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

|  |  |
| --- | --- |
| **Equipe de Trabalho: [nome da equipe]** | |
| **Participante** | **Função** |
| Nilton dionisio guerra | Escritor/redator |
|  |  |

|  |
| --- |
| **Trabalho da Equipe** |
| DFF |

SUMÁRIO

[1 Revisão e atualização da política 3](#_Toc162363117)

[1.1 Controle de versões 3](#_Toc162363118)

[2 MONITORAMENTO DA POLÍTICA 3](#_Toc162363119)

[3 Introdução 3](#_Toc162363120)

[3.1 Objetivo do documento 3](#_Toc162363121)

[3.2 Escopo de aplicação 4](#_Toc162363122)

[3.3 Responsabilidades 4](#_Toc162363123)

[3.4 Comunicação e conscientização 4](#_Toc162363124)

[4 Princípios gerais 6](#_Toc162363125)

[5 Política de controle de acesso 6](#_Toc162363126)

[5.1 Responsabilidades da função de provisionamento 6](#_Toc162363127)

[5.2 Responsabilidades dos proprietários de ativos 7](#_Toc162363128)

[5.3 Responsabilidades do usuário 8](#_Toc162363129)

[6 Gerenciamento de acesso de usuário 9](#_Toc162363130)

[6.1 Cadastro de usuário 9](#_Toc162363131)

[6.2 Cancelamento do registro de usuário 9](#_Toc162363132)

[6.3 Provisionamento de acesso de usuário 10](#_Toc162363133)

[6.4 Remoção ou ajuste de direito de acesso 10](#_Toc162363134)

[6.5 Gestão de direitos de acesso privilegiado 11](#_Toc162363135)

[6.6 Revisão de direitos de acesso do usuário 11](#_Toc162363136)

[7 Autenticação de usuários, senhas e credenciais 12](#_Toc162363137)

[7.1 Senhas e credenciais 12](#_Toc162363138)

[8 Procedimentos operacionais 13](#_Toc162363139)

[8.1 Procedimentos específicos 13](#_Toc162363140)

[8.2 Controles de medidas de segurança 13](#_Toc162363141)

[8.3 Mitigação e controle de riscos 14](#_Toc162363142)

[9 Redes e sistemas 14](#_Toc162363143)

[10 CONFORMIDADE 15](#_Toc162363144)

[11 Aprovações 15](#_Toc162363145)

[12 Anexos e referências 16](#_Toc162363146)

# Revisão e atualização da política

## Controle de versões

|  |  |  |  |
| --- | --- | --- | --- |
| **Versão** | **Data** | **Autor** | **Notas da Revisão** |
| 1.0 | 15/03/2024 | Nilton Dionisio Guerra |  |
|  |  |  |  |

# MONITORAMENTO DA POLÍTICA

A fim de assegurar a contínua relevância e eficácia da presente política de controle de acesso, 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.

Quaisquer alterações ao conteúdo deste documento devem ser analisadas e autorizadas pelo Diretor de Segurança da Informação.

# Introdução

## Objetivo do documento

Nesta política, serão estabelecidas diretrizes para gerenciar o controle de acesso aos recursos do sistema, incluindo procedimentos para recuperação de acesso, autenticação no sistema e definição de níveis de acesso. Adotaremos o modelo de Controle de Acesso baseado em papéis (RBAC), complementado pelo uso de tokens de acesso.

## Escopo de aplicação

Esta política se estende a todos os indivíduos envolvidos em transações de vendas ou compras dentro do sistema, bem como a qualquer programador responsável por fazer modificações na plataforma.

Parte superior do formulário

## Responsabilidades

O usuário é responsável por fornecer o email correto para receber o token de acesso ao sistema, garantindo a segurança dos dados e evitando vazamentos indesejados de informação. O compartilhamento do token com terceiros é estritamente proibido.

A plataforma compromete-se a manter em sigilo os dados fornecidos pelo usuário e não os compartilhar com empresas terceiras. No entanto, reserva-se o direito de utilizar esses dados internamente para personalização de conteúdo e otimização de publicidade.

A empresa garante a emissão de tokens de acesso válidos apenas para usuários cadastrados, visando manter a integridade do ecossistema da 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.

Requisitos de negócio do controle de acesso

Ao conceder acesso a sistemas e informações, os sistemas de informação da FomeFácil devem cumprir os seguintes princípios de Controle de Acesso baseado em papéis (RBAC):

1. Função atribuída: uma entidade pode executar ou exercer permissões em um sistema somente se tiver sido atribuída uma função ou um grupo (ou seja, administrador/ vendedor ou cliente).

2. Função Autorizada: Uma função ou grupo ativo de assunto deve ser autorizado. Em conjunto com a Função Atribuída, essa regra garante que os sujeitos possam assumir apenas funções para as quais estão autorizados

3.Transação Autorizada: uma entidade pode usar determinadas permissões para executar uma ação em um sistema ou acessar informações somente se o usuário estiver autorizado a essa permissão específica, de acordo com sua atribuição de função ou grupo na hierarquia de estrutura baseada em função. Esta regra específica que a Função Atribuída e a Função Autorizada foram exercidas

Quando houver falta de orientação na Política de Controle de Acesso, os Princípios de Controle de Acesso e as práticas recomendadas devem ser seguidos.

# Princípios gerais

Esta política estabelece as diretrizes fundamentais para garantir a segurança dos recursos de informação da organização por meio de um controle de acesso eficaz, baseado nos seguintes princípios orientadores:

**Princípio do Menor Privilégio:** Os usuários terão acesso somente aos recursos necessários para desempenhar suas funções, limitando-se aos privilégios mínimos requeridos para suas atividades.

**Princípio da Necessidade de Conhecimento**: O acesso a informações sensíveis será concedido apenas a usuários com uma necessidade legítima de conhecimento, limitando-se ao mínimo essencial para suas funções.

**Princípio da Separação de Funções**: As responsabilidades e privilégios serão distribuídos de forma a evitar conflitos de interesse. Funções críticas serão separadas para garantir a prestação de contas e mitigar riscos de fraude ou abuso.

**Princípio da Autenticação Forte**: A autenticação dos usuários será realizada de forma robusta, utilizando múltiplos fatores para verificar sua identidade antes de conceder acesso aos recursos protegidos.

Esta política será aplicada em todos os aspectos do controle de acesso, desde o provisionamento inicial de acesso até o monitoramento e auditoria contínuos das atividades dos usuários. A revisão periódica garantirá que esta política permaneça alinhada com as melhores práticas de segurança e os requisitos regulamentares em constante evolução.

# Política de controle de acesso

## Responsabilidades da função de provisionamento

Designação da Função de Provisionamento: A equipe de Segurança da Informação é responsável por designar uma "Função de Provisionamento" encarregada das atividades de controle de acesso, de acordo com suas responsabilidades.

Mecanismos de Confirmação de Identidade: Implementar e gerenciar mecanismos de desafio e/ou resposta para confirmar as identidades dos usuários antes de realizar qualquer alteração em suas credenciais.

Manutenção de Lista de Acesso Autorizado: Manter uma lista centralizada de aplicativos, funções e usuários autorizados para acesso, garantindo a conformidade com as políticas de segurança da informação.

Suspensão Oportuna de Acessos: Colaborar com os gerentes de linha para suspender os direitos de acesso aos ativos de forma oportuna, quando necessário, em casos de término de contrato ou outras circunstâncias relevantes.

Procedimento para Concessão de Autorizações: Definir e seguir um procedimento formal para verificar e conceder autorizações de registro de usuário, assegurando a integridade do processo de atribuição de privilégios.

Atualização e Encerramento de Conexões de Fornecedores: Atualizar ou encerrar as conexões de fornecedores mediante notificação do proprietário do contrato ou da parte responsável pelo serviço, garantindo a conformidade com os termos acordados.

## Responsabilidades dos proprietários de ativos

Estabelecimento de Regras de Controle de Acesso: Definir, em colaboração com a equipe de "Provisionamento", regras de controle de acesso, direitos específicos e restrições apropriadas para as funções de usuário em seus ativos.

Revisão e Autorização de Solicitações de Acesso: Revisar e formalmente autorizar, em conjunto com a equipe de "Provisionamento", solicitações de acesso aos ativos de informação, assegurando que a autorização seja concedida por uma parte independente do solicitante.

Gerenciamento de Credenciais de Acesso: Trabalhar com a equipe de "Provisionamento" para identificar, remover ou desabilitar regularmente credenciais de acesso redundantes ou desnecessárias.

Estabelecimento de Controles Físicos e Lógicos: Determinar, em colaboração com o departamento de Segurança da Informação, controles físicos e lógicos para seus ativos.

Definição de Controles de Acesso Considerando a Criticidade: Estabelecer controles de acesso considerando a criticidade e o impacto nos negócios, mantendo consistência entre os direitos de acesso e os requisitos de segurança da informação.

Garantia de Conformidade Legal e Contratual: Colaborar com as áreas jurídica, de continuidade de negócios e de conformidade para assegurar que os controles de acesso estejam em conformidade com a legislação e os contratos pertinentes.

Autoridade para Concessão e Revisão de Acessos: Assegurar que a autoridade para conceder, revisar e revogar acessos seja exclusiva do proprietário do ativo ou de uma função designada e autorizada por ele.

Capacitação de Usuários com Contas Privilegiadas: Garantir que os usuários com contas privilegiadas possuam conhecimento técnico suficiente para compreender as implicações do uso de suas contas.

## Responsabilidades do usuário

Compromisso com a Política de Segurança: É fundamental compreender e aderir às declarações estabelecidas nesta política.

Responsabilidade na Proteção de Acesso: Os usuários têm a responsabilidade de desempenhar seu papel na proteção do acesso concedido, garantindo sua integridade e segurança.

Uso Adequado de Contas de Acesso: Certifique-se de que sua conta seja utilizada de forma apropriada e não seja utilizada para fins indevidos ou abusivos em relação à organização.

Respeito aos Privilégios e Controles de Acesso: Os usuários não devem modificar ou remover os controles de acesso concedidos, nem tentar elevar seus privilégios, a menos que seja aprovado por canais apropriados.

Reporte de Desvios de Controle: É importante relatar imediatamente qualquer desvio dos controles de segurança descritos neste documento para garantir a pronta correção e a manutenção da conformidade.

# Gerenciamento de acesso de usuário

## Cadastro de usuário

Configuração de Senhas Fortes: Todas as contas devem ser configuradas com senhas fortes, conforme definido na política de senhas estabelecida anteriormente.

Identificadores Únicos para Contas de Usuário: Cada conta de usuário será associada a um nome de usuário exclusivo, que não é compartilhado com outros usuários e está vinculado a um indivíduo específico.

Processamento de Solicitações com Procedimentos Formais: Todas as solicitações serão processadas de acordo com um procedimento formal, garantindo verificações de segurança apropriadas e obtenção de autorização antes da criação da conta de usuário.

Criação de Contas com Adesão a Princípios de Segurança: A criação de contas de usuário seguirá os procedimentos formais definidos e aderirá aos princípios de "segregação de funções", "necessidade de saber" e "privilégio mínimo".

## Cancelamento do registro de usuário

Suspensão Inicial de Contas de Usuário: As contas de usuário devem ser inicialmente suspensas ou desativadas e não excluídas, a fim de preservar informações de trabalho de ex-funcionários, se necessário.

Não Reutilização de Nomes de Conta de Usuário: Os nomes de conta de usuário não devem ser reutilizados para evitar confusão em investigações posteriores.

Procedimentos de Desativação de Contas: A solicitação para desativação de uma conta deve ser feita pelo próprio usuário, seja ele consumidor ou prestador de serviços. No entanto, caso o usuário seja um colaborador, é dever e responsabilidade da equipe informar sobre o desligamento da empresa.

Suspensão de Acesso ao Deixar a Organização: Quando um funcionário deixa a organização sob circunstâncias normais, seu acesso a sistemas e dados de computador deve ser suspenso no encerramento do expediente no último dia útil do funcionário.

## Provisionamento de acesso de usuário

Atribuição de Direitos de Acesso: Cada usuário receberá direitos de acesso e permissões aos sistemas e dados de computador, alinhados com os requisitos comerciais e os princípios de "privilégio mínimo" e "necessidade de saber".

Gerenciamento de Perfis Baseados em Função: Os perfis baseados em função serão criados, atribuídos e mantidos, com qualquer exceção de particularidade devidamente documentada.

Manutenção Periódica de Funções de Grupo: As funções de grupo serão periodicamente revisadas de acordo com os requisitos de negócios. Todas as alterações serão formalmente autorizadas, documentadas e controladas por meio de um processo de gerenciamento de mudanças.

## Remoção ou ajuste de direito de acesso

Atualizações de Acesso Sob Solicitação: As atualizações de direitos de acesso ou permissões serão realizadas conforme necessário e solicitadas por meio de um processo válido de gerenciamento de mudanças, como em casos de mudança de papel individual.

Remoção de Acessos Desnecessários: É garantido que acessos não mais necessários sejam removidos prontamente das contas de usuário.

## Gestão de direitos de acesso privilegiado

Identificação de Acessos Privilegiados: Os direitos de acesso privilegiado, como aqueles associados a contas de nível de administrador, devem ser claramente identificados para cada ativo.

Restrição do Uso de Contas Privilegiadas: Os usuários técnicos não devem fazer uso diário de contas de usuário com acesso privilegiado.

Atribuição de Acesso Administrativo Qualificado: Acesso a permissões de nível de administrador deve ser atribuído apenas a indivíduos qualificados, cujas funções exijam tal acesso e que tenham recebido treinamento relevante para entender as implicações de seu uso, seja técnico ou não.

Mitigação de Riscos em Rotinas Automatizadas: O uso de contas de usuário com acesso privilegiado em rotinas automatizadas, como trabalhos em lote ou de interface, deve ser evitado sempre que possível. Quando necessário, as credenciais de autenticação devem ser protegidas (por exemplo, por meio de criptografia, sem armazenamento de texto não criptografado, e com rotação regular de senhas).

## Revisão de direitos de acesso do usuário

Revisão Periódica de Contas de Acesso: Regularmente, uma pessoa designada conduzirá revisões das contas de usuário com acesso privilegiado para garantir a conformidade com esta política.

Análise Conjunta de Acesso a Ativos e Sistemas: Os proprietários de ativos e sistemas, juntamente com a equipe de Provisionamento, realizarão revisões periódicas para analisar o acesso às suas áreas de responsabilidade e identificar:

i. Pessoas que não devem ter acesso (por exemplo, abandonando)

ii. Contas de usuário com excesso de acesso para suas funções

iii. Alocações de função incorretas em contas de usuário

iv. Contas de usuário com identificação inadequada, como contas genéricas ou compartilhadas.

v. Quaisquer outras discrepâncias não conformes com esta política.

# Autenticação de usuários, senhas e credenciais

A autenticação do usuário será feita via senha, como está definido na política de senhas fortes e através de token enviado para o email do usuário, isso se aplicará tanto para o consumidor de serviços, prestador de serviços como também para os colaboradores do sistema.

## Senhas e credenciais

As credenciais de usuário só podem ser utilizadas pelas pessoas para as quais foram emitidas, não sendo permitido seu uso por terceiros.

Todas as credenciais de sistemas são consideradas informações confidenciais e não devem ser anotadas ou transmitidas sem criptografia. Isso inclui senhas, autenticadores e outras chaves privadas.

A identidade de um usuário deve ser verificada por mecanismos adequados de desafio e resposta antes de qualquer alteração em suas credenciais.

Senhas, chaves SSH e outros autenticadores criptográficos devem ser alterados caso sejam perdidos ou considerados comprometidos.

Quando possível, todas as senhas de sistemas e aplicativos devem seguir uma política de senhas fortes desenvolvida.

As senhas não devem ser codificadas ou armazenadas em formato de texto sem formatação em aplicativos de software.

O token criado e enviado para o email do usuário terá validade de 5 minutos. Após esse período, o sistema gerará outro token para acesso à conta.

# Procedimentos operacionais

## Procedimentos específicos

Para criar uma conta, o usuário deverá fornecer seu email. Antes de concluir o processo de registro, será enviado um token via email para o usuário. Este token deverá ser inserido durante o registro para confirmar a veracidade do email fornecido, que será utilizado para enviar futuros tokens. Para acessar o sistema, o usuário deverá sempre fornecer uma senha e utilizar o token enviado via email.

Parte superior do formulário

## Controles de medidas de segurança

Com relação ao controle de medidas de segurança irá ser implementado:  
Verificação de Identidade durante o Cadastro:

Antes de concluir o processo de registro, será implementada a verificação de identidade por meio do envio de um token via email para o endereço de email fornecido pelo usuário.

O usuário será obrigado a inserir este token durante o processo de cadastramento para confirmar a veracidade do email, fortalecendo assim a autenticidade das informações fornecidas.

Uso de Tokens para Acesso ao Sistema:

Para acessar o sistema, os usuários serão obrigados a fornecer uma senha e utilizar um token enviado via email para seu número de celular registrado.

O uso de dois fatores de autenticação (senha e token) aumentará a segurança do acesso, mitigando o risco de acesso não autorizado.

Monitoramento e Auditoria:

Será implementado um sistema de monitoramento e auditoria para registrar todas as tentativas de acesso ao sistema, incluindo o uso de tokens.

Os registros de acesso serão revisados regularmente para detectar e investigar atividades suspeitas ou não autorizadas.

Treinamento de Usuários:

Serão fornecidos treinamentos regulares aos usuários sobre a importância da segurança da informação e as melhores práticas para proteger suas credenciais de acesso e informações pessoais.

Atualizações e Revisões:

Esta política será revisada periodicamente para garantir sua conformidade contínua com as melhores práticas de segurança e os requisitos regulamentares aplicáveis.

Alterações significativas no ambiente de ameaças ou na infraestrutura de TI exigirão uma revisão imediata desta política para garantir sua eficácia contínua na proteção dos recursos de informação da organização.

## Mitigação e controle de riscos

Se ocorrerem mais de sete tentativas incorretas de senha ou token, o acesso ao sistema será temporariamente bloqueado por um período de 24 horas. Em caso de recorrência deste bloqueio por mais de 10 vezes, a conta será permanentemente bloqueada como medida de segurança. Para recuperar o acesso à conta após o bloqueio permanente, será necessário entrar em contato com o suporte técnico da empresa para realizar o procedimento de desbloqueio.

# Redes e sistemas

1. Os sistemas e/ou dispositivos não devem ser conectados à rede da Fome Fácil sem a autorização prévia do proprietário do ativo da Fome Fácil correspondente.

2. A Função de Provisionamento deve ser responsável por manter o controle de acesso à rede e impedir que dispositivos não autorizados acessem a rede.

# CONFORMIDADE

Todos os funcionários, prestadores de serviço ou consumidores de serviço devem aderir aos requisitos descritos neste documento, a menos que uma exceção seja identificada e exigida pelos órgãos reguladores aos quais a Fome Fácil está sujeita. Qualquer exceção ou desvio à Política de Segurança da Informação e suas diretrizes de suporte deve ser fundamentado em requisitos legislativos ou exclusivos do negócio. Solicitações de exceção à política podem ser encaminhadas ao Diretor de Segurança da Informação para avaliação. Tais solicitações devem ser devidamente documentadas, com uma avaliação de risco relacionada e submetidas ao Líder de Risco de Segurança da Informação ou seu delegado antes da implementação da exceção.

Todas as exceções ou desvios aprovados devem ser registrados e gerenciados no registro de risco e revisados anualmente. A Fome Fácil reserva-se o direito de aplicar medidas disciplinares, incluindo demissão, em relação a qualquer desvio da Política de Segurança da Informação ou outras políticas relacionadas. Dependendo da gravidade da violação, pode ser iniciado um processo de acordo com a lei local.

# Aprovações

|  |  |  |
| --- | --- | --- |
| **Cargo** | **Nome/Assinatura** | **Data** |
| [nome de cargo] | [nome/assinatura do responsável] | [data] |
|  |  |  |

# Anexos e referências

Lista documentos de apoio: legislação, regulamentações, políticas, normas e procedimentos.