

Biometria - Quando o corpo fala !

José Luis Amâncio
financeir@globo.com

A Biometria é uma ciência que possibilita o reconhecimento e autenticação segura de determinada pessoa utilizando características físicas (como impressão digital, altura, peso, íris, reconhecimento facial, geometria das mãos, voz...) e padrões de comportamento (como a escrita, através de padrões de assinatura).

Através de softwares e algoritmos que tornam o reconhecimento seguro e rápido e tecnologia de hardware foi possível chegar ao desenvolvimento e aplicação da Biometria. Os sistemas de reconhecimento biométrico podem fazer a autenticação segura de usuários em meio segundo, através da leitura e armazenamento seguro dos dados.

As soluções de identificação e acesso baseadas em biometria têm um fator de segurança maior porque os cartões, senhas, crachás e números de acesso podem ser roubados e/ou emprestados, enquanto os dados biométricos são inerentes ao indivíduo.

As soluções de reconhecimento biométrico podem ter um custo inicial eventualmente superior aos demais meios, porém devido ao fato de dispensar mídias de reconhecimento (chips, cartões magnéticos, cartões inteligentes, crachás...) possuem custos de manutenção e utilização menores, o que viabiliza sua utilização.

Estas soluções são pouco utilizadas porque desconhecidas por muitas pessoas ou por dúvidas quanto ao custo e retorno dos investimentos necessários. No entanto, atualmente existem tecnologias de análise e autenticação biométrica suficientemente diversificadas, desenvolvidas e com um preço acessível a um grande número de empresas e entidades interessadas na correta e segura identificação de usuários de seus serviços e ou produtos.

A biometria é aplicável em atividades tais como:

Autenticação de usuários de sistemas :(internet, sistemas operacionais, redes corporativas, gestão do conhecimento, soluções em e-learning...). Normalmente para este tipo de aplicação há a utilização de um leitor de impressões digitais, de voz (microfone) ou de íris. Diferentemente de uma senha, estas características

pessoais não podem ser emprestadas ou copiadas, o que resulta em maior segurança.

Controle de acesso físico: aplicável em empresas (ponto e assiduidade de funcionários), condomínios, bancos, clubes, escolas, aeroportos, hospitais e tantos outros locais de circulação de pessoas.

Transações financeiras: aplicável a quiosques eletrônicos, consultas bancárias, transações e pagamentos eletrônicos, reconhecimento de assinaturas.

Portanto, não se surpreenda se num futuro próximo, ao invés de usar um cartão magnético, você simplesmente olhar para a catraca de acesso para poder entrar.

José Luis Amancio, 35 anos, é diretor da Consultoria Metis Quality, economista, com especialização em Comércio Eletrônico, Planejamento Empresarial e Logística e atualmente Pós Graduando da FGV – E-mail: financeir@globocom.com