

Dupla Autenticação de Cadastro



Dupla Autenticação de Cadastro

Dados da Empresa

Razão Social	MARCHA LTDA
CNPJ	58.300.812/0001-32
Endereço	Avenida Paulista, Nº 1337, Bairro Bela Vista, São Paulo-SP.
CEP	01.311-200

Informações Gerais

Título	Dupla Autenticação de Cadastro
Versão	V1.0.01
Aprovador	Diretoria Executiva
Data da Aprovação	20/01/2026
Próxima Revisão	—
Responsável pela Política	Zijie Pan
Classificação da Informação	Interna

Dupla Autenticação de Cadastro

SUMÁRIO

- 1.OBJETIVO E ESCOPO
- 2.DEFINIÇÕES
- 3.GOVERNANÇA E RESPONSABILIDADES
- 4.FLUXO DE DUPLA AUTENTICAÇÃO NO CADASTRO (KYC/MFA)
- 5.VANTAGENS DA DUPLA AUTENTICAÇÃO NO CADASTRO
- 6.OBRIGATORIEDADE EM AÇÕES CRÍTICAS
- 7.DOCUMENTAÇÃO E INTEGRAÇÃO REGULATÓRIA
- 8.DISPOSIÇÕES FINAIS

Dupla Autenticação de Cadastro

OBJETIVO E ESCOPO

I. Objetivo

Esta Política estabelece a obrigatoriedade da implementação e uso da Dupla Autenticação (2FA) ou Autenticação Multifator (MFA) como medida técnica de segurança compulsória para acesso a sistemas, ambientes e, principalmente, para a validação de identidade em Ações Críticas. O objetivo é mitigar o Risco Cibernético, a Fraude de Tomada de Conta (Account Takeover - ATO) e garantir o princípio da não-repúdio nas transações de alto impacto, reforçando a proteção dos dados e da liquidez do Gateway.

II. Escopo

Esta política de segurança é mandatória e aplica-se a:

- a. Todos os Lojistas e Parceiros que acessam o Portal Administrativo.
- b. Todos os colaboradores com acesso a ambientes de Tecnologia, repositórios de código-fonte (PI) e sistemas de liquidação.
- c. Todas as etapas do processo de onboarding (Cadastro e KYC).
- d. Todas as ações críticas que alteram dados sensíveis ou financeiros.

Dupla Autenticação de Cadastro

DEFINIÇÕES

- I. **Dupla Autenticação (2FA) / Autenticação Multifator (MFA):** Método de segurança que exige a comprovação de identidade por meio de dois ou mais fatores de categorias diferentes (conhecimento, posse, inerência).
- II. **Ação Crítica:** Qualquer alteração em dados ou execução de comando que possa resultar em perda financeira, regulatória (LGPD, BACEN) ou operacional (indisponibilidade).
- III. **Não-Repúdio:** O princípio que assegura que o usuário que realizou determinada ação (Ex: Alteração de conta de repasse) não possa negar a autoria, comprovada pelos fatores múltiplos de autenticação.
- IV. **OTP (One-Time Password):** Senha de uso único, geralmente gerada por aplicativo ou enviada por SMS/E-mail.

Dupla Autenticação de Cadastro

GOVERNANÇA E RESPONSABILIDADES

- I. **Diretoria (Alta Administração):** Responsável por aprovar os padrões tecnológicos utilizados no MFA/2FA e por garantir a alocação de recursos (TI/Segurança Cibernética) para a manutenção da infraestrutura de autenticação.
- II. **Área de Tecnologia/Segurança Cibernética:** Responsável pela implementação técnica e enforcement do MFA nos sistemas, pela gestão das chaves criptográficas de recuperação e pela garantia de que apenas métodos de autenticação seguros e modernos (Ex: App Tokens) sejam utilizados.
- III. **Área de Compliance:** Responsável por auditar a aderência de Lojistas e Parceiros à obrigatoriedade do MFA/2FA, integrando este controle aos dossiês de KYC e PLD.

Dupla Autenticação de Cadastro

FLUXO DE DUPLA AUTENTICAÇÃO NO CADASTRO (KYC/MFA)

A Dupla Autenticação é uma etapa essencial do processo de Conhecimento do Cliente (KYC) e deve ser aplicada sequencialmente para a validação da identidade do Administrador/Sócio do Lojista.

- I. Cadastro Inicial:** Coleta dos dados primários (CNPJ, Razão Social, Nome do Administrador).
- II. Primeira Verificação (Posse - E-mail):** Envio de código OTP ao endereço de e-mail fornecido, validando a posse do canal de comunicação.
- III. Segunda Verificação (Posse/Inerência - Celular/2FA):** Configuração obrigatória de um segundo fator robusto, preferencialmente um Token por Aplicativo (OTP App) ou Biometria, vinculado ao dispositivo do administrador. A conta do Lojista permanece bloqueada até que esta etapa seja concluída.
- IV. Validação Documental/Biométrica (KYC):** Etapa de Background Check e verificação biométrica (inerência) para conclusão do processo KYC, assegurando que o portador das credenciais eletrônicas é a pessoa física legitimamente identificada.

Dupla Autenticação de Cadastro

VANTAGENS DA DUPLA AUTENTICAÇÃO NO CADASTRO

A obrigatoriedade do MFA/2FA no onboarding confere à MarchaPay vantagens estratégicas e de compliance:

- I. Prevenção à Fraude de Identidade:** Impede que fraudadores usem credenciais roubadas (senha e e-mail) para ativar a conta, exigindo um segundo fator sob posse física (celular/token).
- II. Fortalecimento do KYC:** Integra o controle de autenticação ao compliance regulatório, atestando que o Lojista é quem diz ser.
- III. Não-Repúdio Reforçado:** O uso de múltiplos fatores de categorias diferentes (posse, conhecimento, inerência) gera evidência de auditoria robusta, essencial em disputas legais (Direito Civil/Empresarial) sobre a autoria de transações.
- IV. Mitigação do Risco Cibernético:** Cumpre os requisitos de segurança do BACEN, protegendo o Gateway de acessos não autorizados por falha de senha.

Dupla Autenticação de Cadastro

OBRIGATORIEDADE EM AÇÕES CRÍTICAS

Além do login inicial, o MFA/2FA é mandatório para confirmar a identidade antes de executar as seguintes Ações Críticas:

- I. Alteração de Dados de Liquidação:** Qualquer mudança na conta bancária para repasse de recebíveis do Lojista.
- II. Alteração de Credenciais de API:** Redefinição ou emissão de chaves de API que dão acesso transacional ao Gateway.
- III. Criação/Modificação de Usuário Administrador:** Concessão de novos acessos com privilégios.
- IV. Acesso a Dados Pessoais Sensíveis:** Acesso a dashboards ou sistemas internos que contenham dados de KYC/PLD.
- V. Operações de Alto Impacto (Interno):** Comandos em ambientes de Produção e Deploy de código-fonte.

Dupla Autenticação de Cadastro

DOCUMENTAÇÃO E INTEGRAÇÃO REGULATÓRIA

Esta Política de Dupla Autenticação está formalmente integrada ao Framework de Compliance da MarchaPay, sendo respaldada pelos seguintes documentos:

- I. Política de Segurança da Informação e Privacidade:** O MFA/2FA é o controle técnico primário para garantir a Confidencialidade dos dados pessoais, conforme exigido pela LGPD.
- II. Termos de Uso e Contrato do Usuário:** Esta Política e a obrigatoriedade do MFA/2FA são referenciadas nos Termos Contratuais firmados com o Lojista, estabelecendo-a como obrigação contratual para uso da plataforma.
- III. Documentação de Conformidade Regulatória:** Os procedimentos de MFA/2FA são documentados nos relatórios de conformidade (Ex: Auditorias do BACEN) como evidência da adoção de controles robustos de acesso e segurança cibernética.
- IV. Documentação Técnica e de Processos (Interno):** Os requisitos de MFA/2FA são detalhados nos manuais operacionais da Área de Tecnologia e Compliance, especificando a arquitetura de autenticação, o ciclo de vida das credenciais e os procedimentos de recuperação de acesso (sem comprometer a segurança).

Dupla Autenticação de Cadastro

DISPOSIÇÕES FINAIS

- I. **Vigência e Revisão:** Esta Política entra em vigor na data de sua aprovação pela Diretoria e deve ser revista anualmente, ou sempre que houver a incorporação de novas tecnologias de autenticação ou mudanças regulatórias.
- II. **Sanções:** A falha do Lojista em manter o MFA/2FA ativo ou a falha do colaborador em aplicá-lo resultará na suspensão imediata do acesso ao sistema e sujeitará o responsável a medidas disciplinares internas, conforme o Código de Ética e a Política de Segurança Cibernética.
- III. **Comunicação:** Esta política deve ser comunicada de forma clara a todos os Lojistas e Parceiros, reforçando o caráter mandatório do controle de segurança.