# Propósito

A Norma de Gestão de Vulnerabilidades **NOR-SGSI-006** complementa a Política de Segurança da Informação, definindo as diretrizes para uma gestão eficaz de vulnerabilidades técnicas do parque tecnológico da **Demarco**.

# Escopo

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

# Glossário

* **Pentest:** Abreviação de Penetration Test, também conhecido como teste de intrusão. Consiste na realização de testes de segurança de um ambiente, serviço, dispositivo ou aplicação.
* **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.
* **Soluções Demarco:** Bancodoc, DMAnalytics, DMPeople, Audtool, Gente e Gestão, Sisnec, Frota Legal, Demarco Academy, DMProcess e DMCenter.
* **Vulnerabilidades técnicas:** Fraqueza de um *ativo* ou *controle* que pode ser explorado por uma ou mais ameaças.
* **Vulnerabilidade:**fraqueza de um ativo ou controle que pode ser explorada por uma ameaça, com recurso ou método de ataque.

# Diretrizes

Dentro de um ambiente tecnológico diversificado, é possível encontrar muitos tipos de computadores que apresentam problemas técnicos, seja devido a erros no programa, no firmware ou nos componentes físicos. Os dispositivos suscetíveis a esses problemas incluem:

* **Componentes de rede**: switch, hub, firewall, câmeras, impressoras etc.;
* **Dispositivos tecnológicos**: computadores (desktop e notebooks), servidores, celulares;
* **Softwares e firmwares**: Sistema operacional (SO), softwares em geral (adobe, excel e todos outros programas de computador, incluindo as soluções desenvolvidas pela **Demarco**).

As vulnerabilidades podem ser alvo de ameaças, como hackers, que podem explorá-las como ponto de entrada ou de escalação de privilégios no ambiente tecnológico da **Demarco**. Visando preservar a segurança de nosso ambiente interno, estabelecemos as seguintes diretrizes:

## Identificação de vulnerabilidades

Existem diversos meios que permitem a identificação de vulnerabilidades técnicas em diferentes tipos de equipamentos computacionais. No mínimo, devem ser cumpridos os seguintes requisitos para a identificação de vulnerabilidades em equipamentos:

1. **Computadores, notebooks e servidores controlados pela Demarco:** Devem possuir software que escaneie vulnerabilidades técnicas no SO e softwares;
2. **Soluções Demarco:** Devem ser utilizados softwares para a identificação de vulnerabilidades no processo de desenvolvimento de todas as soluções e promoverem a realização de **um** Pentest ao ano nas soluções de maior relevância ou que tenham exigência contratual para tal.
3. **Plataforma de computação em nuvem:** Deve ser mantida ferramenta para escaneamento de conformidade com a Segurança da Informação.

## Classificação de vulnerabilidades

As vulnerabilidades técnicas identificadas através dos diferentes processos devem ser classificadas com base em sua gravidade, levando em consideração o potencial impacto que podem causar aos equipamentos computacionais da **Demarco,** bem como sua probabilidade de ocorrência.

## Priorização e mitigação de vulnerabilidades

1. O responsável pelo ativo de informação no qual a vulnerabilidade foi identificada deve priorizar a correção das vulnerabilidades de acordo com a sua classificação, devendo adotar as medidas que forem necessárias para a sua correção;

A priorização deve seguir a seguinte tabela:

|  |  |  |
| --- | --- | --- |
| **SEVERIDADE** | **DESCRIÇÃO** | **PRAZO** |
| **ALTA** | Vulnerabilidade de fácil exploração, tem sido ativamente explorada por agentes maliciosos e certamente causará grande impacto a segurança da informação da **Demarco** caso seja explorada. | ATÉ 20 DIAS ÚTEIS PARA CORREÇÃO |
| **MÉDIA** | Vulnerabilidade de difícil exploração, e que não tem sido ativamente explorada por agentes maliciosos. Pode causar grande impacto a segurança da informação da **Demarco** caso for explorada. | ATÉ 40 DIAS ÚTEIS PARA CORREÇÃO |
| **BAIXA** | Vulnerabilidade trivial, sua exploração pode ser fácil ou difícil e tem pouca chance de causar impacto a segurança da informação da **Demarco** caso for explorada. | ATÉ 60 DIAS ÚTEIS PARA CORREÇÃO |

1. Não é necessário resolver vulnerabilidades, desde que sejam reconhecidas como aceitáveis. Devem ser comunicadas ao responsável, acompanhadas de uma explicação que justifique a decisão de não as corrigir. A aceitação de não tratar as vulnerabilidades deve ser formalizada e devidamente registrada.
2. Evidências das correções devem ser mantidas e avaliadas para confirmar que as vulnerabilidades foram tratadas de acordo com a prioridade definida.

# Papéis e Responsabilidades

## INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO

1. Assegurar a contratação de Pentests anuais para as soluções de maior relevância da **Demarco**;
2. Analisar justificativas para não correção de vulnerabilidades e aceitar ou recusar formalmente;
3. Registrar vulnerabilidades de forma manual ou automática na ferramenta de gestão;
4. Contratar serviço ou implementar solução para a identificação de vulnerabilidades técnicas nos computadores e servidores da **Demarco**;
5. Assegurar que seja utilizada solução para a identificação de vulnerabilidades na plataforma de computação em nuvem.

## RESPONSÁVEIS PELOS SISTEMAS

1. Priorizar e mitigar as vulnerabilidades identificadas para o sistema pelo qual é responsável;
2. Implementar, manter e utilizar ferramenta para identificação de vulnerabilidades no desenvolvimento das soluções da **Demarco**.

## COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

1. Acompanhar e verificar se o tratamento das vulnerabilidades está sendo realizado dentro do prazo estabelecido.

# 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 | 06/10/2023 | CSIP | Criação |
| 0.2 | 10/07/2024 | CSIP | Revisão e ajustes |
|  |  |  |  |