POLÍTICA DE PREVENÇÃO A FRAUDES E GOLPES

NTQA	0060	-	00
SIGLA	NÚMERO/PARTE		REVISÃO

Data da Homologação:	10/09/2025

Elaboração:	Aprovação:	Localização:
Controles Internos	Eduardo Martins Comitê de Ética	Central de Serviços Grupo ENM

1.0 OBJETIVO

Estabelecer diretrizes e orientações para prevenir, identificar e responder a situações de fraude ou golpe que possam ocorrer no ambiente corporativo, protegendo o Grupo ENM, seus colaboradores, clientes, fornecedores e demais partes interessadas.

2.0 DOCUMENTOS COMPLEMENTARES

NTQA-0018 – Política de Compras
NTQA-0052 – Política de Senhas
PROC-CORP-0214 - Procedimento para confirmação de dados na primeira compra e mudança de conta bancária
PROC-CORP-0273 - Alteração de endereço de entrega e/ou retirada de mercadoria - Automotivo

3.0 TERMOS E DEFINIÇÕES

CPF: Cadastro Nacional de Pessoa Física

CNPJ: Cadastro Nacional de Pessoa Jurídica

Fraude: ato intencional de enganar, omitir ou distorcer informações para obter vantagem indevida ou causar prejuízo a terceiros. Geralmente ocorre dentro da própria organização ou com participação de alguém que tem acesso legítimo a recursos ou informações.

Golpe: tentativa externa ou interna de enganar alguém com o objetivo de obter informações, valores ou benefícios de forma ilícita. Geralmente vem de fora (mas pode ter participação interna) e é mais pontual, visando enganar alguém para obter dados, dinheiro ou bens rapidamente.

Informações sensíveis: dados que, se forem acessados, usados ou divulgados sem autorização, podem causar prejuízo financeiro, danos à reputação ou violar a privacidade de uma pessoa ou empresa.

Phishing: é um tipo específico de golpe, normalmente digital, usado para roubar informações sensíveis (senhas, dados bancários, documentos) através de e-mails, sites ou mensagens falsificadas.

TI: Setor responsável pela Tecnologia da Informação

Token: código único e temporário usado para autenticar ou autorizar uma ação, como acessar um sistema, confirmar uma transação ou validar uma identidade.

4.0 APLICAÇÃO

Esta política se aplica a todas as Unidades de Negócio do Grupo ENM.

5.0 ATIVIDADES, RESPONSABILIDADES E AUTORIDADES

Atividades	Responsabilidades	Autoridades
Observar e estar atento a possíveis fraudes e golpes	Todos os colaboradores	Todos os líderes
Comunicar imediatamente à liderança possíveis fraudes e golpes suspeitos ou identificados	Todos os colaboradores	Todos os líderes
Reportar à TI ou ao Comitê de Ética possíveis fraudes e golpes suspeitos ou identificados	Todos os colaboradores	Todos os líderes
Investigar possíveis fraudes e golpes	Comitê de Ética, equipe do Financeiro e equipe de TI	Comitê de Ética Gerência de TI Gerência Financeira

5.1 Disposições Gerais

Em nenhum momento será admitido, a qualquer profissional ou terceiros, invocar o desconhecimento desta norma para justificar violações ou falta de cumprimento dela. A inobservância às normas estabelecidas sujeita o infrator e aqueles que colaborarem com ele, à sansões previstas nas regulamentações da área de Gestão Humana ou nos contratos pelo qual o usuário se vincula à empresa, sem prejuízo a outras ações administrativas, legais e penais, no caso de eventuais danos e prejuízos causados a empresa ou a terceiros.

6.0 DESCRIÇÃO DAS ATIVIDADES

Esta Política, é parte integrante do Programa de Integridade do Grupo ENM, e tem como base os seguintes princípios:

Tolerância zero: O Grupo adota postura rígida e inegociável contra qualquer forma de fraude ou golpe, seja praticada por colaboradores, fornecedores, clientes ou terceiros. Toda ocorrência será investigada de forma imparcial e caso confirmado, serão aplicadas medidas disciplinares internas e/ou encaminhamento às autoridades competentes. Não existem exceções, independentemente de cargo, tempo de casa ou relação comercial.

Responsabilidade compartilhada: A prevenção a fraudes e golpes é um dever coletivo. Cada colaborador deve estar atento a situações suspeitas e seguir as orientações desta política, comunicando imediatamente à liderança qualquer indício ou tentativa. Pequenas irregularidades podem ser sinais de problemas maiores. A omissão diante de indícios de fraude ou golpe também será considerada descumprimento desta política.

Confidencialidade e proteção contra retaliação: Qualquer denúncia ou relato de suspeita será tratado de forma sigilosa, preservando a identidade do denunciante, salvo exigência legal em contrário. O Grupo garante que nenhum colaborador sofrerá retaliação, punição ou tratamento desfavorável por relatar de boa-fé uma possível fraude ou golpe. Denúncias infundadas feitas de má-fé, com intenção de prejudicar alguém, poderão gerar medidas disciplinares.

Transparência e integridade: As decisões, comunicações e processos internos devem ser conduzidos com clareza, evitando brechas que possam permitir a ocorrência de fraudes ou golpes. Documentos e registros devem refletir fielmente as operações. Toda transação, seja financeira ou cadastral, deve ser autorizada, registrada e passível de auditoria.

6.1 Medidas preventivas

6.1.1 Sigilo de informações

Nunca compartilhe senhas, códigos de acesso, tokens ou dados pessoais e/ou corporativos com terceiros. Mesmo que entre funcionários do Grupo. Utilize senhas fortes (mistura de letras, números e caracteres especiais) e troque-as periodicamente, conforme orientações previstas na Política de Senhas (NTQA-0052).

Sempre bloqueie o computador e dispositivos móveis ao se afastar da estação de trabalho, mesmo que por curto período. Assim você previne que informações sejam compartilhadas de forma indevida.

Sempre que possível armazene documentos físicos sigilosos (contratos, relatórios, outros) em armários com chave ou salas de acesso restrito. Ao descartar documentos certifique-se que não há dados e informações sigilosas ou que possam ser utilizadas por pessoas de má fé.

Cuidado com conversas em locais públicos (corredores, restaurantes, outros) que possam expor informações sensíveis a pessoas não autorizadas.

Atenção com reuniões remotas (online). Certifique-se de não compartilhar a tela com informações sensíveis ou sigilosas especialmente se a reunião estiver sendo gravada.

6.1.2 Atenção a e-mails e mensagens

Fraudes e golpes por e-mail, mensagens de texto ou aplicativos de conversa instantâneas (como whatsapp e telegram) são comuns e podem ser difíceis de identificar. Para se proteger observe as orientações a seguir:

a) Não clique em links suspeitos ou abra anexos enviados por remetentes desconhecidos ou não esperados.

b) Verifique cuidadosamente o endereço do remetente e observe alterações sutis que imitam o endereço legítimo. *Exemplo:* Correto: financeiro@empresa.com.br Falso: financeiro@empresa**a**.com.br ou financeiro@empresa.com

c) Desconfie de e-mails ou mensagens com erros de ortografia, gramática estranha ou formatação incomum, especialmente quando o remetente afirma ser de uma instituição oficial.

d) Nunca informe dados pessoais ou corporativos (senhas, números de documentos, dados bancários) em resposta a e-mails ou mensagens não solicitadas. *Exemplo:* um suporte técnico não solicitado.

e) Cuidado com mensagens que criam senso de urgência ou medo para forçar uma ação rápida. *Exemplo:* “Sua conta será bloqueada em 1 hora se não confirmar seus dados.”

f) Sempre confirme solicitações incomuns por um canal oficial e independente antes de agir. *Exemplo:* se receber um e-mail do “diretor da empresa” pedindo transferência urgente, ligue para ele ou para o financeiro para validar.

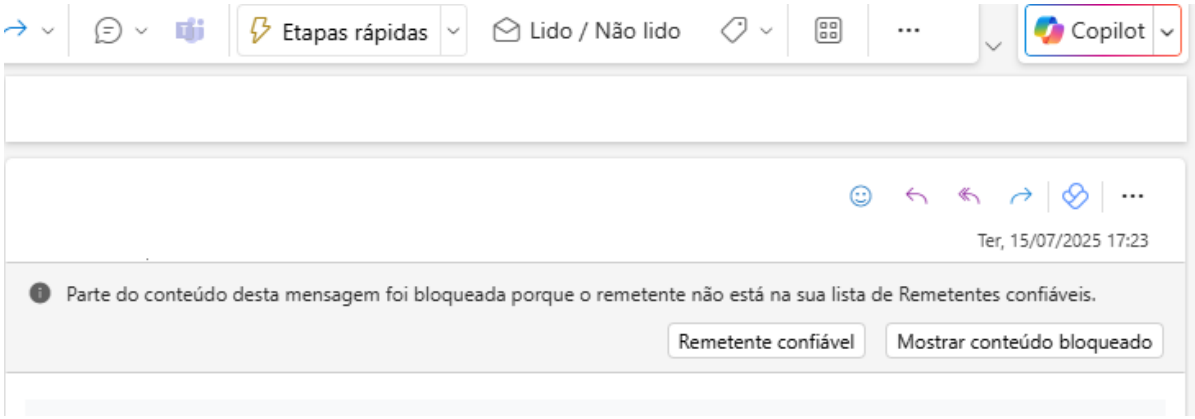
g) Passe o mouse sobre links (sem clicar) para visualizar o endereço real antes de acessá-lo. *Exemplo:* link escrito “www.seubanco.com.br” que, ao passar o mouse, mostra http://outrodominio.ru/login.

h) No caso de mensagens instantâneas, verifique se o número é realmente oficial. Empresas legítimas geralmente usam contas comerciais verificadas (selo). Golpistas podem usar fotos e nomes iguais aos de colegas para se passar por eles.

i) Ao receber anexos inesperados, mesmo que de remetente conhecido, confirme antes de abrir. *Exemplo:* arquivo chamado “Orçamento_2025.zip” vindo de um fornecedor que não costuma enviar arquivos compactados.

Ao receber e-mails ou mensagens suspeitas elas deverão ser encaminhadas à TI, via ticket no Movidesk, para análise, antes de qualquer ação.

Nota: Atenção! O outlook, ferramenta oficial para envio e recebimento de e-mails, alerta quando o remetente não envia e-mails frequentes, conforme exemplo abaixo. **Este é um sinal de alerta importante!**



6.1.3 Pagamentos e alterações em dados bancários

Os golpes que envolvem alteração de dados bancários ou pedidos de pagamento indevidos podem gerar prejuízos significativos. Como prevenção observe as seguintes diretrizes:

a) Confirme sempre os dados bancários antes de efetuar qualquer pagamento, mesmo que já tenha pago anteriormente para aquele fornecedor. *Exemplo:* antes de pagar um boleto, confira o nome do beneficiário no campo “cedente”. Ele deve coincidir exatamente com o nome do fornecedor no contrato ou cadastro. Mais detalhes a serem observados nos boletos disponível no Anexo 1 deste documento.

b) Nunca efetue alterações cadastrais ou pagamentos baseados apenas em e-mails ou mensagens. Valide a solicitação por pelo menos um canal diferente daquele solicitado. *Exemplo:* caso tenha recebido uma solicitação por e-mail ou mensagem entre em contato pelo telefone **cadastrado no sistema** (nunca aquele informado no e-mail) confirmando a solicitação de alteração. Se o pagamento for por regido por um contrato, é necessário um termo aditivo alterando as informações de pagamento, antes de realizá-lo.

c) Fique atento a pedidos de urgência ou pressão para concluir o pagamento rapidamente, pois esse é um comportamento típico de golpistas. *Exemplo:* “Se não pagar agora, vamos cancelar seu pedido” ou “Precisamos que o valor seja depositado em outra conta, mas tem que ser hoje”.

d) Desconfie de mudanças de conta bancária, especialmente se o novo banco for diferente do habitual. Golpistas costumam indicar contas de bancos digitais ou de pessoas físicas para receber valores. Caso seja necessária a alteração legítima, exija documentação formal assinada e validada pelo responsável pelo recebimento.

e) Sempre utilize contas e meios de pagamento registrados no sistema da empresa. Evite efetuar pagamentos “fora do fluxo oficial” sem autorização formal.

f) No caso de pagamento via PIX, confira atentamente: Nome e CNPJ/CPF do destinatário; Banco recebedor; Se o favorecido é pessoa física, questione o motivo.

g) Mantenha registros de todas as transações (comprovantes, e-mails de solicitação, notas fiscais) para possibilitar auditoria e rastreabilidade.

h) Em caso de dúvida ou suspeita, interrompa imediatamente o processo e comunique ao gestor direto ou ao setor financeiro para análise.

Um golpe frequente é do falso teste PIX. Acontece quando um golpista se passa por cliente ou fornecedor e solicita que seja feito um teste de transferência via PIX para “confirmar que a conta está funcionando” ou “validar o sistema de pagamento”. Na prática, o valor enviado nunca retorna. O suposto “teste” é, na verdade, um pagamento real para a conta do golpista. Lembre-se: qualquer transferência via PIX, mesmo de R$ 1,00, é imediata e irreversível. Se houver dúvida, valide a solicitação por telefone oficial ou canal formal de atendimento.

6.1.4 Compras e contratações

As fraudes e golpes em compras e contratações podem ocorrer tanto na escolha de fornecedores quanto na execução de contratos e pagamentos. Para prevenir riscos observe as seguintes orientações:

a) Realize cotações apenas com fornecedores previamente homologados pela empresa, que passaram por análise documental, financeira e de compliance. Essa etapa evita contratação de empresas fantasmas, com histórico de irregularidades ou incapacidade técnica.

b) Verifique a idoneidade do fornecedor antes de qualquer contratação. Conferir CNPJ, situação cadastral na Receita Federal e certidões negativas, além de consultar listas de sanções, processos judiciais ou notícias negativas.

c) Seguir as cotações mínimas estipuladas na Política de Compras (NTQA-0018) para cada aquisição, garantindo transparência e competitividade.

d) Evite tratar negociações comerciais por canais não oficiais, como mensagens em números pessoais, redes sociais ou e-mails particulares. Utilize sempre o e-mail corporativo ou plataformas homologadas pela Grupo. Isso mantém o histórico e facilita auditorias.

e) Não aceite propostas ou acordos informais sem registro no sistema corporativo. Golpistas podem enviar arquivos manipulados ou alterar condições verbalmente.

f) Exija que todas as propostas e documentos estejam em papel timbrado ou formato eletrônico com assinatura digital válida. Documentos sem identificação ou sem dados completos podem indicar tentativa de fraude.

g) Cuidado com fornecedores que pedem pagamento antecipado integral sem garantias contratuais. Sempre que possível, utilize condições de pagamento vinculadas à entrega ou execução do serviço.

h) Formalize todas as negociações em contrato, e-mail ou documento equivalente, detalhando prazos, valores, condições de pagamento e penalidades. Evite acordos apenas por telefone.

i) Acompanhe a execução do contrato e registre não conformidades. Empresas fraudulentas podem entregar materiais de qualidade inferior ou quantidade menor do que a contratada.

6.1.5 Primeira venda para novos clientes

Clientes que realizam a primeira compra com o Grupo exigem atenção especial, pois é neste momento que há maior risco de fraude, inadimplência ou golpes. Para mitigar esses riscos, é necessário seguir os seguintes cuidados:

a) Solicitar todas as informações cadastrais obrigatórias, incluindo: razão social, CNPJ, endereço completo, contatos, e-mails corporativos e nome do responsável pelas compras.

b) Confirmar a situação cadastral do CNPJ junto à Receita Federal e verificar se o endereço informado existe e corresponde ao cliente.

c) Realizar análise de crédito antes de liberar condições de pagamento a prazo.

d) Para clientes sem histórico, priorizar pagamento antecipado, à vista ou com garantia.

e) Em caso de venda a prazo a entrega do produto deverá ser, obrigatoriamente, no endereço cadastral do cliente, para confirmação. **Não é permitido utilizar a modalidade de Cliente Retira na primeira compra.**

f) Evitar liberar grandes quantidades ou valores elevados até consolidar um histórico de compras e pagamentos.

g) Desconfiar de clientes que se comunicam apenas por e-mail genérico (ex.: gmail, hotmail) ou que evitam contatos diretos por telefone ou videoconferência.

h) Atentar-se a divergências entre o local de entrega e o endereço cadastrado.

6.1.6 Recebimento utilizando cheque

Apesar da redução no uso de cheques, eles ainda podem ser alvo de fraudes, especialmente em transações comerciais que envolvem valores altos ou clientes novos.

A fraude pode ocorrer de diferentes formas, como: cheques sem fundos (emitidos sem saldo suficiente); cheques falsificados (dados ou assinaturas adulteradas); cheques roubados ou extraviados (emitidos por pessoas não autorizadas) ou; alteração de valor ou data após a emissão.

Observe as seguintes diretrizes para evitar riscos envolvendo recebimentos com cheque.

a) Identificação do emitente. Solicitar documento de identidade e confirmar se o nome e a assinatura correspondem aos dados do cheque. Para pessoa jurídica, verificar se quem assina tem poderes legais para isso.

b) Validação do cheque. Conferir número do banco, agência e conta para verificar possíveis inconsistência. Consultar se há histórico de sustação, roubo ou extravio junto à instituição financeira.

c) Analisar as informações do cheque com a linha no seu rodapé, conforme exemplo no Anexo 2 desta Política.

d) Análise física do documento. Observar qualidade do papel, impressão, marca d'água e elementos de segurança. Desconfiar de rasuras, escrita em caneta diferente ou alteração no valor/data.

e) Evitar liberar mercadoria antes da compensação efetiva do cheque, especialmente em valores altos ou clientes novos.

6.2 Phishing

O Phishing é um tipo de golpe no qual criminosos se passam por pessoas ou empresas legítimas para enganar a vítima e obter informações confidenciais, como senhas, dados bancários, números de cartão ou informações corporativas.

Geralmente, ocorre por meio de e-mails, mensagens instantâneas, redes sociais ou sites falsos que imitam páginas oficiais.

Os riscos envolvidos neste tipo de golpe incluem: roubo de dados pessoais e corporativos que podem ser usados para fraudes financeiras ou invasão de sistemas; instalação de malwares (vírus, e outros) no computador ou celular; perda financeira direta através de transferências, compras não autorizadas ou desvio de pagamentos e; exposição de informações sigilosas da empresa, comprometendo clientes, fornecedores e a reputação institucional.

Fique atento, verifique o endereço do remetente e procure por alterações sutis; passe o mouse sobre links antes de clicar para visualizar o endereço real e verificar se é legítimo; não abra anexos inesperados ou enviados por remetentes desconhecidos; desconfie de mensagens com erros de ortografia, formatação incomum ou que gerem urgência; nunca informe senhas ou dados sigilosos em resposta a e-mails ou mensagens; acesse sites digitando o endereço no navegador em vez de clicar em links recebidos por mensagem e; utilize filtros antispam e soluções de segurança recomendadas pelo setor de TI.

6.2.1 Spear phishing

O spear phishing é um tipo de ataque cibernético que visa um indivíduo, grupo ou organização específica, utilizando técnicas de engenharia social para manipular as vítimas a revelar informações confidenciais, baixar malware ou enviar dinheiro a um invasor. Ao contrário do phishing comum, que é um ataque em massa, o spear phishing é altamente direcionado e personalizado, tornando-o mais convincente e difícil de detectar.

6.3 Como agir em caso de suspeita

Ao identificar ou desconfiar de uma possível fraude ou golpe, o colaborador deve agir com rapidez, cautela e seguindo o protocolo abaixo.

a) Interromper imediatamente a ação solicitada. Não efetuar pagamentos, transferências ou autorizações até que a solicitação seja confirmada por canais oficiais. Não clicar em links nem abrir anexos suspeitos. Em compras ou contratações, suspender a negociação até validar a legitimidade do fornecedor.

b) Registrar e preservar todas as evidências. Salvar e-mails recebidos (não deletar). Fazer prints de tela de mensagens, conversas ou sites suspeitos. Guardar cópias de documentos, boletos, comprovantes ou propostas recebidas. Anotar data, hora, nome das pessoas envolvidas e resumo da situação.

c) Comunicar imediatamente aos responsáveis. Acionar o gestor direto e informar todos os detalhes. Enviar evidências para o setor de TI, Controles Internos e Jurídico, conforme a natureza do caso.

d) No caso de incidentes digitais, informar também o time de Tecnologia da Informação para bloqueio e análise.

e) Registrar no Canal de Respeito e Ética (quando aplicável). Utilizar o canal oficial da empresa para formalizar o relato, garantindo tratamento sigiloso e registro do caso. Informar de forma objetiva: o que aconteceu, quando, como foi identificado e quais ações já foram tomadas. Envie todas as evidências disponíveis.

f) Evitar alertar o suspeito ou divulgar amplamente a situação. Não confrontar a pessoa diretamente, caso seja um possível envolvido interno. Manter o sigilo para não prejudicar a investigação.

g) Colaborar com a apuração. Fornecer todas as informações adicionais solicitadas durante a investigação. Disponibilizar documentos, registros ou dispositivos que possam conter provas.

7.0 FORÇA MAIOR

Todas as prerrogativas desta Política deverão ser respeitadas, salvo em casos de força maior e com a aprovação da Diretoria e Presidência.

8.0 GESTÃO DA POLÍTICA

A área de Controles Internos em conjunto com a área responsável por esta política serão as responsáveis pela manutenção e atualização desta Política com a aprovação da Presidência.

9.0 BIBLIOGRAFIA

N/A

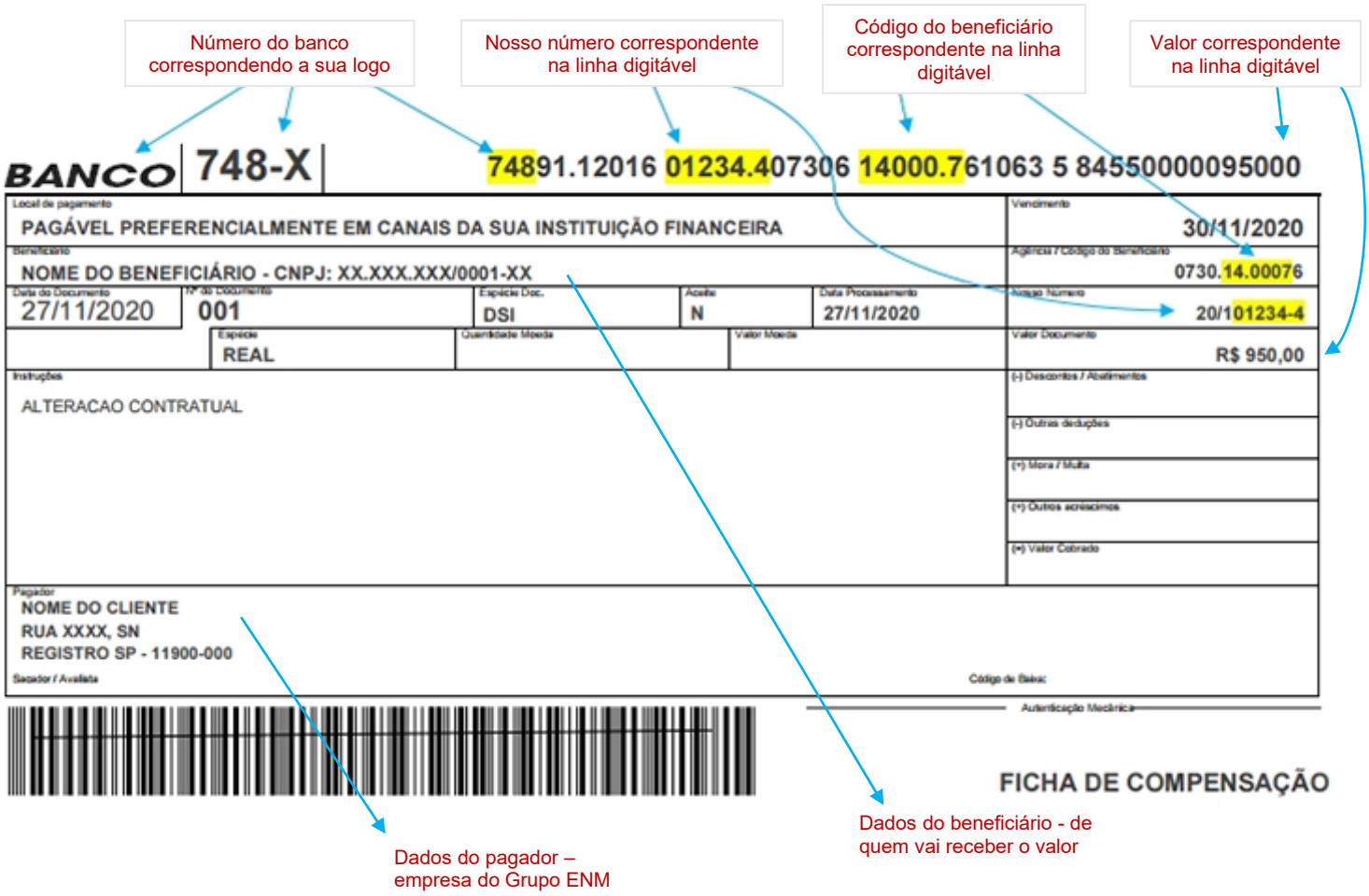
10.0 LISTA DE ANEXOS

Anexo 1: Verificação de boleto antes do pagamento

Anexo 2: Verificação de cheque antes do recebimento

Anexo 1: Verificação de boleto antes do pagamento

Antes de realizar o pagamento de qualquer boleto, verifique as informações nele apresentadas, conforme imagem abaixo.



Anexo 2: Verificação de cheque antes do recebimento