

POLÍTICAS CORPORATIVAS

POLÍTICA DE ACESSO REMOTO SEGURO AO AMBIENTE DA REDE CORPORATIVA DA TRACES

DOCUMENTO

Política de Acesso Remoto Seguro

VERSÃO

1.0

VIGÊNCIA

Dezembro de 2026

CLASSIFICAÇÃO

Documento Público

CONTROLE DO DOCUMENTO

VERSÃO	DATA	RESPONSÁVEL	RESUMO
1.0	Janeiro/2026	TRACES Consultoria em Informática Ltda.	Criação da política

1. OBJETIVO

A presente Política de Acesso Remoto Seguro ao Ambiente da Rede Corporativa da TRACES ("Política") estabelece diretrizes mínimas de segurança aplicáveis ao acesso remoto aos sistemas, redes, recursos tecnológicos e ambientes corporativos disponibilizados ou administrados pela TRACES Consultoria em Informática Ltda. ("TRACES").

Seu objetivo é reduzir riscos relacionados a acessos não autorizados, exposição de informações, uso indevido de credenciais, comprometimento de dispositivos e demais incidentes de segurança relacionados ao acesso remoto.

2. ABRANGÊNCIA

Esta Política aplica-se aos funcionários, administradores, prestadores de serviços, fornecedores, parceiros, terceiros, prepostos e colaboradores que, devidamente autorizados, necessitem acessar remotamente recursos tecnológicos da TRACES ou ambientes disponibilizados pela TRACES para execução de suas atividades.

Quando o acesso envolver ambiente pertencente a cliente da TRACES, deverão ser observadas também as políticas, normas e requisitos específicos estabelecidos pelo respectivo cliente.

Havendo conflito entre esta Política e regra específica de segurança estabelecida pelo cliente para acesso ao seu próprio ambiente, deverá ser observada a regra mais restritiva ou aquela formalmente determinada pelo proprietário do ambiente.

3. PRINCÍPIOS DE ACESSO

- a) utilização exclusivamente para finalidade profissional legítima;
- b) concessão de acesso somente a pessoas previamente autorizadas;
- c) utilização do menor nível de privilégio necessário à execução da atividade;
- d) individualização das credenciais de acesso sempre que tecnicamente possível;
- e) proteção das credenciais contra compartilhamento ou utilização indevida;
- f) observância das políticas de segurança aplicáveis ao ambiente acessado.

4. CREDENCIAIS DE ACESSO

As credenciais disponibilizadas para acesso aos ambientes são pessoais e intransferíveis, salvo nos casos em que a própria arquitetura do sistema ou procedimento formalmente estabelecido determine a utilização de conta técnica ou de serviço.

É vedado:

- a) compartilhar senhas ou credenciais pessoais com terceiros;
- b) divulgar senhas por meios públicos ou não autorizados;
- c) armazenar credenciais de maneira desprotegida;
- d) tentar obter ou utilizar credenciais pertencentes a outro usuário sem autorização.

Sempre que disponível e aplicável, poderá ser exigida autenticação multifator (MFA).

5. MECANISMOS DE ACESSO REMOTO

O acesso remoto deverá ocorrer por mecanismos considerados adequados ao ambiente acessado, tais como:

- VPN;
- bastion host ou jump server;
- soluções de Privileged Access Management (PAM);
- plataformas de acesso remoto seguro;
- ferramentas de suporte remoto autorizadas;
- mecanismos de acesso disponibilizados pelo próprio cliente;

6. DISPOSITIVOS UTILIZADOS NO ACESSO

Sempre que aplicável, os equipamentos utilizados para acesso remoto deverão possuir condições razoáveis de segurança, incluindo:

- a) sistema operacional suportado e atualizado;
- b) mecanismos de proteção contra códigos maliciosos quando compatíveis com o equipamento;
- c) bloqueio de tela;
- d) controle de acesso mediante senha ou mecanismo equivalente;
- e) atualizações de segurança compatíveis com as políticas corporativas aplicáveis.

7. ACESSO A AMBIENTES DE CLIENTES

O acesso a ambientes de clientes deverá ocorrer exclusivamente quando necessário para prestação dos serviços contratados e de acordo com as autorizações concedidas.

O profissional não deverá acessar sistemas, bancos de dados, servidores, arquivos ou recursos que não estejam relacionados às atividades para as quais tenha sido autorizado.

Credenciais, informações, configurações, inventários, diagramas, dados ou demais conteúdos obtidos durante o acesso deverão ser tratados como informações confidenciais, observadas as obrigações contratuais aplicáveis.

8. TRANSFERÊNCIA E ARMAZENAMENTO DE INFORMAÇÕES

Informações obtidas durante a execução dos serviços não deverão ser copiadas, transferidas ou armazenadas fora dos ambientes autorizados quando isso não for necessário para a execução da atividade.

Quando houver necessidade operacional de transferência ou armazenamento temporário, deverão ser utilizados mecanismos compatíveis com os requisitos de segurança aplicáveis ao ambiente.

Dados de clientes não deverão ser utilizados para finalidades distintas daquelas relacionadas à prestação dos serviços contratados.

9. REGISTRO E MONITORAMENTO

Os acessos a recursos tecnológicos poderão ser registrados e monitorados para fins de:

- a) segurança da informação;
- b) auditoria;
- c) investigação de incidentes;
- d) cumprimento de obrigações contratuais ou legais;
- e) suporte e continuidade operacional.

Os registros poderão incluir, entre outras informações, identificação do usuário, data e horário, origem do acesso, recurso acessado e demais informações técnicas disponíveis nos respectivos sistemas.

10. INCIDENTES DE SEGURANÇA

Qualquer suspeita de comprometimento de credencial, acesso indevido, perda de equipamento utilizado para acesso, malware, exposição de informações ou outro evento que possa representar risco aos ambientes acessados deverá ser comunicada à TRACES assim que identificada.

A TRACES poderá suspender preventivamente credenciais ou acessos quando houver indício razoável de risco de segurança, até que sejam realizadas as verificações necessárias.

11. RESPONSABILIDADES DOS USUÁRIOS

Cada usuário é responsável por:

- a) utilizar adequadamente as credenciais que lhe forem disponibilizadas;
- b) proteger os meios utilizados para autenticação;
- c) observar esta Política e demais regras de segurança aplicáveis;
- d) comunicar situações que possam representar risco de segurança;
- e) utilizar o acesso somente dentro das autorizações concedidas.

12. PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

O tratamento de informações e dados pessoais eventualmente acessados durante a execução das atividades deverá observar a legislação aplicável, incluindo a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), quando aplicável.

As informações acessadas no contexto da prestação dos serviços deverão ser utilizadas exclusivamente para as finalidades autorizadas.

13. EXCEÇÕES

Situações excepcionais que demandem procedimento distinto daquele previsto nesta Política poderão ser autorizadas pela TRACES ou, tratando-se de ambiente de terceiro, pelo respectivo responsável pelo ambiente.

A exceção deverá limitar-se à necessidade específica que justificou sua utilização.

14. ATUALIZAÇÃO DA POLÍTICA

Esta Política poderá ser atualizada periodicamente pela TRACES em razão de alterações tecnológicas, regulatórias, operacionais ou relacionadas às práticas de segurança da informação.

A versão vigente estará disponibilizada em: <https://www.traces.com.br/politicas/>

As alterações produzirão efeitos a partir da data de vigência indicada na respectiva versão, respeitadas as disposições contratuais aplicáveis.

15. DISPOSIÇÕES FINAIS

A concessão de acesso remoto não gera direito permanente de acesso a qualquer sistema, ambiente ou recurso tecnológico.

Permissões poderão ser modificadas ou revogadas a qualquer momento quando necessário à segurança ou à adequada prestação dos serviços.

O descumprimento desta Política poderá resultar na suspensão ou revogação do acesso e na adoção das medidas contratuais, administrativas ou legais cabíveis, conforme a natureza e gravidade da ocorrência.

APROVAÇÃO E VIGÊNCIA

Empresa	TRACES Consultoria em Informática Ltda.
Versão vigente	1.0 - Janeiro de 2026
Publicação	https://www.traces.com.br/politicas/