DEFESA DO CIDADÃO

O GUIA DA OAB/RN CONTRA FRAUDES BANCÁRIAS

OAB
RIO GRANDE DO NORTE
Comissão de Direito Bancário e Instituições Financeiras

DIRETORIA DO CONSELHO SECCIONAL - 2025/2027

PRESIDENTE
Carlos Kelsen Silva dos Santos

VICE-PRESIDENTE
Bárbara Paloma Fernandes de Vasconcelos Bezerra

SECRETÁRIO-GERAL
Ricardo Victor Pinheiro de Lucena

SECRETÁRIO-GERAL ADJUNTO
Marcos Aurélio Santiago Braga

DIRETORA-TESOUREIRA
Marília Almeida Mascena Bezerra

PROJETO GRÁFICO E DIAGRAMAÇÃO
Assessoria de Comunicação e Marketing

REALIZAÇÃO

RIO GRANDE DO NORTE

COMISSÃO DE DIREITO BANCÁRIO E INSTITUIÇÕES FINANCEIRAS

PRESIDENTE
Bruna Paula da Costa Ribeiro

VICE-PRESIDENTE
Jonilson Vilela Cid Júnior

SECRETÁRIO
Neffer André Torma Rodrigues

MEMBROS

Algacy Chaves de Almeida Junior
Álvaro Andriellys de Brito Alves
Alyssa Geórgia Bezerra e Silva
Ana Carolina Viana Nascimento
Ana Carolyne Barbosa de Araujo
Andressa Baranoski Mello
Anne Karolline Davin de Morais
Antônio Uemerson de Carvalho
Arlisson Pereira da Silva
Arthur Augusto Alves de Almeida
Brígida Brenda Faustino de Oliveira
Bruno Pinheiro de Lima Filho
Christiane Serejo Cardoso
Danielle Costa Alves
Douglas Rodrigues da Silva
Gabriel Carvalho Rodrigues de Oliveira
Giovane Victor Nascimento da Silva
Hellen Sthefane dos Santos Fernandes
Ingrid Quirino Ribeiro
Itamara Pinheiro Rodrigues
Jesebel Lorena Batista Oliveira da Silva
João Vinícius Lucena Lopes
João Vitor de Araujo Pereira
José Alberto Veloso de Carvalho
José Leonardo de Araújo Jales
Lorena Silva de Moraes
Luana Noel da Silva
Luciana Lucena Bezerra de Azevedo Galvão
Luna Raquel Acurcio Almeida
Marcos Délli Ribeiro Rodrigues
Maria do Socorro Freire Câmara
Melissa Cristine de Oliveira e Santos
Michelle Dantas Ferreira
Natália Ribeiro Linhares
Pedro Henrique Oliveira da Costa
Raulisson Bruno Xavier da Silva
Renata Soares Dantas Viana
Ricardo Luiz Paiva Medeiros
Rodrigo Cavalcanti
Shirley Saionara Linhares de Oliveira
Sthéfanie de Melo Medeiros Queiroz
Thiago Marques Calazans Duarte
Vitoria Machado Domingo
Weuder Martins Câmara
Wilton de Medeiros Lima

PREFÁCIO

Vivemos um momento em que a tecnologia **transformou a forma como nos comunicamos, trabalhamos e administramos** nossas finanças. Essa evolução trouxe inúmeros benefícios, mas também abriu espaço para novas ameaças. Os golpes bancários, cada vez mais sofisticados, passaram a fazer parte da realidade cotidiana, atingindo milhares de cidadãos — em especial os mais vulneráveis.

Diante desse cenário, a advocacia potiguar, por meio da Comissão de Direito Bancário da OAB/RN, apresenta esta cartilha como um **instrumento de defesa e conscientização**. Mais do que informar, **este material tem a missão de capacitar a sociedade a reconhecer os principais golpes, prevenir-se e agir corretamente diante de situações de risco.**

Acreditamos que o **conhecimento é a ferramenta mais poderosa contra a fraude**. Ao unir linguagem acessível, exemplos práticos e orientações objetivas, esta cartilha busca transformar informação em proteção, fortalecendo a confiança da população no ambiente digital e bancário.

Trata-se de um **esforço coletivo que reflete o compromisso da OAB/RN com a cidadania e com a construção de uma sociedade mais segura**. Que este guia seja utilizado como referência e partilhado amplamente, cumprindo sua função de multiplicar conhecimento e reduzir os danos causados pela criminalidade digital.

SUMÁRIO

1

A ENGENHARIA SOCIAL DA FRAUDE

A criminalidade bancária atual não se resume a simples tentativas amadoras de enganar o cidadão. O cenário é marcado por grupos altamente organizados, que utilizam técnicas sofisticadas de persuasão, tecnologia avançada e informações pessoais obtidas de diversas fontes para aumentar suas chances de sucesso.

Esse fenômeno é conhecido como engenharia social: o uso de manipulação psicológica para convencer alguém a agir contra seus próprios interesses. Em vez de forçar sistemas bancários com ataques técnicos, os golpistas exploram emoções humanas como medo, urgência, confiança e até ganância.

NA PRÁTICA, ISSO SIGNIFICA QUE CRIMINOSOS CONSEGUEM

Montar centrais de atendimento falsas, com scripts de atendimento profissional.

Criar sites e aplicativos idênticos aos de instituições bancárias.

Utilizar dados vazados de processos judiciais ou cadastros para dar credibilidade ao golpe.

Operar em redes coordenadas, muitas vezes com divisão de tarefas entre quem coleta informações, quem aplica o golpe e quem movimenta o dinheiro.

Essa sofisticação transforma o cidadão comum em alvo fácil, independentemente de sua escolaridade ou experiência digital. Até pessoas com alto nível de instrução podem ser enganadas quando estão sob pressão ou acreditam estar diante de uma situação legítima.

Assim, **compreender a lógica da engenharia social é essencial: não se trata apenas de golpes isolados, mas de um mercado ilícito estruturado, que evolui rapidamente e se adapta a cada nova tecnologia ou regulamentação.**

2

COMO AGEM OS GOLPISTAS

GOLPES COM PIX

Um dos meios de pagamento mais utilizados no Brasil, o PIX, tornou-se também um dos principais alvos dos criminosos. A rapidez e a facilidade que garantem a eficiência desse sistema também são exploradas para induzir vítimas ao erro.

O chamado **"Golpe do PIX Errado"** ocorre quando o golpista cria uma narrativa de urgência — como um parente em situação de emergência ou uma cobrança que precisa ser quitada de imediato — e convence a vítima a transferir valores para uma conta indicada. O apelo emocional, somado à pressão do tempo, reduz a capacidade crítica do cidadão, que realiza a transação sem checar os dados. Esse tipo de prática se enquadra em fraude por indução em erro, configurando manipulação dolosa, que pode ensejar responsabilização civil e até penal.

O **"Capturador de Sessões"** é ainda mais sofisticado. Trata-se de um programa malicioso instalado no celular ou computador da vítima, muitas vezes por meio de links fraudulentos. Esse software permite que o criminoso acompanhe, em tempo real, as operações bancárias, desviando valores ou coletando credenciais. A situação guarda relação direta com a responsabilidade objetiva das instituições financeiras, já consolidada na Súmula 479 do STJ, segundo a qual os bancos respondem pelos danos causados por fraudes decorrentes de falha na prestação de serviços de segurança.

O **“Golpe do QR Code Falso”** representa outra variação bastante comum. O fraudador substitui o código legítimo por outro adulterado, seja em sites, materiais impressos ou até mesmo em estabelecimentos f ísicos. A vítima, acreditando realizar pagamento ao fornecedor, transfere os valores para o criminoso.

Esse tipo de fraude se relaciona ao dever de cautela do consumidor, mas também à responsabilidade solidária das instituições f inanceiras e das plataformas envolvidas na operação, uma vez que o ordenamento jurídico brasileiro (CDC e jurisprudência do STJ) protege a parte hipossuf iciente nas relações de consumo.

GOLPES COM WHATSAPP

O WhatsApp se tornou terreno fértil para fraudes, pela confiança que os usuários depositam em suas conversas pessoais. A **"Clonagem de WhatsApp"** é um dos golpes mais disseminados: criminosos se apropriam do número da vítima, geralmente obtendo o código de verificação por meio de engano, e passam a solicitar transferências em nome dela. Aqui, observa-se a exploração da boa-fé objetiva dos contatos da vítima, que acreditam estar ajudando um amigo ou familiar.

Outro expediente é a criação de **"Perfis Falsos"**, nos quais o fraudador utiliza a foto e o nome de pessoas conhecidas para pedir dinheiro. Embora tecnicamente simples, esse golpe gera grande impacto social e jurídico, pois envolve o uso indevido da imagem e pode configurar crimes contra a honra, além de fraudes patrimoniais.

Já o **"Golpe do Sorteio via WhatsApp"** consiste na promessa de prêmios inexistentes, exigindo informações pessoais ou depósitos prévios para sua liberação. Além do evidente caráter fraudulento, essa prática se enquadra como publicidade enganosa e prática abusiva, vedada pelo Código de Defesa do Consumidor.

GOLPES ELETRÔNICOS GERAIS

O **Phishing** e o **Smishing** consistem no envio de e-mails ou SMS fraudulentos com links que levam a páginas falsas. A vítima, ao inserir dados, fornece acesso direto à sua conta. Além de crime de estelionato eletrônico, caracteriza violação ao direito básico do consumidor à segurança (art. 6º, I, CDC).

O **Boleto Falso** é um dos golpes mais antigos e ainda eficazes. Com frequência, os criminosos falsificam boletos de concessionárias de energia, telefonia e escolas. Por envolver sistema bancário, os tribunais têm reconhecido a responsabilidade solidária das instituições.

Já o **Golpe do Investimento Falso** apela à ganância. Oferece retornos rápidos e irreais, sustentados por falsos depoimentos e até aluguéis de bens de luxo para dar aparência de sucesso. Esse golpe pode ser enquadrado como crime contra a economia popular (Lei 1.521/1951).

O Cavalo de Troia é outro exemplo de fraude digital, em que um programa espião instalado no dispositivo captura senhas e dados bancários.

Muitos criminosos usam sites falsos com certificados digitais clonados para parecerem legítimos. Aquele "cadeado" no navegador não significa que o site é seguro, apenas que há criptografia. Sempre confira o endereço completo (URL) e, no caso de bancos, acesse digitando manualmente, nunca por links recebidos em e-mails ou SMS.

FRAUDES POR CONTATO TELEFÔNICO

O **Golpe da Falsa Central de Atendimento** é um dos mais sofisticados. Criminosos ligam com número semelhante ao do banco e informam compras suspeitas no cartão da vítima. Para “bloquear a fraude”, induzem a digitar senhas ou instalar aplicativos que dão acesso remoto. Em termos jurídicos, trata-se de falha de segurança bancária, ensejando responsabilidade objetiva.

O **Golpe do Motoboy** explora a confiança em supostos funcionários de bancos. O fraudador liga informando que o cartão foi clonado e envia um motoboy para buscá-lo, pedindo que a vítima forneça senha e chip. Apesar de ser golpe já amplamente noticiado, ainda faz milhares de vítimas. O STJ já consolidou entendimento de que os bancos respondem pelos danos, pois cabe a eles orientar seus clientes.

O **Golpe do Falso Leilão** envolve sites que imitam portais oficiais, anunciando veículos ou imóveis com preços atrativos. Ao pagar, a vítima descobre que o bem não existe. A prática pode configurar estelionato e, em alguns casos, crime contra a economia popular.

O ato de “cortar o cartão” pode parecer seguro, mas o chip intacto ainda funciona. Se precisar descartar um cartão, destrua o chip, corte-o em vários pedaços e descarte separadamente.

O **golpe do falso advogado** é uma modalidade de fraude em que criminosos se passam por advogados ou integrantes de escritórios jurídicos para enganar vítimas e obter pagamentos indevidos. Eles costumam usar informações verídicas (como nomes reais de advogados, números de registro na OAB e dados de processos judiciais) combinadas com documentos falsificados, para dar aparência de legitimidade ao contato.

É uma fraude grave que combina falsificação, estelionato e abuso da confiança. A vítima, muitas vezes em situação de fragilidade por acreditar ter direitos a receber, acaba lesada financeiramente e emocionalmente. Por isso, conhecer o modus operandi do golpe é fundamental para preveni-lo. Desconfiançar de contatos que pedem dinheiro adiantado, verificar sempre a identidade do profissional (no site da OAB) e nunca pagar taxas para liberação de valores judiciais são regras de ouro na prevenção.

No golpe do falso advogado, muitos criminosos usam números de OAB verdadeiros de profissionais reais para dar credibilidade. Só que a consulta é simples: no site da OAB, qualquer pessoa pode verificar gratuitamente se o advogado existe, se está ativo e até em qual seccional está inscrito.

A consulta pode ser realizada através do seguinte domínio: **https://cna.oab.org.br/**

3

ASPECTOS JURÍDICOS

A sofisticação dos golpes praticados no ambiente bancário brasileiro não apenas impõe riscos econômicos ao cidadão comum, mas também desafia o ordenamento jurídico a dar respostas efetivas na esfera penal, cível e consumerista. É fundamental compreender como cada modalidade de fraude se enquadra juridicamente, quais responsabilidades recaem sobre criminosos e instituições financeiras, e de que forma o consumidor pode buscar reparação.

ENQUADRAMENTO **PENAL**

O Código Penal brasileiro dispõe de diversos dispositivos que permitem enquadrar os golpes bancários. O mais recorrente é o crime de estelionato (art. 171), definido como obter vantagem ilícita em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento. Golpes como o PIX errado, o boleto adulterado e o perfil falso em aplicativos de mensagem se encaixam diretamente nessa tipificação, pois envolvem manipulação da vítima para a entrega voluntária de valores.

Com o advento das fraudes eletrônicas, o legislador aprovou a Lei nº 14.155/2021, que inseriu no art. 171, §2º-A, a forma qualificada do estelionato eletrônico. Nessa modalidade, a fraude é cometida mediante uso de informações fornecidas pela vítima por meio eletrônico, como redes sociais, emails, mensagens instantâneas ou ligações telefônicas. A pena foi agravada para reclusão de 4 a 8 anos, e multa, podendo ser aumentada em até dois terços quando o crime é praticado contra idoso ou vulnerável. Golpes digitais como o phishing, o smishing e o capturador de sessões encontram aqui seu enquadramento penal específico.

Outros dispositivos do Código Penal também são acionados. A falsidade ideológica (art. 299) é aplicável quando o criminoso insere informações falsas em documentos, como boletos, contratos ou intimações falsas. A falsificação de documento público ou particular (arts. 297 e 298) recai sobre adulterações em ofícios judiciais, precatórios ou identidades falsas. O uso de documento falso (art. 304) complementa esse quadro, punindo o aproveitamento de tais falsificações. Já o art. 307, que trata da falsa identidade, alcança os criminosos que se passam por advogados, funcionários de banco ou parentes das vítimas em aplicativos de mensagem.

Importante também mencionar o art. 47 da Lei de Contravenções Penais, que pune o exercício ilegal da advocacia. Nos golpes em que criminosos se passam por advogados oferecendo falsas soluções jurídicas, além do estelionato, há a configuração de contravenção, tutelando-se a dignidade da profissão.

Em todos os casos, além das penas privativas de liberdade e multa, os criminosos respondem por perdas e danos na esfera cível, reforçando a conexão entre o ilícito penal e a reparação civil.

4

ASPECTOS DA PREVENÇÃO

ENTENDENDO OS PRINCIPAIS **MECANISMOS DE SEGURANÇA**

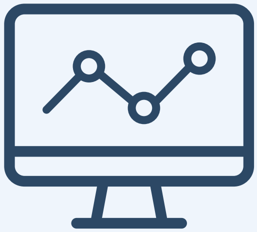
A prevenção contra golpes bancários depende da combinação entre a atuação das instituições financeiras e a postura cautelosa do próprio cliente. Do lado dos bancos, existe um dever legal de segurança, previsto no Código de Defesa do Consumidor e consolidado pela Súmula 479 do STJ, que obriga os fornecedores de serviços financeiros a adotar mecanismos robustos de proteção. Essa responsabilidade se traduz em práticas como a autenticação em múltiplos fatores, que exige a combinação de senha, biometria ou token para validar operações; o monitoramento constante de transações para identificar movimentações suspeitas; e a possibilidade de configurar limites de valores e horários para transferências, especialmente via PIX.

A autenticação em múltiplos fatores é uma das barreiras mais importantes contra fraudes bancárias. Ela exige que o cliente confirme a operação com mais de um elemento de segurança, como senha, token físico ou digital, código enviado por SMS, biometria ou reconhecimento facial. Essa combinação torna muito mais difícil que um golpista, mesmo tendo obtido parte das informações da vítima, consiga concluir uma transação. No campo jurídico, reforça a ideia de que o banco adotou medidas adequadas de proteção, cumprindo o dever de segurança previsto no Código de Defesa do Consumidor.

Autenticação em multiplos fatores

Confirmação com mais de um elemento de segurança

Monitoramento antifraude



Identificação de atividades suspeitas

Limites de valor e de horário

Restrições de quantia e período para transações

O consumidor, por sua vez, também deve exercer um papel ativo na autoproteção. A prevenção começa com a atenção redobrada às comunicações recebidas: links enviados por e-mail, SMS ou aplicativos de mensagem não devem ser utilizados para acessar páginas bancárias, já que frequentemente redirecionam a sites falsos. Da mesma forma, QR Codes devem ser conferidos com cautela, observando sempre o destinatário que aparece na tela do aplicativo antes da confirmação do pagamento.

No campo da segurança digital, é indispensável manter dispositivos atualizados, com antivírus ativo e sistemas operacionais nas versões mais recentes. Recomenda-se ainda evitar a instalação de aplicativos fora das lojas oficiais, pois esses podem conter softwares maliciosos. Outro recurso de proteção essencial é a ativação de verificações adicionais em plataformas de comunicação, como a autenticação em duas etapas no WhatsApp, que dificulta o sequestro de contas.

Além disso, o sigilo de senhas, tokens e códigos de autenticação deve ser absoluto: esses dados não podem ser compartilhados em hipótese alguma, já que nenhuma instituição séria os solicita por telefone, redes sociais ou mensagens instantâneas. O consumidor informado e vigilante contribui decisivamente para a redução dos riscos de fraude e fortalece a própria defesa contra golpes.

DICA ESPECIAL DE **PREVENÇÃO**

Regras de ouro: **Anatomia de uma senha infalível**

Criminosos utilizam softwares sofisticados que podem testar bilhões de combinações por segundo para quebrar senhas fracas. Para construir uma senha que resista a esses ataques, ela deve seguir critérios técnicos rigorosos.

• **Comprimento:** Uma senha deve ter, no mínimo, 16 caracteres. Quanto mais longa, exponencialmente mais difícil será quebrá-la.

• **Complexidade:** É obrigatório o uso de uma combinação de letras maiúsculas (A-Z), letras minúsculas (a-z), números (0-9) e símbolos especiais (!@#$%^&*). Essa variedade aumenta drasticamente o número de combinações possíveis.

- **Imprevisibilidade:** Jamais utilize informações pessoais óbvias, como datas de nascimento, nomes de familiares, endereços ou números de documentos. Evite também palavras comuns encontradas em dicionários e sequências de teclado, como “123456”, “qwerty”; ou “senha123”, pois são as primeiras a serem testadas por programas de ataque.

O erro de segurança mais comum e perigoso que um usuário pode cometer é reutilizar a mesma senha em múltiplos sites e serviços. O risco é imenso: se um site menos seguro (como uma loja online ou um fórum) sofrer um vazamento de dados, os criminosos testarão a combinação de seu e-mail e senha vazados em serviços de alto valor, como seu banco, e-mail principal e redes sociais.

Regras de ouro:
Autenticação de dois fatores (2FA)

A **Autenticação de Dois Fatores**, também conhecida como verificação em duas etapas ou autenticação multifator, é um método de segurança que exige a apresentação de duas formas diferentes de identificação antes de liberar o acesso a uma conta. É como um cofre que exige não apenas a combinação correta (sua senha), mas também a inserção de uma chave física (um código gerado no seu celular).

A força da 2FA reside em sua capacidade de neutralizar o roubo de senhas. Mesmo que um criminoso consiga obter sua senha através de um vazamento de dados, ele ainda será barrado na segunda etapa de verificação, pois não terá acesso ao seu dispositivo físico.

Diversos serviços se beneficiam desse recurso. Instituições financeiras aplicam a 2FA em transações de alto valor ou no acesso inicial a aplicativos bancários; plataformas de e-mail, como Gmail e Outlook, permitem ativar a verificação por código ou aplicativo autenticador; redes sociais como Facebook, Instagram e LinkedIn oferecem 2FA para proteger contas contra sequestros; e sistemas governamentais como o gov.br já exigem autenticação multifatorial em operações sensíveis.

Em todos esses casos, a 2FA funciona como um escudo digital, alinhando tecnologia e responsabilidade jurídica para proteger informações e transações.

1. Acesse as Configurações: Abra o aplicativo ou site e navegue até o menu “Configurações”, “Perfil” ou “Conta”.

2. Encontre a Sessão de Segurança: Procure por uma opção chamada “Segurança e Login”, “Privacidade” ou “Formas de acesso”.

3. Localize e Ative a 2FA: Encontre a opção “Autenticação de Dois Fatores”, “Verificação em Duas Etapas” ou “2FA” e selecione para ativá-la.

4. Siga as Instruções: O Sistema irá guiá-lo. Geralmente, você terá que escolher o método para o segundo fator:
SMS: Você receberá um código de uso único por mensagem de texto toda vez que fizer login em um novo dispositivo.

Celular Seguro: **Proteção Imediata**

O Celular Seguro é um aplicativo oficial do Governo Federal que permite, em caso de roubo, furto ou perda, bloquear rapidamente o aparelho, a linha telefônica e aplicativos bancários vinculados. O serviço é integrado a bancos e operadoras parceiras, garantindo que, ao acionar o bloqueio, o criminoso não consiga acessar contas ou realizar transações.

Esse mecanismo funciona como uma ferramenta de remediação imediata, reduzindo riscos e prejuízos quando o dispositivo é comprometido. Para utilizá-lo, basta ter cadastro no gov.br e registrar previamente o celular junto ao aplicativo.

FUI VÍTIMA, E AGORA?

COMO **AGIR**, O QUE **FAZER**

A remediação, no contexto das fraudes bancárias, corresponde ao conjunto de medidas que a vítima deve adotar após identificar que foi alvo de um golpe. Se a prevenção é o escudo, a remediação é a rede de proteção que busca estancar o prejuízo, reunir provas e acionar os mecanismos jurídicos e administrativos disponíveis. O tempo aqui é decisivo: quanto mais rápido for o movimento do cliente, maiores as chances de bloquear valores, identificar responsáveis e garantir a reparação.

Primeira hora após perceber o Golpe

A prioridade absoluta é interromper novas perdas. Isso significa contatar imediatamente a instituição financeira para bloquear cartões, senhas e acessos, registrar a contestação das operações e, no caso de PIX, solicitar o uso do Mecanismo Especial de Devolução (MED). Também é fundamental anotar protocolos, guardar capturas de tela da movimentação suspeita e salvar todas as mensagens ou documentos enviados pelo golpista. Essa primeira hora é de reação rápida e serve para congelar o problema antes que ele se amplifique.

24 horas seguintes

Superada a urgência inicial, a etapa seguinte é formalizar e documentar a fraude. A vítima deve registrar um Boletim de Ocorrência, preferencialmente já munida das provas reunidas. É também nesse período que se deve notificar órgãos de classe quando aplicável, como a OAB em casos de falso advogado, e abrir chamados em canais oficiais do banco (SAC e Ouvidoria). A comunicação clara e formal cria lastro documental para reforçar a posição da vítima em qualquer disputa.

Três dias seguintes

O foco passa a ser ampliar a proteção e iniciar as medidas de responsabilização. Nesse prazo, recomenda-se registrar reclamação em plataformas de defesa do consumidor, como o Consumidor.gov.br e os Procons estaduais ou municipais, além de avaliar junto a advogado de confiança a viabilidade de uma ação judicial. Esse é também o momento de monitorar contas e cartões, redefinir senhas em todos os dispositivos e aplicativos vinculados, e acompanhar o retorno do banco sobre o pedido de ressarcimento. Ao final de três dias, a vítima terá consolidado um dossiê de provas, acionado as instâncias administrativas e preparado o caminho para, se necessário, judicializar a demanda.

6

CANAIS DE APOIO E DENÚNCIA

Delegacia Especializada de Repressão aos Crimes Cibernéticos de Natal (DRCC/Natal)

Endereço: Avenida Capitão Mor Gouveia, 1339, 1ª andar, Nossa Senhora de Nazaré, Natal/RN, CEP: 59060-400
Telefone: (84) 98658-8037 / (84) 98660-7726
E-mail: drcc@policiacivil.rn.gov.br

Delegacia Especializada de Defesa do Consumidor de Natal (DECON/NATAL)

Endereço: Avenida Coronel José Bernardo, 1001, Central do Cidadão, Alecrim, Natal/RN, CEP: 59037-000
Telefone: (84) 98660-3267
E-mail: decon@policiacivil.rn.gov.br

PROCON - RN

Endereço: Rua Ulisses Caldas, 181, Cidade Alta, Natal/RN, CEP: 59025-090
Telefone: (84) 3232-9050 / (84) 3232-9051 / 151
E-mail: procon.natal@natal.rn.gov.br

Ministério Público do Rio Grande do Norte (MPRN)

Endereço: Rua Promotor Manoel Alves Pessoa Neto, 110, Candelária - Natal/RN, CEP: 59065-555 (segunda à quinta-feira, das 8h às 17h)
Telefone: (84) 99994-6057 (Whatsapp)
E-mail: ouvidoria@mprn.mp.br • sec.ouvidoria@mprn.mp.br
Site: www.mprn.mp.br/paginas/ouvidoria/

OAB/RN - Ouvidoria

Ouvidor-Geral: Diogo Licurgo Meireles Nunes
Telefone: (84) 99956-0238
E-mail: ouvidoria@oabrn.org.br
Site: www.oabrn.org.br

Rua Nossa Senhora de Candelária, 3382
Candelária • Natal/RN • (84) 4008-9400
Site: oabrn.org.br • @oabrnoficial

OAB RIO GRANDE DO NORTE | Comissão de Direito Bancário e Instituições Financeiras