

Termo de Responsabilidade e Uso da VPN Corporativa

Código do Documento: TERM-VPN-001	Versão: 1.0
Data de Aprovação: Janeiro de 2026	Classificação de Informação: Uso Interno
Área Gestora: Segurança da Informação / TI	Aplica-se a: Plataforma SISMETRO (APIs, Web e Arquitetura AWS)

1. Visão Geral e Objetivos

Este documento estabelece as diretrizes e responsabilidades para o uso da Rede Privada Virtual (VPN), o acesso via VPN é fornecido exclusivamente para viabilizar o trabalho remoto, permitindo o acesso seguro a servidores, bancos de dados, ambientes em nuvem (como AWS) e sistemas internos da empresa.

2. Escopo e Concessão de Acesso

O acesso à VPN é concedido estritamente para fins profissionais e de acordo com o perfil e a função do colaborador (ex: Desenvolvedor, Arquiteto de Sistemas, DevOps).

- As credenciais de acesso, certificados e chaves de configuração (ex: perfis do WireGuard, OpenVPN ou clientes nativos) são de uso pessoal e intransferível.
- O acesso a ambientes críticos, como clusters de produção e instâncias de banco de dados (ex: MySQL, Redis), é restrito e monitorado.

3. Deveres e Regras de Uso (Uso Aceitável)

Ao conectar-se à VPN da empresa, o usuário concorda em:

- Utilizar a conexão exclusivamente para acessar recursos corporativos, repositórios de código, esteiras de CI/CD, painéis de infraestrutura e integrações (ex: APIs de ERPs).
- Manter o sistema operacional de sua estação de trabalho (Windows, Linux ou macOS) atualizado e protegido por software antivírus e firewall ativo.
- Garantir que as chaves de acesso corporativas e credenciais de banco de dados não sejam expostas ou salvas em texto claro em dispositivos não criptografados.

- Desconectar a sessão da VPN imediatamente após o término das atividades laborais ou quando o acesso aos recursos internos não for mais necessário.

4. Proibições (Uso Inaceitável)

É expressamente proibido durante o uso da VPN:

- Compartilhar credenciais de acesso, chaves privadas ou perfis de conexão com terceiros, incluindo colegas de trabalho (cada usuário deve possuir sua própria credencial).
- Utilizar a rede corporativa para fins pessoais, download de arquivos com direitos autorais (pirataria/torrents), mineração de criptomoedas, acesso a conteúdo adulto, jogos online ou streaming não relacionado ao trabalho.
- Tentar contornar controles de segurança, regras de firewall, listas de IPs permitidos (whitelists) ou realizar varreduras de rede (port scanning) não autorizadas na infraestrutura interna.
- Modificar as configurações de roteamento da VPN (como desabilitar o *split-tunneling*, se configurado pela administração de rede) para mascarar tráfego pessoal.

5. Monitoramento e Privacidade

A infraestrutura de rede conta com ferramentas de auditoria e segurança.

- A empresa reserva-se o direito de registrar (logar) horários de conexão, endereços IP de origem, volume de tráfego e destinos acessados através da VPN para fins de auditoria de segurança e performance.
- O usuário não deve ter expectativa de privacidade em relação aos dados trafegados através do túnel VPN corporativo.

6. Revogação de Acesso e Sanções

O descumprimento de qualquer diretriz deste termo é considerado uma violação das políticas de segurança da informação da empresa.

- O acesso à VPN pode ser revogado a qualquer momento, sem aviso prévio, caso seja detectada atividade suspeita ou violação de segurança.
- Infrações a este termo podem resultar em medidas disciplinares, que variam desde advertências formais até a rescisão do contrato de trabalho por justa causa, além de possíveis sanções civis e penais em caso de vazamento de dados ou danos à infraestrutura (ex: exposição de instâncias EC2, RDS ou credenciais de integrações ERP).

Termo de Aceite e Assinatura Eletrônica

Declaro ter lido, compreendido e estar plenamente de acordo com todas as regras estabelecidas neste **Termo de Responsabilidade e Uso da VPN Corporativa**.

Comprometo-me a seguir rigorosamente as diretrizes de segurança da informação e assumo integral responsabilidade pelo uso adequado das credenciais de rede, acessos a servidores e chaves criptográficas que me foram confiados.

*A validade jurídica deste termo é assegurada mediante assinatura digital realizada pelo usuário. Este documento deve ser assinado utilizando o portal **Gov.br** (nível Prata ou Ouro), certificado digital padrão **ICP-Brasil**, ou por meio de plataforma de assinaturas eletrônicas homologada pela empresa.*

[Documento Assinado Digitalmente]

(A autenticação da assinatura, identificação do signatário, bem como a data e hora do aceite, encontram-se registradas no respectivo certificado digital ou no relatório/log da plataforma de assinatura vinculado a este arquivo eletrônico).

Revisão #2

Criado 2026-10-26 17:18:28 UTC por Marcio Klitzke

Atualizado: 2026-10-26 17:25:56 UTC por Marcio Klitzke