025;

O Prefeito Municipal de São Mateus, Estado do Espírito Santo, no uso de suas atribuições legais, em vista a Legislação em vigor, especialmente o Artigo 107, Item VI, da Lei Municipal nº. 001/90, de 05 (cinco) de Abril (04) de 1990 – Lei Orgânica do Município de São Mateus-ES:

DECRETA:

Art. 1º Fica aprovada a Versão 01 da Instrução Normativa STI nº. 004/2025, que dispõe sobre o uso de acesso remoto via VPN à rede interna da prefeitura municipal por meio de equipamentos pessoais (byod) e dá outras providências, conforme anexo I do presente decreto.

Art. 2º Este Decreto entra em vigor na data de sua publicação.

Gabinete do Prefeito Municipal de São Mateus, Estado do Espírito Santo, aos 22 (vinte e dois) dias do mês de outubro (10) do ano de dois mil e vinte cinco (2025).

Marcus Azevedo

Batista:07626847717

Assinado de forma digital por

Marcus Azevedo

Batista:07626847717

Dados: 2025.10.22 15:46:51 -03'00'

MARCUS AZEVEDO BATISTA
Prefeito Municipal

ANEXO I

INSTRUÇÃO NORMATIVA STI Nº 004/2025 – DISPÕE SOBRE O USO DE ACESSO REMOTO VIA VPN À REDE INTERNA DA PREFEITURA MUNICIPAL POR MEIO DE EQUIPAMENTOS PESSOAIS (BYOD) E DÁ OUTRAS PROVIDÊNCIAS.

Versão: 01

Aprovação em: 22/10/2025

Ato de aprovação: Decreto nº 18.229/2025

Unidade Responsável: Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho.

Unidade Executora: Todas as unidades da estrutura organizacional da Administração Direta, quando no exercício de atividades relacionadas a este instrumento normativo.

I – FINALIDADE

Esta Instrução Normativa regulamenta, em caráter excepcional e controlado, o uso de computadores pessoais para acesso remoto à rede da Prefeitura Municipal por meio de VPN (Virtual Private Network), visando garantir a continuidade administrativa, a segurança da informação e a conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD).

II – ABRANGÊNCIA

Esta Instrução Normativa aplica-se a todos os servidores públicos, estagiários e colaboradores da Prefeitura Municipal que, em caráter excepcional e devidamente autorizado, necessitem utilizar computadores pessoais para acesso remoto à rede institucional por meio de VPN, bem como às unidades administrativas responsáveis pela autorização, controle e fiscalização desse acesso.

III – CONCEITOS

Para os fins desta Instrução Normativa considera-se:

3.1. VPN (Virtual Private Network): tecnologia que permite a conexão remota e segura à rede interna da Prefeitura, mediante autenticação e criptografia.

3.2. Dispositivo pessoal (BYOD – Bring Your Own Device): equipamento de informática de propriedade do usuário, utilizado em caráter excepcional para acesso remoto autorizado.

3.3. Usuário autorizado: servidor, empregado público, estagiário ou colaborador que recebeu permissão formal para acessar a rede via VPN, mediante assinatura de Termo de Responsabilidade.

3.4. Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho (TI): unidade responsável pela disponibilização, monitoramento e auditoria do serviço de VPN.

3.5. Encarregado de Proteção de Dados (DPO): pessoa designada para atuar como canal de comunicação entre o controlador, os titulares de dados pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

IV – BASE LEGAL E REGULAMENTAR

- a) Constituição Federal de 1988;

- b) Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- c) Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- d) Decreto Federal nº 10.046/2019;
- e) Normas da ABNT e ISO/IEC 27001 e 27002;
- f) Demais legislações e normativos internos aplicáveis à segurança da informação e ao uso de recursos tecnológicos na Prefeitura Municipal.

V – DAS RESPONSABILIDADES

Para a efetividade desta Instrução Normativa, ficam estabelecidas as seguintes responsabilidades:

5.1. Do Usuário Solicitante

- 5.1.1. Formular o pedido formal de acesso remoto via VPN, apresentando justificativa funcional;
- 5.1.2. Assinar o Termo Individual de Responsabilidade (ANEXO II), reconhecendo ciência das regras desta norma;
- 5.1.3. Utilizar o acesso VPN exclusivamente para fins funcionais relacionados às atividades laborais;
- 5.1.4. Manter o dispositivo pessoal atualizado, com antivírus ativo e senha segura, realizando troca quinzenal de senhas e sem utilizar a opção de senha salva;
- 5.1.5. Não compartilhar senhas, dispositivos, credenciais ou arquivos confidenciais com terceiros;
- 5.1.6. Informar imediatamente à chefia e à Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho qualquer incidente de segurança, perda ou comprometimento de credenciais;
- 5.1.7. Responder administrativa, civil e penalmente por uso indevido ou descumprimento desta norma, inclusive por meio de Processo Administrativo Disciplinar (PAD).

5.2. Da Chefia Imediata

- 5.2.1. Analisar a pertinência da solicitação e encaminhar ao Secretário da Pasta;
- 5.2.2. Acompanhar e fiscalizar o cumprimento das regras estabelecidas nesta Instrução Normativa;
- 5.2.3. Solicitar a revogação do acesso VPN ao Secretário Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho quando cessada a necessidade e em caso de desligamento do servidor.

5.3. Do Secretário da Pasta

- 5.3.1. Decidir sobre a necessidade do acesso VPN, aprovando ou indeferindo a solicitação do servidor;
- 5.3.2. Registrar formalmente a decisão no processo administrativo;
- 5.3.3. Solicitar a revogação do acesso VPN ao Secretário Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho quando cessada a necessidade e em caso de desligamento do servidor;
- 5.3.4. No caso de solicitação feita pelo próprio Secretário, a decisão caberá ao Prefeito ou autoridade designada, sujeita à análise técnica da Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho e avaliação do DPO.

5.4. Da Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho.

5.4.1. Analisar tecnicamente o pedido aprovado pelo Secretário da Pasta, verificando requisitos de segurança e viabilidade técnica;

5.4.2. Liberar o acesso VPN após aprovação administrativa e assinatura do Termo de Responsabilidade;

5.4.3. Manter registros detalhados de logs de acesso e monitoramentos periódicos;

5.4.4. Suspender imediatamente o acesso em caso de descumprimento, risco identificado ou solicitação administrativa;

5.4.5. Encerrar automaticamente acessos de servidores que deixarem o quadro funcional;

5.4.6. Realizar, no mínimo, verificação mensal dos acessos ativos, de modo a confirmar se os usuários permanecem no quadro funcional;

5.4.7. Manter registros das verificações realizadas, de forma a possibilitar auditoria posterior.

5.5. Do Encarregado de Proteção de Dados (DPO)

5.5.1. Emitir parecer sobre os riscos relacionados à proteção de dados pessoais no uso do acesso VPN;

5.5.2. Orientar usuários e administração quanto às boas práticas de proteção de dados;

5.5.3. Comunicar ao Controlador eventuais inconformidades identificadas;

5.5.4. Notificar a Autoridade Nacional de Proteção de Dados (ANPD) em caso de incidentes relevantes, conforme a LGPD.

VI – REQUISITOS TÉCNICOS MÍNIMOS

6.1. Dispositivo Pessoal (BYOD)

O equipamento pessoal utilizado para acesso remoto via VPN deverá atender aos seguintes critérios:

I - sistema operacional atualizado e com suporte oficial do fabricante;

II - antivírus ativo, atualizado e com verificação periódica de ameaças;

III - bloqueio automático de tela por senha, PIN ou biometria;

IV - proibição absoluta de compartilhamento de credenciais, tokens ou dispositivo com terceiros;

V - proibição de utilização de opção de senha salva ou automática em navegadores ou aplicativos;

VI - proibição de armazenamento local de dados sensíveis ou confidenciais sem criptografia aprovada pela Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho;

VII - cumprimento das políticas de segurança da informação estabelecidas pela Prefeitura.

6.2. – Auditoria e Conformidade

6.2.1. A Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho poderá realizar auditorias técnicas periódicas para verificar a conformidade dos dispositivos e acessos;

6.2.2. Eventuais não conformidades deverão ser comunicadas à chefia imediata e ao DPO;

6.2.3. O acesso poderá ser suspenso imediatamente em caso de risco identificado ou descumprimento dos requisitos técnicos.

VII – LOGS E MONITORAMENTO

7.1. Todo acesso VPN será registrado em logs (usuário, data/hora, duração, sistemas acessados e IP);

7.2. Os registros serão armazenados por no mínimo 12 meses;

7.3. Logs destinam-se exclusivamente à auditoria, segurança e investigação de incidentes;

7.4. O acesso aos logs é restrito à Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho e auditores autorizados, com possibilidade de solicitação pelo DPO;

7.5. Alterações ou exclusões de registros só ocorrerão mediante processo formal e justificado.

VIII – DISPOSIÇÕES FINAIS

8.1. O cumprimento desta IN não dispensa a observância das demais normas legais aplicáveis;

8.2. O acesso remoto via VPN será concedido apenas em caráter excepcional, temporário e condicionado ao estrito cumprimento desta norma;

8.3. O descumprimento acarretará revogação imediata do acesso, responsabilização administrativa, civil e penal;

8.4. O Controle Interno poderá solicitar auditorias de conformidade sempre que necessário;

8.5. Situações omissas ou excepcionais serão analisadas pela Administração Superior, ouvidas a Secretaria Municipal Ciência, Tecnologia, Inovação, Educação profissional e Trabalho e o DPO;

8.6. A IN deverá ser atualizada sempre que mudanças legais ou técnicas assim exigirem;

8.7. Esta Instrução Normativa entra em vigor na data de sua publicação.

São Mateus, ES, 22 de outubro de 2025.

RODRIGO PETER

PETERLE:05500238795

RODRIGO PETER PETERLE

Controlador Geral
Decreto N° 17.075/2025

Assinado de forma digital por RODRIGO
PETER PETERLE:05500238795
Dados: 2025.10.23 08:44:21 -03'00'
Versão do Adobe Acrobat Reader:
2025.001.20756

ANEXO II

TERMO INDIVIDUAL DE RESPONSABILIDADE PARA USO DE VPN (BYOD)

Eu, _____, matrícula nº _____, cargo/função _____, lotado(a) em _____, declaro para os devidos fins que:

1. Estou ciente das regras estabelecidas na Instrução Normativa STI nº 004/2025, especialmente quanto à segurança da informação, proteção de dados pessoais e responsabilidade pelo uso da VPN em dispositivo pessoal (BYOD);
2. Comprometo-me a utilizar o acesso VPN exclusivamente para fins funcionais relacionados às minhas atividades laborais;
3. Assumo integral responsabilidade administrativa, civil e penal por uso indevido, vazamento de dados ou descumprimento das regras;
4. Reconheço que o acesso poderá ser revogado a qualquer tempo por decisão administrativa, técnica ou de segurança;
5. Comprometo-me a manter o dispositivo atualizado, com antivírus ativo e autenticação multifator.

São Mateus, ____ de _____ de xxxx.

Nome e assinatura do Servidor: _____

Assinatura da Chefia Imediata: _____

Assinatura do Secretário de Municipal de Ciência, Tecnologia, Inovação, Educação profissional e Trabalho _____