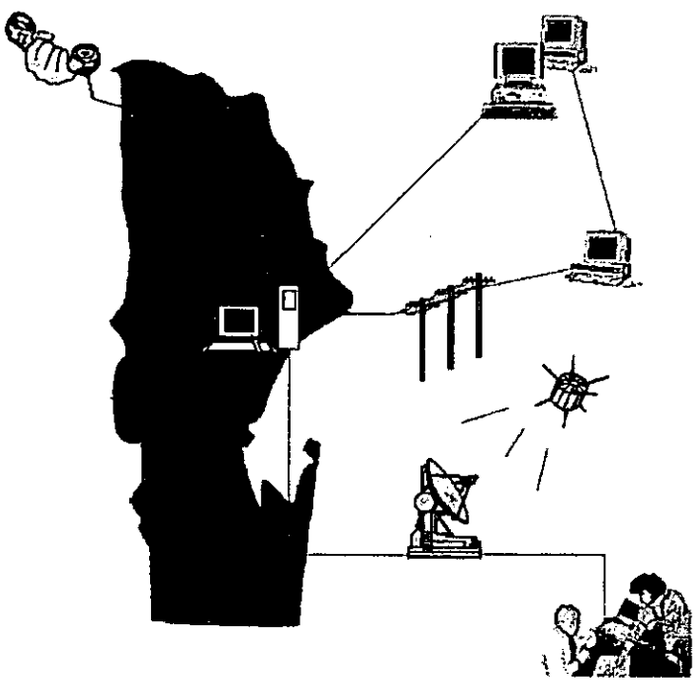
UNIVERSIDADE EDUARDO MONDLANE

Faculdade de Ciências

Departamento de Matemática e Informática

Trabalho de Licenciatura

Tema: O Acesso pelas Faculdades à Aplicação de Gestão de Alunos



Autor:

Marcelo Viriato Munguanaze

IT-182

UNIVERSIDADE EDUARDO MONDLANE

Faculdade de Ciências

Departamento de Matemática e Informática

Trabalho de Licenciatura

Tema:

O Acesso pelas Faculdades à Aplicação Gestão de Alunos

Supervisores:

dra. Otília G. Fernandes da Graça

eng. Venâncio Massingue

Autor:

Marcelo Viriato Munguanaze

Maputo, Junho de 1997

Agradecimentos

A todos que directa ou indirectamente contribuíram na realização deste trabalho, em especial:

À minha supervisora dra. Otília Gonçalves Fernandes da Graça que incansavelmente me deu todo o seu apoio e disponibilidade desde o início até ao fim.

Aos meus professores do curso, que me transmitiram conhecimentos, experiência e ideias, manifesto-me particularmente grato.

Aos meus colegas de curso, e de profissão (Departamento de Software e Aplicação - CIUEM) que sempre me mostraram o caminho correcto para a efectivação desta tarefa, vai uma expressão de apreço.

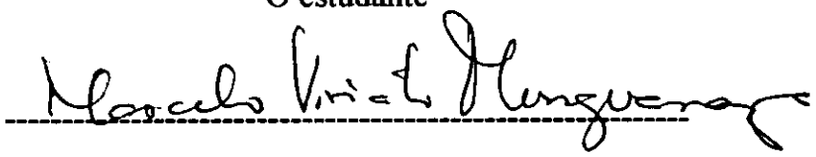
Aos meus pais que me garantiram a protecção moral e que sempre, souberam estimular-me.

Marcelo Viriato Munguanaze

Declaração

Declaro que este trabalho é resultado da minha própria investigação, que não foi submetido para outro grau que não seja o indicado - Licenciatura em Matemática e Informática pela Universidade Eduardo Mondlane.

O estudante



Munguanaze, Marcelo Viriato

Resumo

O desenvolvimento de sistemas de informação é uma das actividades mais complexas levadas a cabo numa organização. Estes sistemas devem possuir boa qualidade.

A qualidade de um sistema pode ser determinada pelo grau de segurança que o mesmo oferece. E, por sua vez, a segurança de um sistema pode ser abordada em diferentes perspectivas.

O presente trabalho é um estudo sobre a segurança no acesso a um sistema de informação multi utilizador.

No capítulo 1 e 2 define-se o âmbito do problema como sendo a aplicação de gestão de alunos e apresentam-se os métodos do estudo.

Os capítulos 3,4, 5 e 6 dedicam-se ao estudo de segurança num sistema de informação e na da base de dados ORACLE e das formas de providenciar o acesso a sistemas de informação usando meios de comunicação.

Constatou-se que a segurança dos dados está definida a nível da base de dados e que a segurança nos meios de transferência não é determinante.

Índice

1. Introdução

A Universidade Eduardo Mondlane (UEM) é uma instituição de ensino superior que exerce suas actividades nas áreas académica, investigação e extensão. Para a execução destas actividades precisa de instrumentos de canalização da informação actualizada a pessoas correctas no momento exacto.

Em 1992 foi aprovada a "Política de Informática da UEM" que agrupa as necessidades da instituição em áreas de informatização, entre elas, a Direcção do Registo Académico (DRA), Gestão de Património, Recursos Humanos etc. Nela se definem ainda as áreas prioritárias sendo uma delas a DRA, cujas actividades de informatização estão já em curso. É no âmbito destas actividades que nasce o presente trabalho propondo estudar a segurança dos dados da Aplicação de Gestão de Alunos (AGA), quando acessada pelas faculdades.

Não se pretende encontrar um produto acabado, mas sim, um resultado que contribua na concepção e adopção de procedimentos seguros na implantação de sistemas de nível de segurança aceitável na instituição.

A UEM é uma instituição de ensino composta por vários órgãos, entre faculdades dispersas por diferentes pontos da cidade de Maputo, a Direcção do Registo Académico (DRA), na Reitoria, sito na baixa da cidade e outros órgãos de carácter administrativo e técnico.

A Direcção do Registo Académico (DRA), é o órgão responsável pela gestão da informação dos estudantes e, está em constante iteração com os outros sectores que directa ou indirectamente lidam com informação académica (figura 1).

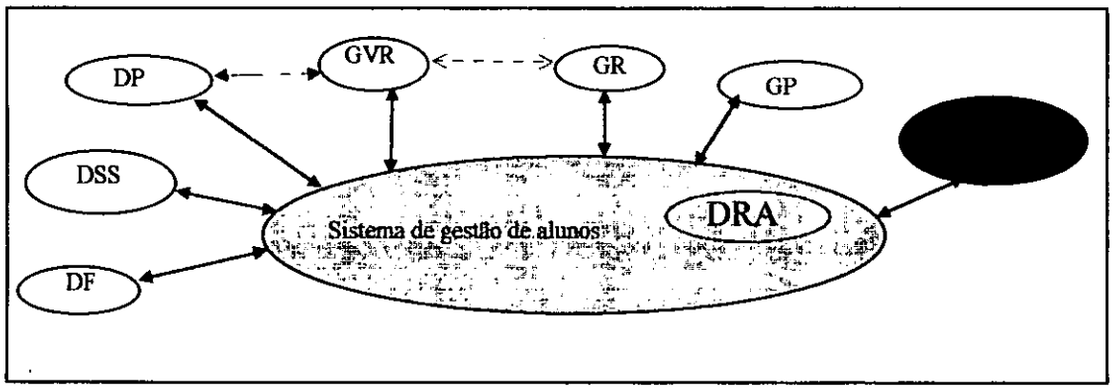


Figura 1: A troca de Informação do sistema de Gestão de Estudantes e outros sectores

Legenda:

DF - Direcção de Finanças
DSS - Direcção dos Serviços Sociais
DP - Direcção Pedagógica
DRA - Direcção do Registo Académico
GR - Gabinete do Reitor
GVR - Gabinete do Vice-reitor
GP - Gabinete de Planificação

Constituem actividades principais da DRA as seguintes:

- Regular o processo de matrículas e sua renovação;
- Lançamento no processo individual do estudante das inscrições nas várias disciplinas, procedendo à respectiva validação;
- Inscrição nos exames de recorrência;
- Lançar no processo individual do estudante as notas constantes das actas;
- Validação da informação curricular do estudante;
- Emissão de certificados;
- Emissão de declarações;
- Elaborar propostas de redução/renovação/inibição das bolsas de estudo (ou isenção de propinas)
- etc.

1.1 Identificação e âmbito do problema

A necessidade de um instrumento ou procedimentos que assegurem a segurança e integridade dos dados do sistema de gestão de estudantes (AGA) constitui o objectivo principal do presente estudo.

O problema da segurança levanta-se, por um lado, pela existência de constantes ameaças locais e, por outro, pela necessidade de uma futura descentralização do sistema que hoje funciona ao nível central (DRA).

A descentralização deste sistema consistiria na extensão da sua funcionalidade ao nível das faculdades o que envolve, logicamente, outro tipo de detalhe. Deve-se encontrar uma infra-estrutura de comunicação que permita essa conexão. As redes de dados têm também, as suas fraquezas na segurança; são susceptíveis *aos "hackers"* (indivíduos que realizam ataques aos sistemas usando facilidades das redes de computadores).

De modo a clarificar a definição do problema segue-se uma retrospectiva histórica desde nascimento ao estágio actual do sistema em estudo.

1.2 História do nascimento do sistema

Em 1992 iniciou-se o desenvolvimento do ARIS - Academic Register Information System, um sistema que tem por finalidade informatizar o registo académico, como forma de atender às necessidades de informação para uma gestão eficaz dos dados estudantis.

O principal objectivo do projecto ARIS foi o desenvolvimento da Aplicação de Gestão de Alunos (AGA) hoje instalada na Reitoria (DRA).
Este desenvolvimento compreende três fases (Plano de informatização da DRA, 1992); duas já foram executadas.

Primeira fase

Correspondeu à análise do sistema para a definição de requisitos do usuário até à compra do pacote de software; na escolha do pacote foram visitadas as empresas ITS – *Integrated Tertiary Software da* África do Sul e a Universidade do Porto (UP).

A escolha recaiu no pacote da UP, pois, o seu sistema é compatível com requisitos e necessidades de processamento do Registo Académico (RA) em Moçambique; é suficientemente flexível, adaptando-se também à realidade moçambicana (Plano de informatização da DRA, 1992).

A escolha de hardware recaiu sobre a empresa sul africana HP- Hiperformance system sobre a plataforma de sistema operativo UNIX.

A base de dados usada é a definida centralmente, o ORACLE.

Como departamento de suporte, o CIUEM é responsável pelo desenvolvimento e implementação deste sistema de informação multi-utilizador.

Segunda fase

Iniciou-se no segundo semestre de 1996 e tinha como tarefas as seguintes:

- Modificação do sistema;
- Instalação do sistema ao nível da Reitoria;
- Treino do pessoal da reitoria;
- Teste do sistema;
- Documentação dos procedimentos de desenvolvimento;
- Implementação do sistema;

A conclusão desta fase está programada para o final do primeiro semestre de 1997.

Terceira fase

O presente trabalho enquadra-se nas actividades desta fase que preconiza a extensão de algumas das funções do sistema AGA para o nível das faculdades. Isto vai trazer largas vantagens na vida da instituição, na medida em que, muitos procedimentos e necessidades de informação (perguntas) poderão ser respondidas directamente a partir das faculdades. Constituem tarefas desta fase as seguintes:

- Aquisição de software/hardware para as faculdades;
- Definição e especificação de segurança do sistema;
- Treino dos utilizadores das faculdades;
- Definição de procedimentos de manutenção;

Deve-se assinalar que numa primeira etapa as faculdades só terão a permissão para a leitura dos dados.

A aplicação de gestão de alunos é um sistema de informação multi departamental que serve não só as necessidades do órgão responsável pela manutenção do Registo Académico central, como também os Registos Académicos das faculdades sob responsabilidade da DRA. Ela representa o funcionamento da DRA na administração e gestão de informação académica dos alunos. Os seus dados são muito sensíveis (matrículas, resultados, planos de inscrições) e não devem ser acedidos por indivíduos estranhos; mas, o sistema está conectado a um ambiente de rede sujeito a acções de vários indivíduos. A partilha de dados é desejável, mas precisa-se de um mecanismo de controlo que assegure o acesso ao sistema por indivíduos autorizados.

1.3 Objectivos

1.3.1 Gerais

Estudar a segurança no acesso a aplicação de gestão de alunos (AGA).

Estudar os níveis de acesso postos à disposição pela aplicação.

1.3.2 Específicos

Estudar a segurança e integridade de dados de um sistema de informação;

Estudar os sistemas de gestão de base de dados;

Estudar a segurança oferecida pela base de dados ORACLE e

Estudar o uso dos níveis de acesso definidos na AGA.

2. Materiais e Métodos

Para a elaboração deste trabalho foi consultada a bibliografia que trata de assuntos ligados aos seguintes tópicos:

- Segurança de sistemas de informação;
- Segurança de bases de dados;
- Redes de computadores;
- Documentação do sistema;

3. Segurança de um Sistema de Informação (SI)

Sistema de informação (SI) é uma colecção de componentes de hardware e software que pode ser usada para recolher, processar, armazenar e fornecer informação (Warman, 1993). Um SI não depende necessariamente da presença do computador. O presente estudo refere-se a um sistema computarizado.

3.1 O que é segurança e integridade de dados

Uma questão fundamental a que especialistas em segurança de computadores tentam prestar atenção é o facto de que um SI está sujeito a ataques e erros. Isto pode resultar num número de ameaças à organização ou à informação dos usuários (Warman, 1993).

O sistema de informação precisa de ser protegido porque pode estar comprometido pela ignorância das pessoas, malícia ou acidente. O ponto crucial é preservar a integridade de dados e o sentido geral de segurança pode ser entendido como o estado de certeza de que o SI não pode ser acedido e alterado por pessoas não autorizadas.

Em sistemas de usuário único presume-se que toda informação pertence a uma só pessoa, autorizada a fazer o que quiser mas, em sistemas compartilhados, o SI é um recurso organizacional que é partilhado por vários usuários de capacidades e necessidades diferentes tornando-se importante que se controle exactamente quem pode fazer o quê. A razão disto é *a confidencialidade.* A maioria dos dados é confidencial em maior ou menor grau (Date, 1985).

O usuário tem que estar garantido que a parte dos dados que tem acesso está segura daí a necessidade de adoptar medidas de segurança e protecção do sistema.

O termo *segurança* significa protecção dos dados do sistema contra revelações ou destruições não autorizadas, e o termo *integridade* usa-se para referir à sua precisão, correcção ou validade.

Um sistema de computação ou comunicação seguro é aquele que está livre de uso impróprio por parte de um indivíduo e do mau funcionamento do hardware e software. O objectivo da segurança nos sistemas de informação está em assegurar a disponibilidade e manter a integridade em caso de falha no sistema.

3.2 Caminhando para um sistema seguro

A segurança é implementada restringindo a área física, em volta do sistema, a pessoas autorizadas, usando software especial e pelos mecanismos internos de processamento e ainda acções para prevenir acessos não autorizados quer acidental quer intencionalmente.

As medidas de segurança devem ser especificadas nos momentos iniciais do ciclo de desenvolvimento do sistema para permitir a sua planificação detalhada. A gestão deve alocar responsabilidade nas especificações de segurança, assegurando que todos os usuários saibam e entendam os procedimentos que devem cumprir. É importante desenhar um sistema que permita um controlo manual e automático.

Os principais tipos de controlo de acesso são:

- Controlo físico
- Controlo de rede (comunicações)
- Controlo lógico

O controlo físico aponta para o controlo de acessos aos componentes físicos de processamento de informação ou dispositivos de armazenamento, i.e., o acesso a estes componentes deve ser restrito a pessoas autorizadas; por exemplo, o acesso à sala do servidor pode ser controlado por guardas.

A segurança de comunicações consiste no controlo de acesso ao sistema de processamento de informação e seus dados que podem ser providenciados pela rede. Muitas vezes, os *"hackers"* tentam usar seus computadores pessoais e modem para se introduzirem nos sistemas alheios por telefone.

O controlo lógico provê controle adicional aos utilizadores autorizados, restringindo o

acesso a um conjunto de dados, pela validação de todas as operações (inserção, actualização, remoção) sobre os dados, para se certificar de que estão correctas.

Ao se implementar medidas de segurança tenta-se lidar com as ameaças, trabalhando sobre certos objectivos, um dos quais a prevenção - tarefa de tentar parar com ataques e falhas a partir de antecipação de certos eventos.

Para a prevenção ser possível requer-se um entendimento de como e quais as ameaças podem ocorrer e então identificar e implementar as medidas apropriadas que, pelo menos, dificultarão a sua ocorrência (Warman, 1993),

Assim, o passo inicial na construção de um esquema de segurança é saber o que se pretende proteger, contra quem protege os seus dados, e ainda, quais os recursos disponíveis para a obtenção da protecção desejada.

Segundo (Woolf et al. 1987, Madron 1992) a protecção pode ser categorizada em protecção contra perda física ou dano no hardware, software ou dados, contra a cópia de dados e contra correcções não autorizadas de dados. A falta de protecção resulta em perdas que podem traduzir-se em elevados prejuízos para a organização.

As perdas de dados e os custos suportados pelas organizações são o resultado directo de erros humanos, acidentes e omissões. A principal ameaça à segurança são as pessoas e constituem o maior perigo para qualquer sistema de computadores. A acção de usuários autorizados é responsável por 75% das quebras de segurança (figura 2).

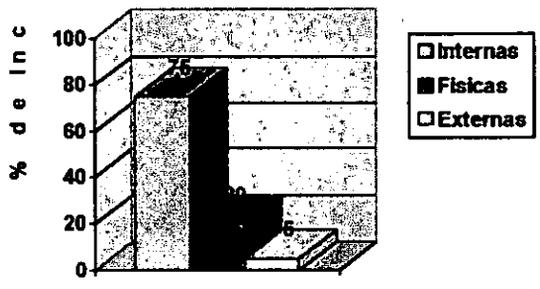


Figura 2: A origem das quebras de segurança

A ameaça é uma potencial acção ou evento cuja ocorrência pode resultar nalguma forma de perda.

O analista deve examinar o sistema para identificar todas as quebras de segurança que podem afectar o desempenho, sejam deliberadas ou acidentais, a fim de desenvolver uma estratégia de prevenção para minimizar as perdas. Madron (1992) distingue três tipos de ameaças: internas, externas e físicas. A sua ocorrência deve-se a desastres naturais, sabotagem e roubos.

Um sistema de informação é seguro se tem assegurada

- a privacidade;
- a integridade;
- a disponibilidade e
- a consistência dos seus dados

A quebra destes factores representa uma quebra da segurança da organização. O importante é tomar medidas tendentes a reduzir (até um certo nível) as perdas esperadas da ocorrência duma ameaça.

A privacidade

Significa proteger o acesso à informação contra qualquer pessoa que não foi explicitamente autorizada.

A integridade

A integridade dos dados visa garantir que a informação não é alterada ou destruída sem a devida permissão. Este conceito envolve garantir que, o que o usuário procura fazer esteja correcto. Os dados devem ser protegidos para que não sejam degradados ou tornados indisponíveis sem a devida autorização.

A disponibilidade

A perda de disponibilidade ou seja, se o sistema não está disponível quando um usuário autorizado precisa dele, é tão mau quanto um sistema que tenha os dados apagados.

A consistência

Assegura que o sistema se comporte como o usuário espera; imagine que o usuário emite o comando "login aplicação A", e em vez de A o sistema executa a aplicação B!

3.3 O que significa ter segurança

A resposta a esta questão não é simples nem fácil, pois, envolve algum tipo de estimativas da relação (razão) entre os benefícios resultantes de um sistema protegido e do custo da obtenção dessa protecção. Essa razão varia de companhia para companhia ou de uma organização para outra, devendo cada uma definir as suas políticas de segurança, que devem coadunar com o tipo de actividades e o meio em que a organização se encontre inserido.

O paradoxo para os especialistas em segurança é que a segurança absoluta não pode ser conseguida. Nenhum sistema pode ser inteiramente seguro; as precauções a serem feitas dependem muito do controlo e não do hardware (Warman, 1993).

Em situações nas quais os dados sejam suficientemente sensíveis, ou quando o processamento efectuado sobre os dados seja suficientemente crítico, torna-se necessário um suporte para a auditoria.

Um suporte de auditoria pode ser visto como um arquivo do banco de dados especial, no qual o sistema automaticamente guarda referências de todas operações executadas pelos usuários sobre a base de dados normal.

Uma entrada típica deste suporte (Date,1985) pode conter as seguintes informações:

- Operação feita (ex.: update);
- Terminal do qual foi solicitada a operação;
- Usuário que solicitou a operação;

- Data e hora da operação;
- Tabela, registo e campo afectados;
- valor anterior do campo;
- Novo valor do campo;

3.4 Identificação de usuários

A segurança de dados depende também da identificação correcta do usuário no terminal. Existem vários métodos para controlar os acessos ou verificação de identidade: *passwords*, perguntas, impressões digitais, assinaturas.

O *password* é uma palavra confidencial que identifica um usuário, a pergunta consiste no uso de alguma informação já conhecida do usuário, por exemplo para o acesso à aplicação o sistema pode perguntar *"quem é o seu avô"*. Uma das vantagens deste método é o uso de uma informação memorável, mas, pode envolver um diálogo longo. Outros métodos como a verificação das impressões digitais ou da assinatura oferecem outros níveis de segurança, mas a sua implementação pode ser muito onerosa.

3.4.1 Identificação do usuário ao nível do sistema operativo UNIX

UNIX é um sistema operativo multi utilizador, isto é, permite que diferentes utilizadores usem o mesmo computador ao mesmo tempo. Permite também controlar o acesso aos ficheiros, bases de dados e outros recursos do sistema. Neste controlo de acessos, UNIX usa "*accounts* " (uma área de trabalho reservada para um utilizador). Todo o usuário do sistema deve ter um account composto por duas partes: "*username* e *password*". Esta informação é armazenada no ficheiro /etc/passwd.

Como um mecanismo de segurança o administrador do sistema pode criar grupos de utilizadores, o que permite associar um grupo a cada utilizador recém criado.

O uso de grupos permite restringir o acesso a informações sensíveis especificando aqueles que têm permissão para executar certas operações tais como acesso a ficheiro, directorias.

4. Sistema de Gestão de Base de Dados (SGBD)

A partir dos anos 60 as organizações investiram em mecanismos que providenciam facilidades na organização e acesso aos dados. Estes mecanismos são conhecidos como Sistema de Gestão de Base de Dados (SGBD) e têm sido usados também para designar a organização dos dados e software necessário para a sua manipulação (Elbra, 1992). O propósito principal é manter a informação e fazer com que esteja disponível sempre que for precisa.

Base de Dados *é* um repositório para uma colecção de ficheiros de dados relacionados entre si, com a finalidade de servir múltiplas aplicações (Date 1990 , Elbra 1992).

O SGBD facilita o usuário na execução de várias operações incluindo as seguintes:

- Adicionar um novo ficheiro;
- Inserir um novo dado num ficheiro já existente;
- Aceder os dados de ficheiros existentes;
- Apagar os dados;
- Remover os ficheiros da base de dados;

4.1 Classificação dos SGBD

De todas questões tratadas em SGBD, a mais importante tem sido o mecanismo de representação da estrutura de uma base de dados. A evolução de base de dados nos últimos 30 anos consistiu no desenvolvimento de novas tecnologias para melhorar a representação da estrutura de informação.

4.1.1 Bases de dados hierárquicas

Nesta estrutura, os dados são guardados hierarquicamente, isto é um conjunto de registos de tipos diferentes estão relacionados entre si através de uma hierarquia do tipo Pai-Filho, podendo o registo pai ter vários registos filhos mas apenas um registo pai. Este modelo não

é suficiente para representar todas estruturas de informação possíveis dado que, muitas vezes, a informação não segue uma ordem hierárquica.

4.1.2 Bases de dados em rede

As bases de dados em rede resolvem os problemas acima mencionados ao permitir que se faça todas conexões possíveis entre os dados, podendo se representar todas estruturas.

Os dois modelos permitem a percepção dos dados pelos usuários, pois, reflectem o mundo real de informação; infelizmente, associam uma única estrutura aos dados, dificultando o acesso aos mesmos, usando uma estrutura diferente da pré-definida.
Tornam a programação e manutenção difíceis devendo fechar a base de dados para as modificações.

4.1.3 Bases de dados relacionais

A frustração criada pela rigidez dos SGBD hierárquico e em rede fizeram com que aparecesse outra abordagem, o SGBD relacional. Este sistema resolve o problema de rigidez, armazenando as associações do nível mais baixo na base de dados, confiando às aplicações a tarefa de reconstruir o nível mais alto dos dados. Nesta abordagem os ficheiros são tratados como tabelas bi-dimensionais consistindo de linhas e colunas, ou, por outras palavras, a tabela é chamada relação, as linhas túplas e as colunas atributos. Cada túpla é unicamente identificada por um atributo designado chave primária.

4.2 Vantagem do uso de um SGBD

Organizações que não usam SGBD têm uma heterogeneidade de aplicações usando cada uma seus dados privados podendo, um mesmo dado aparecer em diferentes ficheiros. Um SGBD fornece um controle centralizado dos dados (Woolf et al. 1987, Date 1990), ou seja, o acesso e actualização é controlado centralmente o que permite uma melhor segurança e integridade dos dados. No mesmo conceito de controlo centralizado, Date (1990) identifica

as seguintes vantagens: redução da redundância, diminuição da inconsistência, integridade, reforço de padrões, independência de dados e restrições de segurança .

A redundância de dados

É frequente noutros sistemas de base de dados (*nondatabase systems*) em que cada aplicação tem seus próprios ficheiros o que pode provocar o aparecimento dum dado em ficheiros diferentes, resultando numa má utilização de disco; por exemplo, uma aplicação de gestão de bolsas e outra que gere a informação académica de estudantes podem ter um ficheiro contendo endereço. Estes ficheiros podem ser integrados se a administração de dados estiver consciente dos requisitos das duas aplicações, não significando, porém, que a redundância pode ou deve ser completamente eliminada mas sim, deve ser cuidadosamente controlada se existir.

A inconsistência pode ser evitada

A redundância pode encaminhar a base de dados a um estado de inconsistência; por exemplo, numa dada aplicação de estudantes tem-se que a um aluno é concedido um beneficio B se obtiver uma classificação de 15 valores. Este facto é representado por duas entradas diferentes na base de dados. Se apenas uma entrada (B) altera, a base de dados entra num estado de inconsistência. Se um facto é representado por uma só entrada, a inconsistência nunca ocorre. Alternativamente, se a redundância não é removida mas é controlada, o SGBD pode garantir a consistência da base de dados assegurando que, qualquer mudança feita a qualquer das entradas é aplicada automaticamente noutra.

A integridade pode ser mantida

O problema de integridade é assegurar que o dado na base de dados está preciso. A inconsistência entre duas entradas que pressupõem representar o mesmo facto é um exemplo de falta de integridade. O controlo automatizado da base de dados pode ajudar na solução

deste problema pela execução de procedimentos de validação de dados no momento em que se fazem as operações de criação, remoção ou modificação.

Os padrões podem ser reforçados

Pretende-se que os formatos de dados sejam padronizados para facilitar a sua utilização entre diferentes utilizadores, podendo igualmente esta utilização ser para diferentes sistemas de informação.

Provisão de independência de dados

O SGBD permite uma imunidade das aplicações a mudanças na estrutura de armazenamento ou na estratégia de acesso - o que significa, naturalmente, que as aplicações não dependem de qualquer estrutura de armazenamento ou estratégia de acesso específica.

Restrições de segurança podem ser aplicadas

A administração de base de dados deve definir canais de acesso à base de dados de modo a garantir que as únicas vias de acesso à base de dados sejam através de canais adequados; definir ainda a execução de verificações de autorização sempre que for tentando o acesso a dados sensíveis e estabelecendo, para o efeito, diferentes verificações para cada tipo de acesso (leitura, modificação, remoção, etc.) e para cada parte de informação.

4.3 ORACLE como uma base de dados relacional

Na gestão de dados, a abordagem relacional difere da que se pode fazer numa abordagem hierárquica ou em rede- é possível, teoricamente medir o quanto um SGBD é relacional.

Uma gama de produtos que reclamam ser relacionais, estão disponíveis no mercado mas, de facto, têm pouco ou nada do proposto no modelo original de Codd e, de acordo com Date (citado por Rolland 1990), há três partes num modelo relacional: estrutura de dados, manipulação e integridade de dados.

Estrutura dos dados

Como foi dito acima (parágrafo 4.1.3), uma base de dados relacional usa ficheiros apresentados como tabelas bi-dimencionais constituídas por linhas e colunas. Uma importante propriedade nestas tabelas é que o valor encontrado na intersecção de qualquer linha e coluna *é* atómico, isto é, não pode ser decomposto. Este facto permite a definição de um conjunto de operadores para sistemas relacionais que satisfaz com todos os requisitos de recuperação dum SGBD.

O SGBD ORACLE satisfaz a definição relacional em termos de sua estrutura básica dos dados.

Manipulação dos dados

Para extrair dados do sistema, todo SGBD requer um conjunto de operações para a manipulação de dados. Para efectuar todas combinações possíveis de extracção de dados, um sistema relacional requer apenas oito tipos de operações, cinco das quais (*select, project union, minus* e *times*) são primitivas e outras três (*join, intersect e divide*) podem ser obtidas das anteriores.

Para um SGBD ser relacionalmente completo deve suportar as estruturas de dados anteriormente mencionadas e prover a funcionalidade completa das oito operações relacionais. Portanto, segundo esta definição o sistema ORACLE é relacionalmente completo.

Integridade dos dados

O SGBD ORACLE é relacionalmente completo, mas, não é completamente relacional. Para um produto ser completamente relacional deve ser relacionalmente completo, permitir ainda a definição de domínio e definição de integridade de entidade (*entity integrity*) e integridade referencial (*referential integrity*).

ORACLE tem domínios pré-definidos tais como *integer, number, character, real e date.* O usuário do sistema não tem facilidades para definir seus próprios domínios.

"Entity integrity" é baseada no uso da chave primária para identificar unicamente uma túpla. Esta chave pode ser composta por um ou mais atributos. *Entity integrity* requer que para qualquer atributo que participa numa chave primária duma relação, nenhuma túpla pode ter valor nulo para o mesmo atributo. Assegura que uma relação não tenha valores duplicados.

"Referential integrity" diz que numa relação, qualquer atributo ou conjunto destes que compõe a chave estrangeira, o valor associado a este atributo deve existir na relação em que o mesmo é chave primária.

4.4 Arquitectura da base de dados ORACLE

O usuário de uma base de dados relacional tem a percepção de que os dados estão armazenados numa série de tabelas. Estas tabelas constam de uma visão lógica do dado que é manuseado dos ficheiros físicos que são escritos e lidos do disco pelo sistema operativo.

Qualquer SGBD seja hierárquico, em rede ou relacional requer um software que sirva de *interface* para o mapeamento dos dados armazenados fisicamente, em visão lógica do utilizador.

O modelo ANSI/SPARC (Rolland, 1990) aborda o interface necessário em três níveis: externo, interno e conceptual (figura 3).

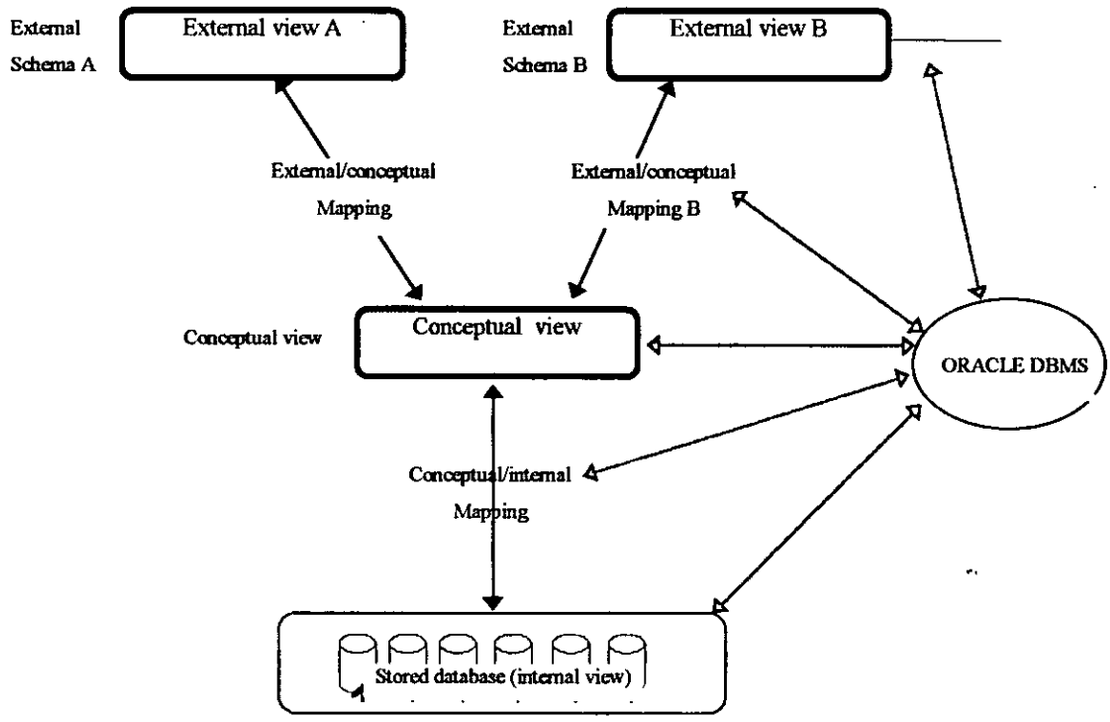


Figura 3: A arquitectura de ORACLE em 3 níveis.

O **nível externo é** o conjunto de visões (*views*) que os usuários da base de dados têm do sistema.

Consiste de estrutura lógica de ficheiros, direitos e permissões disponíveis para cada um.

O **nível interno** cria o *interface* entre a estrutura dos ficheiros peculiares da base de dados e a estrutura de ficheiros usados pelo sistema operativo do computador.

O **nível conceptual** representa o *interface* entre os níveis externo e interno. É uma representação lógica do conteúdo interno da informação contida na base de dados.

4.5 ORACLE e segurança de dados

Para a comunidade de usuários, uma base de dados ORACLE consiste de um conjunto de áreas de trabalho - esquemas - contendo cada uma um conjunto de objectos pertencentes a um usuário. Geralmente, este esquema ostenta o nome do usuário e está protegido por um *password*. A figura mostra um esquema com seus objectos.

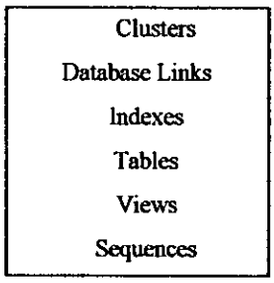


Figura 4: Objectos dum esquema

ORACLE SGBD é fornecido com algumas ferramentas (SQL*Plus, SQL*Forms, SQL*Report, SQL*Menu) que facilitam a interacção do usuário com os dados.

A habilidade de um usuário executar uma operação na base de dados ORACLE ou nos seus objectos é determinada pelos privilégios (direito de executar certas operações no sistema ou nos seus objectos) atribuídos ao seu esquema.

Um novo usuário da base de dados será criado cada vez que o seu administrador executa o comando CREATE USER cuja sintaxe é a seguinte:

CREATE USER {user}
IDENTIFIED BY{passw|EXTERNALLY}
[DEFAULT TABLESPACE tablespace]
[TEMPORARY TABLESPACE tablespace]
[PROFILE profile]
[QUOTA {n|UNLIMITED} ON tablespace]

Onde:

User	- Identifica o nome do novo usuário,
By passw	- Especifica o password do usuário
EXTERNALLY	- Permite a verificação a partir do sistema operativo
Default tablespace	- Para os usuários com privilégio *'CREATE'* os seus objectos serão criados em "*tablespace*"
Temporary tablespace	- espaço para o armazenamento temporário de instruções SQL do utilizador
Quota	- Espaço máximo de disco em cada *tablespace* por usuário
Profile	- É o perfil associado ao usuário

Depois da criação dum usuário, o administrador da base de dados começa a fornecer selectivamente autorizações de operações específicas a usuários específicos, usando uma instrução SQL especial denominada *GRANT* :

```
GRANT{privilégio_sys(,privilégio_sys...)}
ON object
TO {user[, user...]|role | PUBLIC}
[WITH ADMIN OPTION];
```

```
GRANT{privilégio_obj(,privilégio_obj...)|ALL}
[(columns)]
ON object
TO {user[, user...]|role | PUBLIC}
[WITH GRANT OPTION];
```

Onde:

Privilégio_sys,privilégio_obj	- é o privilégio a fornecer ao usuário *user*
ALL	- especifica a atribuição de todos os privilégios sobre os objectos.
Columns	- especifica as colunas sobre as quais se fornece privilégio
PUBLIC	- fornece os privilégios especificados em "privilégio" a todos usuários da base de dados
WITH GRANT OPTION	- permite a um usuário dar privilégios a outros.
WITH ADMIN OPTION	- permite ao usuário com esta opção fornecer privilégios de sistema a outros.

Os privilégios podem ser fornecidos ao nível do sistema ou ao nível dos objectos.

Ao nível do sistema, ORACLE define 3 tipos de privilégios:

- CONNECT
- RESOURCE e
- DBA.

Privilégio CONNECT

Um usuário só pode conectar à base de dados depois duma atribuição explícita do privilégio *CONNECT.*

Privilégio RESOURCE

O usuário com este privilégio pode criar suas tabelas e dar sobre elas certos privilégios a outros utilizadores.

Privilégio DBA

O DBA tem os mais altos privilégios, permite ao seu portador executar qualquer operação válida no sistema, inclusive, a de fornecer/revogar privilégios a outros utilizadores.

Ao nível dos objectos ORACLE define outros privilégios, alguns dos quais estão na tabela abaixo:

Tabela 1:

Objectos duma base de dados e privilégios sobre eles

	Objectos			
Privilégio	Table	View	Sequence	Procedure
Alter	✓		✓	
Delete	✓	✓	✓	
Execute				✓
Index	✓			
Insert	✓	✓†		
Select	✓	✓	✓	
Update	✓	✓†		
References	✓			

Nota

† De modo a permitir este privilégio, uma visão (View) deve ser actualizável, i.e., deve ser de uma única tabela, sem funções de grupo.

Um dos mecanismos de segurança usados no ORACLE é o conceito de visão. Uma visão pode ser vista como uma "janela" sobre os dados reais. Para além de permitir que os mesmos dados sejam vistos de maneiras diferentes por usuários diferentes, as views constituem um meio automático de segurança para dados que não podem ser revelados. A sua criação é feita por um comando SQL com o seguinte formato:

CREATE VIEW viewname

AS Select statement

Exemplo:

Sobre a tabela *"conce_equiv"* que guarda a informação sobre pedidos de concessão de equivalência na aplicação de gestão de alunos, pode-se criar várias visões para restringir o acesso aos seus utilizadores;

1) CREATE View Estado_concessão

AS Select aluno, confirmada

FROM conce_equiv

2) CREATE View ano_de_inscrição

AS Select aluno, ano_ins

FROM conce_equiv

GRANT Select ON nível TO Ldmi00

GRANT Select ON nível TO Lciencia

O utilizador "*Ldmi00*" pode executar operações select nos campos "aluno, confirmada" da tabela conce_equiv e o utilizador "Lciencia" nos campos aluno e ano_ins.

5. O Acesso Remoto a uma Aplicação

As redes de comunicação são essenciais ao desenvolvimento fazendo parte das instituições públicas e privadas, na medida em que permitem uma utilização racional dos recursos técnicos, partilha de informação e rapidez de comunicação a custos relativamente baixos.

Existem diversas formas de estabelecer a comunicação de dados, das quais pode-se destacar as seguintes:

- Comutação telefónica
- Comunicação via rádio;
- Ligação via LAN (s) e gateway (s);

5.1 Comutação telefónica

Consiste na utilização de um modem e linha telefónica para conectar dois pontos (figura 5). A ligação pode ser realizada de duas formas, "*dial-up* "e "*leased line* " (linha dedicada).

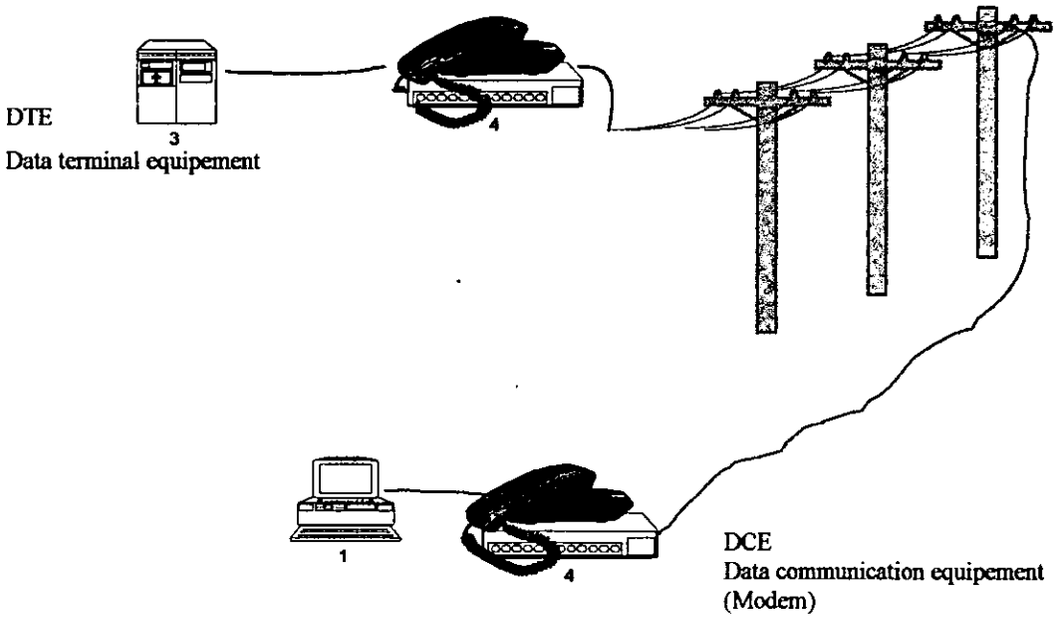


Figura 5: Ligação telefónica via modem

Em "*leased line*", uma linha dedicada estabelece uma ligação permanente entre os pontos enquanto que, na ligação "dial-up" a comunicação não é estabelecida permanentemente salvo nos casos em que um dos pontos solicita a conexão.

Um linha alugada tem a desvantagem de ser cara e não permitir a partilha de linha entre mais pontos, pois os extremos (nós) mantêm a interacção permanente. É útil para manusear grandes volumes de informação. O *dial-up* é um método prático para o transporte dum volume reduzido de informação e quando a transmissão da mesma não exige uma interacção contínua.

5.2 Comunicação via rádio

Consiste na ligação via rádio para o estabelecimento da comunicação. A transmissão de sinais é feita a partir de antenas colocadas em pontos altos, podendo ser também efectuada a partir de um sistema microondas - um sistema de transmissão direccional por ondas electromagnéticas do espectro de frequência de rádio (figura 6).

Este sistema será usado na rede de EMU*Net* (Eduardo Mondlane University Network) com a construção de um Rádio-Link de Microondas com uma transmissão de 140 Mbps (Plano de desenvolvimento da EMU*Net*, 1996).

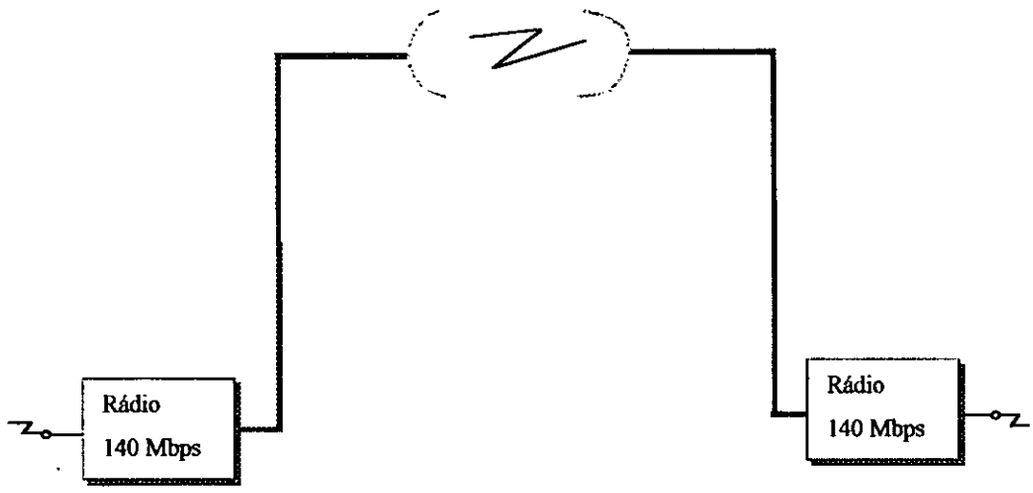


Figura 6: Rádio Link da EMUNET

5.3 Ligação via LAN (s) e gateway (s)

Consiste na utilização de uma linha telefónica dedicada entre o gateway e o servidor, partilhada pelos terminais (figura 7). Para à segurança de dados pode-se usar o "*firewall*" - um módulo que agrupa componentes de software e hardware responsável para a protecção e segurança dos dados. Implementa uma política de controle de acessos para agentes externos a uma rede local.

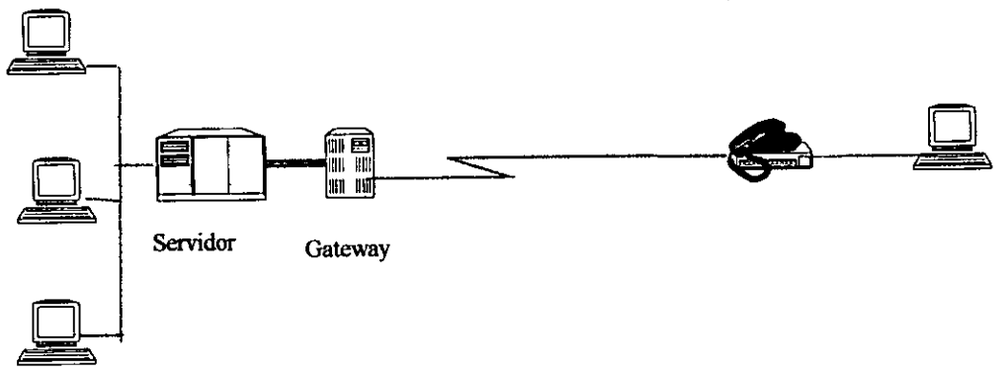


Figura 7: A ligação via linha alugado (leased line)

A **EMU***Net* (Eduardo Mondlane University Network) é um projecto de rede multimédia para a transferência de informação entre os diferentes sectores da UEM. Está particionada em pequenas redes locais (LAN).

Esta rede permitirá a implementação de sistemas de informação, como o ARIS, que apoiarão as actividades da instituição.

6. A Aplicação de Gestão de Alunos (AGA)

A Aplicação de Gestão de Alunos (AGA) é um banco de dados para a gestão de informação dos estudantes; é partilhada por vários utilizadores, uns conectados directamente ao sistema (utilizadores locais) e outros conectados a partir das faculdades (utilizadores remotos).

Os utilizadores locais repartem a responsabilidade de manutenção de informação do sistema ao nível dos diversos cursos, isto é, um determinado utilizador terá certos privilégios sobre alguns cursos de uma ou mais faculdades podendo inserir, alterar e remover os dados.

Os utilizadores remotos têm, neste momento, a permissão para a leitura (READ ONLY) dos dados; nos próximos anos, quando da descentralização das tarefas do Registo Académico Central, esta situação irá mudar.

6.1 Definição de perfis e privilégios na AGA

A aplicação define 2 perfis de acesso aos dados: chefe de secção de alunos (CSA) e funcionário (FUN).

O perfil "CSA" define um utilizador especial; aquele que não tem restrições de acesso aos dados; pode ainda definir ou alterar os privilégios dos outros utilizadores.

O "FUN" é o perfil que define uma restrição das operações a certos objectos de certos cursos. Por exemplo, ao nível do curso de Matemática e Informática, o utilizador "Ldmi00" pode lançar os resultados das frequências sem, no entanto, ter a permissão para alterar este dado.

A manutenção de informação do sistema envolve certas actividades representadas por operações críticas, sobre as quais se faz o registo das devidas autorizações. Algumas operações e as devidas permissões são apresentadas na tabela 2.

Tabela 2:

Operações sobre AGA contidas na tabela de controlo de privilégios

Campo da tabela (Operação)	**Descrição**
Autorizado	Permissão para aceder à aplicação
Data de entrada	Data de criação do novo utilizador
Candidaturas fora do prazo	Permissão para efectuar candidaturas fora do prazo
Lançamento de resultados	Permissão para fazer o lançamento de resultados
Alteração de resultados	Permissão para fazer a alteração de resultados em cadeiras
Inserir disciplina	Permissão para inserir disciplinas no currículo
Alterar disciplina	Permissão para alterar disciplinas no currículo
Retirar disciplina	Permissão para efectuar a remoção de disciplinas no currículo
Media_final	Permissão para calcular a média final
Confirmar equivalência	Permissão para confirmar a concessão de equivalência
Conclusão	Permissão para determinar o ano de conclusão
Cursos	Lista de cursos sobre a qual se define os privilégios

Para um dado funcionário aceder a estas e outras informações tem que ser, em primeiro lugar, utilizador da base de dados e possuir na sua área objectos da aplicação (tabelas, formulários, visões, etc.) e alguns privilégios sobre os mesmos.

Os privilégios sobre a aplicação são descritos numa tabela do sistema (tabela 2). Esta tabela fornece, informação ao próprio sistema, que permite validar todas as operações que o usuário tenta executar. Será assim possível controlar muito detalhadamente as tarefas de cada um na aplicação.

Definição de privilégios na aplicação AGA.

A titulo de exemplo examine-se a definição de privilégio de três utilizadores; dois locais (Lciencia e Ldmi00) e o terceiro remoto (rciencia) criados para acessos diferentes e a partir de locais distintos:

1) CREATE USER **Lciencia**
IDENTIFIED BY cienciaL
DEFAULT TABLESPACE dados
TEMPORARY TABLESPACE tmp
PROFILE default

Foi criado um utilizador local, cujo nome é ***Lciencia*** que vai manipular os dados de todos cursos da faculdade de ciências.

2) CREATE USER **Rciencia**
IDENTIFIED BY EXTERNALLY
DEFAULT TABLESPACE dados
TEMPORARY TABLESPACE tmp
PROFILE default

Rciencia é um utilizador remoto da base de dados. Oracle usará o password do sistema operativo para a autenticação

3) CREATE USER **Ldmi00**
IDENTIFIED BY dmi00L
DEFAULT TABLESPACE dados
TEMPORARY TABLESPACE tmp
PROFILE default

Ldmi00 é um usuário local com privilégios para único curso – Matemática e Informática

Atendendo à função do utilizador *Lciencia*, a sua tabela de privilégios deverá conter valores como se mostra na tabela 3.

Tabela 3

Valores típicos dos campos na definição de privilégios: O caso dum utilizador CSA

Campo da tabela (Operação)	**Valor**
Login	Lciencia
Nome	Utilizador reservado da faculdade de ciências
Perfil	CSA
Autorizado	Sim
Data de entrada	dd/mm/yy
Candidaturas fora do prazo	Sim
Lançamento de resultados	Sim
Alteração de resultados	Sim
Inserir disciplina	Sim
Alterar disciplina	Sim
Retirar disciplina	Sim
Media_final	Sim
Confirmar equivalência	Sim
Conclusão	Sim
Lista de cursos	Todos da faculdade de ciências

O utilizador "*Lciencia*" é um utilizador conectado ao sistema e com privilégios DBA sobre a base de dados, perfil CSA na aplicação.

O utilizador com a autorização para trabalhar apenas no curso de Matemática e Informática, por exemplo, terá a sua tabela de privilégios como se segue.

Tabela 4:

Valores típicos dos campos na definição de privilégios: O caso dum utilizador FUN, local.

Campo da tabela (Operação)	**Valor**
Login	Ldmi00
Perfil	FUN
Nome	Funcionário do Departamento de Matemática e Informática
Autorizado	Sim
Data de entrada	23/06/97
Candidaturas fora do prazo	Não
Lançamento de resultados	Sim
Alteração de resultados	Não
Inserir disciplina	Sim
Alterar disciplina	Sim
Retirar disciplina	Não
Media_final	Não
Confirmar equivalência	Não
Conclusão	Não
Lista de cursos	Curso de Matemática e Informática.

"*Ldmi00*" é um utilizador conectado directamente com acesso restrito a um único curso, Matemática e Informática. Como se vê, tem permissão para efectuar algumas operações.

Tabela 5:

Valores típicos dos campos na definição de privilégios: O caso dum utilizador FUN, remoto

Campo da tabela (Operação)	**Valor**
Login	Rciencias
Perfil	FUN
Nome	Funcionário remoto da faculdade de ciências
Autorizado	Sim
Data de entrada	23/06/97
Candidaturas fora do prazo	Não
Lançamento de resultados	Não
Alteração de resultados	Não
Inserir disciplina	Não
Alterar disciplina	Não
Retirar disciplina	Não
Media_final	Não
Confirmar equivalência	Não
Conclusão	Não
Lista de cursos	Todos da faculdade de ciências

"*Rciencia*" é um funcionário com acesso a todos cursos da faculdade de ciências mas apenas para a leitura.

Conclusão:

A tabela do sistema é um recurso muito importante na definição de níveis de acesso à aplicação:

- permite restringir o acesso a apenas operações singulares;
- permite delimitar a visualização de informação a nível do cursos;

- facilita a monitoração de operações realizadas por todo utilizador, por parte do gestor do sistema.

6.2. O acesso remoto à Aplicação de Gestão de Alunos

O servidor ORACLE da aplicação dos estudantes está instalado na Reitoria e os seus utilizadores remotos (as faculdades), estão geograficamente dispersos por 6 pólos (figura 8): Reitoria, Engenharias e Ciências, Direito, Medicina, Arquitectura, Campus (Ciências, Economia, Letras, Agronomia, UFICS).

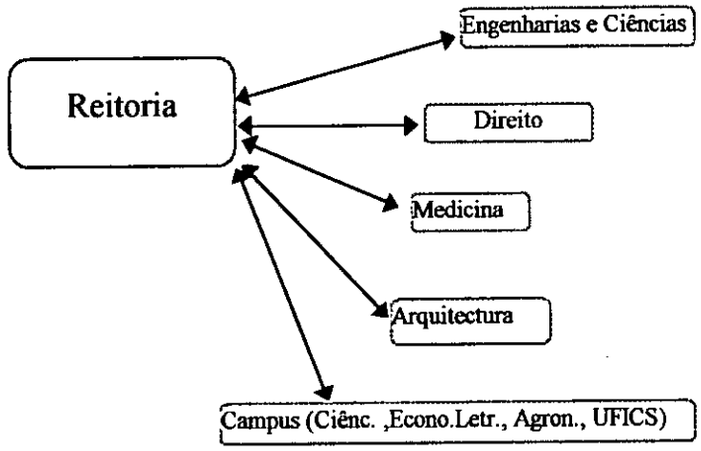


Figura 8. As faculdades e a Reitoria

A distância que separa estes utilizadores é de algumas dezenas de metros para uns, e de quilómetros para outros, o que torna necessária uma estrutura de comunicação que possibilite a transferência de dados com o sistema central.

A figura 9 mostra um esquema de ligação entre estes utilizadores. Note-se que, a transferência de dados entre a AGA e um utilizador remoto e vice-versa, pode ser feita através de um meio de comunicação de dados, podendo ser um dos descritos anteriormente.

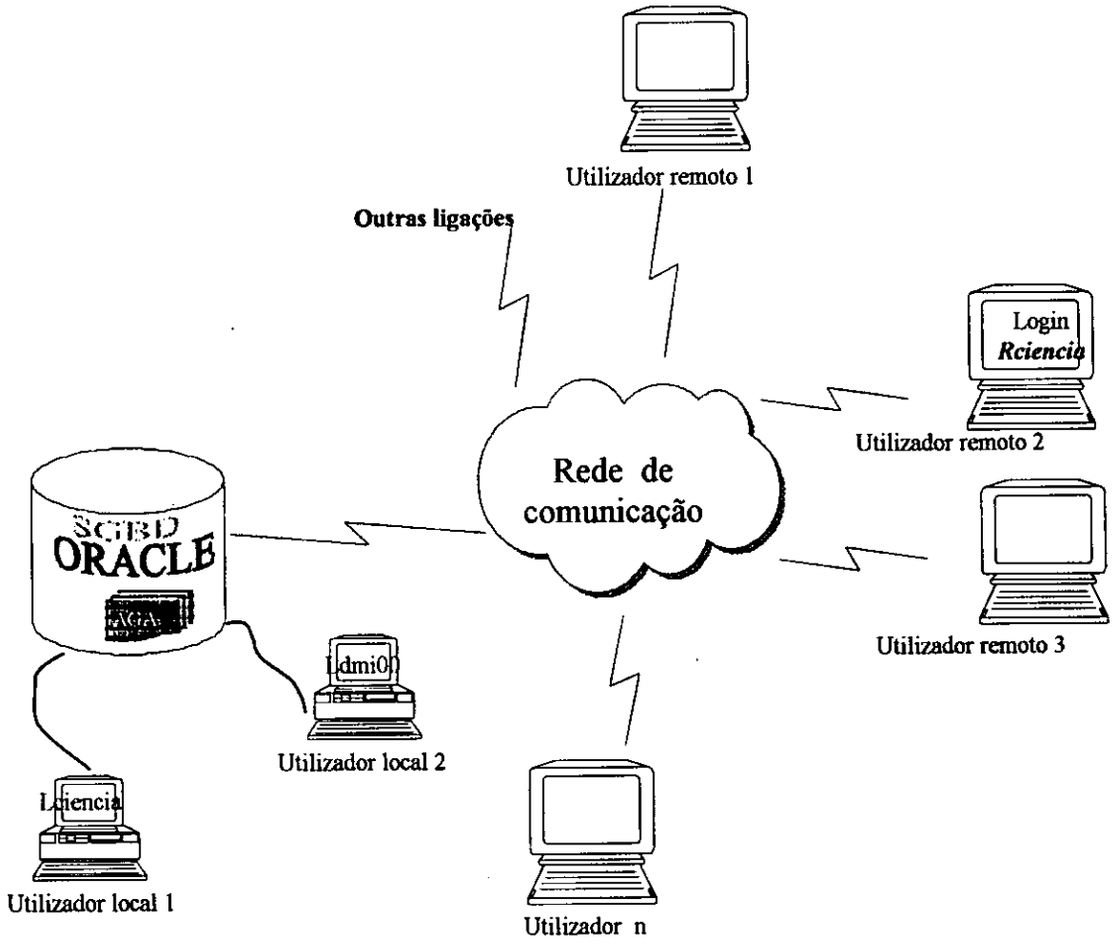


Figura 9: Esquema de ligação entre os utilizadores da AGA

7. Conclusões

Foi dito que a segurança de um sistema de informação não pode ser total; o importante é identificar os possíveis focos de ameaça e implantar um sistema de segurança composto por procedimentos que minimizem os possíveis danos que resultariam da ocorrência de uma dada ameaça.

O esquema de segurança para um dado sistema deve ser concebido nas fases iniciais do seu desenvolvimento.

ORACLE é um bom sistema de gestão de base de dados porque oferece mecanismos adequados de criação da base de dados bem como possibilita a partilha dos dados, controlo centralizado dos dados, eliminando as redundâncias possíveis, possibilitando, desta forma, que diferentes aplicações acedam os mesmos dados e os recebam organizados de acordo com as suas necessidades.

Todos os sistemas de informação da UEM deveriam estar assentes na EMUNET. Assim, até que esta rede esteja implantada recomenda-se o uso da comutação telefónica nas ligações remotas. Esta solução encontra sustentabilidade na disponibilidade de recursos necessários para este tipo de transferência.

Os principais procedimentos de segurança devem ser criados a nível da aplicação e sistema operativo, ou seja, independentemente dos meios de comunicação; a aplicação deve identificar correctamente os seus usuários e servir os seus objectos de acordo com os privilégios dum dado utilizador.

Relativamente à AGA os perfis definidos satisfazem as necessidades de segurança para a nossa instituição, pois permitem definir diferentes níveis de acesso aos dados.

Como recomendações, pode-se citar:

O acesso à sala do servidor, terminais assim como aos seus componentes seja restrito a pessoas autorizadas.

Deve-se definir, claramente, as tarefas de cada utilizador, sejam locais sejam remotos e que cada um saiba exactamente qual é a sua função na aplicação.

Perante o quadro anterior , o gestor da aplicação deverá definir o perfil e privilégios para cada utilizador; *passwords* para o acesso ao sistema operativo, base de dados ou aplicação, devem ser de tal forma que sejam difíceis de serem descobertos.

Os *passwords* devem ser mudados constantemente, pelo menos uma vez por mês. Atendendo à sensibilidade dos dados geridos, pela aplicação em causa, deve-se fazer, periodicamente uma auditoria, de forma a se detectar, a tempo, qualquer anomalia.

É necessário implementar-se uma verdadeira política de segurança, que tenha como principal factor a consciencialização e o treinamento do pessoal ligado ao sistema.

Finalmente, podia-se pensar já em termos de legislação para a protecção de dados, especialmente, os dados sensíveis como os tratados no sistema do Registo Académico ou no sistema de gestão de pessoal e salários. Na Europa e na América este tipo de dados, encontra-se protegido por lei.

Moçambique, um país em desenvolvimento, devia pensar neste tipo de legislação, que permitiria proteger as pessoas que têm seus dados em base de dados e que obrigaria os analistas e gestores a terem mais cuidado com segurança dos dados.

8. Bibliografia

1. Date, C.J., (1985). Banco de Dados. Editora Campos, Brazil, Campus

2. Date, C.J, (1990). An Introduction to Database Systems. Vol. I, 5ªEd. Addison-Wesley pub.

3. Elbra, T (1992). Database for the Small Computer User. England, The National Computing Centre Limited.

4. Madron, T.W., (1992). Network Security in the '90s Issues and Solutions for Managers, John Wiley & Sons.

5. CIUEM (1992). Plano de Informatização da DRA.

6. CIUEM (1996). Plano de desenvolvimeto da EMUNET.

7. Warman, A. R. (1993). Computer Security Within Organizations, Hong Kong, MacMillan.

8. Woolf, E., S. Tanna, K. Singh (1987). Systems Analysis and Design. G. Britain, Hutchinson.

Acrónimos

AGA- Aplicação de Gestão dos Alunos

ARIS - Academic Register Informatiom System

CSA- Chefe da Secção de Alunos

DBA- Administrador da Base de Dados

DRA - Direcção do Registo Académico

FUN- Funcionário

RA - Registo Académico

UEM - Universidade Eduardo Mondlane

UFICS – Unidade de Formação e Investigação em Ciências Sociais