Biometria digital :

Processo de Extração[[editar](https://pt.wikipedia.org/w/index.php?title=Biometria&veaction=edit&section=2) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Biometria&action=edit&section=2)]

No que diz respeito ao cadastramento, análise e validação dos processos biométricos, eles se assemelham por utilizarem a mesma estrutura, independente da parte do corpo utilizada. Isso se deve ao fato desses sistemas serem base de dados acessíveis e de rápida análise, facilitando assim a comprovação da identidade da pessoa em questão.[[5]](https://pt.wikipedia.org/wiki/Biometria#cite_note-5) Os processos são:

* **Captura**

A primeira etapa é o registro em si do que será utilizado para a comprovação identitária. Ou seja, é o processo de botar a digital no leitor; repetir “casa”, “martelo”, “cachorro”, “praia por favor” ou qualquer outra coisa demandada por aquela tecnologia. O sistema pode pedir pra você repetir esse processo caso a coleta não tenha sido suficientemente fiel ou clara.

* **Extração:**

A extração é etapa onde os dados coletados são traduzidos em informações identificáveis pelo sistema utilizado. Cada sistema possui seu próprio método de tradução, variando em termos de confiabilidade e rigor análitico para transformar a imagem ou arquivo em bits inteligíveis pela máquina.

* **Criação de Padrão:**

Após ter traduzido as informações para a linguagem computacional, o próprio sistema cria um padrão único para esse cadastro, de acordo com as características reconhecíveis pelo sistema biométrico. Essa parte é o formato inicial traduzido em formato final para armazenamento; ou seja, é a sintetização da imagem como um todo (no que diz respeito à biometria ocular, por exemplo) em um padrão facilmente acessível pelo sistema, diminuindo o tempo de análise como um todo.

* **Comparação:**

Após o registro e a criação do padrão, a comparação é feita para comprovar a eficiência com a qual o sistema cadastrou as informações necessárias. Caso o sistema retorne com falhas de identificação – ou até mesmo falsos positivos devido à baixa qualidade das informações retiradas – o processo é refeito até que a comparação retorne com resultados coerentes e confiáveis.[[6]](https://pt.wikipedia.org/wiki/Biometria#cite_note-6)

Alguns dos principais sistemas de leitura biométrica:

* A) **Veias**: fiabilidade média , difícil de fraudar, alto custo.
* B) **Impressão digital**: Sistema que capta a imagem da impressão digital com um leitor biométrico óptico e compara com um banco de dados de imagens com as digitais gravadas. Método rápido, de alta confiabilidade e baixo custo.
* C) **Reconhecimento da face**: menor fiabilidade, rápido e de baixo custo.
* D) **Identificação pela íris**: muito fiável, imutável com o passar dos anos, alto custo.
* E) **Reconhecimento pela retina**: fiável, imutável, leitura difícil e incómoda na medida em que exige que a pessoa olhe fixamente para um ponto de luz, alto custo.
* F) **Reconhecimento de voz**: menos fiável, problemas com ruídos no ambiente, problemas por mudança na voz do utilizador devido a gripes ou stress, demora no processo de cadastramento e leitura, baixo custo.
* G) **Geometria da mão**: menos fiável, problemas com anéis, o utilizador precisa de encaixar a mão na posição correcta, médio custo.
* H) **Reconhecimento da assinatura**: muito fiável, algumas assinaturas mudam com o passar do tempo, porém características como pressão, movimentos aéreos, entre outras são únicas de cada indivíduo, tornando extremamente difícil sua falsificação. Método prático e ágil, acessível a todos os públicos, médio custo.
* I) **Reconhecimento da digitação**: pouco fiável, demora no cadastramento e leitura, baixo custo.
* J) **Tecnologias futuras:** odores e salinidade do corpo humano, padrões das veias por imagens térmicas do rosto ou punho, análise de DNA.
* K) **Estilo de Escrita**: biometria comportamental baseada no estilo de escrita [[7]](https://pt.wikipedia.org/wiki/Biometria#cite_note-BROC2017-7).

Biometria Facial:

## Reconhecimento Facial[[editar](https://pt.wikipedia.org/w/index.php?title=Biometria&veaction=edit&section=8) | [editar código-fonte](https://pt.wikipedia.org/w/index.php?title=Biometria&action=edit&section=8)]

Esse processo coleta imagens tridimensionais e analisa as métricas dos componentes, a partir de pontos de medida do rosto, que faz uma ligação algorítmica de traços e tamanhos, entre outros detalhes processando e comparando com as imagens cadastradas. Há duas opções para esse tipo de biometria: ou o sistema em si faz o reconhecimento e a autorização; ou há um técnico que analisa a coerência entre a imagem disposta e a face da pessoa em questão.

A confiabilidade desse sistema depende plenamente da consolidação do programa em si, e os algoritmos utilizados. Quão maior for o número de traços e métricas analisados, mais confiável será o sistema. No entanto, ao mesmo tempo que métricas a mais ajudem no que diz respeito à confiabilidade dos processos de segurança nele contidos, eles também tornam o sistema mais devagar e menos responsivo. Isso se deve pelo fato do algoritmo precisar analisar todas as imagens com as mesmas métricas utilizadas para cadastrá-las.

No Brasil, esse sistema foi implementado para combater fraudes no sistema de transporte público[[12]](https://pt.wikipedia.org/wiki/Biometria#cite_note-12), sendo testado no final do ano passado em Campinas. De acordo com dados oficiais, 25% dos 155 mil indivíduos possuem algum tipo de benefício indevido (normalmente isso se resume aos pais ou avôs emprestando os cartões com passe livre para amigos e filhos), ou seja, mais de 30 mil pessoas usufruem do sistema sem pagar as devidas taxas.[[13]](https://pt.wikipedia.org/wiki/Biometria#cite_note-13)

A tecnologia de reconhecimento facial tem evoluído e hoje é capaz de reconhecer emoções. Esta ferramenta pode levar a ajudar policiais reconhecendo emoções de estresse, raiva e comportamento suspeito.

Biometria da íris

A íris é um músculo no olho, a parte visível do olho humano responsável pela coloração do olho.

A cor e a estrutura do olho humano são definidas geneticamente. Porém, a forma que a íris ganha é única e é formada no período pré-natal devido a alguns processos biológicos.

Uma característica fundamental da íris, que a torna um ótimo meio para se reconhecer indivíduos através da biometria, é a sua unicidade. Isso significa que a íris de cada indivíduo é diferente da íris de outro. A íris começa a se desenvolver no terceiro mês de gestação e só desenvolve sua forma completa no oitavo mês (embora a coloração possa continuar mudando após o nascimento). O desenvolvimento da íris (mas não da cor dos olhos) não segue nenhum padrão genético e ela se forma quase que totalmente de forma aleatória. A probabilidade de uma íris ser idêntica a outra é aproximadamente 1 em 1072. Essa probabilidade praticamente garante que não haverá nenhuma íris idêntica a outra no mundo.

 a íris permanece a mesma desde um ano de idade até a morte do indivíduo, ela não é contaminada com nenhum tipo de substância estranha ao organismo e não sofre nenhum efeito com idade.

A localização da imagem de uma íris é muito importante, por que, obviamente, se a imagem for capturada de forma errada a identificação do usuário pode falhar. De fato, existem vários fatores que devem ser considerados ao se capturar a imagem de uma íris e que podem afetar o desempenho do processo como um todo. Reflexos, movimentação do olho no momento de captura da imagem, pálpebras e cílios podem atrapalhar na aquisição da imagem de uma íris.

Para adquirir a imagem de uma íris é recomendado o uso de uma boa câmera digital (alguns celulares e pen-drives hoje em dia já possuem sistema de reconhecimento de íris). Uma técnica muito utilizada é a iluminação da íris utilizando luz infra-vermelha, de forma a não incomodar o usuário (pois é invisível ao usuário), iluminar a íris para uma melhor aquisição e através da variação do brilho da luz, verificar se houve dilatação da púpila, para prevenir que olhos falsos sejam utilizados para enganar o sistema.

doenças no olho podem prejudicar a identificação, como catarata, conjuntivite, tremor nos olhos ou alergias.

Biometria de retina:

 retina é a parte do olho sensível a luz. Ela contém milhões de células fotossensíveis chamadas de cones e de bastonetes. Estas transformam energia luminosa em impulsos nervosos que serão interpretados pelo cérebro. No fundo do olho próximo ao centro há uma pequena depressão, onde existem apenas cones, que é chamada de fóvea (Figuras 1 e 2). Esse é o local onde a imagem se forma com maior nitidez. O eixo que liga a pupila à fóvea é conhecido como eixo óptico.

        Os impulsos nervosos são transmitidos pelo nervo óptico. Como a região por onde ele sai da retina não possui cones ou bastonetes, nenhuma imagem é processada ali. Por isso, essa região é conhecida como ponto cego. Ele pode ser visto na figura 2, como a região mais clara também chamada de disco óptico.Do mesmo ponto, saem também os vasos sanguíneos que abastecem a retina. O padrão de distribuição desses vasos é único para cada pessoa, sendo tão complexo que até gêmeos idênticos não possuem a mesma configuração. Além disso, ele não muda durante toda vida do indivíduo, exceto em caso de mutilação ou condições médicas que alterem o olho de alguma forma (Fig. 2).

 O fato de a retina possuir uma configuração única e ser muito estável ao longo da vida (é muito difícil alterá-la) faz dela, não só ideal para servir de parâmetro para uma biometria, como também uma das biometrias mais confiáveis conhecidas.

Funciona por meio da captação/ mapeamento dos vasos sanguíneos no olho, problemas como astigmatismo ou miopia podem influenciar no resultado, dificultando a obtenção de dados. É um sistema de altos custos e funciona muito bem, baixas chances de erros. A distância pode influenciar na hora de obter os dados da retina.

One time password:

**Senha descartável** ou **senha de uso único** (em [inglês](https://pt.wikipedia.org/wiki/L%C3%ADngua_inglesa): *One-time password* - OTP) é uma [senha](https://pt.wikipedia.org/wiki/Senha) que é válida somente para uma sessão de [login](https://pt.wikipedia.org/wiki/Login) ou transação, em um sistema de computadores ou outros dispositivos digitais.[[1]](https://pt.wikipedia.org/wiki/Senha_descart%C3%A1vel#cite_note-1) OTPs evitam uma série de deficiências que estão associadas às autenticações tradicionais (estáticas), baseada em uma senha; uma séries de implementações também incorporam autenticação de dois fatores, garantindo que a senha de uso requer acesso a algo que uma pessoa tem (como um pequeno chaveiro OTP ou um celular específico), bem como algo que a pessoa sabe (como um PIN)

A vantagem mais importante que é dada pelas OTPs é que, em contraste com as senhas estáticas, elas não são vulneráveis a ataques replay. Isso significa que um potencial intruso que consiga capturar uma OTP que já foi usada para fazer login em um serviço ou uma transação, não conseguirá utilizá-la, uma vez que ela não será mais válida. Uma segunda maior vantagem é que um usuário que usa a mesma senha (ou similar) para múltiplos sistemas, não fica vulnerável em todos eles, se a senha de um deles for conseguida pelo atacante.

O uso de senhas descartáveis OTP é uma das mais simples soluções e de fácil implementação. A finalidade é fazer com que o usuário informe senhas diferentes a cada acesso.[[*carece de fontes*](https://pt.wikipedia.org/wiki/Wikip%C3%A9dia:Livro_de_estilo/Cite_as_fontes)]

Se porventura uma senha de acesso for capturada, ela não terá nenhum valor, já que para um novo acesso, uma nova senha deverá ser informada, claro que diferente da atual. Isso acontece porque no momento que a [conexão](https://pt.wikipedia.org/wiki/Conex%C3%A3o) é aceita, automaticamente a senha que foi usada para [autenticação](https://pt.wikipedia.org/wiki/Autentica%C3%A7%C3%A3o) é descartada, fazendo com que a próxima conexão seja informada uma senha diferente.[[*carece de fontes*](https://pt.wikipedia.org/wiki/Wikip%C3%A9dia:Livro_de_estilo/Cite_as_fontes)]

Existem varias formas de gerar senhas, sendo com o uso de [calculadoras](https://pt.wikipedia.org/wiki/Calculadora) de senhas ou essas mesmas calculadoras implementadas em sistemas operacionais, [PDA](https://pt.wikipedia.org/wiki/PDA" \o "PDA)’s, celulares ou até mesmo soluções multiplataformas, como [Java](https://pt.wikipedia.org/wiki/Java_(linguagem_de_programa%C3%A7%C3%A3o)), que permite o funcionamento através de navegadores convencionais. O uso desta calculadora melhora bastante a segurança, em geral causa pouco incomodo visto que podem estar disponíveis em um dispositivo que o usuário carrega consigo.[[*c*](https://pt.wikipedia.org/wiki/Wikip%C3%A9dia:Livro_de_estilo/Cite_as_fontes)

Reconhecimento de voz:

<https://www.tecmundo.com.br/curiosidade/3144-como-funciona-o-reconhecimento-de-voz-.htm>

Token:

<https://en.wikipedia.org/wiki/Tokenization_(data_security)>

SQRL:

**S**ecure **Q**uick **R**eliable **L**ogin

A highly secure, comprehensive, easy-to-use replacement  
for usernames, passwords, reminders, one-time-code  
authenticators**. . .** and everything else.

<https://www.grc.com/sqrl/sqrl.htm>

LOCALIZAÇÃO GEOGRÁFICA:

http://www.scielo.br/pdf/rec/v15n1/a05v15n1.pdf