ISABELLY CRISTINA FERREIRA

LARISSA DA SILVA DI' RICO RAMOS

SEGURANÇA POR MEIO DE MÉTODOS BIOMÉTRICOS

Artigo aprovado como requisito parcial à obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/Americana.

Área de concentração: Segurança da Informação

Banca Examinadora:

_____

Prof. Dr. Daives Arakem Bergamasco
Doutor
Faculdade de Tecnologia de Americana

_____

Prof. Luciano Camilo Malvesti
Especialista
Faculdade de Tecnologia de Americana

_____

Profª. Silvia Aparecida Jose e Silva
Mestra
Faculdade de Tecnologia de Americana

Americana, 30 de Junho de 2021.

Segurança por meio de métodos biométricos
Security through biometric methods

Isabelly Cristina Ferreira[1]
Larissa da Silva Di' Rico Ramos[2]
Daives Arakem Bergamasco[3]

Resumo
O conceito de biometria está cada vez mais sendo implantado, ainda mais quando se trata de segurança em suas variadas aplicações. Neste artigo será abordado o tema segurança da informação, e a importância de proteger as informações seja pessoal ou de uma organização, tipos de controle de acesso, o físico e lógico, o conceito de biometria e alguns dos vários tipos biométricos que temos na nossa atualidade, abordamos que a biometria é classificada de duas maneiras, a fisiológica onde os métodos consistem nas características relacionadas a forma do corpo, e a comportamental que está relacionada ao comportamento da pessoa.
E por fim, é apresentado um comparativo da qualidade dos métodos biométricos que foram abordados sobre qual seria o mais adequado para o controle de acesso.
Palavra-chave: Biometria. Controle de Acesso. Segurança. Métodos Biométricos.

Abstract
The concept of biometrics is increasingly being implemented, especially when it comes to security in its various applications. This article will address the subject of information security, and the importance of protecting information whether personal or from an organization, types of access control, the physical and logical, the concept of biometrics and some of the various biometric types that we have today, we approach that biometrics is classified in two ways, the physiological one where the methods consist of the characteristics related to the body shape, and the behavioral that this related to the person's behavior.
And finally, a comparison of the quality of the biometric methods that were approached on which would be the most suitable for access control is presented.
Keywords: Biometrics. Access Control. Security. Biometric Methods.

1. INTRODUÇÃO

Toda a ideia da biometria é conhecida pelo homem desde os primórdios, afinal de contas, distinguir um indivíduo do outro através das suas características físicas é um conceito que existe há muito tempo.

A proteção de informações essenciais para o bom andamento de um negócio, é para todos, desde a grande empresa multinacional, até o pequeno empreendedor autônomo. O que diferencia esses dois extremos é o conhecimento de técnicas e ferramentas, e a importância de se proteger essas informações ou locais que não devem ser acessados por pessoas não autorizadas.

O objetivo geral deste trabalho é apresentar os principais métodos biométricos existentes na nossa atualidade, explicando o funcionamento de cada um, e fazendo um comparativo entre eles quanto a sua eficiência na proteção de informação.

2. O QUE É SEGURANÇA DA INFORMAÇÃO

Podemos definir Segurança da Informação como uma área do conhecimento dedicada a proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade. (SÊMOLA, 2003)

Segurança da Informação conforme definido pela NBR ISO/IEC 17799 (2001, p. 2) "é a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de investimentos e oportunidades".

A segurança da informação é caracterizada pela preservação dos seguintes atributos básicos (NBR ISO/IEC 17799, 2001, p. 4):

a) Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso;

b) Integridade: salvaguarda da exatidão e precisão da informação e dos métodos de processamento;

c) Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Faculdade de Tecnologia de Americana
[1] isabelly.ferreira@fatec.sp.gov.br
[2] larissa.ramos2@fatec.sp.gov.br
[3] daives.bergamasco@fatec.sp.gov.br

A Tríade conhecida por CIA (*Confidentiality, Integrity and Availability*) apresentada na figura 1 a seguir, representa os princípios básicos da Segurança da Informação, conforme descrito acima pela NBR ISO/IEC 17799 (2001, p. 4):

Figura 1 - Segurança da Informação - Tríade CIA

Fonte: ABREU (2011).

A segurança da informação visa garantir a confidencialidade, integridade e disponibilidade da informação, a impossibilidade de que agentes participantes em transações ou na comunicação repudiem a autoria de suas mensagens, a conformidade com a legislação vigente e a continuidade dos negócios. (SÊMOLA, 2003).

3. CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação das informações dentro de uma empresa, tem por objetivo identificar o nível de segurança de cada informação pertinente a empresa. Identificar e classificar os tipos de informações e quem vai ter acesso a mesma.

Segundo Dejan Kosutic, não existe uma regra a seguir de como é feita a classificação da informação, segundo a ISO 27001. É uma prática adotada por cada empresa que pode fazer à sua maneira, seguindo as suas políticas e preferências da mesma.

Assim como é feito o inventário de recursos físicos, as informações também devem passar por esse processo de classificação, para saber onde os recursos financeiros devem ser mais investidos. Com isso, também é necessário fazer a segurança quanto ao armazenamento e acesso à essas informações.

A informação pode ser classificada de três a quatro tipos, dependendo de cada empresa: secreta, com alto nível de confidencialidade; confidencial, somente os ligados a informação tem acesso a mesma; interna onde a informação é de interesse e posse dos colaboradores da empresa e a informação pública que está disponível para todos.

Essa classificação pode trazer benefícios para a empresa, tais como proteger informações de grande valia ao negócio, compartilhar a responsabilidade da informação com os demais envolvidos, semear e cultivar a cultura da segurança da informação através dos bons hábitos e conscientização, de acordo com o Prof. Leonardo Lemes Fagundes, da Unisinos.

3.1. Secreta

Consiste no nível mais alto de confidencialidade de uma informação, (assunto que será abordado posteriormente), somente a alta gerência, proprietário da informação e pessoas chaves, possuem conhecimento desse ativo de valor para o negócio. As informações assim classificadas têm grande poder no negócio, a divulgação destas podem trazem prejuízos financeiros ou nas relações com clientes, fornecedores etc.

Segundo Francine Spanceski (2004, pág. 17) estas informações devem ser acessadas por um número restrito de pessoas e o controle sobre o uso destas informações deve ser total, são informações essenciais

para a empresa, portanto, sua integridade deve ser preservada. O acesso interno ou externo por pessoas não autorizadas a esse tipo de informação é extremamente crítico para a instituição.

3.2. Confidencial

Essas informações geralmente são pertinentes aos grupos de trabalho que lidam com essa informação em específico, que ela é necessária para a realização das tarefas pertinentes. Não sendo necessário que os demais nichos de trabalho da empresa tenham acesso a essas informações.

De acordo com a Francini Spanceski (2004, pág. 18), as informações confidenciais devem ficar restritas ao ambiente da empresa, o acesso a esses sistemas e informações é feito de acordo com a sua estrita necessidade, ou seja, os usuários só podem acessá-las se estes forem fundamentais para o desempenho satisfatório de suas funções na instituição. O acesso não autorizado à estas informações podem causar danos financeiros ou perdas de fatia de mercado para o concorrente.

3.3. Interna

Toda e qualquer informação que circule dentro da empresa, de livre acesso a todos, como horários, pautas, clientes, valores, custos, culturas, fornecedores etc. Podem ser classificadas como informação interna, não querer tanta privacidade como as demais citadas, e todos podem fazer uso e ter acesso as mesmas. O ideal seria que essas informações permanecessem dentro dos limites da empresa, para que demais pessoas, e até mesmo concorrentes do ramo, não venham a ter acesso e fazer mal uso desta.

Para Francini Spanceski (2004, pág. 18), essas informações não devem sair do âmbito da instituição. Porém, se isto ocorrer as consequências não serão críticas, no entanto, podem denegrir a imagem da instituição ou causar prejuízos indiretos não desejáveis.

3.4. Públicas

As informações que requerem menos proteção, que podem e devem ser de conhecimento de pessoas e/ou outras empresas, sejam parceiras de negócios, fornecedores, clientes e até mesmo concorrentes, são as informações públicas, que podem ser de conhecimento de uma porcentagem maior de pessoas/colaboradores, que não vão causar grandes prejuízos financeiros ou a imagem da empresa.

4. O QUE É CONTROLE DE ACESSO

O controle de acesso é qualquer mecanismo ou equipamento que limite a entrada de pessoas/usuários a determinados ambientes ou informação, ou seja, é a garantia da segurança dos dados, bens ou pessoas, impedindo que pessoas não autorizadas tenham acesso. Existem os tipos de controle de acesso lógico e físico, que iremos abordar e exemplificar a seguir.

4.1. Controle de acesso lógico

O controle de acesso lógico é um conjunto de medidas, procedimento e softwares que tem por objetivo proteger os dados contra tentativas de acesso não autorizadas feitas por alguma pessoa desconhecida, colaborador da empresa ou até mesmo um programa de computador.

4.1.1. O usuário sabe

Para conseguir o acesso, o usuário precisa saber dados como nome, senha, PIN, etc. Ou seja, informações que ele precisa, necessariamente, conhecer para ser autenticado. Esse tipo de acesso tem a vantagem de ser muito conhecido e simples de ser utilizado, mas pode ser facilmente burlada quando um terceiro consegue descobrir este tipo de dado, ainda que o faça de forma grosseira, como um simples processo de tentativa e erro.

Figura 2 – Acesso por senha.

Fonte: Site Comtele – 2021

4.1.2. O usuário possuí

São os itens que o usuário precisa ter em mãos para conseguir ter acesso. Como por exemplo: um código de validação via SMS, que só o proprietário do telefone informado, terá acesso ao código enviado. Cartão chave de segurança, onde existem vários números no cartão e um determinado código é solicitado para libera o acesso. Em alguns casos a própria empresa oferece, ou vincula o acesso, a algum aplicativo gerador de senhas para smartphones. Este tipo de acesso já é mais seguro que o anterior, pois necessita da posse do cartão ou do token para que seja liberado o acesso. Porém, ela não é à prova de riscos, pois técnicas de engenharia social já se mostraram eficientes para burlar este tipo de dado.

Figura 3 – Token de segurança.

Fonte: Site Comtele – 2021

4.1.3. Característica física do usuário

Nesse tipo de acesso, a autenticação por biometria tem a vantagem de ser mais rigorosa, pois utiliza fatores que, na sua maioria, não podem ser copiados, raras exceções. A leitura da impressão digital é a mais comum e mais antiga, mas há o reconhecimento facial da íris, de veias, reconhecimento de voz, etc. Talvez um contraponto seja em alguns casos, como gêmeos idênticos partilharem dos mesmos traços, assim podendo haver uma falha dessa identificação. Mas ainda não existe nenhum controle de acesso cem por cento antifalhas. (Mandarini, 2005)

Figura 4 – Biometria.

Fonte: Site IBTecnologia – 2021

4.2. Controle de Acesso Físico

Controle de acesso físico refere-se à utilização de medidas de segurança física (passivas e ativas), e de protocolos de gerenciamento, projetados para impedir o acesso não autorizador a áreas, pessoal, equipamentos, documentos, contraespionagem, sabotagem, atos de terrorismo, danos, furto e roubo.

É composto basicamente, por uma barreira perimetral (muro, cerca, alambrado ou combinações desses), um ou mais pontos de acessos (portarias), controlados por dispositivos mecânicos (exemplo: portões e cancelas) ou eletrônicos (exemplo: catracas e fechaduras eletrônicas) e por políticas e procedimentos de segurança física.

Refere-se a medidas de segurança física adotadas explorando-se os meios físicos e tecnológicos disponíveis, utilizando-os como barreira de proteção ao acesso a um ambiente físico controlado e a ativos críticos. É usado para gerenciar o fluxo de pessoas, veículos e bens físicos. (Marcondes, 2020)

5. BIOMETRIA: O QUE É E O QUE FAZ?

Em Segurança da Informação, a biometria consiste na aplicação de métricas a atributos biológicos, para fins de verificação de um indivíduo. Controla o acesso, físico e lógico, de pessoas à ambientes e arquivos, identificar e localizar criminosos, e serve como barreira que impede pessoas não autorizadas acessem dados sigilosos, protegidos por autores ou guardião daquela informação.

O termo biometria [bio (vida) + metria (medida)] é o estudo estatístico das características físicas ou comportamentais dos seres vivos e pode ser utilizada numa grande variedade de aplicações, pelo que é difícil defini-la de forma exclusiva. No entanto, uma das definições que nos parece mais adequada refere que a biometria é a utilização automatizada de características fisiológicas ou comportamentais para determinar ou verificar entidades. (Silva et al. 2007)

A biometria e os laboratórios criminais têm muito em comum. A biometria usa as características físicas ou comportamentais para determinar ou confirmar uma identidade. O laboratório criminal usa o mesmo tipo de informação para estabelecer fatos em investigações civis ou criminais. (Silva et al. 2007)

A biometria é um dos caminhos mais seguros para a identificação de pessoas e proteção de dados. Diferentemente de usar cartões magnéticos, senhas ou palavras de passa, a biometria pode verificar ou reconhecer, por exemplo impressões digitais, face, geometria das mãos e dados, íris, vasos da retina, entre outras diversas características humanas. (VIGLIAZZI, 2006)

Em uma linguagem muito simples, as soluções de biometria não fazem mais do que ler ou medir características únicas dos indivíduos e compará-las com as mesmas que já tinham sido recolhidas e armazenadas anteriormente num sistema (normalmente uma base de dados). Quase todos nós já estamos habituados a identificarmo-nos regularmente nas mais diversas situações – apresentando o bilhete de identidade, o passaporte ou outro cartão, ou ainda introduzindo códigos as palavras de passe. (Silva et al. 2007)

Além do rigor da identificação, podemos classificar as soluções de biometria em três categorias. Uma primeira categoria inclui as soluções que se baseiam em características comportamentais – coisas que fazemos de forma consistente (verificação da voz ou da escrita manual, por exemplo). Numa segunda categoria

incluem-se as soluções que se baseiam em características fisiológicas que se mantém estáveis ao longo da vida de qualquer pessoa, nomeadamente as características faciais, a geometria da mão e a escrita manual. A terceira categoria inclui as soluções que se baseiam em características discretas, por exemplo, a estrutura vascular da retina. (Silva et al. 2007)

6. TIPOS DE IDENTIFICAÇÃO BIOMÉTRICA

Existem várias formas de realizar a identificação pela biometria que são classificadas em duas classes principais.

- *Fisiológicas*: são relacionadas a forma do corpo. Onde temos como exemplo a impressão digital, reconhecimento facial, geometria da mão e palma e de reconhecimento da íris.
- *Comportamentais:* são relacionadas ao comportamental de uma pessoa. Onde temos como exemplo a verificação de assinatura, dinâmica de digitação e voz. (Barbosa et al. 2014)

Abaixo vamos exemplificar alguns modelos de identificação biométrica e explicar um pouco como funciona cada:

Figura 5 – Impressão Digital

Fonte: A segurança através da biometria

O método biométrico mais antigo e utilizado é a identificação por digital, é muito popular e devido a sua popularização, o de menor custo financeiro para implementação. É extremamente confiável, dada a baixíssima mutabilidade dos dados ao longo do tempo. Migrou suavemente dos meios analógicos para o digital.

Consiste na captura da formação de sulcos na pele dos dedos e das palmas das mãos de uma pessoa. Esses sulcos possuem determinadas terminações e divisões que diferem de indivíduo para indivíduo. Para esse tipo de identificação existem três tipos de tecnologia mais usadas: óptica, que faz uso de um feixe de luz para ler a impressão digital; capacitiva, que mede a temperatura que sai da impressão, e ultrassônica, que mapeia a impressão digital através de sinais sonoros. Um exemplo de aplicação de identificação por impressão digital é seu uso em fechaduras eletrônicas, onde o usuário deve colocar seu dedo em um leitor que ao confirmar a identificação, liberará seu acesso. (Silva et al. 2007)

Por digitais se manterem as mesmas ao longo da vida, a única possibilidade de apresentar problemas é caso ocorra da pessoa perder as suas digitais, por algum motivo. Devido a isso, o método pode ser utilizado sozinho ou combinado com outros.

Figura 6 – Reconhecimento Facial

Fonte: Site revista Digitalsecurity – 2021

O reconhecimento facial, onde o equipamento ou software utilizado faz as medições e parâmetros, cerca de 80 ângulos nodais no rosto do usuário, como distância entre os olhos, nariz e boca, e boca e queixo, para a identificação do mesmo. As medidas do rosto podem permanecer as mesmas com o passar do tempo, porém o envelhecimento ou até mesmo procedimentos cirúrgicos no rosto, podem fazer com que a somatória dessas informações sofra algumas alterações no resultado final. Ou até mesmo se o indivíduo possuir um irmão gêmeo idêntico, o mesmo pode ter acesso à informação protegida por esse método.

Apesar desta tecnologia não ser tão exata como a de impressões digitais, o reconhecimento facial tem várias vantagens na verificação automatizada e como ferramenta de identificação. O processo de fotografia digital que utiliza é algo a que as pessoas estão habituadas, não se sentido, portanto, desconfortáveis com esta forma de identificação. Por outro lado, o reconhecimento facial pode ser realizado à distância, sem a necessidade de o indivíduo tocar no dispositivo de captura biométrico. (Silva et al. 2007)

Figura 7 – Reconhecimento Íris

Fonte: A segurança através da biometria

O reconhecimento da íris mede os padrões da íris, ou seja, da área colorida em torno da pupila do olho. A íris é normalmente considerada como a característica biométrica mais exata, uma vez que pode ser medido em volume de informação mais significativo. O reconhecimento da íris pode ser realizado a curtas distâncias do leitor e utiliza uma fonte de luz de infravermelhos de baixa intensidade, similar ao que é utilizado no controle remoto de um televisor. O reconhecimento da íris tem vindo a ganhar popularidade naquelas áreas em que as pessoas têm de utilizar luvas ou outra roupa protetora na sua atividade normal, uma vez que a recolha de impressões digitais não é muita prática. O reconhecimento da íris também está sendo utilizado para o acesso a instalações e em aplicações de controle fronteiriço. (Silva et al. 2007)

O scanner da íris pode parecer futurístico, mas o centro do sistema é uma simples câmera digital CCD. O escaneamento usa tanto a luz quanto à luz infravermelha para ter uma foto clara e de alto contraste da íris. Próximo à luz infravermelha, a pupila de uma pessoa fica bem escura, facilitando a separação, pelo computador, da pupila e da íris.

Quando você olha para um scanner de íris, ou a câmera focaliza automaticamente ou você usa um espelho ou um feedback sonoro do sistema para ter certeza de que seu posicionamento está correto. Normalmente seu olho fica de 7,5 cm a 25 cm da câmera.

Quando ela tira uma foto, o computador localiza:

- O centro da pupila
- A beirada da pupila
- A beirada da íris
- As pálpebras e os olhos

Em seguida o scanner analisa os modelos da íris e os traduz para um código. Os scanners de íris estão se tornando mais comuns nos aplicativos de alta segurança, porque os olhos das pessoas são únicos (a possibilidade de trocar o código de uma íris pelo de outra é de 1 em 10 elevado à 78ª potência). Os olhos também permitem mais de 200 pontos de referência para comparação, diferente dos 60 ou 70 pontos das impressões digitais.

A íris é uma estrutura visível, mas protegida, e não se modifica com o tempo, tornando-se ideal para a identificação biométrica. Na maioria das vezes, os olhos das pessoas permanecem ilesos após uma cirurgia ocular e mesmo as pessoas cegas podem usar scanner de íris, desde que seus olhos tenham íris. Os óculos e as lentes de contato normalmente não interferem nem causam inexatas. (Silva et al. 2007)

Figura 8 – Biometria Vascular

Fonte: A segurança através da biometria

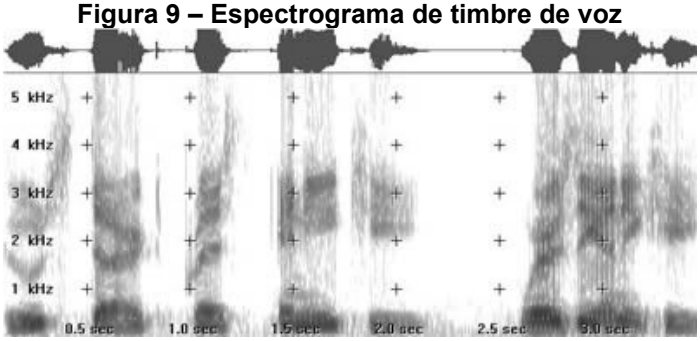
Quanto ao reconhecimento do padrão das veias, é uma tecnologia biométrica nova que utiliza luz projetada para a pele de uma pessoa, para permitir uma comparação de alto contraste dos padrões de veias nos dedos ou na área da mão. O padrão das veias de sangue é único para cada indivíduo e este padrão não varia ao longo da vida das pessoas. A medição de características que estão por baixo da pele faz com que sejam mais difíceis de observar pelos outros, tornando assim a característica biométrica do padrão das veias, um método de verificação especialmente seguro.

Assim como a íris e as impressões digitais, as veias de uma pessoa também são características exclusivas. Gêmeos não têm veias idênticas e as veias de uma pessoa são bem diferentes nos lados esquerdo e direito. Muitas não são visíveis através da pele, tornando-se extremamente difíceis de serem falsificadas ou manipuladas. Suas formas também se modificam muito pouco com a idade.

Para usar um sistema de reconhecimento de veias, você simplesmente posiciona seu dedo, pulso, palma ou as costas das mãos no scanner ou bem próximas a ele. Uma câmera captura uma foto digital usando luz infravermelha. A hemoglobina presente no sangue absorve a luz, de forma que as veias aparecem escuras na foto. Assim como com todos os outros tipos biométricos, o software cria um padrão de referência baseado no formato e na localização da estrutura das veias.

Os scanners que analisam a geometria das veias são totalmente diferentes dos usados nos testes hospitalares. Os scanners com finalidades médicas normalmente usam partículas radioativas. Já os scanners da segurança biométrica apenas usam uma luz parecida com a luz que vem de um controle remoto. (Silva et al. 2007)

Figura 9 – Espectrograma de timbre de voz



Fonte: A segurança através da biometria

A identificação por voz funciona através da dicção de uma frase que atua como senha. O usuário deverá informar a um reconhecedor a tal frase sempre que for necessária sua identificação. O entrave dessa tecnologia é que ela deve ser usada em ambientes sem ruídos, pois estes podem influenciar no processo. Além disso, se o indivíduo estiver rouco ou gripado sua voz sairá diferente e poderá atrapalhar sua validação. Por esta razão, a identificação por voz ainda é pouco aplicada. (Barbosa et al. 2014)

Quando as pessoas pensam no timbre de voz, normalmente pensam na onda que variam em um osciloscópio. Mas os dados usados no timbre de voz são um espectrograma de som e não o formato de uma onda. Um espectrograma é basicamente um gráfico que exibe a frequência do som no eixo vertical e o tempo no eixo horizontal. Diferentes sons de falas criam diferentes formatos dentro do gráfico. Os espectrogramas também usam cores ou tons de cinza para representar as qualidades acústicas do som.

Algumas empresas usam o reconhecimento do timbre de voz para que as pessoas tenham acesso à informação ou possam passar informações sem estar fisicamente presentes. Em vez de aproximar-se de um scanner de íris ou de um leitor de geometria das mãos, alguém pode fazer uma autorização dando um simples telefonema. Infelizmente, as pessoas conseguem enganar alguns sistemas, principalmente os que funcionam por telefone, com uma simples gravação de voz de uma pessoa autorizada. (Silva et al. 2007)

Figura 10 – Sistema biométrico para identificação por assinatura

Fonte: O uso da biometria em sistemas de segurança

Esse tipo de identificação consiste na comparação da assinatura com uma versão gravada em um banco de dados. Além disso, é feita a verificação da velocidade da escrita, a força aplicada, entre outros fatores. É um dos mecanismos mais usados em instituições financeiras, embora não se trate completamente de um método biométrico. É importante frisar que todos esses métodos possuem alguns entraves que os fazem necessitar de aperfeiçoamento ou, dependendo do caso, da aplicação de outra solução. Por exemplo, na identificação por retina, a pessoa que estiver usando óculos deve retirá-lo; na identificação por face, um ferimento ou um inchaço no rosto pode prejudicar o processo; na identificação da geometria da mão, um anel também pode trazer problemas; na identificação por voz, ruídos externos, rouquidão ou até mesmo uma imitação da voz de um indivíduo pode pôr em dúvida o procedimento; na comparação de assinaturas, o estado emocional da pessoa pode atrapalhar e há ainda o fato da escrita mudar com o passar do tempo. (Barbosa et al. 2014)

7. COMPARATIVO ENTRE A QUALIDADE DOS MÉTODOS PARA O CONTROLE DE ACESSO

Qualquer característica humana, seja ela fisiológica ou comportamental pode ser usada como característica biométrica, desde que satisfaça os seguintes requisitos básicos (Clark, 1994; Jain 2000.):

- **Universalidade**: consiste na capacidade de ser aplicável a todos os indivíduos, ou seja, todas as pessoas devem possuir a característica biométrica a ser utilizada como medida;
- **Unicidade**: consiste na capacidade de distinguir todos os indivíduos, indicando que a característica biométrica utilizada deve ser única para cada indivíduo, à possibilidade de pessoas distintas possuírem características idênticas deve ser nula ou desprezível;
- **Permanência ou Imutabilidade**: consiste na capacidade da característica não modificar ao longo da vida do indivíduo. Algumas alterações podem ocorrer devido ao envelhecimento, emocionais ou no processo de aquisição;
- **Mensurabilidade**: Consiste na possibilidade da característica biométrica ser medida quantitativamente;

Além desses requisitos, existem outras exigências importantes referentes ao funcionamento do sistema de reconhecimento biométrico, que são (Clark, 1994; Jain 2006):

- **Desempenho**: consistem na precisão, velocidade e segurança do sistema biométrico em reconhecer corretamente o indivíduo e os fatores ambientais que afetam a precisão do sistema;
- **Aceitação**: consiste na capacidade do indivíduo integrar a esse tipo de tecnologia no seu cotidiano, isto é, o quanto as pessoas estão dispostas a aceitar a biometria utilizada;
- **Circunvenção**: consiste na facilidade de burlar a característica biométrica através da utilização de técnicas fraudulentas;
- **Maturidade da pesquisa**: consiste na quantidade de pesquisas e resultados relevantes sobre a característica biométrica;

- **Tamanho do padrão**: consiste no número de bytes necessários para fins de armazenamento do padrão;
- **Tamanho do sensor**: consiste das dimensões do sensor e implicam se o sistema pode ser aplicado a meios móveis e se será percebido pelo indivíduo;
- **Tipo do sensor**: consiste na divisão dos sensores em classes: não-invasiva ou invasiva.

Tabela 1 – Comparação das tecnologias biométricas.

Biometria	Universalidade	Unicidade	Permanência	Desempenho	Aceitação	Circunvenção
Impressão Digital	Média	Alta	Alta	Alta	Média	Média
Reconhecimento Facial	Alta	Alta	Média	Baixa	Alta	Alta
Reconhecimento íris	Alta	Alta	Alta	Alta	Baixa	Baixa
Biometria vascular	Média	Média	Média	Média	Média	Baixa
Identificação voz	Média	Baixa	Baixa	Baixa	Alta	Alta
Identificação por assinatura	Baixa	Baixa	Baixa	Baixa	Alta	Alta

Fonte: Investigação de um modelo de arquitetura biométrica multimodal para identificação pessoal

A tabela 1 (Jain, 2004; Jain, 2006.) mostra a avaliação do grau (alta, média ou baixa) que cada característica biométrica satisfaz as propriedades desejáveis, é certo, que nenhuma característica biométrica consegue satisfazer com perfeição aos requisitos de uma característica biométrica ideal, cada uma possui suas vantagens e desvantagens em relação as demais, por isso a escolha da(s) característica(s) deve ser a que melhor atende aos requisitos desejados.

A seguir será apresentado mais detalhadamente cada método de biometria expondo suas vantagens e desvantagens, segundo Eric Silva:

- **Impressão digital**: este é o método mais rápido, possui alta confiabilidade e baixo custo. Por ser um dos métodos mais simples de implantar-se, este foi o método mais difundido até o momento. Devido ao pequeno tamanho dos leitores, é um método considerado pouco intrusivo pelos usuários.
- **Reconhecimento da face**: método não tão confiável, porém rápido e de baixo custo. Este método é o mais natural dentre os outros. Nele são registrados vários pontos delimitadores do rosto, definindo proporções entre queixo, orelhas, olhos etc. A identificação é difícil pelo fato de a aparência facial mudar constantemente (ângulo, estilo de cabelo, expressões faciais, barba etc.).
- **Reconhecimento pela íris:** método muito confiável, imutável com o passar dos anos (estrutura não se altera), porém de alto custo. Normalmente, os sistemas de reconhecimento de íris não são invasivos e requerem uma menor interação do usuário do que nos outros métodos biométricos. Este método apresenta como principal vantagem a baixa taxa de falsa aceitação.
- **Reconhecimento de voz:** este é um dos métodos menos invasivos e tem como o reconhecimento de fala, a sua forma mais natural de uso. Possui uma menor confiabilidade, além de ter problemas com ruídos oriundos do ambiente e problemas por mudança na voz do usuário causados por gripes ou estado emocional e o processo de cadastramento e leitura é demorado, porém possui baixo custo.
- **Geometria da mão:** possui uma menor confiabilidade, apresenta problemas com anéis e é necessário que o usuário encaixe a mão na posição correta, porém possui médio custo, requer pouco espaço de armazenamento e pouco esforço ou atenção por parte do usuário durante a verificação.
- **Reconhecimento da assinatura:** possui uma menor confiabilidade, há algumas assinaturas que são modificadas com o passar do tempo, existem também problemas na velocidade e pressão durante a escrita e possui médio custo. É um método que já é muito utilizado e popular, uma vez que em todos os cheques a verificação é feita através das assinaturas. Dentro deste método, são duas as técnicas de identificação: comparação da assinatura escrita com um modelo já armazenado (não consegue identificar fotocópias da assinatura) e análise da dinâmica da assinatura (sujeita ao humor, ambiente etc.). (Silva,2007)

8. CONSIDERAÇÕES FINAIS

A informação é o bem mais precioso que uma organização possuí. As informações do negócio, informações dos funcionários e clientes, tem alto valor para a organização, e proteger adequadamente essa informação é essencial para evitar danos futuros. Depois de classificar a informação e conhecer os tipos de biometria, é possível escolher o método para proteger essas informações, quanto mais relevante a informação, mais alto deve ser o nível de segurança protegendo-a. Afirmar que um método é melhor do que outro é subjetivo, tudo vai depender da necessidade e orçamento da organização. O método mais seguro de controle de acesso, é o que vai atender e suprir todas as necessidades da organização, assim sendo, cabe a equipe gestora analisar e escolher o melhor método para assegurar essas informações.

Alguns fatores que podem ser levados em consideração na hora de fazer estes levantamentos, são: custo-benefício, de fácil ou acessível manutenção/instalação, fácil utilização, rápida resposta do programa, fazer a leitura de maneira rápida e eficiente, suporte ao usuário, entre outros tópicos. Seja qual o método escolhido, o importante é as informações estarem seguras e apenas disponível para quem lhe for devido, quando e onde.

Dentre qualquer um dos métodos a escolher, é importante ressaltar que é necessário fazer calibragem e recadastramento de tempos em tempos, de acordo com a necessidade. Com o passar do tempo, nossas características físicas, vão sofrendo a ação do tempo e idade, a pele vai ganhando rugas, as digitais vão ficando mais finas, e essas marcas do tempo podem aparecer ainda mais rápido dependendo da ocupação do usuário. Então é necessária essa atualização cadastral do método para que ele seja e continue sendo o mais eficaz.

Com base nas pesquisas e resultados do artigo, os dois métodos mais indicados para o controle de acesso, podem ser o leitor de digital e o de reconhecimento facial. São os mais utilizados, de fácil acesso e manutenção e de simples utilização no dia a dia, com respostas rápidas as solicitações. Com o decorrer dos anos, a qualidade de captura de imagem aumentou muito e assim tornando ainda mais fácil o uso e manuseio desses meios. Se a tecnologia continuar a caminhar e se desenvolver nessa mesma linha de desenvolvimento, o futuro desses métodos, digital e facial, tende a ser ainda mais promissor, fazendo valer ainda mais o investimento.

9. REFERÊNCIAS

ABREU, Leandro Farias dos Santos. **A segurança da informação nas redes sociais, 2011**. Disponível em: <http://www.fatecsp.br/dti/tcc/tcc0023.pdf> acesso em 27 de março de 2021.

A. Jain, L. Hong, and S. Pankanti. **Biometric Identification**. COMMUNICATIONS OF THE ACM. v. 43, n. 2. February 2000 pp.91- 98

A. K. Jain. **Biometric System Security.** Dept. of Computer Science and Engineering Michigan State University. Japan January 2006. Disponível em <http://biometrics.cse.msu.edu> acesso em 05 de maio de 2021.

A. K. Jain, A. Ross and S. Prabhakar. **An Introduction to Biometric Recognition.** IEEE Transactions on Circuits and Systems for Video Tecnhology, v.14, n.1 2004. pp. 4–20.

A. K. Jain, A.Ross, S.Pankanti. **Biometrics: A Tool for Information Security.** IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 1, NO. 2, JUNE 2006

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799: **Tecnologia da informação – código de prática para a gestão da segurança da informação.** Rio de Janeiro, 2001.

BARBOSA T.; SOUZA J.; CARVALHO M.; VIDAL L. **O uso da biometria em Sistemas de Segurança.** Artigo Científico. 9p. Associação Educacional Dom Bosco - (AEDB), 2014.

FAGUNDES, Leonardo Lemes. **Classificação da informação.** Disponível em: < http://professor.unisinos.br/llemes/Aula07/Aula07.pdf> acesso em 27 de março de 2021.

KOSUTIC, Dejan. **Classificação da informação segundo ISO 27001**. Disponível em: <https://advisera.com/27001academy/pt-br/blog/2014/05/14/classificacao-da-informacao-de-acordo-com-a-iso-27001/>, acesso em 27 de março de 2021.

MANDARINI, Marcos; **Segurança Corporativa Estratégica**. 1ª Editora Manole, Barueri, 2005.

R. Clarke. **Human identification in information systems: management challenges and public policy issues.** Information Technology & People, v.7 n.4.1994. pp.6–37.

Revista Digital Security. **Oitchau aposta em reconhecimento facial e comando de voz para controle de ponto.** Disponível em: <https://revistadigitalsecurity.com.br/wp-content/uploads/2019/02/shutterstock_717365779-1170x780.jpg> acesso em 04 de maio de 2021.

SANTOS, Raphael Sapucaia dos; Fabris, Jonas Pedro. **Tecnologias biométricas de controle de acesso.** Universidade Federal de Sergipe, Artigo científico exposto no Simpósio Internacional de Tecnologia e Inovação; 2019.

SÊMOLA, M. **Gestão da Segurança da Informação Uma Visão Executiva.** Rio de Janeiro: Editora Campus, 2003.

Silva C.; Miranda D.; Oliveira F.; Ferreira J.; Falbo L.; Silveira P. **A segurança através da biometria.** Artigo Científico. 12p. Associação Educacional Dom Bosco - AEDB, 2007.

SILVA, Eric. **Varredura da Retina**. Disponível em: <https://www.gta.ufrj.br/grad/07_2/eric/> acesso em 22 de maio de 2021.

Site Comtele. **Autenticação dois fatores via SMS**. Disponível em: <https://comtele.com.br/autenticacao-dois-fatores-sms/> acesso em 08 de maio de 2021.

Site IBTecnologia. **Controle de Acesso**. Disponível em: <https://ibtecnologia.com.br/controle-de-acesso> acesso em 08 de maio de 2021.

VIGLIAZZI, Douglas. **Biometria: medidas de segurança.** Florianópolis: Visual Books, 2006 p. 5.