# Propósito

A Norma de Segurança para Trabalho e Acesso Remoto **NOR-SGSI-004** complementa a Política de Segurança da Informação, definindo as diretrizes para a realização de trabalho remoto e as condições para a concessão, controle e monitoramento de acessos remotos.

# Escopo

Esta norma é aplicável ao escopo definido na Política de Segurança da Informação.

# Glossário

* **Acesso remoto**: Capacidade de acessar um computador, rede ou sistema de um local diferente no qual este está localizado fisicamente.
* **Antivírus**: Trata-se de programas que têm a função de detectar, alertar, limpar, isolar, apagar e prevenir sistemas contra vírus e suas variações.
* **Ativo de informação**: Os dados, informações, aplicações, sistemas, equipamentos de rede, hardware, software e firmware utilizados pela **Demarco**.
* **Equipamentos** **computacionais**: Dispositivos eletrônicos capazes de realizar cálculos e processar dados/informações, como celulares, tablets, smartphones, computadores, notebooks etc.
* **Túnel** **de** **VPN:** Recurso utilizado para criar uma conexão segura para a transferência de arquivos e dados entre computadores ou redes de computadores.
* **VPN:** Rede virtual privada construída através de uma rede pública para conectar dispositivos e redes de computadores.
* **VPN** **Client** **to** **Site:** Túnel de VPN que conecta um equipamento a uma rede de computadores.
* **VPN SSL:** Túnel de VPN utilizado para criação de acesso remoto na camada de aplicação.
* **VPN** **IPSec:** Túnel de VPN utilizado para criação de acesso remoto na camada de rede.

# Diretrizes

A modalidade de trabalho predominante na **Demarco** é o remoto e para assegurar a confidencialidade, integridade e disponibilidade dos ativos de informação da **Demarco**, devem ser observadas as diretrizes estabelecidas a seguir.

## Trabalho remoto

1. Colaboradores que realizam trabalho remoto devem no mínimo assegurar que:
   1. O computador possua as configurações mínimas definidas pela área de Infraestrutura e Segurança da Informação;
   2. Esteja cadastrado na lista de computadores permitidos pela área de Infraestrutura e Segurança da Informação;
   3. Evitem a utilização de redes públicas e redes wi-fi compartilhadas para o acesso ou compartilhamento de informações críticas, pois as informações podem ser interceptadas por cibercriminosos;
   4. Garantam que indivíduos não autorizados não tenham acesso ou visualizem conteúdo confidencial durante a realização do trabalho em regime remoto.
   5. Comuniquem, imediatamente, a perda de um dispositivo controlado ou pessoal que possua acesso a recursos ou informações da **Demarco** paraa área de Infraestrutura e Segurança da Informação;
2. Colaboradores autorizados a utilizar dispositivos pessoais para a execução de suas atividades devem assumir a responsabilidade pela segurança de seus próprios dispositivos. Recomenda-se que os colaboradores que utilizam máquinas pessoais observem os seguintes requisitos:
   1. Utilizem um antivírus com licença válida;
   2. Atualizem regularmente o sistema operacional e os softwares de sua máquina;
   3. Evitem a realização de acesso remoto em sua máquina;
   4. Somente utilizar sistema operacional ou softwares licenciados, evitando que a máquina seja contaminada por malware e que ocorra a violação de direitos autorais.
3. A **Demarco** não será responsável por fornecer suporte, atualização, manutenção, reposição de peças, licenciamento de softwares, reembolso ou cobrir qualquer tipo de custo referente ao uso de dispositivos pessoais;
4. Colaboradores que possuírem acesso a informações de nível confidencial, servidores, VPN, código fonte ou funções privilegiadas em nossos sistemas devem possuir máquina controlada pela **Demarco;**
5. Todas as informações produzidas através do regime de trabalho remoto, independente do dispositivo utilizado para a produção, pertencem a **Demarco**.

## Requisitos de configuração para acesso remoto

1. É proibida a utilização de softwares não homologados para a realização de acesso remoto nos equipamentos computacionais, exceto nos casos em que for necessário e autorizado;
2. O acesso remoto a ativos/serviços de informação e recursos computacionais da empresa deve ser restringido no mínimo por credencial de acesso;
3. Túneis de VPN *Client to Site* para os equipamentos computacionais da empresa devem utilizar recursos como VPN SSL ou VPN IPSEC;
4. O algoritmo de encriptação utilizado deve ser equivalente ou superior ao SHA-256 e utilizar de chave simétrica ou assimétrica;
5. É proibida a disponibilização de acesso remoto através de protocolo RDP diretamente pelo IP público da empresa;
6. Equipamentos computacionais utilizados para acesso remoto devem atender aos requisitos de configuração estabelecidos por norma específica.

## Concessão e uso do acesso remoto

1. O acesso remoto a ativos/serviços de informação e recursos computacionais da **Demarco** é altamente restrito a usuários que necessitem deste recurso para execução das suas atividades profissionais;
2. A concessão de credencial para realização de acesso remoto deve seguir os padrões estabelecidos na norma de gestão de acesso;
3. O acesso remoto a ativos/serviços de informação e recursos computacionais da **Demarco** deve ser concedido com o mínimo de privilégios necessários para a execução de suas atividades profissionais;

## Concessão e uso do acesso remoto para terceiros

1. O acesso remoto a ativos/serviços de informação e recursos computacionais da empresa poderá ser concedido a terceiros ou prestadores de serviço, caso seja necessário para a execução de suas atividades;
2. O acesso remoto de terceiros e prestadores de serviço a ativos/serviços de informação ou recursos computacionais da empresa somente poderá ser concedido após a efetivação do acordo de confidencialidade entre as partes;
3. A concessão do acesso deverá ser limitada automaticamente ao tempo necessário estimado da atividade do terceiro ou prestador de serviço, não excedendo ao máximo de 30 (trinta) dias corridos por concessão;
4. O usuário terceiro, bem como a empresa onde ele trabalha, serão os únicos responsáveis por toda ação executada com suas credenciais de acesso remoto, incluindo qualquer atividade não autorizada exercida por outras partes de posse de suas credenciais de acesso remoto;
5. O acesso remoto de terceiros a ativos/serviços de informação e recursos computacionais da empresa deve ser concedido com o mínimo de privilégios necessários para a execução de suas atividades;
6. Equipamentos computacionais utilizados por terceiros para acesso remoto devem possuir ferramentas para proteção contra códigos maliciosos aderentes às diretrizes da empresa e firewall local ativo.

## Monitoramento do acesso remoto

1. Toda informação que é acessada, transmitida, recebida ou produzida através do acesso remoto a ativos/serviços de informação ou recursos computacionais da **Demarco** está sujeita a monitoramento, não havendo por parte do usuário qualquer expectativa de privacidade;
2. Durante o monitoramento do acesso remoto a seus ativos/serviços de informação ou recursos computacionais, a empresa se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, gravar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário.

# Papéis e Responsabilidades

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Avaliar se os dispositivos para o qual está sendo permitida a realização de acesso remoto atendem aos critérios mínimos de segurança;
2. Manter lista atualizada de softwares de acesso remoto homologados;
3. Assegurar que configurações de VPN para acesso a rede estão de acordo com os requisitos definidos nesta norma;
4. Conceder acesso remoto conforme necessário e de acordo com os requisitos desta norma para os usuários;
5. Monitorar conexões remotas aos ativos da empresa.

## RECURSOS HUMANOS

1. Validar durante a contratação se máquinas pessoais atendem aos requisitos mínimos de configuração;

## COLABORADORES E TERCEIROS

1. Seguir os requisitos estabelecidos para a realização de trabalho e acesso remoto da **Demarco.**

# Gestão de versões

A revisão, aprovação e alteração desta política segue os requisitos estabelecidos na Política de Segurança da Informação.

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data:** | **Responsável**  **Alteração:** | **Tipo de modificação:** |
| 0.1 | 07/08/2023 | CSIP | Criação da política |
| 0.2 | 05/07/2024 | CSIP | Revisão |
| 0.3 | 18/07/2024 | CSIP | Ajustes |