POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

SISTEMAS DE BASES DE DADOS

Engenharia Informática, regimes Diurno e Pós-Laboral

2.º Ano 2.º Semestre 2020/2021

FICHA 1

Segurança em Bases de Dados (parte 2)

Objetivos:

- Gerir limites de recursos
- Gerir perfis de utilizadores

Antes de iniciar a resolução desta ficha de trabalho deverá responder às seguintes questões:

1. Diga o entende por:
   a. Perfil;

2. Apresente um exemplo do comando que permite realizar cada uma das seguintes ações:
   a. Retirar um privilégio de sistema de um role;
   b. Atribuir um perfil a um utilizador;
   c. Criar perfis de utilizador.

CASO DE ESTUDO

Uma determinada escola de condução dedica-se ao ensino da condução a membros da comunidade com mais de 18 anos de idade.

Para ser-se aluno e ter acesso às aulas de condução é necessário realizar uma inscrição. Quando uma inscrição for paga, a data de pagamento será registada e o valor do atributo *paga* será automaticamente atualizado.

Para obter aprovação à categoria automóvel de uma inscrição, cada aluno deve realizar exame: se reprovar nesse exame, terá de fazer nova inscrição. Cada exame é preparado pela Direção Geral de Viação para vários alunos: cada aluno obtém a categoria respetiva assim que o resultado do exame for definido, sendo a data do exame aquela que define a data de obtenção da categoria correspondente.

ALUNO

bi	nome	morada	data_nasc	ult_categ_obtida	data_ult_categ_obtida	total_reprovacoes	username
1777	Carlos Sousa	Rua das Tijoleiras	26/02/1997	*NULL*	*NULL*	2	C1777
1888	Susana Costa	Rua da Beleza	29/08/1984	*NULL*	*NULL*	1	S1888
1999	Filipe da Silva	Av. Vidal Pinheiro	01/01/1995	C	05/02/2019	0	F1999

EXAME

id	local	data	categoria
10809	Estádio da cidade	03/12/2020	C
10900	Estádio da cidade	04/12/2020	A
10901	Escola	01/01/2021	C
10902	Estádio da cidade	07/02/2021	A
10903	Escola	09/02/2021	A
10904	Centro de Testes Automóveis	12/03/2020	B
10905	Centro de Testes Automóveis	13/03/2021	A
10906	Centro de Testes Automóveis	01/04/2021	B
10907	Estádio da cidade	10/04/2021	B

INSCRICAO

id	data_insc	paga	data_pagamento	categoria	***bi_aluno***	***id_exame***	resultado_exame
7089	08/11/2020	S	08/12/2020	C	1999	10901	A
7090	01/12/2020	S	04/01/2021	A	1777	10900	R
7091	08/12/2020	S	04/01/2021	C	1888	10901	R
7092	10/01/2021	N	*NULL*	B	1999	*NULL*	*NULL*
7093	11/01/2021	S	12/01/2021	A	1777	10902	R
7094	10/01/2021	S	20/01/2021	A	1777	10903	NULL
7095	08/02/2021	N	*NULL*	D	1777	*NULL*	*NULL*

Figura 1 – Modelo Lógico da Base de Dados.

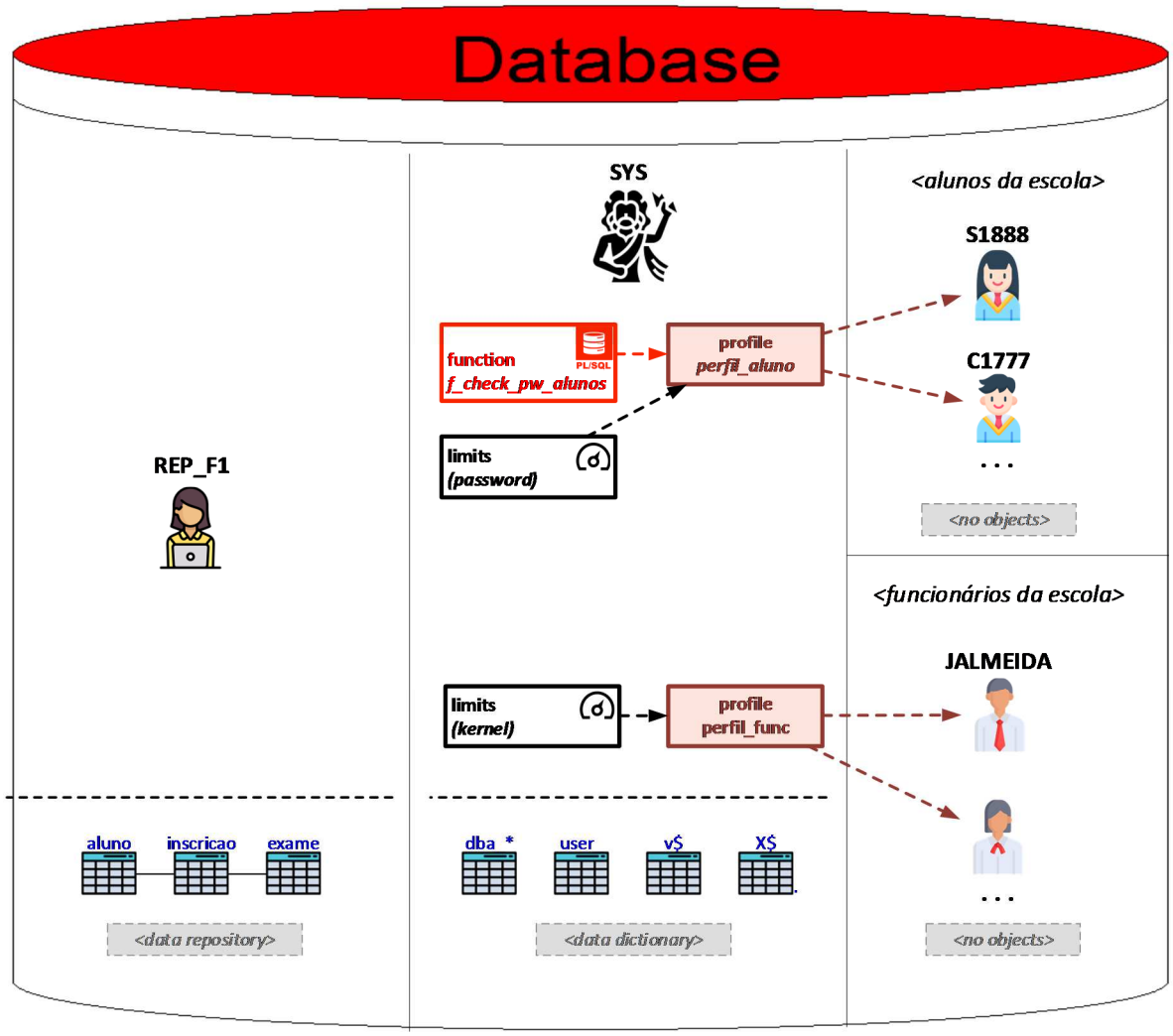

Figura 2 – Arquitetura **pretendida** ao nível da segurança.

Notas prévias

a) A presente parte da ficha pressupõe que foram realizadas as tarefas da parte 1.

b) **Verifique e teste** todas as alterações realizadas sobre os objetos ou privilégios da base de dados, consultando os objetos envolvidos e/ou o dicionário de dados.

c) **Guarde num ficheiro** *sql* a sequência exata e completa dos comandos executados, juntamente com os apontamentos relevantes sobre o contexto da execução. Este ficheiro, quando executado de forma integral, deverá permitir resolver na íntegra toda a ficha.
Após terminar os exercícios, renomeie o ficheiro para <n.º_estudante_SBDficha1.2.sql) e submeta-o no Moodle utilizando o link apropriado (por exemplo, o estudante n.º 2100001 submeterá o ficheiro *2100001_SBDficha1.2.sql*).

Os exercícios assinalados com **(*)** deverão ser realizados em estudo autónomo.

Perfis de utilizador

1. Após uma auditoria de rotina à base de dados relativamente à forma como os alunos da escola de condução acedem à base de dados, o DBA apercebeu-se que os alunos da escola de condução tendem a não respeitar boas práticas na gestão das suas *passwords*. Por exemplo, 45% das alterações de *password* utilizam a *password* anterior e 82% dos alunos não altera a sua *password* durante o período em que é aluno.
Tendo em conta estas estatísticas preocupantes, o DBA irá reimplementar a política de segurança para *passwords* dos alunos da forma que é descrita de seguida:

a) A *password* de cada aluno deverá:

- Ter pelo menos 6 caracteres;
- Ter letras e números;
- Ser diferente da anteriormente utilizada;
- Ser diferente de "*password*" (maiúsculas ou minúsculas) e de "qwerty";
- **(*)** Ser diferente da anterior em pelo menos 3 caracteres (a diferença entre *strings* ou "*distância de Levenshtein"* pode ser calculada utilizando a função `ORA_STRING_DISTANCE`, já existente no utilizador `sys`);

b) **(*)** Utilize a função `ORA_COMPLEXITY_CHECK`, já existente no utilizador `sys`, para impor as mesmas regras que implementou anteriormente.

c) **(*)** Utilize um dicionário de palavras/expressões que confira maior dinamismo à verificação de *passwords* proibidas.

d) Para cada aluno é necessário garantir que:

- Durante o processo de *login*, o utilizador pode errar a *password* até 3 vezes consecutivas, após as quais será bloqueado durante 2 minutos;
- A *password* expira a cada 15 dias, mas o utilizador será notificado nos 5 dias que antecedem o limite de alteração;
- A *password* pode ser reutilizada, mas só após 30 dias e apenas se já tiver sido alterada pelo menos duas vezes;
- **(*)** A conta fica bloqueada se não for utilizada durante 90 dias.

e) **(*)** Descubra como poderá desbloquear-se um utilizador que tenha sido bloqueado após 3 tentativas falhadas de *login* e antes do desbloqueio automático que ocorre passados 2 minutos.

f) Crie situações realistas que permitam testar todos os limites definidos.

2. Relativamente aos funcionários da escola, o DBA descobriu também situações de utilização imprópria da base de dados, desta vez ao nível dos recursos do SGBD: por exemplo, 34% dos funcionários deixam as suas sessões abertas por longos períodos de tempo (+ de 150 minutos); 75% dos funcionários utiliza mais de 4 sessões em simultâneo.

Numa tentativa de racionar estes e outros recursos, o DBA definiu as seguintes regras para os funcionários da escola de condução:

- Cada utilizador só pode ter 2 sessões ativas em simultâneo;
- Não há limite para o consumo de CPU em cada sessão;
- Cada comando SQL executado pode consumir até 5 segundos de CPU;
- Cada sessão pode durar, no máximo, 2 minutos;
- No processamento de um comando SQL não pode haver uma leitura de mais de 10 blocos de dados;
- Cada sessão não pode ler mais de 100 blocos de dados.

NOTA: Crie situações realistas que permitam testar todos os limites definidos.

Remoção de privilégios

3. **(*)** Retire aos *roles role_aluno* e *role_func* os privilégios concedidos até ao momento. Verifique e teste as alterações.