# Propósito

A Norma de Configuração Segura **NOR-SGSI-007** complementa a Política de Segurança da Informação, definindo as diretrizes e requisitos para a configuração segura de dispositivos tecnológicos.

# Escopo

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

# Glossário

* **Plataforma de computação em nuvem:** Serviços de computação, incluindo servidores, armazenamento, banco de dados, rede, software, análise e inteligência provisionados através da internet por terceiros.
* **Vulnerabilidades:** fraqueza de um ativo ou controle que pode ser explorada por uma ameaça, com recurso ou método de ataque.
* **Componentes de rede**: switch, hub, firewall, câmeras, impressoras etc.;
* **Dispositivos tecnológicos**: computadores (desktop e notebooks), servidores, celulares;

# Diretrizes

Assegurar que dispositivos tecnológicos e componentes de rede possuam uma configuração segura é um elemento crucial para a segurança cibernética da **Demarco**. Através da configuração segura, conseguimos impedir que agentes maliciosos explorem falhas ou vulnerabilidades geradas por configurações inadequadas nestes recursos. As seguintes diretrizes devem ser observadas:

## Desktops, Notebooks e Servidores corporativos

1. Para a utilização de dispositivos como desktops, notebooks e servidores é necessário que estes possuam um sistema operacional (SO) que permita a interação do usuário com o dispositivo. Existem diversos sistemas operacionais que podem ser utilizados para diferentes finalidades. Para fins de segurança da rede da **Demarco**, devem ser estabelecidos os SO’s considerados padrão, incluindo servidores:

* Deve ser definido pela TI o tipo de SO permitido para uso nos dispositivos corporativos;
* Deve ser definido pela TI a versão mínima do SO;
* Deve ser mantida e atualizada pela TI uma imagem padrão contendo as configurações seguras para o SO, como serviços que devem estar desabilitados, firewall, usuários padrão, chaves de registro, bitlocker, integração com o Active Directory etc.

1. Dispositivos corporativos devem estar dentro do padrão de nomenclatura estabelecido pela TI para fins de identificação e rastreio;
2. Para garantir que os dispositivos estejam seguros e que potenciais ataques cibernéticos sejam detectados, os dispositivos devem possuir ferramenta anti-malware instalada e sob controle da TI ou de equipe de cibersegurança especializada;
3. Os softwares possuem vulnerabilidades técnicas, e cada dispositivo pode ter muitos desses softwares. É importante manter uma ferramenta adequada para identificar essas vulnerabilidades técnicas nos dispositivos e, se necessário, uma ferramenta separada para corrigir esses softwares por meio de patches.;
4. Sistemas operacionais e softwares devem ser mantidos atualizados para assegurar seu funcionamento apropriado e redução de vulnerabilidades técnicas. Para garantir que o SO e seus softwares estão atualizados, deve ser mantida uma ferramenta para controlar e gerir a atualização de patches do parque tecnológico;
5. Para assegurar que os dispositivos atendam padrão mínimo estabelecido pela TI, deve ser mantida uma ferramenta que avalie a conformidade dos desktops e notebooks corporativos;
6. Mudanças realizadas em configurações devem ser registradas e analisadas periodicamente.

## Smartphones corporativos

1. A configuração padrão de smartphones da **Demarco** deve ser apropriada para garantir a funcionalidade dos dispositivos e manter níveis adequados de segurança. No mínimo, esta configuração deve abranger:

* Sistema operacional padrão para os dispositivos, contendo as configurações e aplicações pré-definidas;
* Usuários devem possuir permissões limitadas de alteração do sistema, não podendo alterar configurações ou instalar aplicações;
* Os dispositivos devem possuir bloqueio de tela habilitado e um tempo padrão para bloqueio após inatividade;
* Os dispositivos devem estar com configuração de criptografia habilitada;
* Não deve ser permitida a realização de jailbrake ou root dos dispositivos;

1. Mudanças realizadas em configurações devem ser registradas e analisadas periodicamente.

## Desktops e notebooks pessoais

1. Dispositivos que são de propriedade do colaborador devem no mínimo atender aos seguintes critérios de configuração segura:

* Sistema operacional Windows 10 ou 11, Linux ou MacOS;
* Build do sistema operacional deve ser superior a versão 22h2;
* Atualizações automáticas devem estar habilitadas;
* Firewall do Windows deve estar habilitado;
* Antivírus corporativo da **Demarco** deverá ser instalado;
* A máquina utilizada pelo colaborador deverá ser registrada no intune, para assegurar a deleção remota de dados, em caso de perda do dispositivo.

## Dispositivos de rede

1. Quando forem utilizados dispositivos de rede em um coworking ou ambiente físico da **Demarco**, é necessário empregar configurações a fim de garantir o funcionamento adequado e seguro desses dispositivos. No mínimo, a configuração deve abranger:

* Desativação de configurações, serviços ou portas desnecessárias;
* Alteração, caso possível, de portas padrões utilizados nos dispositivos de rede;
* Alteração de nomes de usuário e senhas do dispositivo, observando requisitos para a criação de usuários e senhas.

1. Quando forem utilizadas redes de conexão sem fio, deve ser utilizado:

* O protocolo de autenticação (chave compartilhada com o usuário para acesso) mais seguro e atual. Protocolos como WEP, WPA TKIP devem ser abolidos;
* Em redes wireless corporativas, usuários devem se autenticar através de 802.1x TLS ou através de SSO com o dispositivo de proteção de borda;
* Redes utilizadas por visitantes devem ser completamente segregadas da rede interna.

## Azure

1. Assumir que plataformas de computação em nuvem como AWS e Azure são automaticamente seguros pode ter um alto custo para qualquer organização. A segurança de recursos em nuvem é dividida entre o fornecedor e o cliente do serviço, a depender do tipo de serviço contratado. Para garantir a segurança no uso de recursos em nuvem, deve ser utilizado serviço ou recurso que identifique e aponte os melhores padrões de segurança para as configurações utilizadas em serviços de nuvem.
2. Para assegurar que os recursos em nuvem sejam gerenciados de maneira apropriada e segura, deve ser estabelecida documentação específica contendo os padrões para a criação e gestão de: Resource Groups, Vnets, NSGs etc.;
3. As comunicações que circulam entre a rede interna e externa da **Demarco** podem conter ameaças à segurança das informações. Para assegurar a proteção da comunicação interna e externa, deve ser mantido dispositivo de proteção de borda (firewall em nuvem) que possua no mínimo os seguintes recursos:

* Recurso que filtre e permita o controle de acesso a websites;
* Recurso que filtre e permita o controle de uso de aplicações;
* Inspeção aprofundada de pacotes de rede;
* Inspeção de pacotes de rede criptografados;
* Recurso de detecção de malware, como antivírus de borda e sand-box;
* Filtro geográfico;
* Detecção e prevenção a intrusões.

1. Para assegurar um melhor nível de clareza para quem necessita conhecer as configurações e funcionamento dos recursos em nuvem, deve ser criada e mantida atualizada documentação sobre as conexões e arquitetura de rede em nuvem da **Demarco**;
2. Mudanças realizadas em configurações devem ser registradas e analisadas criticamente periodicamente.

## Intune

1. Linha de base de segurança: Para fins de conformidade com os requisitos estabelecidos para a configuração segura dos dispositivos, o intune deve ser utilizado sempre que possível para aplicar e monitorar a configuração de dispositivos. No mínimo, devem ser mantidas políticas com diretrizes de segurança para:

* Windows 10;
* Microsoft 365 Apps.

# Papéis e Responsabilidades

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Estabelecer e manter atualizados os padrões de configuração segura para os dispositivos tecnológicos;
2. Implementar e manter solução para verificação de conformidade dos dispositivos com as configurações seguras;
3. Registrar e controlar mudanças nos dispositivos tecnológicos que forem da **Demarco**;
4. Criar e armazenar, sempre que possível, relatórios de conformidade dos recursos tecnológicos;
5. Assegurar a contratação e implementação de ferramentas como: anti-malware (antivírus), scanner de vulnerabilidade e firewall sempre que necessário;
6. Apresentar relatórios de conformidade de recursos tecnológicos ao CSIP anualmente.

# 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 | 04/09/2023 | CSIP | Elaboração |
| 0.2 | 10/09/2024 | CSIP | Revisão anual |
|  |  |  |  |