

SEGURANÇA E PROTEÇÃO DE DADOS

Prof. Priscilla Cunha

pcunha@uni9.pro.br



SEGURANÇA LÓGICA

- Segurança nunca será 100%, mas medidas para minimizar problemas devem ser tomadas nas empresas.
- Quando pensamos em segurança, a primeira coisa que devemos fazer é impedir que pessoas não autorizadas tenham acesso indevido ao que está armazenado na empresa

- Por mais controles e medidas de segurança que adotemos, sempre pode acontecer de uma pessoa não autorizada acessar nosso ambiente.
- Caso isso ocorra, devemos garantir que essa pessoa não conseguirá ver e usar nossa informação.
- Nossos equipamentos devem ser o mais impenetráveis que conseguirmos.

- A segurança lógica é invisível aos olhos e visa garantir a segurança dos sistemas, informações e acessos da empresa, colocando controles intangíveis e que façam o ambiente ficar com um nível de segurança aceitável, liberando acesso apenas às pessoas autorizadas.

- Regras básicas:
 - Pessoas não autorizadas não devem ter acesso
 - Caso haja um acesso não autorizado, a pessoa não pode conseguir fazer uso da informação
 - Ocorrências desse tipo devem ser monitoradas através dos LOGs gerados

- A segurança lógica como um todo envolve:
 - Confidencialidade;
 - Integridade;
 - Autenticidade.
- O nível de segurança lógica que iremos implementar em ambientes, sistemas ou informações vai depender da importância dos mesmos, assim como da necessidade de acesso de cada um dos usuários.

- Perguntas que devem ser respondidas quando pensamos em segurança lógica:
 - Quem poderá acessar?
 - Acessando, o que esta pessoa poderá fazer?
 - Qual o nível de acesso dessa pessoa?
 - Como monitorar o que foi acessado?
 - Quando monitorar?
 - A que horas a pessoa poderá utilizar o recurso liberado?
 - Como verificar posteriormente o que foi feito pelo usuário X?

An abstract background on the left side of the slide, featuring a complex, overlapping grid of blue and white lines that create a sense of depth and digital connectivity.

PASSOS DA SEGURANÇA LÓGICA

- A segurança lógica envolve 4 passos:
 - Identificação
 - Autenticação
 - Autorização
 - Auditoria

Identificação

- Primeiro item de controle
- Processo de identificar os usuários
- Pode ser feito através de tabelas de usuários e/ou grupos de usuários
- O usuário sempre deve se identificar para ter acesso
- Se o sistema puder fazer a identificação do terminal de acesso, melhor ainda!
- É assim que controlamos quem teve acesso



A login dialog box with a blue header containing a white user icon and the word **LOGIN**. Below the header are two input fields. The first field is labeled **NAME** and is highlighted with a red oval. The second field is labeled **PASSWORD**. At the bottom are two buttons: **OK** (green text) and **CANCEL** (red text).

LOGIN

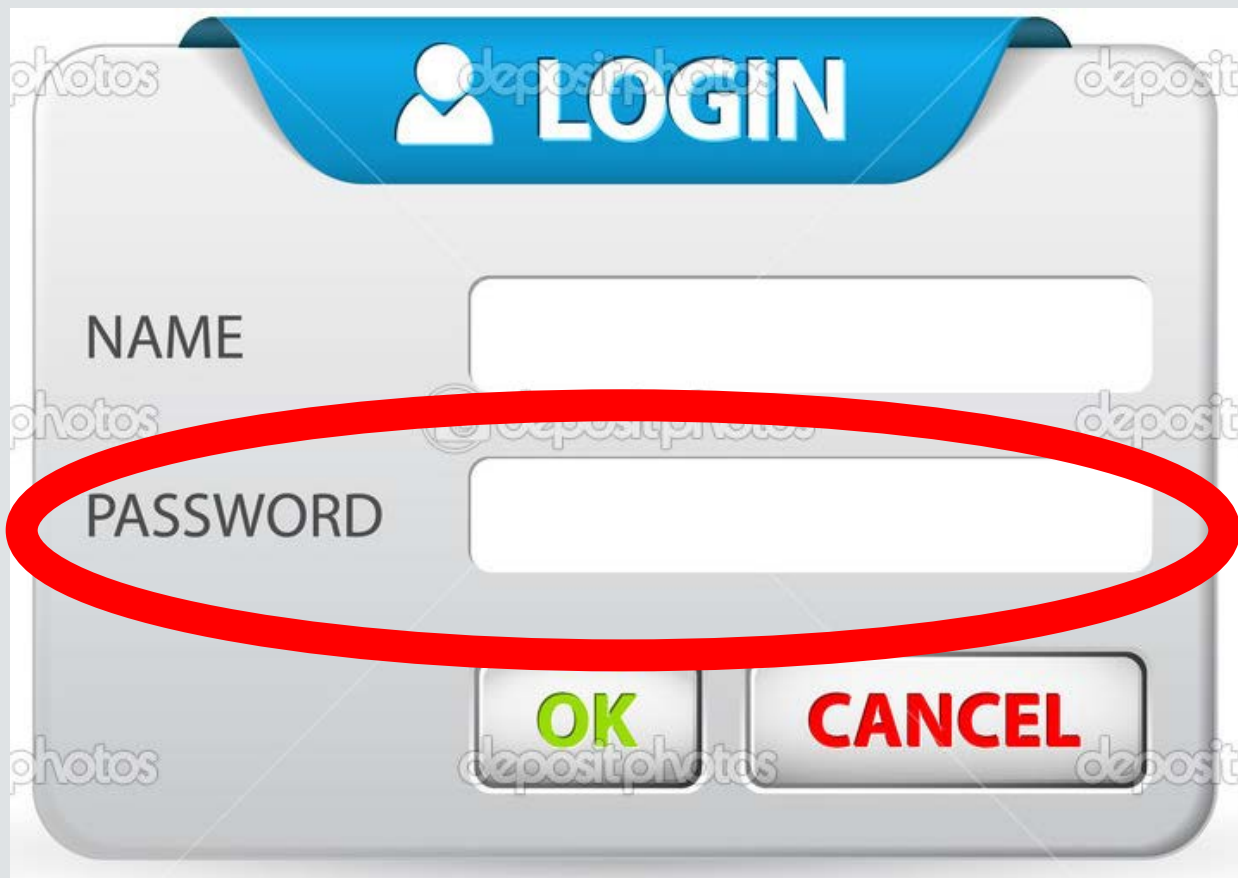
NAME

PASSWORD

OK **CANCEL**

Autenticação

- Processo posterior a identificação
- Quando o usuário, além de dizer quem ele é, prova se ele sabe como ter acesso
- Pode ser feita de 3 formas:
 - Por meio de uma informação que o usuário sabe (senha)
 - Por meio de alguma característica física do usuário (biometria)
 - Por meio de algo que o usuário possui em seu poder (token)
- Quanto mais formas de autenticação forem usadas, mais seguro será o processo. Por isso que quando existe maior criticidade, a combinação de mais de um método é usada.



A login dialog box with a blue header containing a white user icon and the word **LOGIN**. Below the header are two text input fields. The first field is labeled **NAME**. The second field is labeled **PASSWORD** and is circled in red. At the bottom are two buttons: **OK** (green text) and **CANCEL** (red text).

LOGIN

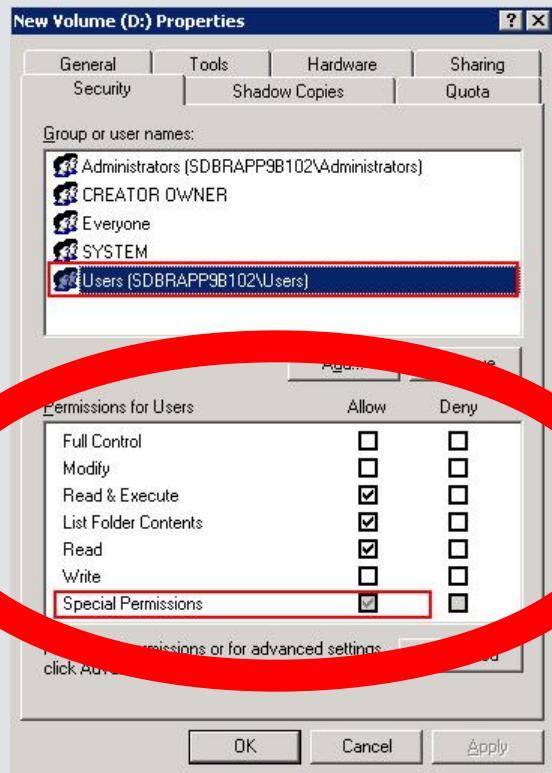
NAME

PASSWORD

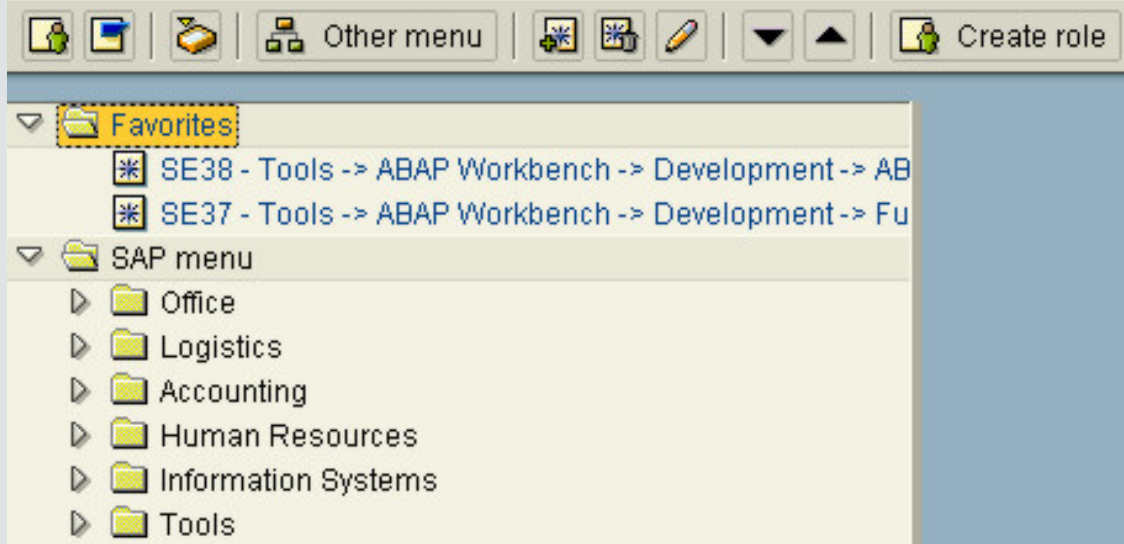
OK **CANCEL**

Autorização

- Processo em que as permissões do usuário são analisadas
- Trabalha com base em concessão / negação de privilégios de acesso
- São as regras que especificam o que o usuário pode fazer
- Quanto mais regras de permissionamento um sistema tem, mais isso afeta seu desempenho



SAP Easy Access



Auditoria

- Processo de monitorar os acessos, gerando logs para conferências futuras
- Como os acessos tem que gerar log, podemos verificar o que o usuário está fazendo, se ele está agindo de acordo com as políticas da empresa, se ele está tentando acessar recursos e informações aos quais ele não tem acesso, etc..
- Registra os acessos, uso dos recursos, tentativas de acesso negadas, horário de início e término do acesso, etc

MENU DOS USUÁRIOS ▼

TABELAS ▼

SEGURANÇA ▶

ENVIAR EMAILS

SAIR

Aplicações

Grupos

Usuários

Mudar Senha

Sincronizar

Logs de acesso

Consulta - Logs de Acesso do sistema

Pesquisa

Ordenação

Gerar Excel

Gerar Word

Impressão

Data ↕	Aplicação ↕	Ação efetuada ↕	Usuário ↕	IP ↕	Registro Alterado ↕
17/07/10	Form Pessoa	ABRIR	adriano	127.0.0.1	730
17/07/10	Form Pessoa	ABRIR	adriano	127.0.0.1	730
17/07/10	Form Pessoa	ABRIR	adriano	127.0.0.1	730
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	730
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	730
17/07/10	Ficha do GM	ATUALIZOU	adriano	127.0.0.1	730
17/07/10	Ficha do GM	NOVO REGISTRO	adriano	127.0.0.1	
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	730
17/07/10	Ficha do GM	DELETOU	adriano	127.0.0.1	731
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	731
17/07/10	Ficha do GM	ATUALIZOU	adriano	127.0.0.1	731
17/07/10	Ficha do GM	NOVO REGISTRO	adriano	127.0.0.1	
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	731
17/07/10	Ficha do GM	NOVO REGISTRO	adriano	127.0.0.1	
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	731
17/07/10	Ficha do GM	NOVO REGISTRO	adriano	127.0.0.1	
17/07/10	Ficha do GM	NOVO REGISTRO	adriano	127.0.0.1	
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	730
17/07/10	Ficha do GM	ABRIU	adriano	127.0.0.1	730



GERENCIAMENTO DE SENHAS

- Senhas são o mecanismo de controle de acesso mais antigo usado para impedir acessos indevidos
- O maior problema são as senhas fáceis de serem adivinhadas (senhas fracas) e o compartilhamento de senhas

- Já existem até ferramentas na internet para quebra de senhas, e às vezes a pessoa mal intencionada precisa apenas fazer um bom trabalho de engenharia social para descobrir senhas óbvias

- Regras para trocas de senha
 - Senhas com mais de 10 caracteres
 - Troca periódica de senhas (a cada 30 dias é ideal)
 - Impedir uso das senhas anteriores (pelo menos das últimas 18), assim como impedir a repetição no mínimo 60% das senhas anteriores

- Usar letras maiúsculas, minúsculas, números e caracteres especiais na mesma senha
- Bloquear a conta após algumas tentativas de acesso sem sucesso (no máximo 3)
- O arquivo de senhas deve ser criptografado

- Deve-se evitar
 - Datas comemorativas – ex: user:
pvcunha senha: 120982
 - Nomes de parentes – ex: user:
pvcunha senha: wilson
 - Placa do carro
 - Número de telefone

- Senha igual ao usuário – ex: user: pvcunha senha: pvcunha
- Repetições, sequências e informações comuns. Ex:
 - Amor / paixão
 - Deus / Jesus / Cristo
 - 1111 / aaaa
 - 1234 / abcd
 - Asdfg / qwerty / 147258369

- 10 senhas mais usadas em 2014:

1. 123456
2. password
3. 12345
4. 12345678
5. qwerty
6. 1234567890
7. 1234
8. baseball
9. dragon
10. football

- 10 senhas mais usadas em 2015:

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball

- 10 senhas mais usadas em 2016:

1. 123456
2. 23456789
3. qwerty
4. 12345678
5. 111111
6. 1234567890
7. 1234567
8. password
9. 123123
10. 987654321

- 10 senhas mais usadas em 2017:

1. 123456
2. Password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. Letmein
8. 1234567
9. football
10. iloveyou

- 10 senhas mais usadas em 2018:

1. 123456
2. password
3. 123456789
4. 12345678
5. 12345
6. 111111
7. 1234567
8. sunshine
9. qwerty
10. iloveyou

- 10 senhas mais usadas em 2019:

1. 123456
2. 123456789
3. qwerty
4. password
5. 1234567
6. 12345678
7. 12345
8. iloveyou
9. 111111
10. 123123

- 10 senhas mais usadas em 2020:

1. 123456
2. 123456789
3. picture1
4. password
5. 12345678
6. 111111
7. 123123
8. 12345
9. 1234567890
10. senha

- 10 senhas mais usadas em 2021:

1. 123456
2. 123456789
3. 12345
4. qwerty
5. password
6. 12345678
7. 111111
8. 123123
9. 1234567890
10. 1234567



BIOMETRIA

- BIO: VIDA MÉTRON:
medida
- Uso de características físicas ou comportamentais do ser humano para identificá-lo
- Uso de tecnologia para analisar essas características

- Uma das técnicas mais usadas em controle de acesso atualmente
- Traz automatização ao processo de autenticação, além da performance
- Componentes necessários para o uso de biometria: leitor biométrico, software, característica biométrica, rede e servidores



VOZ



Íris



Mão



Retina



Rosto



Impressão



Funcionamento

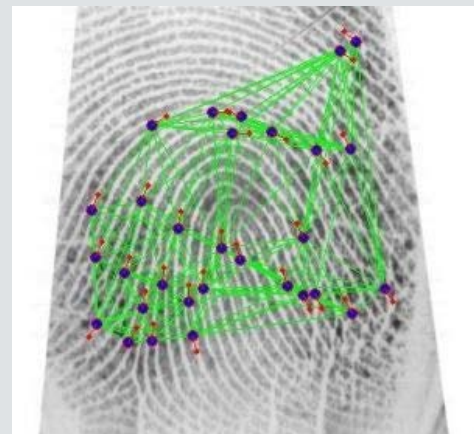
- Usuário cadastra a característica biométrica pelo sensor
- A característica é armazenada em uma planilha biométrica (modelo matemático), que deve estar armazenada no servidor
- Para ter acesso o usuário apresenta sua característica biométrica, que é comparada por um software com a que foi armazenada

- Temos taxas de credibilidade e desempenho, para analisar a performance do sistema, que são definidas por:
 - Falsa aceitação (gera fraudes)
 - Falsa rejeição(gera frustrações)



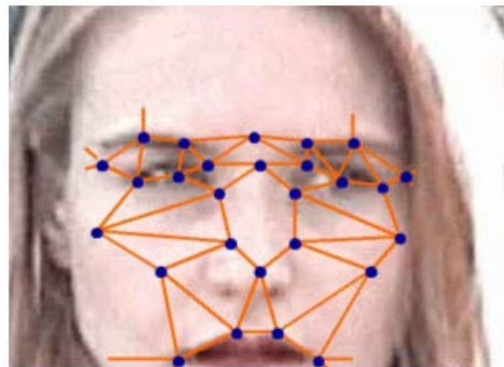
TIPOS DE BIOMETRIA

- Impressão digital
 - Método mais antigo
 - Simples
 - Mais barato
 - Menos seguro
 - Analisa os detalhes dos sulcos da ponta dos dedos; esses detalhes são chamados de minúcias



- Face

- Usa IA
- Faz medida e comparações complexas, mapeando as proporções da face
- Não necessita contato
- Pode ser usado com imagens térmicas



- Assinatura
 - São analisadas características como: modo de assinar, pressão, número de vezes que a caneta é suspensa, ângulo e aceleração no momento de assinar

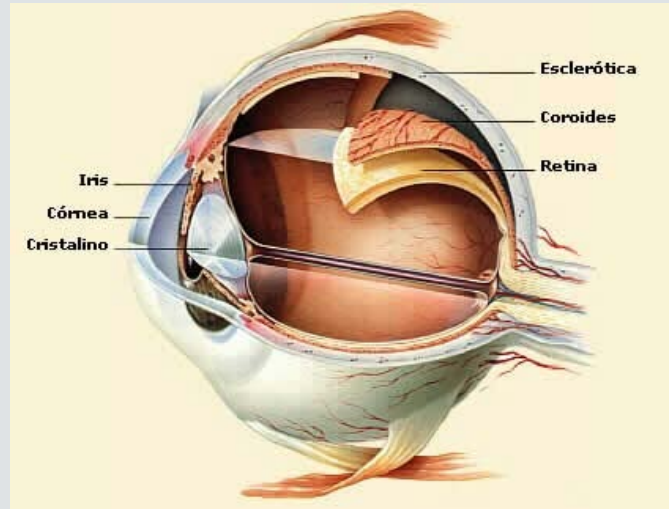


- Geometria das mãos
 - Analisa as características da mão
 - Analisa: imagem 3D, formato e largura
 - O leitor possui pinos que não como uma guia, para o usuário saber onde colocar a mão

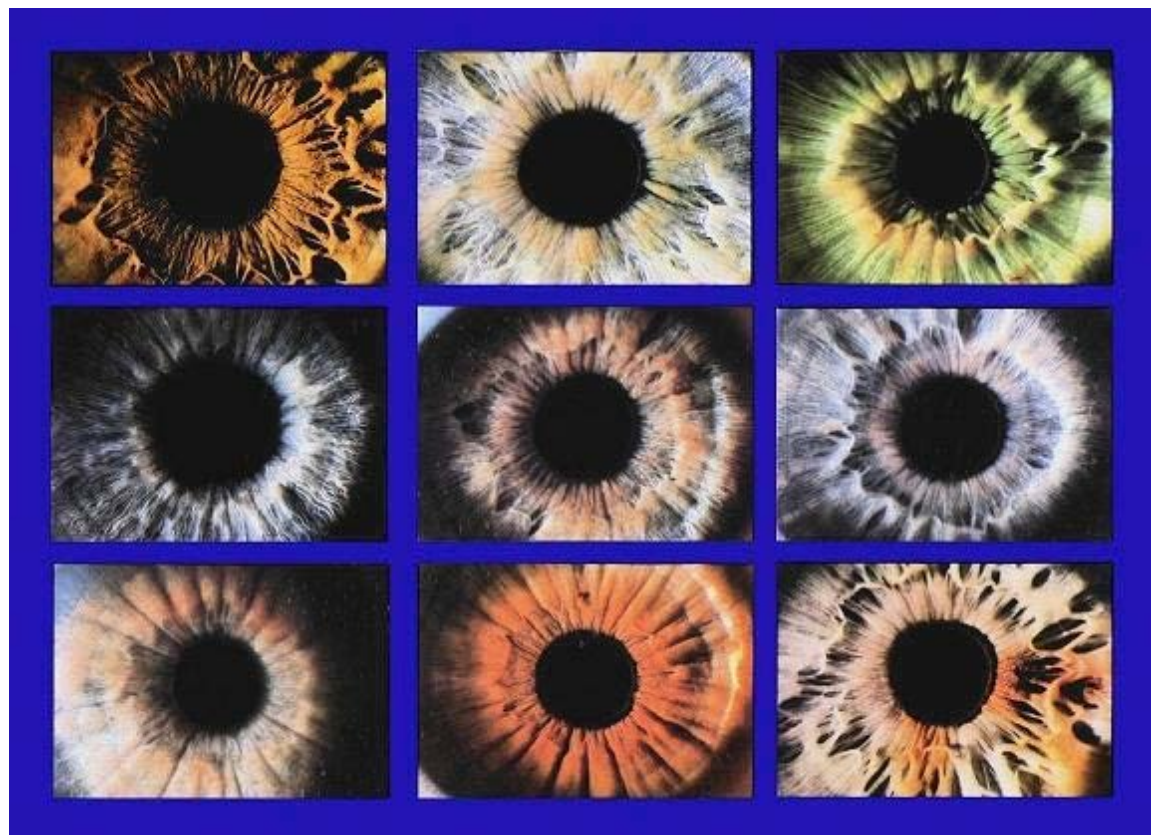


- Voz
 - Transforma a voz (analógica) em sinal digital
 - Pode (ou não) usar texto fixo
 - Afetado por doenças e ruídos externos
- Digitação
 - Analisa velocidade, pausas, pressão nas teclas
 - Difícil de imitar
 - Pode (ou não) usar texto fixo

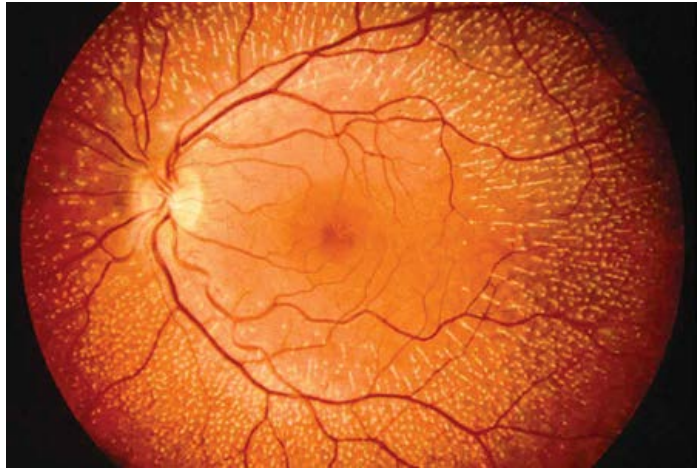
- Olhos
 - Altos níveis de precisão
 - Existem 2 tecnologias: biometria da íris e biometria da retina



- Íris
 - Anel colorido do olho
 - Avalia características como: coroa, glândula, filamentos, sardas, sulcos e estrias
 - Impossível falsificar
 - Lentes não interferem, mas óculos sim
 - Captura: câmera P/B captura a imagem da íris e armazena as características na planilha biométrica para posterior comparação



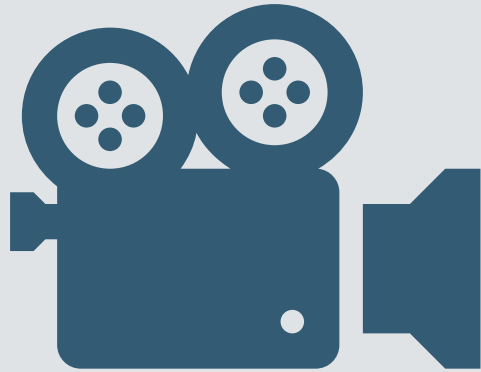
- Retina
 - Padrão de veias na parte de trás do globo ocular
 - Impossível de falsificar
 - Captura: um leitor (laser) faz a varredura da retina depois que o usuário mantém os olhos focados por alguns segundos. O scannemento avalia a fóvea e armazena as características biométricas na planilha biométrica para posterior comparação



- Como escolher um sistema biométrico
 - Custo
 - Precisão
 - Invasão
 - Cooperação



VÍDEOS



- O que é biometria?
<https://www.youtube.com/watch?v=dq-R35c7Sp0>
- Tecnologias biométricas -
https://www.youtube.com/watch?v=3XhIhxdwh_E
- 10 - Microsoft defende regulamentação de tecnologias de reconhecimento facial -
<https://www.youtube.com/watch?v=X-XVJTIYzFk>



**Dúvidas?
Não mais..**