|  |
| --- |
| MAA – DSM – Segurança no Desenvolvimento de Aplicações (DAS) |

|  |  |
| --- | --- |
| Equipe de Trabalho: Os Incríveis | |
| Participante | Função |
| Ana Júlia de Souza Santos | SGSI/PROGRAMADOR/ |
| Nilton Dionisio Guerra | ESCRITOR/PROGRAMADOR |
| Luigi Falcade de Souza | DESENVOLVERDOR/PROGRAMADOR |

|  |
| --- |
| Trabalho da Equipe |
| Delivery- FomeFacil |

**SUMÁRIO**

[**1 Revisão e atualização da política 2**](#_Toc160707898)

[**1.1 Controle de versões 2**](#_Toc160707899)

[**1.2 Processo de revisão 2**](#_Toc160707900)

[**2 Introdução 2**](#_Toc160707901)

[**2.1 Objetivo do documento 2**](#_Toc160707902)

[**2.2 Escopo de aplicação 2**](#_Toc160707903)

[**2.3 Responsabilidades 2**](#_Toc160707904)

[**2.4 Comunicação e conscientização 2**](#_Toc160707905)

[**3 Princípios gerais 3**](#_Toc160707906)

[**3.1 Definições e termos 3**](#_Toc160707907)

[**3.2 Princípios orientadores 3**](#_Toc160707908)

[**4 Procedimentos operacionais 3**](#_Toc160707909)

[**4.1 Procedimentos específicos 3**](#_Toc160707910)

[**4.2 Controles de medidas de segurança 3**](#_Toc160707911)

[**4.3 Mitigação e controle de riscos 3**](#_Toc160707912)

[**5 Aprovações 3**](#_Toc160707913)

[**6 Anexos e referências 4**](#_Toc160707914)

# Revisão e atualização da política

## **Controle de versões**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data** | **Autor** | **Notas da Revisão** |
| 1.0.0 | 14/03/2024 | Nilton Dionisio Guerra, Ana Julia de Souza santos e Luigi Falcade de Souza | Essa é a primeira versão técnica criada. |
|  |  |  |  |

## **Processo de revisão**

A fim de assegurar a contínua relevância e eficácia da presente política de senhas, será realizada uma revisão sistemática a cada seis meses. Ademais, qualquer alteração significativa no código de proteção de dados do país em que o sistema estiver operando acarretará uma revisão imediata e abrangente desta política. Esta prática assegura que a política permaneça em conformidade com as regulamentações vigentes e que permaneça adequadamente alinhada com as melhores práticas de segurança da informação.

# Introdução

## **Objetivo do documento**

Nesta política, abordaremos a importância da criação de senhas seguras como meio de conscientizar os usuários sobre a necessidade de estabelecer credenciais de acesso robustas. O objetivo é fornecer orientações claras sobre como criar senhas que possuam um nível adequado de segurança, a fim de proteger as informações confidenciais e os ativos da organização contra acesso não autorizado.

## **Escopo de aplicação**

A presente política destina-se aos usuários da plataforma ao criarem ou atualizarem suas senhas em nosso sistema. Seu propósito é fornece diretrizes claras e abrangentes para garantir a segurança e integridade das credenciais de acesso utilizadas na plataforma. Estas diretrizes visam promover boas práticas de segurança da informação, minimizando os riscos de comprometimento da segurança das contas dos usuários e protegendo os dados sensíveis armazenados no sistema.

## **Responsabilidades**

O sistema tem o compromisso de manter as senhas dos usuários seguras e protegidas em seus servidores, utilizando os mais altos padrões de segurança, com o objetivo primordial de preservar a confidencialidade dos dados dos usuários.

Por sua vez, cabe ao usuário a responsabilidade de manter sua senha em segurança e não a compartilhar com qualquer outra pessoa. Essa prática visa garantir a integridade e a privacidade dos dados pessoais e sensíveis armazenados na plataforma.

## **Comunicação e conscientização**

A presente política estará disponível em uma página dedicada dentro de nosso sistema, acessível através de um link localizado no rodapé e quando o usuário por criar uma conta em nosso sistema iremos disponibilizar um link na página de cadastramento para que a pessoa leia a política e depois marque em um checkbox que está ciente das políticas estabelecidas. Sua divulgação e conscientização serão realizadas sempre que um usuário estiver criando ou alterando sua senha de acesso. Esta prática visa garantir que todos os usuários estejam cientes e concordem com as diretrizes estabelecidas para a criação e manutenção de senhas seguras, fortalecendo assim a segurança e a integridade do sistema.

# Princípios gerais

## **Definições e termos**

* Backend: Refere-se à parte do sistema que opera nos servidores, sendo responsável pelo processamento e armazenamento de dados, bem como pela lógica de negócios e pela interação com o banco de dados. O backend é essencial para a funcionalidade do sistema, porém não é acessível diretamente pelos usuários finais.
* Frontend: Corresponde à parte do sistema com a qual o usuário interage diretamente. É responsável pela apresentação dos dados e pela interface com o usuário, incluindo elementos visuais e interativos. O frontend é projetado para oferecer uma experiência de usuário intuitiva e amigável.
* Regex (Expressões Regulares): Trata-se de uma anotação criada na programação para inclusão ou exclusão de caracteres, com o objetivo de criar uma máscara de dados ou identificar uma string por meio de características específicas. As expressões regulares são utilizadas para realizar operações de busca, validação e substituição em strings de texto, oferecendo um método poderoso e flexível para manipulação de dados.
* Token: Consiste em um objeto digital que contém informações sobre a identidade do principal que faz a solicitação e para que tipo de acesso ele está autorizado. Os tokens são frequentemente utilizados em sistemas de autenticação e autorização para validar e controlar o acesso dos usuários a recursos específicos. Eles fornecem uma forma segura e eficiente de gerenciar a segurança e o controle de acesso em sistemas distribuídos e na web.

## **Princípios orientadores**

Complexidade das Senhas: Senhas devem ser complexas, incluindo letras maiúsculas, minúsculas números e caracteres especiais.

* Rotação Regular de Senhas: Os usuários devem alterar suas senhas periodicamente para reduzir o risco de comprometimento da conta.
* Não Compartilhamento de Senhas: Senhas não devem ser compartilhadas e não devem ser armazenadas em locais facilmente acessíveis.
* Uso de Senhas Únicas: Cada conta de usuário deve ter uma senha exclusiva.
* Proteção de Senhas Armazenadas: Senhas armazenadas devem ser protegidas com técnicas de hash e criptografia.
* Monitoramento de Atividade Suspeita: Implementação de mecanismos para detectar atividades suspeitas relacionadas a senhas.
* Mecanismos de Autenticação Multifator: Sempre que possível, usar autenticação multifator.
* Política de Bloqueio de Conta: Estabelecer uma política clara de bloqueio de conta para lidar com tentativas de login malsucedidas ou atividades suspeitas.
* Revisão e Atualização Regular da Política: Revisar e atualizar a política de senhas conforme necessário para refletir as mudanças nas ameaças de segurança e nas melhores práticas da indústria.

Essa política foi estabelecida com o objetivo de garantir a segurança das contas de usuário e dos dados da organização, seguindo as práticas recomendadas de segurança da informação e mantendo-se atualizada diante das evoluções do cenário de ameaças cibernéticas.

Parte superior do formulário

# Procedimentos operacionais

## **Procedimentos específicos**

As senhas serão obrigatoriamente formadas por:

Mínimo 8 caracteres

Máximo de 16 caracteres

2 letras maiúsculas

2 letras minúsculas

3 caracteres números.

Sem a permissão de colocar símbolos.

Permitido repetir caracteres.

Além de que será necessário que a senha seja trocada uma vez a cada 6 meses, sendo que a senha não poderá ser igual a última senha criada.

## **Controles de medidas de segurança**

A fim de garantir o cumprimento dos requisitos estabelecidos para a criação ou atualização de senhas, será implementada uma máscara de caracteres utilizando REGEX. Essa medida tem como objetivo impedir que o usuário crie uma senha que não esteja em conformidade com os padrões definidos durante o processo de criação ou atualização de senha na tela correspondente; essa máscara em REGEX irá permitir apenas senhas com no mínimo 8 caracteres, 2 letras maiúsculas, 2 minúsculas e 3 números.

## **Mitigação e controle de riscos**

Em caso de perda ou esquecimento da senha por parte do usuário, será disponibilizada a opção de recuperação por meio de confirmação do e-mail cadastrado durante a criação da conta. Esta medida visa garantir que os usuários tenham um meio seguro e confiável de restabelecer o acesso à sua conta em situações de perda de senha.

# Aprovações

|  |  |  |
| --- | --- | --- |
| **Cargo** | **Nome/Assinatura** | **Data** |
| Nilton Dionisio Guerra | Nilton Dionisio Guerra | 07/03/2024 |
|  |  |  |

# Anexos e referências

* **Legislação e Regulamentações:**
* Legislação de Proteção de Dados: GDPR (Regulamento Geral de Proteção de Dados), LGPD (Lei Geral de Proteção de Dados)
* Regulamentações específicas da indústria: PCI DSS (Padrão de Segurança de Dados para a Indústria de Cartões de Pagamento)
* Políticas Internas: a. Política de Senhas b. Política de Proteção de Dados c. Política de Segurança da Informação
* **Normas e Procedimentos: a. Normas técnicas de segurança da informação:**
* ISO/IEC 27001:2013 - Sistemas de gestão de segurança da informação b. Procedimentos de recuperação de senha:
* Procedimento para recuperação de senha por e-mail: Descrever o processo passo a passo para os usuários recuperarem suas senhas por meio de um e-mail de confirmação. c. Procedimentos de monitoramento de atividade suspeita:
* Procedimento de monitoramento de logs de acesso: Especificar como os logs de acesso são monitorados regularmente para identificar atividades suspeitas. d. Procedimentos de bloqueio de conta:
* Procedimento de bloqueio de conta por tentativas de login malsucedidas: Descrever quando e como uma conta é bloqueada após um número específico de tentativas de login malsucedidas.