

GUIA

Antifraude no onboarding: documento, foto e golpe

Quatro artigos do blog sobre fraude no cadastro: o QR Code da CNH digital, os metadados da foto, a lista interna de bloqueio e o golpe aplicado em nome de quem verifica.

NESTE GUIA

1. O QR Code da CNH digital: por que ler o código não é validar o documento
2. Metadados de foto no onboarding: o que o EXIF entrega e por que a ausência não acusa
3. Blocklist interna: quando bloquear um documento e por quanto tempo
4. Golpe em nome do verificador: por que quem faz KYC precisa de um aviso permanente

Gerado em 27 de setembro de 2026

Versão web: <https://unifokal.com/publicacoes#antifraude-no-onboarding>

O QR Code da CNH digital: por que ler o código não é validar o documento

Publicado em 12 de setembro de 2026 · <https://unifokal.com/blog/qr-code-da-cnh-digital>

O que a Resolução CONTRAN 886/2021 diz que o QR Code da CNH carrega, contra o que ele é conferido, e por que um leitor genérico devolve dados sem provar nada sobre o documento.

Chega no atendimento a foto de uma tela de celular: a habilitação do cliente dentro do aplicativo, com um QR Code no canto. Alguém aponta a câmera, o leitor devolve nome, CPF e número de registro, tudo batendo com o cadastro, e o caso segue aprovado. A cena se repete todo dia e tem um problema silencioso no meio dela: ler o QR Code da CNH digital não é validar a CNH digital.

A diferença não é de rigor, é de natureza. Um QR Code, de Quick Response Code, é um símbolo que codifica uma sequência de bytes. O leitor genérico do celular faz uma coisa só: decodifica e devolve o que estava lá. Ele não sabe quem gerou o símbolo, não conversa com base nenhuma e não tem como recusar um código que alguém montou num gerador qualquer cinco minutos antes.

Este artigo separa as duas operações usando o texto da norma que criou esse código: a Resolução CONTRAN nº 886, de 13 de dezembro de 2021, do Conselho Nacional de Trânsito, que regulamenta as especificações, a produção e a expedição da Carteira Nacional de Habilitação, a CNH. O que ela diz sobre o QR Code é curto, específico, e resolve a maior parte das dúvidas de quem monta uma esteira de cadastro.

O que a norma diz que o QR Code carrega

O artigo 2º da Resolução 886/2021 estabelece que a CNH é expedida em meio físico e/ou digital, à escolha do condutor, em modelo único. Três parágrafos desse mesmo artigo tratam do código, e vale lê-los na ordem.

O parágrafo 3º diz que a CNH possui Código de Referência Rápida, gerado a partir de algoritmo específico do órgão máximo executivo de trânsito da União e fornecido pelo sistema central do Registro Nacional de Condutores Habilitados, o RENACH, de modo a permitir a validação do documento.

O parágrafo 4º é o que costuma surpreender quem nunca abriu a norma: o QR Code da CNH armazena todas as informações contidas nos dados variáveis do respectivo documento, inclusive a fotografia, com exceção da assinatura do condutor.

Lidos juntos, os dois parágrafos desenharam o objeto com precisão. O código é uma cópia do conteúdo do documento, retrato incluído, embalada por um algoritmo que a resolução não publica. Ele existe para permitir a validação. Ele não é a validação.

Ler e validar são duas operações diferentes

O parágrafo 5º do mesmo artigo fecha o circuito: o órgão máximo executivo de trânsito da União deve disponibilizar aplicativo específico para a validação de que trata o parágrafo 3º. A norma não descreve o formato do conteúdo, não publica o algoritmo e não abre um procedimento de conferência para terceiros. Ela atribui a conferência a um aplicativo oficial.

A consequência prática é direta. Quando você lê o código com um leitor comum, recebe dados sem procedência: nada no resultado diz de onde ele veio. E a coerência entre o que está impresso na frente do documento e o que sai do código prova menos do que parece, porque quem produziu o documento falso produziu as duas coisas a partir da mesma fonte. Bater um contra o outro é conferir a cópia contra a cópia.

Há um segundo erro, mais sutil: tratar a presença de um QR Code legível como sinal de autenticidade. Um símbolo que decodifica sem erro só prova que alguém o gerou corretamente. O inverso também vale, e custa conversão: um código que não lê costuma ser foco, brilho de tela ou recorte, e não indício de fraude. Vale a disciplina de não transformar rejeição técnica em recusa.

Onde fica o aplicativo oficial

A Secretaria Nacional de Trânsito, a Senatran, mantém o aplicativo da Carteira Digital de Trânsito, apresentado hoje no portal gov.br como CNH do Brasil. É por ele que o condutor acessa a versão digital da habilitação e o documento do veículo. O portal de serviços registra que os documentos digitais têm a mesma validade dos documentos impressos e que o acesso depende de conta gov.br nos níveis bronze, prata ou ouro.

Repare na assimetria que isso cria para quem verifica. O condutor entra no aplicativo com a própria conta e vê o próprio documento. A empresa que recebe um arquivo de imagem por um formulário de cadastro está a duas camadas disso: não tem o aparelho, não tem a sessão e

não tem, pela norma, procedimento próprio de conferência do símbolo. Quem desenha o fluxo admite esse limite em vez de contorná-lo com uma leitura de QR que não valida nada.

O parágrafo 4º também é um problema de minimização

Se o código armazena todos os dados variáveis mais a fotografia, pedir ao usuário a foto do QR Code significa receber um conjunto completo de dados pessoais e uma imagem facial, mesmo quando o fluxo precisava apenas conferir dois campos. Coleta que não foi decidida é coleta que ninguém vai saber justificar depois.

A regra de desenho é a de sempre: definir antes quais campos o caso de uso exige e descartar o resto na borda, como em reduzir o dado antes de enviar ao fornecedor. Um bloco binário decodificado sem plano vira, em silêncio, um depósito de dado sensível dentro do seu log.

O que de fato ajuda na esteira

Se o QR Code não resolve, o que resta é o conjunto de conferências que não depende dele:

1. Aritmética interna dos números. O artigo 4º da Resolução 886/2021 descreve três numerações da CNH: o Número do Registro Nacional, com nove caracteres mais dois dígitos verificadores; o Número do Espelho, com nove caracteres mais um dígito; e o Número do Formulário RENACH, com onze caracteres, cujas duas primeiras posições são a sigla da unidade federativa expedidora. O parágrafo 1º manda calcular o dígito pela rotina módulo 11, com a regra de que resto 0 ou 1 produz dígito 0. É conferência barata e local, e ela reprova erro de digitação e número inventado sem consultar ninguém.
2. Saber qual documento está na mão antes de escolher a conta, porque cada tipo tem leiaute e regras próprias e conferir módulo 11 num documento que não carrega aquele número é exercício vazio.
3. Ligar a pessoa ao retrato. O documento só vale como prova de identidade se alguém demonstrar que é a pessoa retratada nele, o que é trabalho de captura ao vivo e comparação facial, e não de leitura de código. É a camada que uma verificação de identidade de pessoa organiza.
4. Tratar o documento como um objeto que pode ter sido produzido, e não apenas copiado. As técnicas de produção de documento falso miram exatamente na conferência superficial, e um QR Code fabricado junto com o resto do leiaute é uma delas.

Nenhum desses passos substitui o outro, e nenhum vira recusa sozinho. O que muda é a honestidade do registro: em vez de anotar "QR Code validado", o fluxo anota o que foi conferido de fato.

Perguntas frequentes

Ler o QR Code prova que a CNH digital é verdadeira?

Não. O leitor decodifica e devolve os bytes que estavam no símbolo, sem informação sobre quem o gerou. A Resolução CONTRAN 886/2021 diz, no parágrafo 3º do artigo 2º, que o código é gerado por algoritmo específico do órgão máximo executivo de trânsito da União para permitir a validação, e atribui a validação, no parágrafo 5º, a um aplicativo específico desse órgão.

O QR Code da CNH contém a foto do condutor?

Sim. O parágrafo 4º do artigo 2º da mesma resolução diz que o código armazena todas as informações contidas nos dados variáveis do documento, inclusive a fotografia, com exceção da assinatura do condutor. Quem lê o código recebe também a imagem facial, o que pesa na decisão de coletar ou não esse dado.

Se os dados do QR Code batem com os dados impressos, o documento é autêntico?

Não necessariamente. Quem produz um documento falso produz a impressão e o código a partir do mesmo conteúdo, então a coerência entre os dois só mostra que vieram da mesma origem. Coerência interna é conferência de consistência, não de procedência.

Fontes citadas

- Resolução CONTRAN nº 886, de 13 de dezembro de 2021, do Conselho Nacional de Trânsito, artigo 2º (caput e parágrafos 3º, 4º e 5º) e artigo 4º (incisos I a III e parágrafo 1º), no portal do Ministério dos Transportes: gov.br
- Portal gov.br, página do serviço de instalação do aplicativo da Carteira Digital de Trânsito, apresentado como CNH do Brasil, da Secretaria Nacional de Trânsito: gov.br

Metadados de foto no onboarding: o que o EXIF entrega e por que a ausência não acusa

Publicado em 12 de setembro de 2026 · <https://unifokal.com/blog/exif-e-metadados-de-foto>

Data, aparelho e GPS podem estar no arquivo e somem em qualquer reencode. Por que metadado ausente não é sinal de fraude, o que o metadado presente informa e onde a orientação quebra o face match.

O analista abre a imagem que o cliente enviou, roda uma ferramenta de metadados, não encontra nada e escreve na ficha: "metadados removidos, indício de manipulação". Essa frase, repetida por uma esteira inteira, produz recusa de gente honesta em escala. A ausência de metadados EXIF numa foto de onboarding é o resultado normal de um caminho normal, não a assinatura de um fraudador.

O EXIF, de Exchangeable Image File Format, é o bloco de informação que uma câmera grava junto com a imagem: data e hora de captura, fabricante e modelo do aparelho, parâmetros de exposição, orientação e, quando o aparelho registra, coordenadas de GPS. Ele é especificado pela CIPA, a Camera and Imaging Products Association, no documento DC-008.

Este artigo é sobre foto. A anatomia equivalente em arquivo de documento está em [como saber se um PDF foi editado](#), e a conclusão é parecida nos dois formatos: metadado é sinal fraco por natureza. A diferença é que, na foto, o sinal costuma nem existir.

O metadado mora ao lado da imagem, não dentro dela

Vale entender o mecanismo antes de discutir a interpretação. O formato de arquivo JPEG mais usado é padronizado na Recomendação ITU-T T.871, publicada também como ISO/IEC 10918-5, o JFIF. O item 6.5 dessa norma trata dos segmentos de marcador de aplicação e diz o essencial numa frase: segmentos adicionais podem ser usados para guardar informação específica de aplicação que não afeta a capacidade de decodificar ou exibir o arquivo.

Essa é a definição arquitetural do problema. O bloco de metadados é uma gaveta paralela ao dado comprimido. Remover a gaveta não muda um pixel, e reescrever o conteúdo dela também não. Nada no formato amarra o que está escrito ali ao que está desenhado na imagem.

Compare com o que uma amarração de verdade exige. O item 4.1 do DOC-ICP-15, do Comitê Gestor da ICP-Brasil, define assinatura digital como aquela vinculada ao documento eletrônico de tal modo que qualquer alteração subsequente neste seja plenamente detectável. É esse vínculo que o bloco de metadados de uma foto nunca teve.

Por que o metadado some sozinho

O caminho que uma foto percorre até chegar ao seu servidor passa por etapas que reconstroem o arquivo. A mais comum, e a mais fácil de provar, é o desenho em canvas dentro do navegador.

O padrão HTML descreve, na seção de serialização de bitmap para arquivo, o que acontece quando a página transforma um canvas em imagem: o agente de usuário cria um arquivo no formato pedido, e os dados de pixel desse arquivo devem ser os dados de pixel do bitmap. O único metadado que o algoritmo menciona é a resolução, que deve ser gravada como 96 dpi quando o formato suportar. Nada mais atravessa. O arquivo que sai é uma construção nova feita a partir de pixels.

Qualquer etapa que redimensione, recorte, comprima ou converta a imagem tem o mesmo efeito, a menos que o código copie o bloco de propósito. Uma captura feita pela câmera dentro da página nunca teve EXIF para começar, porque não veio de um arquivo de câmera: veio de quadros desenhados e depois serializados.

A conclusão prática é direta. Metadado ausente é o desfecho esperado de um fluxo web comum. Usar a ausência como sinal de risco é punir o usuário pelo comportamento do navegador dele, e o efeito de uma regra dessas é medido na fila de recusa, não na de fraude.

A orientação é o metadado que quebra coisa de verdade

Há um campo do EXIF que não é opcional na prática: a orientação. O navegador consome esse campo por padrão. A propriedade `image-orientation`, especificada pelo W3C no módulo CSS Images de nível 3, tem valor inicial `from-image`, e a especificação explica que, se a imagem tem orientação declarada nos metadados, como no EXIF, esse valor equivale ao ângulo que os metadados indicam como necessário para orientar a imagem corretamente. Sem metadado de orientação, o valor calculado passa a ser `none`.

O resultado é uma armadilha clássica de esteira: a imagem aparece certa na tela, porque o navegador aplicou a rotação, e chega girada no serviço que vai processá-la, porque a decodificação do lado do servidor ignorou o campo. Detector de rosto em imagem girada encontra menos rosto, ou encontra e extrai um vetor pior. O sintoma chega como queda de aprovação sem causa aparente.

A defesa é aplicar a orientação de forma explícita na entrada, antes de qualquer recorte ou comparação, e registrar que ela foi aplicada. Vale para toda a cadeia: o que sai do upload precisa chegar normalizado ao passo seguinte, e não confiar no acaso de cada decodificador.

Metadado presente informa, mas não prova

Invertido o raciocínio, a pergunta seguinte é o que fazer quando o bloco está lá. A resposta honesta: use como contexto, nunca como prova.

Tudo que está no bloco foi escrito por algum programa, e pela norma citada acima aquele conteúdo não interfere na decodificação, então editá-lo não deixa rastro na imagem. Um campo de data e hora é uma afirmação de quem gravou o arquivo, não uma medição. Isso não o torna inútil: torna-o insumo de priorização, do tipo que entra num score explicável com peso pequeno, e nunca um portão de recusa.

Há ainda um custo de coleta. Se as coordenadas de GPS vierem, você passou a tratar dado de localização de uma pessoa identificada, que é dado pessoal na definição do inciso I do artigo 5º da Lei 13.709/2018, a LGPD. Guardar isso exige finalidade, base legal e prazo, e a alternativa mais barata quase sempre é descartar o bloco na borda, como em reduzir o dado antes de enviar ao fornecedor.

O que colocar na esteira

Traduzindo tudo em regra operacional:

1. Nunca reprove por ausência de metadado. Ela não distingue fraudador de usuário de navegador comum.
2. Aplique a orientação declarada antes de recortar, comparar ou indexar, e registre isso no log do processamento.
3. Trate campo presente como sinal fraco, com peso pequeno, sempre acompanhado de outros sinais.

4. Decida explicitamente se guarda GPS. Se não tem finalidade, descarte antes de armazenar.
5. Guarde no registro o que foi observado e o que foi decidido, porque metadado é justamente o tipo de evidência que ninguém consegue reconstruir depois.

E a nota final, que reposiciona o problema inteiro: o ataque sério contra captura remota não passa pelo arquivo. Ele injeta quadros direto no caminho da câmera, como em injeção de câmera, e aí o arquivo pode até vir com metadados plausíveis. Quem defende essa superfície olha os sinais do dispositivo e a coerência da sessão, numa esteira de antifraude em camadas. O bloco EXIF é o último lugar onde essa resposta está.

Perguntas frequentes

Foto sem EXIF é sinal de fraude?

Não. Qualquer etapa que reconstrói o arquivo elimina o bloco, e o padrão HTML define a serialização de um canvas a partir dos dados de pixel do bitmap, sem transportar metadado de origem. Ausência é o resultado esperado de um fluxo web comum, não um indício.

Dá para confiar na data de captura do EXIF?

Não como prova. O item 6.5 da Recomendação ITU-T T.871 descreve esses segmentos como informação de aplicação que não afeta a decodificação, então reescrevê-los não deixa marca na imagem. A data serve como contexto de priorização, com peso pequeno, nunca como portão de decisão.

Por que a foto aparece certa na tela e girada no servidor?

Porque o navegador aplica a orientação do EXIF por padrão: a propriedade `image-orientation` do CSS Images nível 3 tem valor inicial `from-image`, que equivale ao ângulo indicado pelos metadados. Um decodificador do lado do servidor que ignore esse campo entrega a imagem na rotação bruta.

Fontes citadas

- Recomendação ITU-T T.871, publicada também como ISO/IEC 10918-5, JPEG File Interchange Format, item 6.5, sobre segmentos de marcador de aplicação: itu.int

- CIPA, Camera and Imaging Products Association, documento DC-008, especificação do Exchangeable Image File Format (EXIF), citada por nome como a norma que define o formato de metadados.
- HTML Standard, do WHATWG, seção 4.12.5.5, serialização de bitmap do canvas para arquivo: html.spec.whatwg.org
- W3C, CSS Images Module Level 3, seção 5.1, propriedade image-orientation e o valor from-image: w3.org
- DOC-ICP-15, Visão Geral sobre Assinaturas Digitais na ICP-Brasil, versão 4.0, item 4.1, usado como contraste sobre o que é vínculo detectável entre assinatura e conteúdo: gov.br
- Lei 13.709/2018, a LGPD, artigo 5º, inciso I, definição de dado pessoal, no portal do Planalto: planalto.gov.br

Blocklist interna: quando bloquear um documento e por quanto tempo

Publicado em 3 de setembro de 2026 · <https://unifokal.com/blog/blocklist-interna-de-documentos>

A lista interna de bloqueio é o antifraude mais barato e o mais fácil de envenenar. Critério de entrada, prazo de revisão, hash com pimenta e o que a LGPD cobra de quem bloqueia por sistema.

Toda operação que sofreu fraude cria, cedo ou tarde, uma lista interna de bloqueio. Alguém anota o CPF que usou documento adulterado, o sistema passa a barrar aquela tentativa e o custo por checagem é praticamente zero: uma consulta a uma tabela própria, sem chamar ninguém de fora. É o antifraude mais barato que existe, e por isso mesmo o mais fácil de envenenar.

O envenenamento acontece por acúmulo: uma entrada colocada numa madrugada de incidente, outra derivada de uma reclamação de cliente irritado, outra de uma reprovação isolada que ninguém investigou. Dois anos depois a lista tem milhares de linhas sem justificativa registrada, e ninguém remove nada porque ninguém sabe o que cada linha significa. Deixou de ser controle e virou dívida.

Este texto trata do que separa uma lista útil de um depósito de suspeitas: critério de entrada, prazo de saída, como guardar o identificador sem criar um repositório de CPF em claro, os deveres legais de quem bloqueia por sistema e a diferença entre a sua lista e a do setor.

O que justifica uma entrada, e o que não justifica

O critério precisa ser escrito antes do primeiro caso, porque na urgência todo mundo inclui. A regra que se sustenta é simples: entra na lista o que foi **confirmado**, com evidência guardada.

Justifica entrada:

- Fraude comprovada com prejuízo apurado, como documento adulterado identificado em análise ou uso de identidade de terceiro com registro do fato.
- Confissão, decisão judicial ou determinação de autoridade competente.

- Padrão confirmado depois de investigação, como uma série de cadastros ligados ao mesmo esquema, com o vínculo documentado.

Não justifica entrada:

- Suspeita do analista sem apuração concluída.
- Reprovação isolada de uma verificação, que na maior parte das vezes é foto ruim, luz ruim ou documento gasto, e não fraude.
- Reclamação de cliente ou disputa comercial, que é assunto de atendimento e não de antifraude.
- Score alto de risco, que é sinal para investigar e não conclusão sobre a pessoa.

A distinção importa porque os dois tipos de entrada se parecem no banco de dados e são radicalmente diferentes na consequência. Uma delas barra um fraudador; a outra barra para sempre um cliente que só tinha uma câmera velha, e a diferença entre esses dois casos é exatamente o assunto do falso positivo em verificação. Confundir suspeita com confirmação é o erro que também alimenta a fila de vítimas de fraude com CPF de terceiro: quem teve o documento usado por um golpista é a parte lesada, e mandá-la para a blocklist pune duas vezes a mesma pessoa.

Entrada sem evidência vira dívida invisível

Uma entrada precisa carregar, no mínimo, quatro coisas: o motivo em texto legível, a referência à evidência (o caso, o chamado, o processo), quem incluiu e quando. Sem isso, a linha é irreversível na prática. Ninguém remove o que não entende, e o volume só cresce.

O sintoma clássico aparece na análise de conversão, meses depois: uma fatia de cadastros bloqueada por uma tabela que ninguém audita, com falsos positivos que nunca voltam para reclamar porque simplesmente foram embora. Como o custo é invisível, a lista nunca é revista.

Dois práticas cortam a espiral pela raiz. A primeira é tornar a evidência obrigatória no momento da inclusão, no formulário e no esquema do banco, de modo que não exista caminho para criar uma entrada órfã. A segunda é a trilha de auditoria da própria lista: cada inclusão, alteração e remoção registrada de forma imutável, com autor e horário. Auditar quem bloqueou importa tanto quanto auditar quem aprovou, porque uma lista interna também é alvo de abuso interno.

Prazo e revisão: bloqueio eterno é pena perpétua

Nenhuma entrada deveria nascer sem prazo. Bloqueio permanente decidido por uma tabela é pena perpétua, e há um argumento prático além do moral: a informação envelhece. Um documento envolvido em fraude há seis anos diz pouco sobre quem tenta se cadastrar hoje.

Um desenho razoável tem três elementos. Prazo por tipo de caso, mais longo para fraude grave e mais curto para casos limítrofes, definido pela política de risco e não pelo analista da vez. Revisão periódica agendada, na qual entradas vencidas expiram sozinhas e as que permanecem exigem confirmação explícita. E um caminho de contestação com prazo de resposta, porque bloqueio errado sem canal de saída é o pior atendimento possível. Sair da lista precisa ser tão operacional quanto entrar: se remover exige três aprovações e uma reunião, ninguém remove.

Guardar o identificador sem criar um repositório de CPF

A lista precisa comparar documentos, não exibir documentos. Guardar CPF em claro numa tabela consultada por todo o sistema cria um repositório de dado pessoal atraente, quando o que a função exige é apenas responder "este documento está na lista?".

O reflexo comum é guardar o hash do CPF, e ele é insuficiente sozinho. O espaço de CPFs válidos é pequeno o bastante para ser percorrido inteiro: quem obtiver a tabela pode calcular o hash de todos os números possíveis e recuperar a lista completa, e a conta é banal: cerca de um bilhão de combinações válidas, que hardware comum percorre inteiro em pouco tempo. Hash sozinho, num domínio tão pequeno, não esconde nada. Salgar por linha resolve o vazamento em lote, mas quebra a comparação, porque cada valor teria um sal diferente.

O caminho usual é o hash com pimenta, no sentido que o OWASP Password Storage Cheat Sheet dá ao termo: um segredo único da aplicação, guardado fora do banco, em cofre de segredos ou módulo de hardware, combinado ao documento antes do hash. A tabela continua comparável, já que todas as linhas usam o mesmo segredo, e quem obtiver apenas o banco não consegue enumerar nada sem também obter a pimenta. A rotação precisa ser planejada desde o início, e aqui está a armadilha: se a tabela guarda só o hash, o documento em claro não existe mais e não há o que recalculer. Ou se aceita uma transição, conferindo contra a pimenta velha e contra a nova durante uma janela e re-derivando cada linha na próxima vez que aquele documento aparecer, ou se guarda o identificador cifrado de forma reversível, com a chave no cofre, em vez de resumido.

A sua lista, a lista do setor e o que a lei cobra

Lista própria e lista compartilhada são coisas diferentes em natureza e em regime jurídico. A sua lista reflete a sua experiência: você viu o caso, guardou a evidência e responde por ela. A lista compartilhada entre instituições envolve receber e enviar informação sobre pessoas que nunca tentaram se cadastrar com você, e no sistema financeiro brasileiro esse compartilhamento tem regra própria, a Resolução Conjunta CMN/BCB nº 6, de 23 de maio de 2023, que trata do compartilhamento de dados e informações sobre indícios de fraude entre instituições autorizadas a funcionar pelo Banco Central, com requisitos que valem ler antes de aderir a qualquer arranjo, como detalha a [análise da Resolução Conjunta nº 6](#).

Dos dois lados, a Lei 13.709/2018, a LGPD, impõe deveres concretos. É preciso ter base legal para o tratamento, e a prevenção à fraude costuma ser sustentada pelo legítimo interesse do artigo 7º, inciso IX, ou pelo cumprimento de obrigação legal ou regulatória do inciso II do mesmo artigo, com a avaliação registrada por escrito. Os princípios do artigo 6º cobram necessidade e qualidade do dado, o que em bom português significa não guardar mais do que a função exige e manter a informação exata e atualizada, exigência que uma lista sem revisão viola por definição. O artigo 18 assegura ao titular a confirmação do tratamento, o acesso e a correção, e a eliminação prevista no inciso VI alcança o dado tratado com base no consentimento, não o que se conserva sob outra base: uma lista sustentada em legítimo interesse não se apaga a pedido nos termos daquele inciso. O artigo 20 lhe dá o direito de solicitar revisão de decisões tomadas unicamente por tratamento automatizado, tema desenvolvido em [direitos do titular em KYC](#).

Há uma tensão real aqui: transparência total sobre os critérios entrega o mapa da fraude a quem quer contorná-lo. A saída praticada é responder ao titular sem detalhar o método, informando que houve restrição interna por análise de risco, oferecendo contestação e colocando uma pessoa, e não a mesma regra que bloqueou, para examinar o caso. Vale registrar que essa última parte é escolha de desenho, e não imposição do artigo 20: o parágrafo que obrigaria revisão por pessoa natural foi vetado, e o que a lei garante é a revisão, sem dizer por quem.

Fontes citadas

- Resolução Conjunta CMN/BCB nº 6, de 23 de maio de 2023, sobre o compartilhamento de dados e informações sobre indícios de fraude entre instituições autorizadas a funcionar pelo Banco Central, citada por nome e número no texto.
- Lei 13.709/2018 (LGPD), artigos 6º, 18 e 20, citada por nome e número no texto.

- OWASP Password Storage Cheat Sheet, definição de pimenta como segredo da aplicação guardado fora do banco, citada por nome no texto.

Golpe em nome do verificador: por que quem faz KYC precisa de um aviso permanente

Publicado em 23 de setembro de 2026 · <https://unifokal.com/blog/aviso-antifraude-em-nome-do-verificador>

Quem verifica identidade vira nome de isca. O que o golpe pede, por que ele convence, o que uma verificação legítima nunca faz e onde o aviso antifraude precisa morar.

Uma pessoa abre conta num aplicativo qualquer, tira a selfie, fotografa o documento e conclui o cadastro. Duas semanas depois chega uma mensagem: "Sua verificação de identidade ficou pendente. Reenvie o documento e uma selfie para concluir." A mensagem traz o nome de uma empresa de verificação, um logotipo razoável e um prazo. A pessoa não estranha, porque ela realmente passou por uma verificação em algum lugar.

É esse o golpe, e ele não ataca a tecnologia de ninguém. Ataca a memória da vítima. Este texto interessa a quem opera um produto que usa verificação de identidade e a quem escreve a comunicação dessa empresa, porque a contramedida aqui é editorial antes de ser técnica.

O pretexto é bom porque ele é quase verdadeiro

O fascículo "Golpes: Não se Deixe Enganar", publicado pelo CERT.br, pelo NIC.br e pelo CGI.br, abre com três perguntas de alerta: a mensagem diz que é uma pessoa ou organização conhecida? Envolve dinheiro, vantagem ou informações pessoais? Quer que você faça algo sem tempo para pensar? O golpe em nome de um verificador responde sim às três, e ainda ganha um reforço que a maioria dos golpes não tem: a vítima tem lembrança recente de ter feito exatamente aquilo.

O mesmo material lista, entre os temas cotidianos que devem levantar suspeita, o recadastramento, a atualização de aplicativo e o CPF (Cadastro de Pessoas Físicas) cancelado. São os três disfarces prediletos de quem pede documento e selfie de novo. E há um agravante que o fascículo também trata: suspeite mesmo que a mensagem saiba os seus dados, porque informação vazada e informação pública circulam e fazem o golpe parecer verdadeiro. Um criminoso que acerta nome, CPF e até o nome do aplicativo onde a pessoa se cadastrou não provou nada sobre si; provou apenas que comprou uma lista.

Vale dizer o que o atacante ganha com isso. Documento e selfie entregues de boa vontade chegam melhores do que os que circulam em vazamento: boa luz, enquadramento frontal, foco, e às vezes um vídeo curto. É o mesmo efeito do golpe da vaga falsa que coleta documento e selfie, com um pretexto diferente e o mesmo produto final.

No direito brasileiro isso tem nome

Atribuir-se falsa identidade para obter vantagem é o artigo 307 do Código Penal, o Decreto-Lei 2.848/1940. Obter vantagem ilícita induzindo alguém a erro mediante ardil é o estelionato do artigo 171. E existe figura própria para o meio eletrônico: o parágrafo 2º-A, a fraude eletrônica, incluído pela Lei 14.155/2021, que alcança a fraude cometida com informações fornecidas pela vítima ou por terceiro induzido a erro por rede social, contato telefônico ou correio eletrônico fraudulento.

Do lado de quem recebe esse material, a Lei 13.709/2018 (LGPD) classifica dado biométrico como dado pessoal sensível no artigo 5º, inciso II, e o artigo 11 restringe o tratamento dele. Uma selfie obtida por engano não vira base legal por ter sido "enviada pelo titular": o consentimento que a LGPD reconhece é livre e informado, e não há nada de informado numa pessoa que acredita estar falando com outra empresa.

O que uma verificação legítima nunca faz

A parte prática começa aqui, e ela é curta o bastante para caber num rodapé.

Uma verificação de identidade legítima acontece **dentro** do site ou do aplicativo da empresa que a pediu. Ela começa por um ato do titular, não por um contato frio: a pessoa estava abrindo conta, contratando, alterando cadastro ou pedindo algo. Ela não chega por ligação, mensagem ou e-mail pedindo que o documento seja enviado por fora do fluxo. E o fornecedor de verificação não fala com o titular: quem tem relação com a pessoa é a empresa contratante, e é ela quem atende.

Disso vem uma regra simples para o titular: não existe motivo legítimo para mandar documento ou selfie por aplicativo de mensagens, por e-mail ou para um link recebido. A orientação do fascículo do CERT.br é a mesma, e ela é a mais útil que existe neste assunto: confirme a história com a organização usando um contato oficial ou já conhecido, nunca o contato que veio na mensagem.

Há ainda o tom. O material do CERT.br lista os sinais que quase sempre aparecem: ameaça, pressão, constrangimento, pedido de segredo, obediência à autoridade. Verificação de identidade de verdade não trabalha assim. Ela pode falhar, pode pedir uma nova foto, pode passar por revisão humana, e nada disso envolve prazo de minutos nem ameaça de bloqueio imediato.

E existe uma agravante nova que vale registrar sem alarme: o fascículo alerta que golpistas já produzem imitações de voz e de rosto com inteligência artificial. Isso não muda a regra acima. Muda só a confiança que se pode depositar num áudio ou num vídeo recebido, e reforça a mesma conduta: volte ao canal oficial.

Onde o aviso precisa morar

A contramedida de produto é um aviso permanente, curto, e em todo lugar onde a marca aparece. Permanente porque golpe não tem temporada. Curto porque ele divide espaço com o rodapé. E em todo lugar porque a pessoa que recebeu a mensagem falsa vai procurar a empresa pelo caminho que ela achar primeiro, e esse caminho raramente é a página que alguém escolheu para o aviso.

Três decisões tornam isso barato de manter. A primeira é escrever a frase uma vez só, num módulo, e consumir essa constante em cada superfície: frase repetida em três arquivos envelhece em dois deles. A segunda é declarar o que a **casa** não faz, e nunca o que o produto deixa de detectar: a primeira informação protege o titular, a segunda entrega o roteiro ao criminoso. A terceira é transformar a mesma verdade numa pergunta do FAQ público, porque a pessoa em dúvida pesquisa em forma de pergunta.

Do lado da empresa contratante, duas medidas somam. Manter um canal de retorno oficial que o cliente conheça, como já vale para o golpe da falsa central. E treinar o atendimento para não tratar reenvio de documento como tarefa de rotina, que é a porta usada pela engenharia social contra o atendimento.

Nada disso impede a mensagem falsa de existir. O que isso faz é garantir que, quando a pessoa desconfiar e procurar, ela encontre a resposta em um clique, escrita pela própria empresa, no lugar onde ela foi procurar. Golpe se combate encurtando a distância entre a dúvida e a verdade.

Fontes citadas

- CERT.br, NIC.br e CGI.br, fascículo "Golpes: Não se Deixe Enganar" da Cartilha de Segurança para Internet, março de 2026: cartilha.cert.br
- Código Penal, Decreto-Lei 2.848/1940, artigo 171 (estelionato), parágrafo 2º-A (fraude eletrônica, incluído pela Lei 14.155/2021) e artigo 307 (falsa identidade): planalto.gov.br
- Lei 14.155, de 27 de maio de 2021, que tratou de crimes cometidos por meio eletrônico: planalto.gov.br
- Lei 13.709/2018 (LGPD), artigo 5º, inciso II, e artigo 11: planalto.gov.br

Sobre este guia

Este guia reúne, sem alteração de texto, artigos do blog da UNIFOKAL, plataforma brasileira de verificação de identidade. O endereço original de cada artigo está logo abaixo do título dele, e as fontes citadas continuam no fim de cada um.

A versão web deste guia, com os artigos atualizados, fica em <https://unifokal.com/publicacoes#antifraude-no-onboarding>.