

# Segurança como diferencial competitivo da Qualidade do Produto de Software Nacional

Dr. Antonio Montes e equipe DSSI  
CTI/MCT

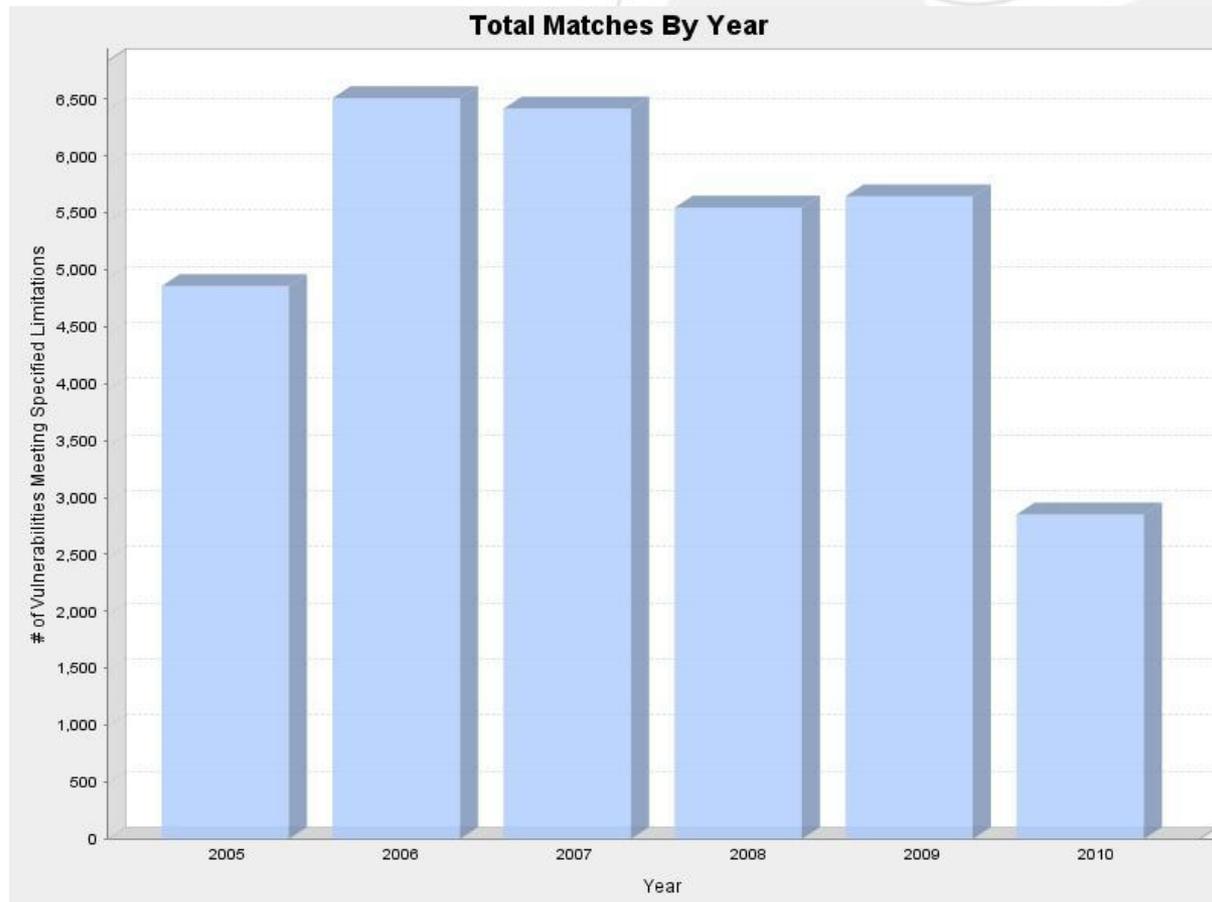
# Roteiro

- Motivação: vulnerabilidades (CVE)
- No mundo: PITAC 05
- Preocupações dos Consumidores
- Segurança de Software
- No Brasil: PCI, OWASP RFP
- Alguns exemplos
- NBR
- Conclusões
- Ações recomendadas

# Vulnerabilidades

- Vulnerabilidade é um estado de um sistema computacional (ou conjunto de sistemas) que:
  - Permite que um atacante execute comandos se fazendo passar por outro usuário;
  - Permite que um atacante acesse dados burlando restrições de acesso aos mesmos;
  - Permite que um atacante aja como outra entidade;
  - Permite que um atacante negue serviço.

# Vulnerabilidades 2005-2010



(Common Vulnerabilities and Exposures - [cve.mitre.org](http://cve.mitre.org))

# Common Vulnerabilities and Exposures (CVE)

- CVE-2010-2882/2863  
19 vulnerabilidades do Adobe Shockwave Player que permitem a execução de código arbitrário na máquina do usuário.  
Publicadas em **26/08/2010**.

# *Cyber Security: A Crisis of Prioritization*

- No relatório ao presidente dos EUA, intitulado *Cyber Security: A Crisis of Prioritization* [[PITAC 05](#)], o seu Comitê Assessor em Tecnologia da Informação dramatizou o problema de vulnerabilidades de software da seguinte maneira:

# Citação sobre segurança de software

“O desenvolvimento de software ainda não é uma ciência ou uma disciplina rigorosa, e o processo de desenvolvimento em grande parte não é controlado de forma a minimizar as vulnerabilidades que atacantes exploram. Hoje em dia, como acontece com um câncer, software vulneráveis podem ser invadidos e modificados de forma a causar danos a software anteriormente livres de problemas, os quais, por sua vez, podem se replicar e ser transmitidos através da rede para causar danos a outros sistemas. Como um câncer, esses processos danosos podem ser invisíveis para leigos no assunto, enquanto que especialistas reconhecem que essas ameaças estão crescendo. E como no caso do câncer, **ações preventivas e pesquisas são críticas, a primeira para minimizar os danos a curto prazo e a última para estabelecer a base de conhecimentos e competências que vão embasar a redução de riscos e minimizar os prejuízos no longo prazo.**”

# Preocupações dos Consumidores

- A integridade de recursos críticos depende da confiabilidade e segurança de software que são usados para gerar e controlar estes recursos.
- Existe uma grande escassez de recursos humanos com as competências necessárias para desenvolver software seguro.
- Questionam a capacidade dos fornecedores de desenvolver e entregar software seguro, com níveis de integridade adequados, e demonstrar a adoção de um mínimo de práticas responsáveis.

# Riscos

- Sistemas de informação dependem de suas componentes de software, apesar destes serem os elos mais frágeis desses sistemas.
- Tamanho e complexidade de software, obscurecendo suas intenções e dificultando o processo de testes de segurança.
- Terceirização do desenvolvimento de software e dependência de cadeias de suprimento não credenciadas

# Riscos

- Disponibilidade de software de ataque sofisticados que facilitam a exploração de fragilidades e vulnerabilidades de software e usuários.
- Reuso e interfaceamento de software legado com novas aplicações, em ambientes e redes dispares e crescentemente complexos, resultando em conseqüências inesperadas e no crescente número de alvos vulneráveis.

# Segurança de Software

- Segurança de Software surgiu, então, como uma resposta ao dramático aumento de riscos às missões e negócios, que são sabidamente atribuíveis à exploração de software vulneráveis.

# Segurança de Software

- **Previsibilidade:** pode-se estar justificadamente confiante de que o software, quando executado, irá funcionar como se espera;
- **Confiabilidade:** não há nenhuma vulnerabilidade explorável ou lógica maliciosa no software, que tenha sido inserida por descuido ou intencionalmente;
- **Resiliência:** se comprometido, os danos ao software serão minimizados, e ele vai recuperar rapidamente um nível aceitável de capacidade operacional;
- **Conformidade:** garantir, de forma sistemática e planejada, que processos e produtos de software estejam conformes com os requisitos, e procedimentos e normas aplicáveis.

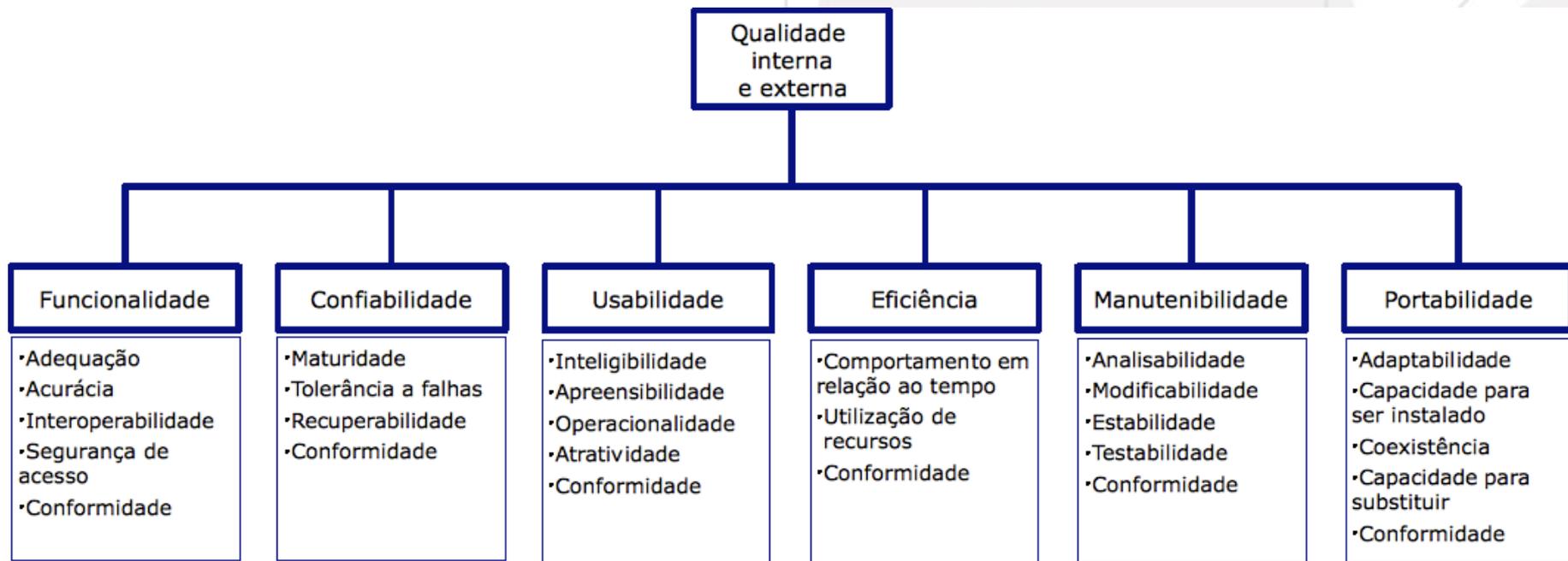
# No Brasil

- O único esforço sistemático (caveat) em andamento está associado à indústria de cartões de crédito, que aplica o padrão PCI-DSS, o qual exige que aplicações de comércio eletrônico que façam uso de cartões de crédito, submetam suas aplicações Web a auditorias periódicas de segurança.

# No Brasil

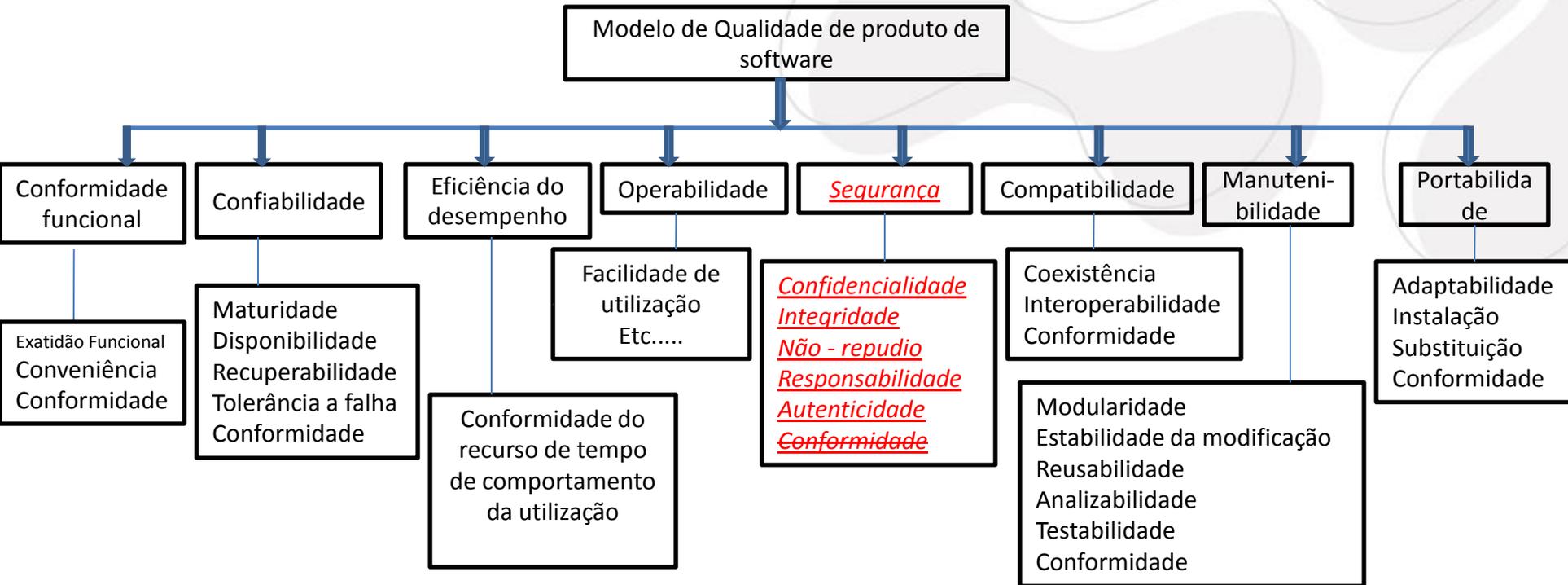
- Algumas organizações, principalmente na área governamental, estão adotando as recomendações do Open Web Application Security Project (OWASP), mas ainda de forma incipiente.
- Discussões sobre a norma ISO/IEC 25010 que irá substituir a norma NBR ISO/IEC 9126, que estabelece os padrões de qualidade de produtos de software.

# NBR ISO/IEC 9126



## Modelo de Qualidade de Produto de Software

# Modelo de Qualidade



Em estudo na : Software Engineering - Software Product Quality Requirements and Evaluation (SQuARE) Quality model - ISO 25010

# Conclusões

- O que se conclui do cenário mundial e da situação no Brasil é que os usuários e operadores de sistemas de informação estão paulatinamente se dando conta de que os problemas de segurança estão estreitamente ligados a vulnerabilidades e fragilidades de produtos de software.

# Conclusões

- Isso faz com que o consumidor esteja passando a demandar segurança de software com mais um requisito, na contratação de serviços de desenvolvimento ou na compra de produtos de prateleira.
- Os países desenvolvidos estão investindo fortemente no desenvolvimento de tecnologias de segurança de software, tais como

# Conclusões

- Metodologias de desenvolvimento seguro;
  - Metodologias de contratação ou compra de software seguro (requisitos, aceitação);
  - Desenvolvimento de normas de segurança de software;
  - Metodologias de testes de segurança de software.
- E na formação de recursos humanos qualificados para realizar todas essas tarefas.

# Diferencial Competitivo

- Desta forma, é evidente que a implementação de procedimentos e técnicas para a produção e testes de software que incorporem segurança desde seu projeto até sua manutenção, isto é, no seu ciclo de vida, será, em curto prazo, um diferencial competitivo na venda de serviços e aplicações de prateleira.

# Diferencial Competitivo

- Como a incorporação de segurança no ciclo de vida de software é muito mais um modo de pensar, do que a implementação de processos, o Brasil tem a oportunidade de sair na frente nesta corrida pelo mercado de software seguro, por meio do treinamento adequado de recursos humanos qualificados.

# Recomendações

- Assim, é essencial que a SEPIN passe a estimular os cursos de graduação em computação a agregarem cursos de segurança de software, além de estimular a criação de cursos de pós-graduação nesta área, por meio de discussões com a SBC.

# Recomendações

- É importante também que a indústria de software brasileira seja conscientizada a respeito dos problemas associados a segurança de software e sobre a existência deste nicho de mercado, talvez através da SOFTEX.

# Recomendações

- Uma outra forma de estimular essa mudança consiste em usar o poder de compra do governo para estimular o desenvolvimento de software seguro. Tanto em benefício do governo e seus clientes, quanto para o desenvolvimento das tecnologias e processos necessários para isso.



# Dr. Antonio Montes

Pesquisador

[antonio.montes@cti.gov.br](mailto:antonio.montes@cti.gov.br)

Tel.: +55 19 3746-6085

[www.cti.gov.br](http://www.cti.gov.br)

# Ilustrações

- Nos slides seguintes são mostrados alguns conceitos de segurança de software e apresentados alguns exemplos triviais de ataques contra aplicações.

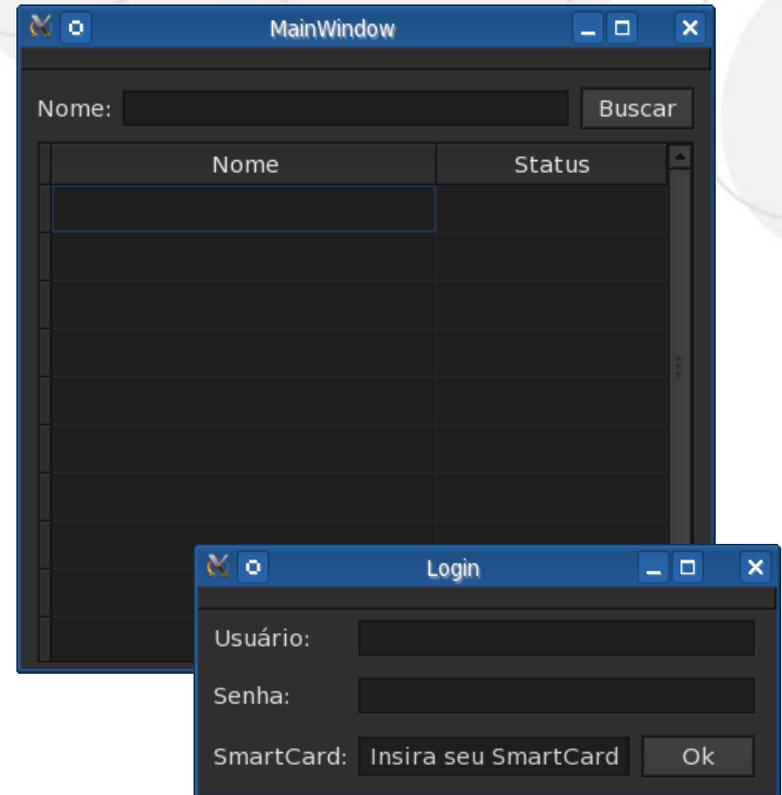
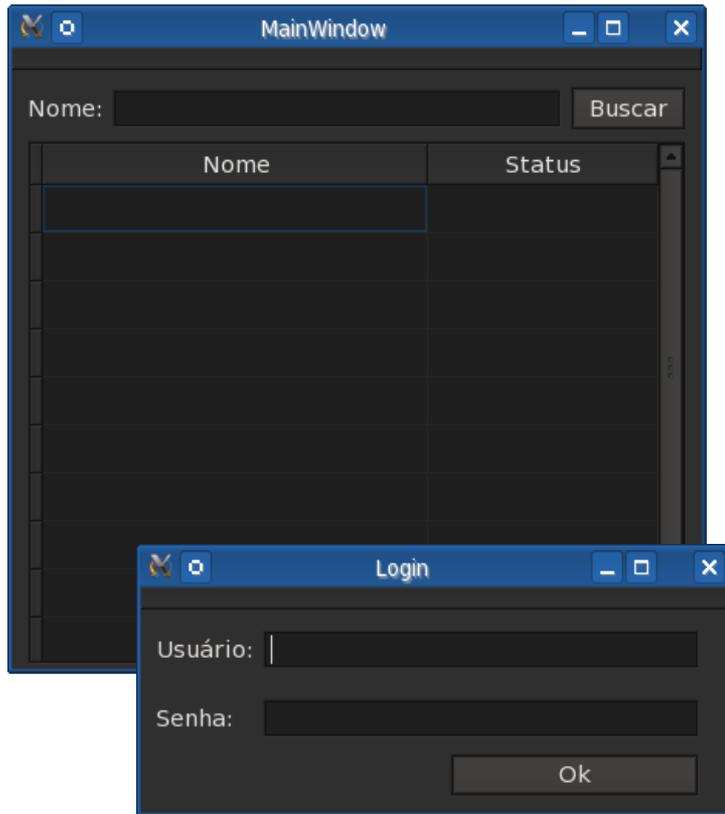
# Segurança no produto de software

- Pode se apresentar de forma **tangível para o usuário final**, modificando:
  - a interface;
  - a forma de interação com o usuário;
  - como o sistema retorna resultados.
- Pode se apresentar de forma **intangível para o usuário final**, não modificando a interface, forma de interação ou resultados.

# Funcional Versus Seguro

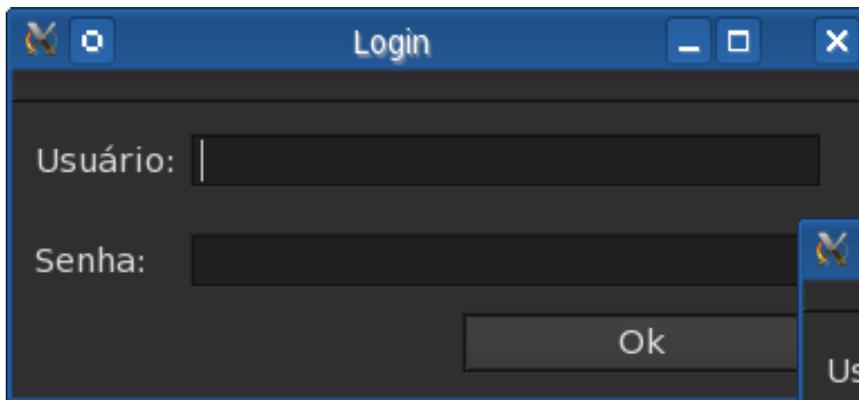
- O exemplo:
  - Um sistema de consultas para **laboratório de análises clínicas**;
  - Armazena os **resultados sigilosos de exames sensíveis**.
- As operações:
  - O **atendente se identifica** no sistema;
  - O **atendente busca** através do nome do paciente o **resultado** do exame.

# Funcional Versus Seguro

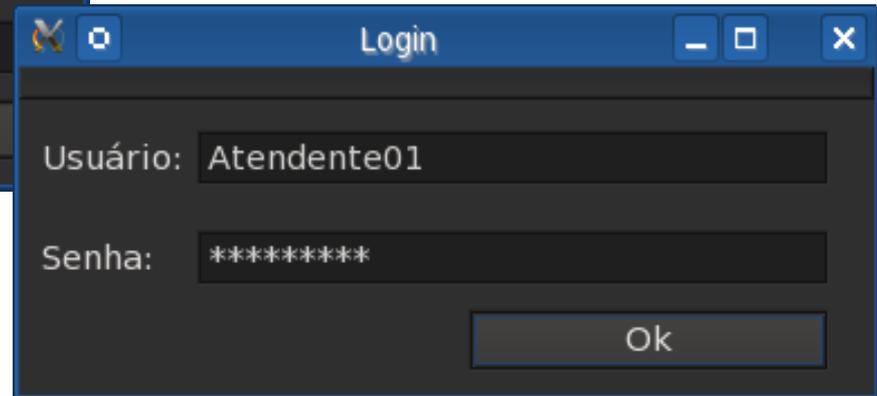


# Exemplo: Identificação e Autenticação

- Software Funcional:
  - Autenticação trivial por usuário e senha;



A screenshot of a Windows-style login window titled "Login". It features two input fields: "Usuário:" and "Senha:". Both fields are currently empty. Below the fields is a single "Ok" button.



A second screenshot of the "Login" window. The "Usuário:" field is filled with the text "Atendente01". The "Senha:" field is filled with ten asterisks "\*\*\*\*\*". The "Ok" button is visible at the bottom right.

# Exemplo: Identificação e Autenticação

- Software Seguro Aspectos Tangíveis:
  - Diferentes fatores de autenticação em classes de fatores diferentes;
  - Identificação de interação com seres humanos;
  - Reforçar a troca de senhas periodicamente;
  - Reforçar uma política de senhas fortes;
  - ...
- Software Seguro Aspectos Intangíveis:
  - Armazenamento seguro de credenciais;
  - Protocolos seguros de autenticação;
  - Tráfego de dados seguro para autenticação;
  - ...

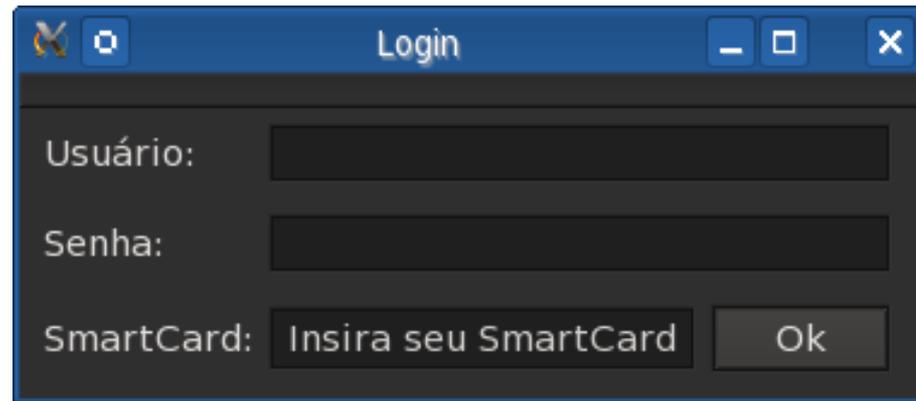
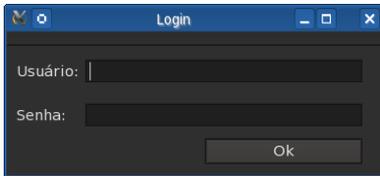
# Exemplo: Identificação e Autenticação

- **Diferentes fatores em classes de fatores diferentes**
  - O que o usuário **sabe**;
    - Senha; Data de nascimento; CPF; RG.
  - O que o usuário **possui**;
    - Um cartão magnético;
    - Um SmartCard (Cartão com chip, e.g.);
    - Um Token (OTP).
  - O que o usuário **é**.
    - Digitais;
    - Íris;
    - Face.



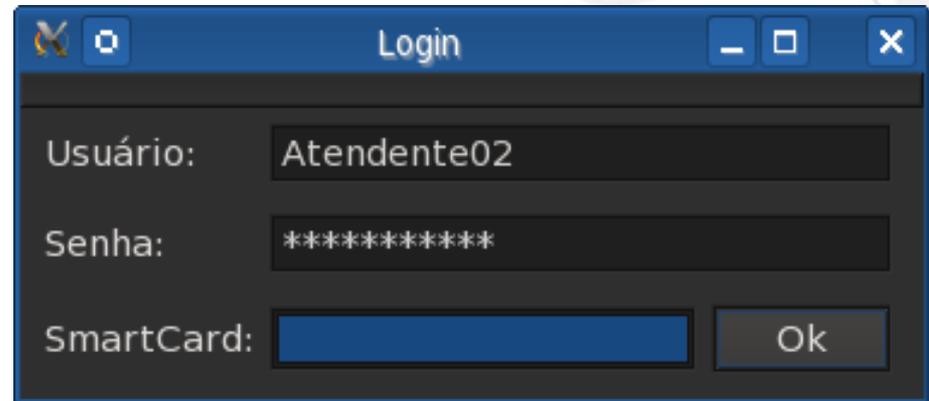
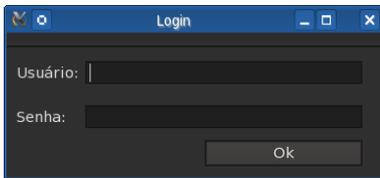
# Exemplo: Identificação Autenticação

- **Diferentes fatores em classes de fatores diferentes**



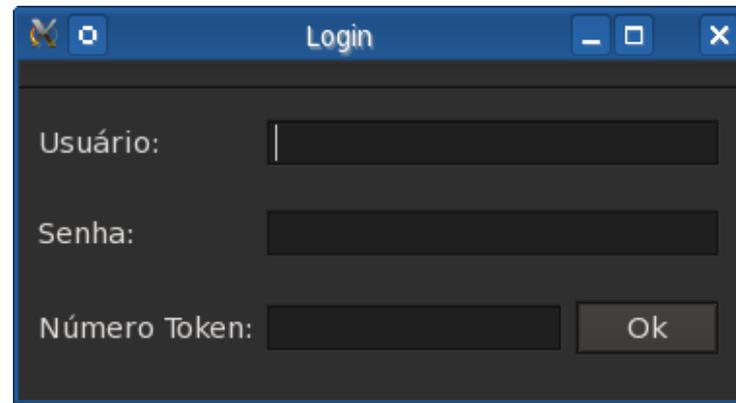
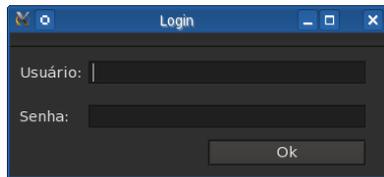
# Exemplo: Identificação Autenticação

- **Diferentes fatores em classes de fatores diferentes**



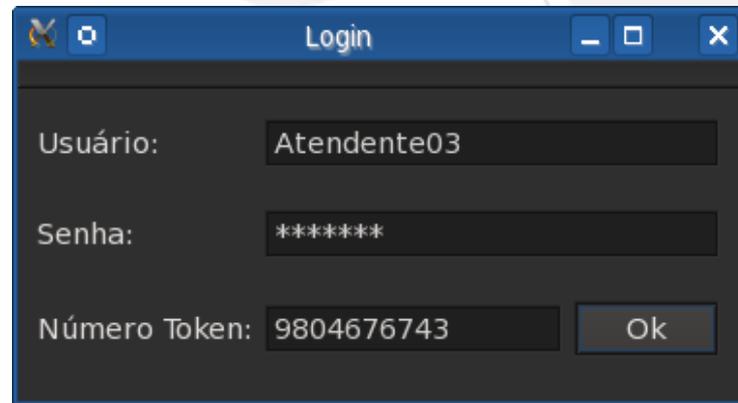
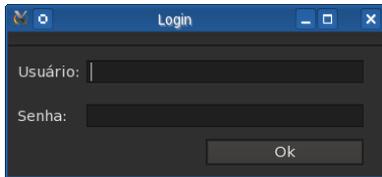
# Exemplo: Identificação Autenticação

- **Diferentes fatores em classes de fatores diferentes**



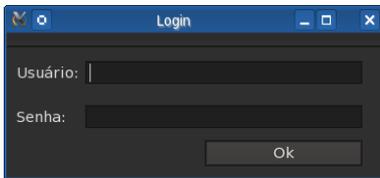
# Exemplo: Identificação Autenticação

- **Diferentes fatores em classes de fatores diferentes**



# Exemplo: Identificação Autenticação

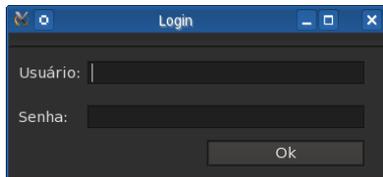
- **Identificação de Interação com Seres Humanos**



- **Um captcha serve para identificar que o sistema está sendo operado por um ser humano e não por um software de quebra de senhas, por exemplo.**

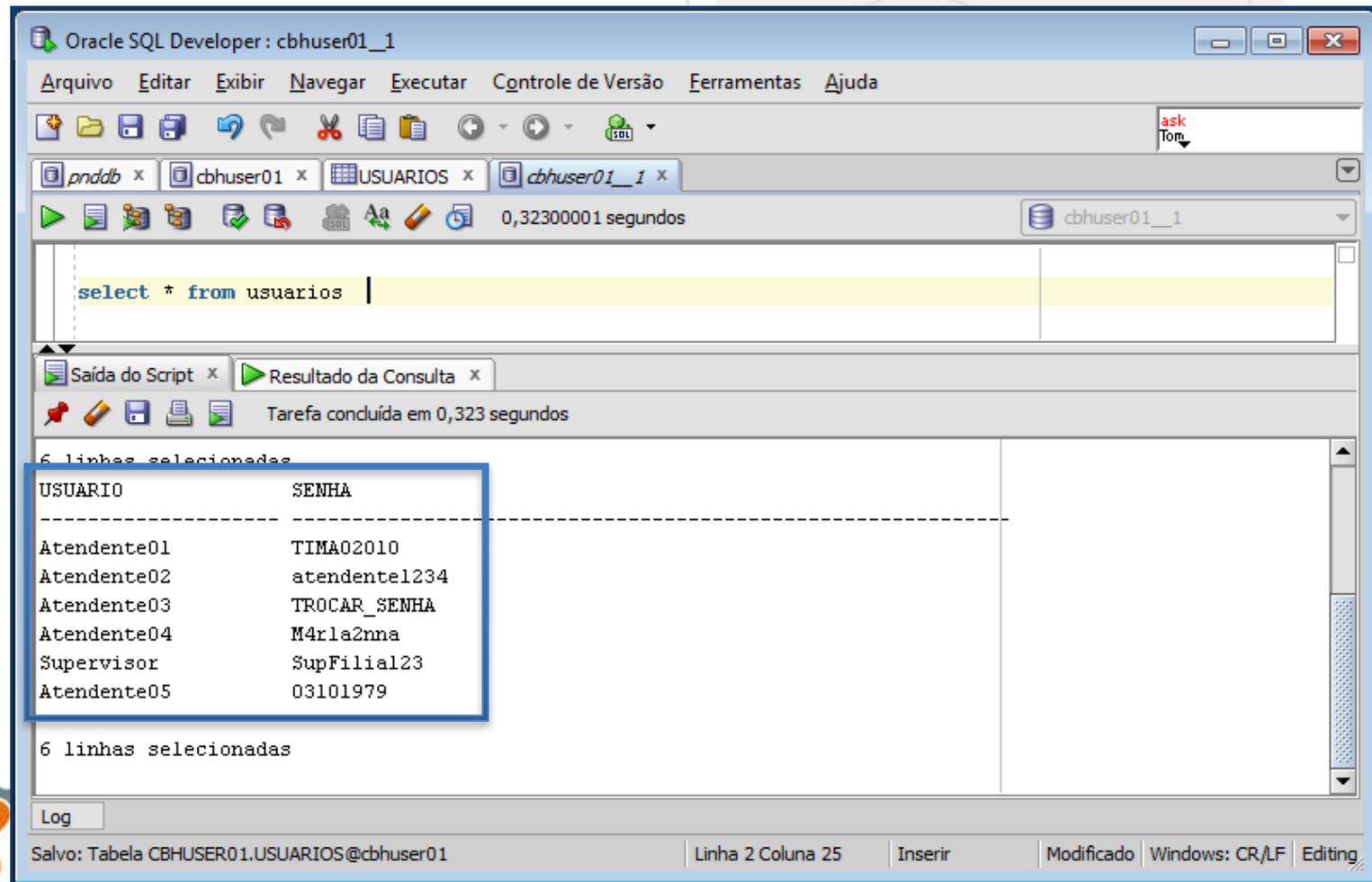
# Exemplo: Identificação Autenticação

- **Identificação de Interação com Seres Humanos**



# Exemplo: Identificação Autenticação

- Armazenamento seguro de credenciais



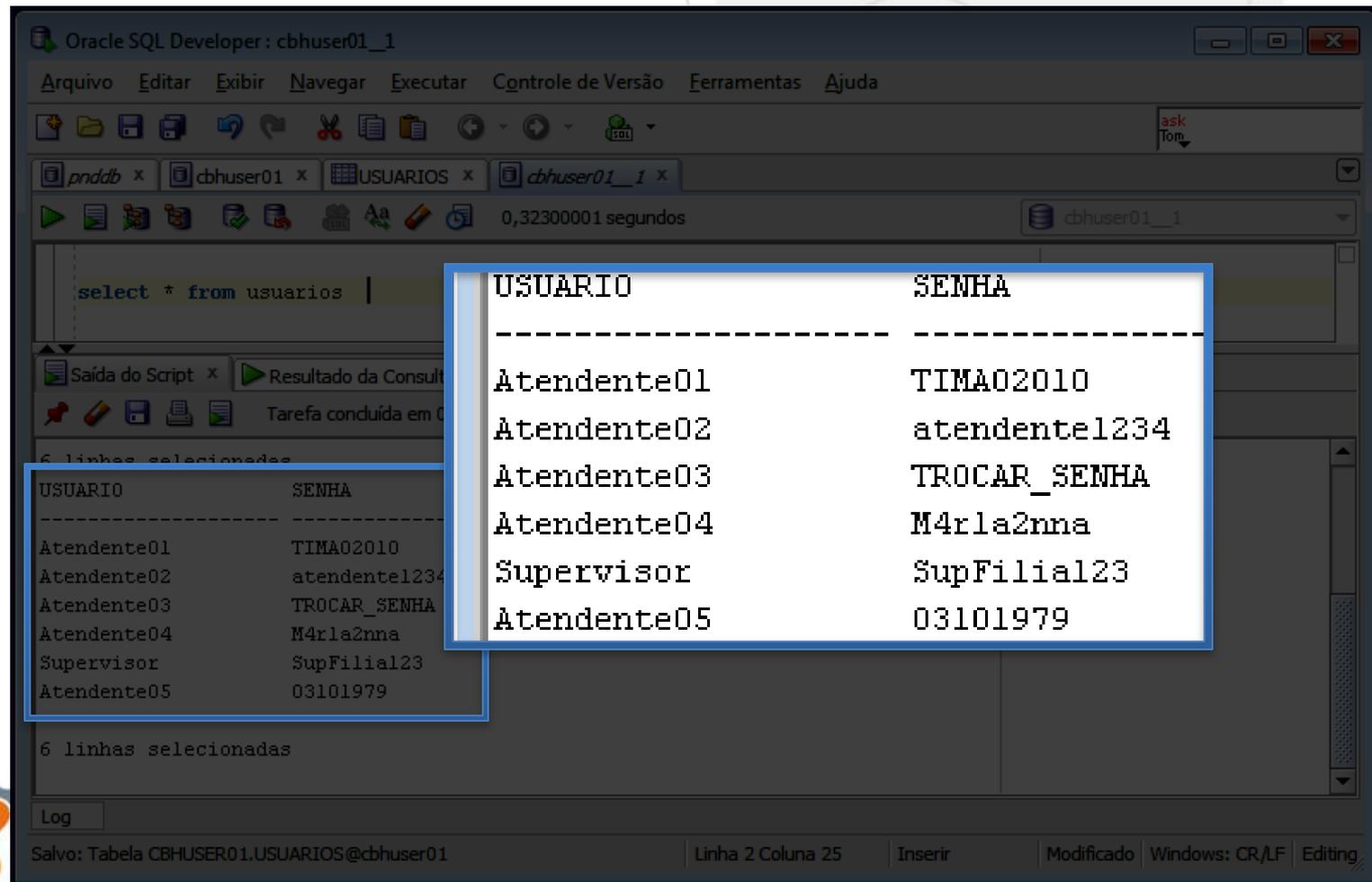
The screenshot displays the Oracle SQL Developer interface. The main window shows a query window with the SQL statement `select * from usuarios`. Below the query window, the 'Resultado da Consulta' (Query Result) pane shows the output of the query. The result is a table with two columns: 'USUARIO' and 'SENHA'. The table contains six rows of data, which are highlighted with a blue border in the image. The status bar at the bottom indicates 'Salvo: Tabela CBHUSER01.USUARIOS@cbhuser01', 'Linha 2 Coluna 25', 'Inserir', 'Modificado', and 'Windows: CR/LF Editing'.

USUARIO	SENHA
Atendente01	TIMA02010
Atendente02	atendente1234
Atendente03	TROCAR_SENHA
Atendente04	M4rla2nna
Supervisor	SupFilial23
Atendente05	03101979



# Exemplo: Identificação Autenticação

- Armazenamento seguro de credenciais



The screenshot shows the Oracle SQL Developer interface. The main window displays a query result for the 'USUARIOS' table. The query is 'select \* from usuarios'. The result is a table with two columns: 'USUARIO' and 'SENHA'. The data is as follows:

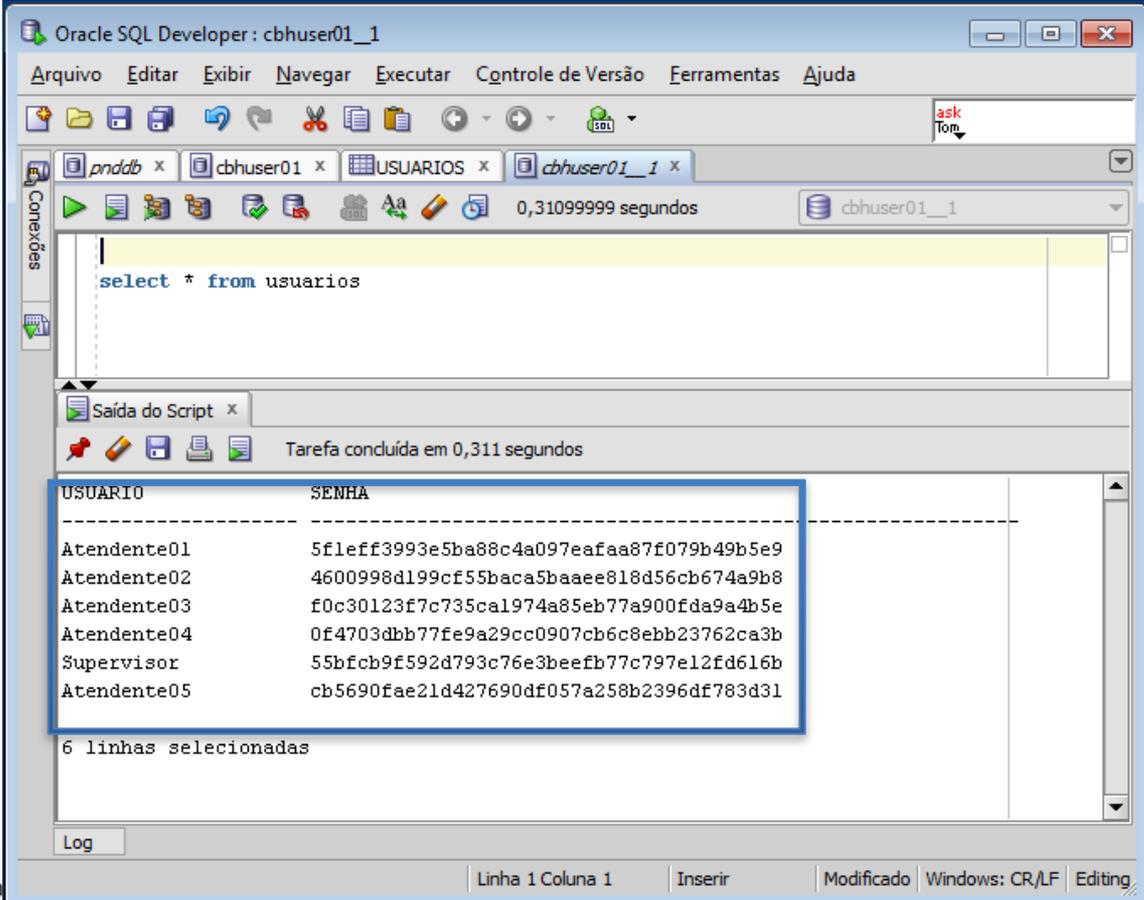
USUARIO	SENHA
Atendente01	TIMA02010
Atendente02	atendente1234
Atendente03	TROCAR_SENHA
Atendente04	M4rla2nna
Supervisor	SupFilial23
Atendente05	03101979

The interface also shows the 'Saída do Script' and 'Resultado da Consulta' tabs, and a status bar at the bottom indicating 'Salvo: Tabela CBHUSER01.USUARIOS@cbhuser01' and 'Linha 2 Coluna 25'.



# Exemplo: Identificação Autenticação

- Armazenamento seguro de credenciais



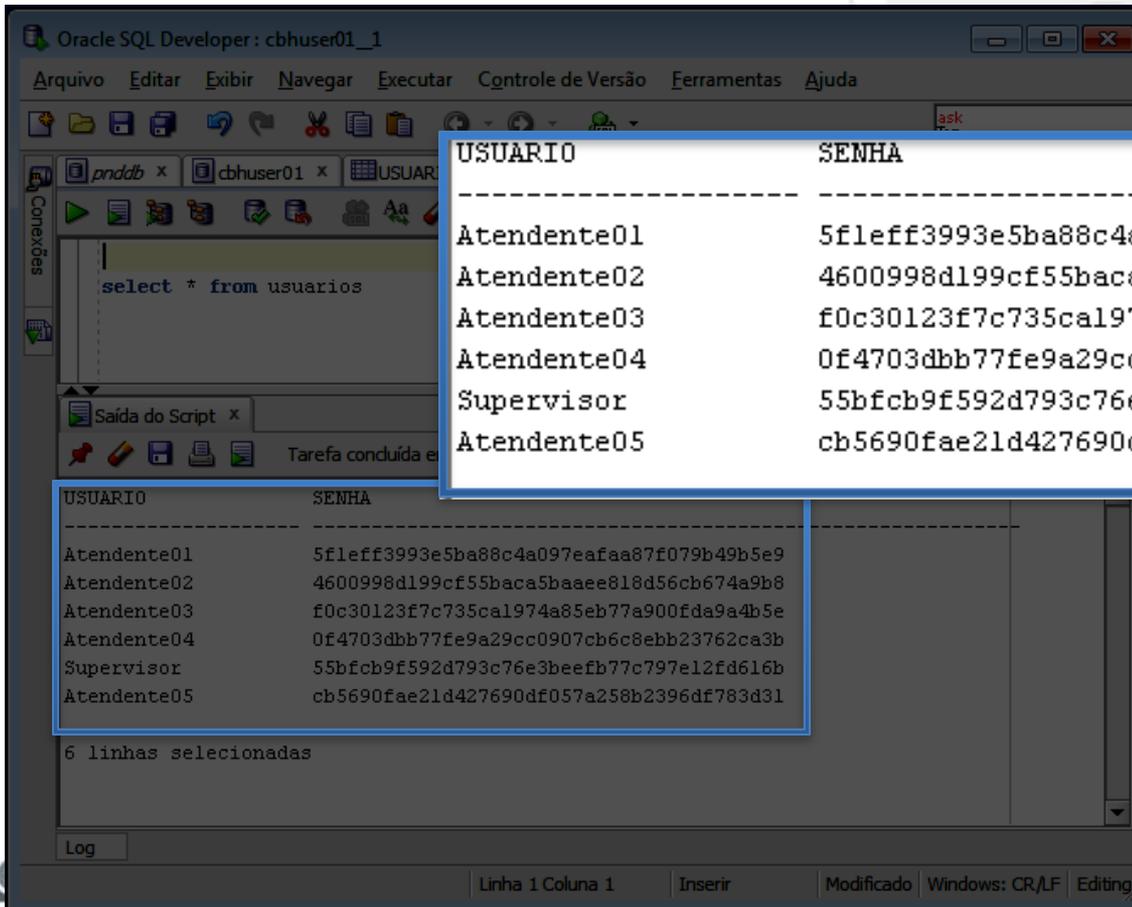
The screenshot shows the Oracle SQL Developer interface. The main window displays a query: `select * from usuarios`. Below the query editor, the 'Saída do Script' (Script Output) window shows the results of the query, which are user credentials. The results are displayed in a table with two columns: 'USUARIO' and 'SENHA'. The data is as follows:

USUARIO	SENHA
Atendente01	5f1eff3993e5ba88c4a097eafaa87f079b49b5e9
Atendente02	4600998d199cf55baca5baaee818d56cb674a9b8
Atendente03	f0c30123f7c735ca1974a85eb77a900fda9a4b5e
Atendente04	0f4703dbb77fe9a29cc0907cb6c8ebb23762ca3b
Supervisor	55bfc9f592d793c76e3beefb77c797e12fd616b
Atendente05	cb5690fae21d427690df057a258b2396df783d31

6 linhas selecionadas

# Exemplo: Identificação Autenticação

- Armazenamento seguro de credenciais



The screenshot shows the Oracle SQL Developer interface. The main window displays a query: `select * from usuarios`. The results pane shows a table with two columns: USUARIO and SENHA. The data is as follows:

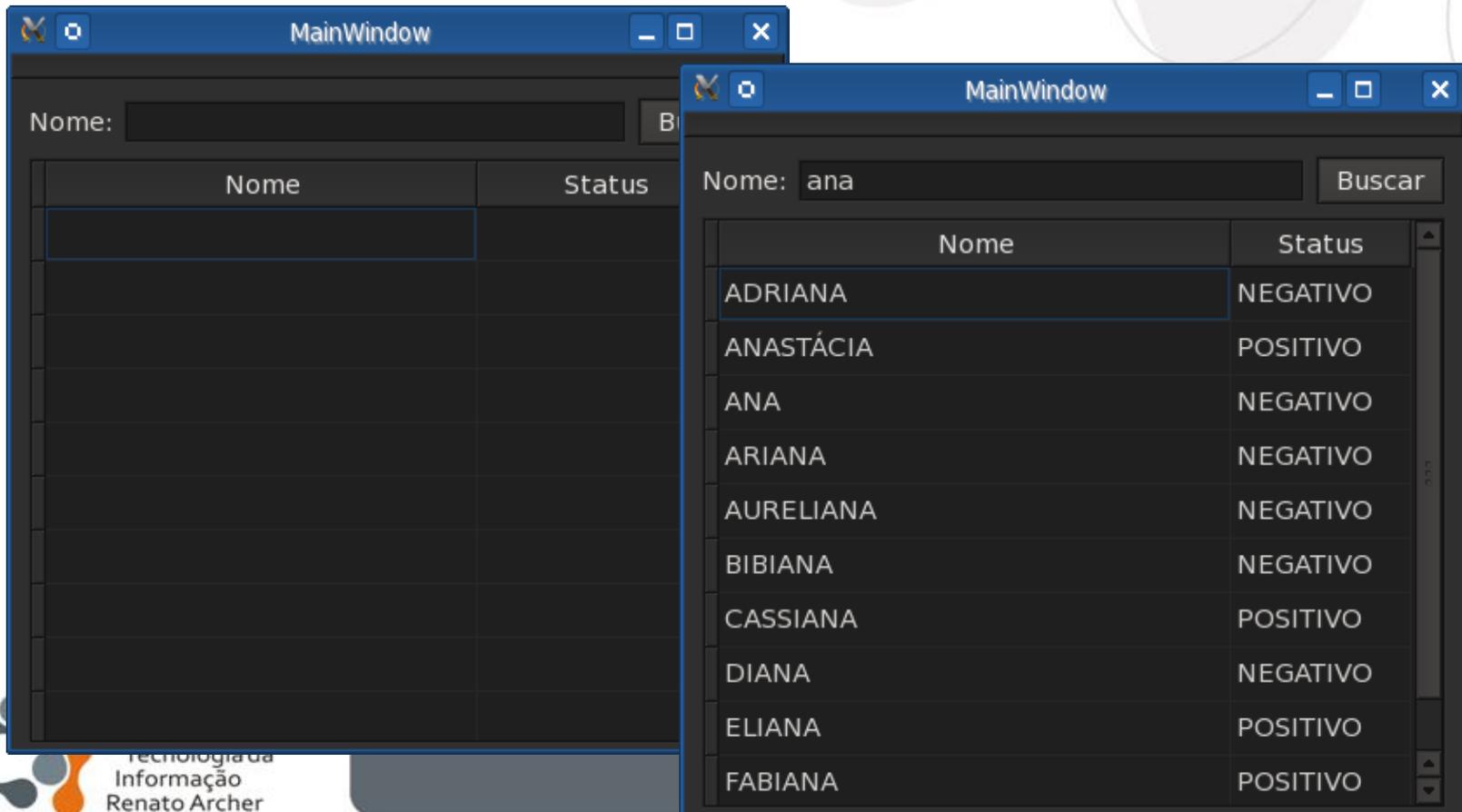
USUARIO	SENHA
Atendente01	5f1eff3993e5ba88c4a097eafaa87f079b49b5e9
Atendente02	4600998d199cf55baca5baaee818d56cb674a9b8
Atendente03	f0c30123f7c735ca1974a85eb77a900fda9a4b5e
Atendente04	0f4703dbb77fe9a29cc0907cb6c8ebb23762ca3b
Supervisor	55bfc9f592d793c76e3beefb77c797e12fd616b
Atendente05	cb5690fae21d427690df057a258b2396df783d31

The status bar at the bottom indicates "6 linhas selecionadas" (6 lines selected).

USUARIO	SENHA
Atendente01	5f1eff3993e5ba88c4a097eafaa87f079b49b5e9
Atendente02	4600998d199cf55baca5baaee818d56cb674a9b8
Atendente03	f0c30123f7c735ca1974a85eb77a900fda9a4b5e
Atendente04	0f4703dbb77fe9a29cc0907cb6c8ebb23762ca3b
Supervisor	55bfc9f592d793c76e3beefb77c797e12fd616b
Atendente05	cb5690fae21d427690df057a258b2396df783d31

# Exemplo: Acesso aos Dados

- Software Funcional:
  - Busca a partir da entrada de um usuário.

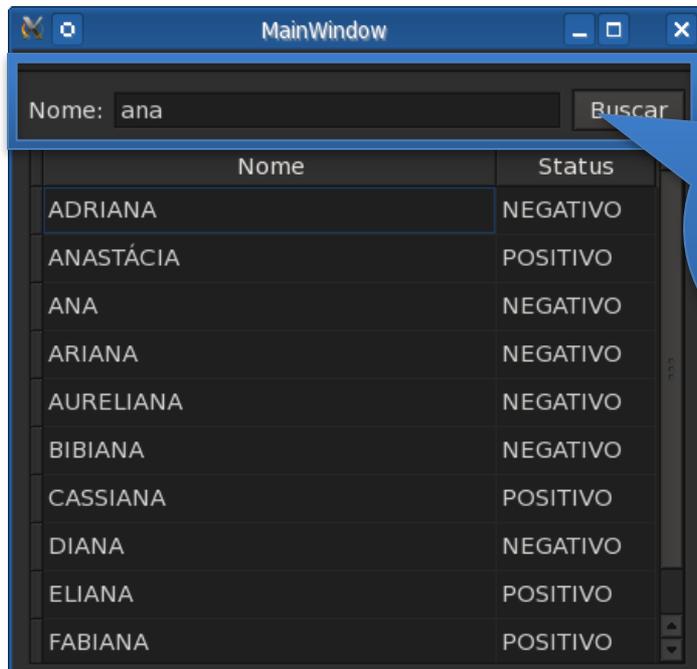


# Exemplo: Acesso aos Dados

- Software Seguro Aspectos Tangíveis:
  - Dificultar extração dos dados de resultados dos exames;
  - Reforçar chaves de buscas não triviais;
  - Definir tempo de sessão (timeout);
  - ...
- Software Seguro Aspectos Intangíveis:
  - Validação das entradas de busca;
  - Consulta segura aos resultados de exames;
  - Segurança na base de dados;
  - Definição granular de papéis e perfis de acesso.
  - ...

# Exemplo: Acesso aos Dados

- Dificultar a extração dos dados de resultados dos exames

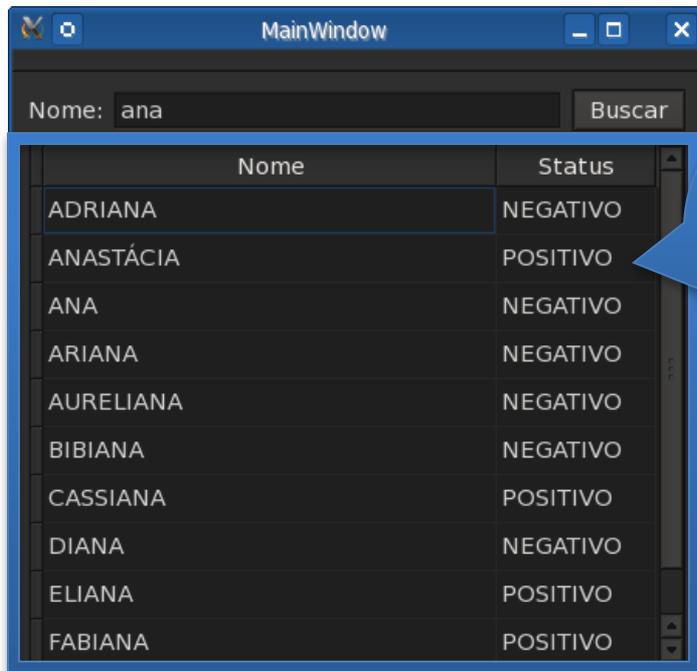


Nome	Status
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO

Entrada do  
Usuário

# Exemplo: Acesso aos Dados

- Dificultar a extração dos dados de resultados dos exames



Nome	Status
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO

Retorno do Sistema

# Exemplo: Acesso aos Dados

- Dificultar a extração dos dados de resultados dos

Máximo de N  
saídas por  
consulta

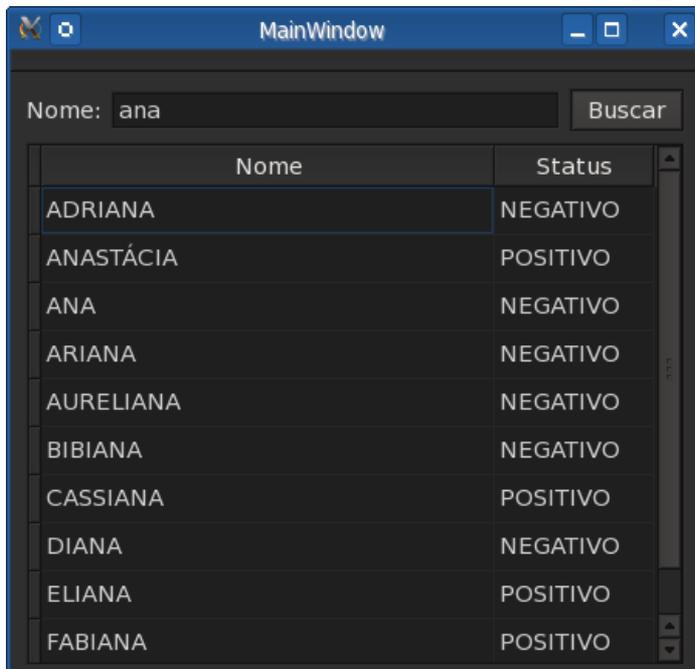
Nome	Status
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO



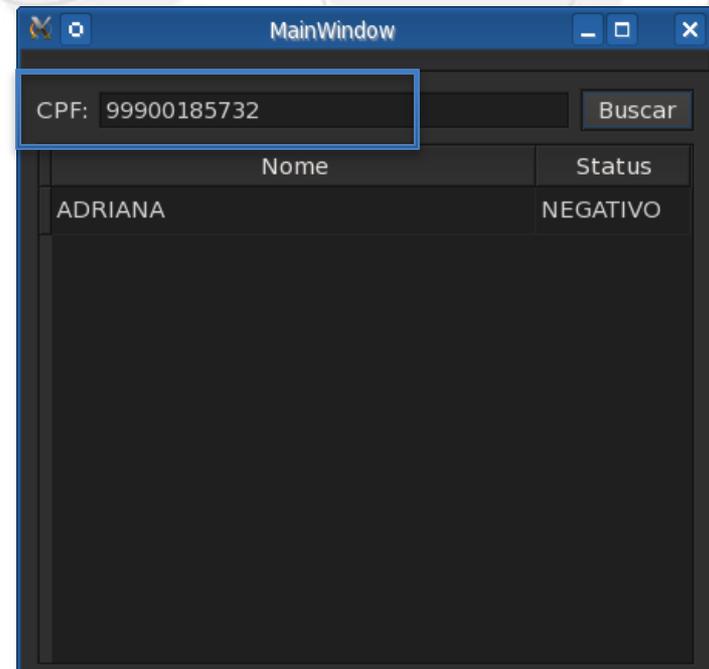
Nome	Status
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO

# Exemplo: Acesso aos Dados

- Forçar o uso de chaves de busca não triviais



Nome	Status
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO



Nome	Status
ADRIANA	NEGATIVO

# Exemplo: Acesso aos Dados

- **Reforça chaves de busca não triviais**

The image displays two screenshots of a software application window titled 'MainWindow'. The left screenshot shows a search for 'ana' in the 'Nome' field, resulting in a list of names and their corresponding 'Status'. The right screenshot shows a search for 'CPF: 99900185732' in the 'CPF' field, with a blue box highlighting the search input and a blue callout bubble pointing to the result.

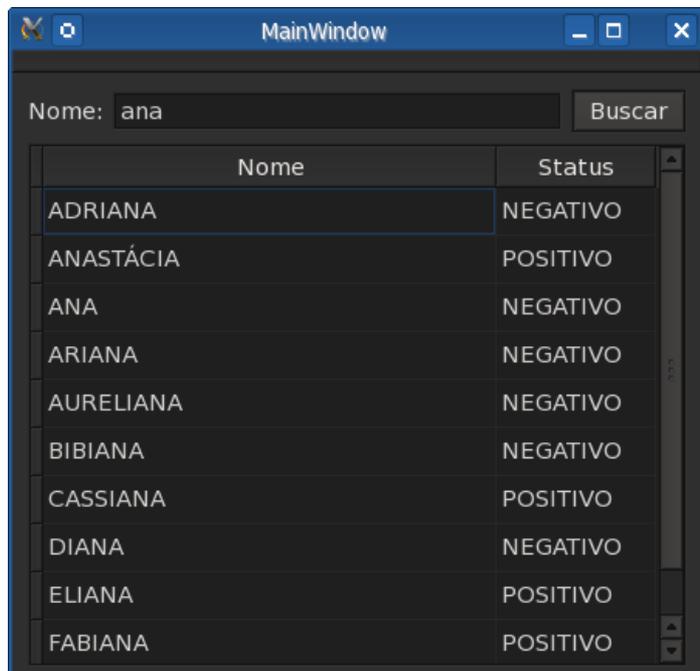
Nome	Status
ADRIANA	NEGATIVO
ANASTASIA	NEGATIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO

CPF: 99900185732

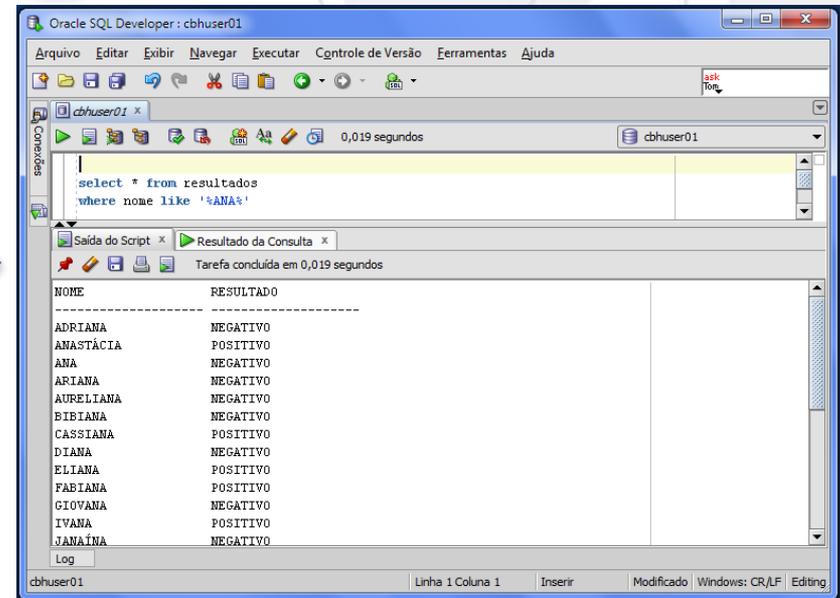
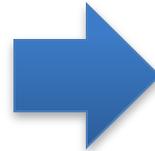
Usuário possui mais dificuldade em "adivinhar" um número de CPF existente no banco de dados

# Exemplo: Acesso aos Dados

- Validação das entradas de buscas



Nome	Status
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO



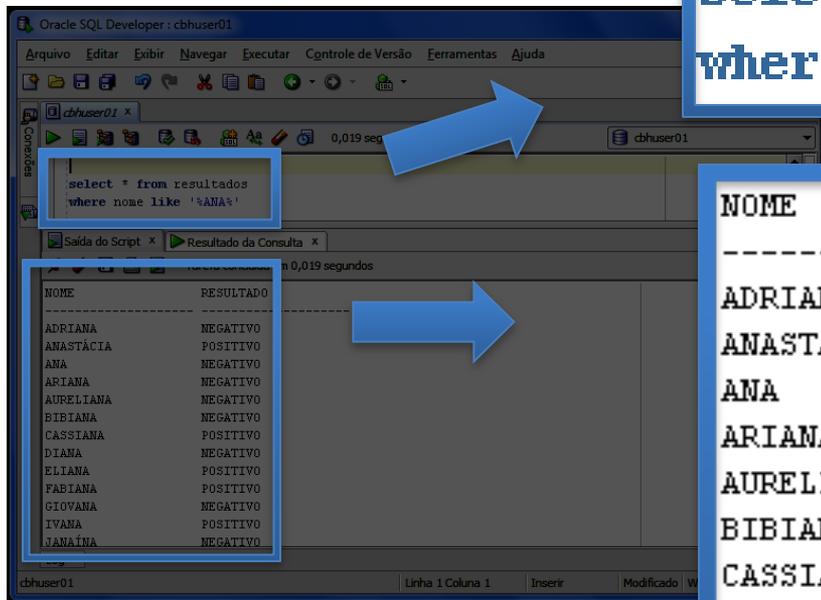
```
select * from resultados
where nome like '%ANA%'
```

NOME	RESULTADO
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO
GIOVANA	NEGATIVO
IVANA	POSITIVO
JANAÍNA	NEGATIVO

# Exemplo: Acesso aos Dados

- Validação das entradas de buscas

```
select * from resultados  
where nome like '%ANA%'
```



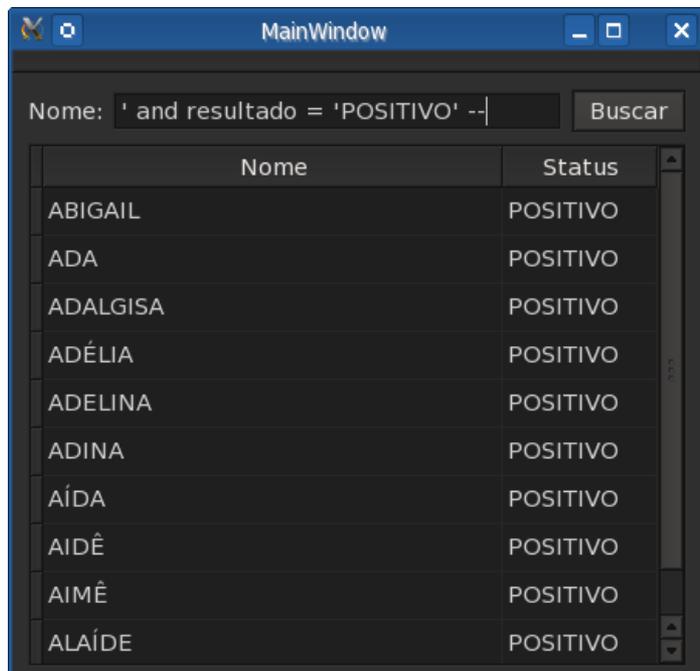
The screenshot shows the Oracle SQL Developer interface. The top menu bar includes 'Arquivo', 'Editar', 'Exibir', 'Navegar', 'Executar', 'Controle de Versão', 'Ferramentas', and 'Ajuda'. The main window displays a SQL query: `select * from resultados where nome like '%ANA%'`. Below the query, the 'Resultado da Consulta' window shows a table with two columns: 'NOME' and 'RESULTADO'. The results are as follows:

NOME	RESULTADO
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO
GIOVANA	NEGATIVO
IVANA	POSITIVO
JANAÍNA	NEGATIVO

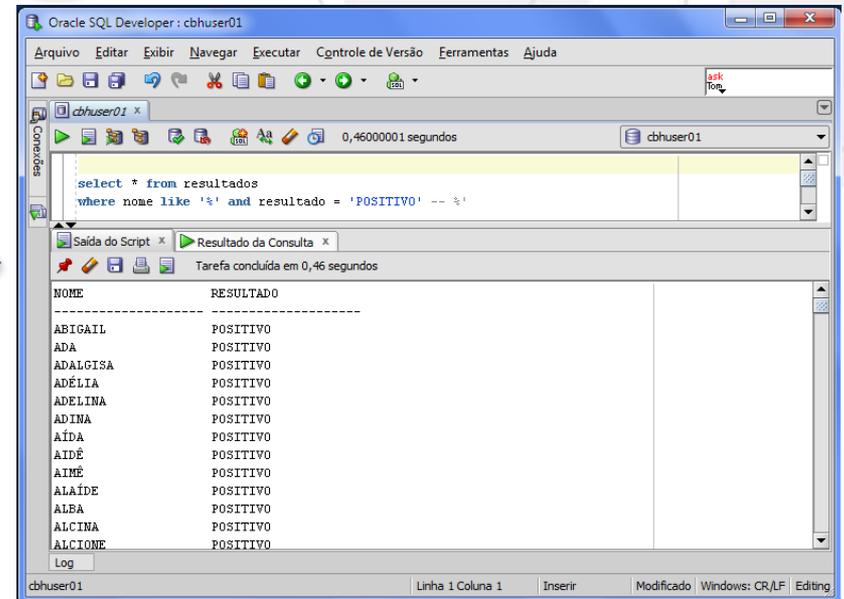
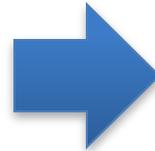
NOME	RESULTADO
ADRIANA	NEGATIVO
ANASTÁCIA	POSITIVO
ANA	NEGATIVO
ARIANA	NEGATIVO
AURELIANA	NEGATIVO
BIBIANA	NEGATIVO
CASSIANA	POSITIVO
DIANA	NEGATIVO
ELIANA	POSITIVO
FABIANA	POSITIVO
GIOVANA	NEGATIVO
IVANA	POSITIVO

# Exemplo: Acesso aos Dados

- Validação das entradas de buscas



Nome	Status
ABIGAIL	POSITIVO
ADA	POSITIVO
ADALGISA	POSITIVO
ADÉLIA	POSITIVO
ADELINA	POSITIVO
ADINA	POSITIVO
AÍDA	POSITIVO
AIDÊ	POSITIVO
AIMÉ	POSITIVO
ALAÍDE	POSITIVO

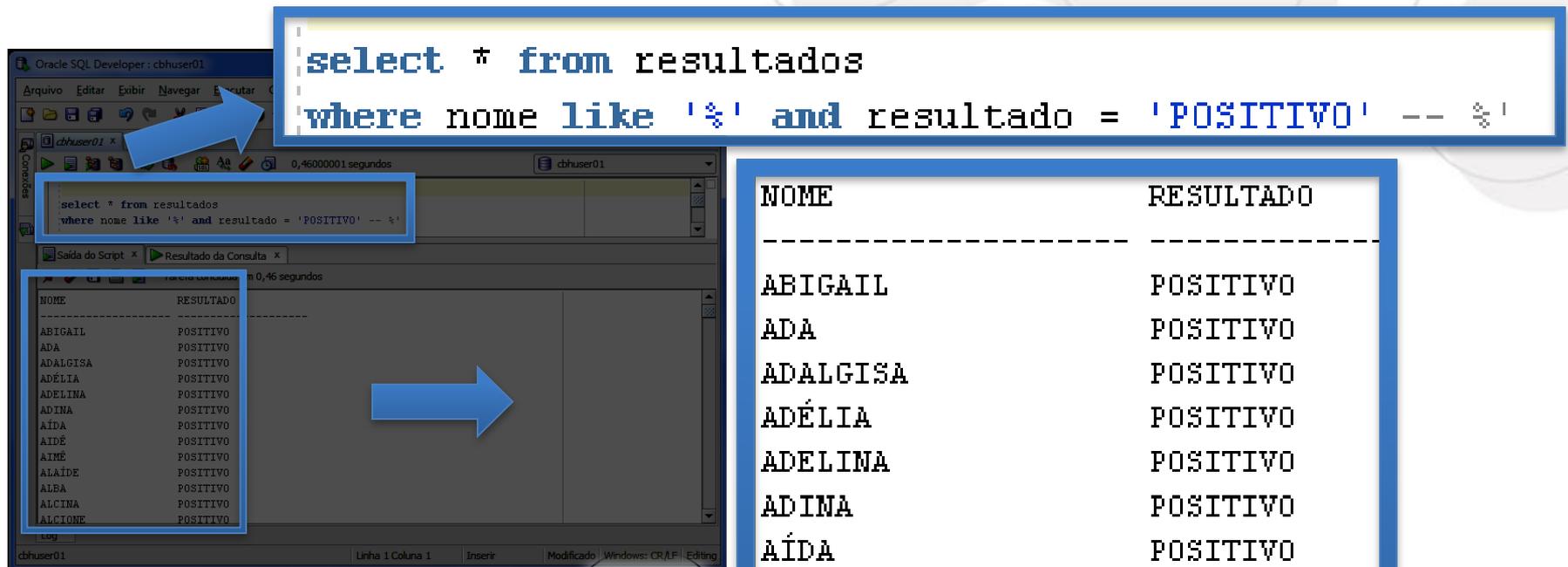


```
select * from resultados
where nome like '% and resultado = 'POSITIVO' -- %'
```

NOME	RESULTADO
ABIGAIL	POSITIVO
ADA	POSITIVO
ADALGISA	POSITIVO
ADÉLIA	POSITIVO
ADELINA	POSITIVO
ADINA	POSITIVO
AÍDA	POSITIVO
AIDÊ	POSITIVO
AIMÉ	POSITIVO
ALAÍDE	POSITIVO
ALBA	POSITIVO
ALCINA	POSITIVO
ALCIONE	POSITIVO

# Exemplo: Acesso aos Dados

- Validação das entradas de buscas



The screenshot shows the Oracle SQL Developer interface. The top window displays the following SQL query:

```
select * from resultados  
where nome like '%&' and resultado = 'POSITIVO' -- %'
```

The bottom window shows the results of the query in a table format:

NOME	RESULTADO
ABIGAIL	POSITIVO
ADA	POSITIVO
ADALGISA	POSITIVO
ADÉLIA	POSITIVO
ADELINA	POSITIVO
ADINA	POSITIVO
AÍDA	POSITIVO
AIDÊ	POSITIVO
AIMÊ	POSITIVO
ALAÍDE	POSITIVO
ALBA	POSITIVO
ALCINA	POSITIVO
ALCIONE	POSITIVO

Blue arrows indicate the flow from the query editor to the results window and then to the detailed table view on the right.



- No brasil: PCI
- Aplicações Web para e-commerce
- OWASP RFP
- Norma NBR
- Exemplos de ataques
- Recomendações