NTIDI

Transforme sua **Visão** em Realidade Digital.

GUIA 2026

Pix Seguro para Empresas

8 Golpes Reais + Checklist Antifraude

Versao: PME

Transforme sua Visao em Realidade Digital.

O que este guia entrega (e por que ele corta risco de verdade)

Perfil: **PME**. Exemplo de contexto: Distribuidora regional com 12 pessoas no administrativo e 2 no financeiro.

• Metodo 3C+ (Canal, Contexto, Conta + Cadencia) para decisao em 20 segundos

• Matriz FAV (Fraude por Alteracao de Favorecido) com limites por porte

• 8 golpes reais no Pix com sinais, bloqueios e scripts prontos para equipe

• Checklist de 10 minutos para aplicar hoje no contas a pagar

• Modelo de Pedido de Pagamento (campos antifraude) e Pacote de Evidencias

• KPIs e ritual semanal para reduzir risco sem virar burocracia

1) Metodo 3C+ - decisao sob pressao

3C: Canal, Contexto, Conta. O **+** e a **Cadencia** (o que foge do padrao). Use em toda solicitacao de Pix, antes de aprovar.

• **Canal**: veio do contato oficial do cadastro? e um canal rastreavel (email corporativo, portal, sistema)?

• **Contexto**: existe urgencia, ameaca, sigilo, pressao para 'pagar agora'?

• **Conta**: nome/CNPJ do recebedor exibido no app confere com o cadastro e o documento?

• **Cadencia**: horario, valor, recorrencia e favorecido estao dentro do normal?

Regra de travamento 2-3: 2 itens amarelos = valida; 3 ou mais = tratar como incidente (conter e revisar).

2) Matriz FAV - onde a fraude mais passa batida

A maior parte do prejuizo corporativo acontece quando o atacante consegue **alterar o favorecido** (conta, chave, QR). A Matriz FAV prioriza travar alteracoes e pagamentos fora do padrao.

Limites de aprovacao recomendados (ajuste por politica interna)	
Ate R$ 1.000	1 aprovador + registro simples
R$ 1.001 a R$ 10.000	4-olhos (2 aprovadores)
Acima de R$ 10.000	2 canais + 4-olhos + evidencia do recebedor

Excecoes que sempre sobem de nivel (qualquer porte): alteracao de favorecido, pedido fora do fluxo, urgencia, fora do horario, ou pedido por WhatsApp/voz.

3) As 8 fraudes Pix mais recorrentes - sinais, bloqueios e scripts

Abaixo estao 8 padroes praticos. O objetivo nao e decorar golpe; e padronizar o bloqueio.

1. Falso fornecedor (alteracao de favorecido)

Exemplo PME: pedido chega no WhatsApp do dono as 18h: 'mudamos a conta, paga hoje para liberar mercadoria'.

Sinais de alerta

• Mudanca de conta/QR 'de ultima hora'

• Pressao por prazo/desconto

• Contato fora do cadastro (numero ou email novo)

Bloqueios (controle operacional)

• Politica 'Mudou favorecido, trava'

• Confirmacao em 2 canais (telefone do cadastro + email corporativo)

• Registrar quem confirmou, quando e quais dados

Script pronto: Script (telefone): Confirmando por politica antifraude: a conta/QR de recebimento mudou para [X]? Confirmo valor [R$] e nota [Y].

2. Comprovante Pix falso (print/PDF)

Exemplo PME: cliente diz 'ja paguei' e manda print para retirar produto imediatamente.

Sinais de alerta

• Pedido de liberacao imediata com print

• Comprovante sem validacao no extrato/app

• Inconsistencias de nome/horario/ID

Bloqueios (controle operacional)

• Regra: print nao confirma pagamento

• Liberar apenas com confirmacao no extrato/app

• Status interno: 'Confirmado no extrato'

Script pronto: Script (atendimento): Por seguranca, liberamos somente apos confirmacao no extrato. Em instantes retornamos.

3. Pix errado + pedido de devolucao

Exemplo PME: desconhecido diz que transferiu errado e pede devolucao para outra chave 'do contador'.

Sinais de alerta

• Pedido para devolver por um novo Pix

• Pressao emocional ou 'urgencia'

• Conta de devolucao diferente do remetente

Bloqueios (controle operacional)

• Devolver somente pela funcao 'Devolver' do app

• Em suspeita de golpe, acionar o banco e perguntar sobre MED

• Nunca 'pix de ajuste' manual

Script pronto: Script (financeiro): Devolucao so via funcao Devolver do Pix. Se for fraude, acionamos o banco pelo procedimento.

4. Falsa central / falso funcionario do banco

Exemplo PME: ligacao dizendo que 'detectou invasao' e orienta fazer Pix para 'conta segura'.

Sinais de alerta

• Ligacao dizendo 'invasao' ou 'bloqueio'

• Pedido de codigo/token/instalacao

• Orientacao para fazer Pix 'para conta segura'

Bloqueios (controle operacional)

• Protocolo Zero Codigo: nunca informar codigos

• Desligar e ligar no numero oficial

• Registrar protocolo e canal usado

Script pronto: Script: Nao confirmo dados por ligacao recebida. Vou retornar pelo canal oficial do banco.

5. QR adulterado (QR falso / quishing)

Exemplo PME: QR recebido em PDF no WhatsApp; no app aparece recebedor diferente do fornecedor.

Sinais de alerta

• QR recebido por canal incomum

• QR que abre site estranho

• Nome/CNPJ do recebedor nao confere

Bloqueios (controle operacional)

• Antes de confirmar: conferir nome/CPF/CNPJ do recebedor

• Preferir QR gerado no portal oficial do fornecedor

• Para valores altos: 2 canais + evidencia do recebedor

Script pronto: Script: Vou validar o recebedor exibido no app. Se nao bater com o cadastro, o pagamento e bloqueado.

6. Falsa venda / fornecedor novo (reserva por Pix)

Exemplo PME: oferta com desconto forte pede Pix para reservar estoque, sem nota/contrato.

Sinais de alerta

• Oferta fora do padrao

• Pedido de Pix para 'reservar' ou 'liberar'

• Fornecedor sem contrato/nota/portal

Bloqueios (controle operacional)

• Regra do Fornecedor Elegivel: Pix so para fornecedor cadastrado

• Excecao exige validacao minima (CNPJ, contrato/nota, canal oficial)

• Pausa antifraude para compras emergenciais

Script pronto: Script (compras): Para pagamento, precisamos do CNPJ, nota e confirmacao no canal oficial. Sem isso, nao aprovamos.

7. Sequestro/Clonagem de WhatsApp (pedido de pagamento)

Exemplo PME: numero do gerente conhecido muda e pede Pix 'sigiloso' para terceiro.

Sinais de alerta

• Mensagem pedindo sigilo/urgencia

• Mudanca de numero do contato conhecido

• Pedido para enviar Pix para conta de terceiro

Bloqueios (controle operacional)

• Regra: pagamento nao nasce no WhatsApp

• Confirmar por telefone do cadastro

• Ativar 2FA no WhatsApp Business e treinar equipe

Script pronto: Script (WhatsApp): Por politica, confirmamos pagamentos por ligacao no numero cadastrado. Envie nota e CNPJ; retorno pelo canal oficial.

8. Boleto/QR Pix trocado (documento adulterado)

Exemplo PME: boleto/QR chega por email fora do dominio do fornecedor; beneficiario no app nao confere.

Sinais de alerta

• Boleto/QR recebido por email suspeito

• Codigo/QR diferente do historico

• Beneficiario divergente no app

Bloqueios (controle operacional)

• Conferir beneficiario/destinatario no app antes de pagar

• Aceitar boletos somente por canais controlados

• Registrar evidencias do arquivo recebido e metadados

Script pronto: Script: Antes de pagar, confirmo o beneficiario exibido no app. Se divergir, bloqueio e aciono o fornecedor pelo canal oficial.

4) Checklist de 10 minutos (aplicacao imediata)

Use este checklist para cortar as falhas mais caras em um unico dia. Ele foi desenhado para funcionar mesmo com pressa e cansaco.

• Ative a regra: print nao confirma pagamento (liberacao so com extrato/app).

• Implemente o Metodo 3C+ como passo obrigatorio antes de qualquer Pix.

• Trave alteracao de favorecido: exigir confirmacao em canal oficial + registro.

• Defina limites de aprovacao por valor e risco (Matriz FAV).

• Adote 'pausa antifraude' para urgencias: 5 a 10 minutos antes de pagar.

• Exija evidencia do recebedor exibido no app (nome/CNPJ) para valores altos.

• Padronize scripts (telefone/email/WhatsApp) e treine equipe.

• Crie um local unico para registrar pagamentos e evidencias (planilha/ERP/ticket).

• Defina quem aciona o banco e como registrar protocolo em suspeita de fraude.

• Agende ritual semanal de revisao (KPIs) e ajuste de limites.

5) Treino em 1 minuto (roteiro para a equipe)

• Regra 1: pagamento nao nasce no WhatsApp.

• Regra 2: se mudou favorecido, trava e valida em 2 canais.

• Regra 3: confirme o recebedor no app antes de aprovar.

• Regra 4: urgencia e sinal de risco. Pausa obrigatoria.

• Regra 5: se suspeitar, nao 'tenta resolver sozinho'. Aciona o protocolo.

6) Modelo - Pedido de Pagamento (campos antifraude)

Copie e cole estes campos no seu formulario interno (Google Forms, ERP, planilha ou sistema). O objetivo e impedir bypass.

• Solicitante (nome, area) e motivo do pagamento

• Fornecedor/recebedor (nome, CNPJ) e chave Pix

• Valor, vencimento e anexos (nota/contrato)

• Canal de origem do pedido (ERP/email corporativo/portal). WhatsApp = nao permitido

• Houve alteracao de favorecido nos ultimos 90 dias? (sim/nao)

• O recebedor exibido no app confere com o cadastro? (sim/nao) - anexar evidencia

• Aprovacao 1 (nome, data) e Aprovacao 2 (quando aplicavel)

• Observacoes de risco (urgencia, fora do horario, excecao)

7) Protocolo de resposta + Pacote de Evidencias

Quando a suspeita surgir, tempo e disciplina importam. O objetivo e conter perda, preservar evidencias e acelerar acao com banco e auditoria.

• Conter: congelar pagamentos relacionados por 15 minutos e revisar o favorecido/valor/canal.

• Registrar: anotar ID da transacao, recebedor exibido no app, horarios, aprovadores e canal.

• Acionar: contatar o banco por canal oficial e registrar protocolo. Em fraude, perguntar sobre MED.

• Preservar: salvar conversas, emails, arquivos e anexos (sem editar) e armazenar em pasta segura.

• Aprender: abrir incidente interno e ajustar travas (limites, 2 canais, scripts).

Pacote de Evidencias (minimo): ID Pix, dados do recebedor exibidos no app, comprovacao de aprovacao (quem/quando), conversa completa, documento (nota/contrato), e protocolo do banco.

8) KPIs + Ritual semanal (reduzir risco sem travar operacao)

Foco em travas simples, sem burocracia: reduzir risco sem travar a operacao.

KPIs recomendados

• % de pagamentos com alteracao de favorecido

• % de pagamentos fora do horario padrao

• Numero de travas acionadas por semana (por motivo)

• Tempo medio de validacao (nao pode virar gargalo)

• Incidentes por canal (WhatsApp, email, ERP, portal)

• Top 10 fornecedores com mais mudancas de dados

Ritual semanal 20-10-5 (global-friendly)

• 20 min - revisar travas acionadas e incidentes (o que tentou passar).

• 10 min - revisar termos e canais de origem (bypass por WhatsApp/email pessoal).

• 5 min - ajustar limites/roteiros e comunicar 1 aprendizagem para a equipe.

Fechamento

Pix seguro em empresa e processo. Quanto mais previsivel o seu fluxo, mais caro fica para o golpista operar. Este guia existe para padronizar a defesa, nao para depender de 'atencao perfeita'.

NTIDI - ntidi.com.br | antigolpecontabil.com