UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO

INSTITUTO DE CIENCIAS SOCIAIS E APLICADAS

DEPARTAMENTO DE ADMINISTRAÇAO PUBLICA

TECNOLOGIA DA INFORMAÇÃO

Profª. Me. Raphaela Rangel
rangeladmrural@gmail.com

ASSUNTOS MAIS ABORDADOS NAS PROVAS ANTERIORES

- **Conceito de software (ciclo de vida software)**
- **SGBD (banco de dados)**
- **TICs e Comunicação Unificada**
- **ISO/IES 17799:2005 e Gestão da Segurança da Informação**
- **ERP ou SIG e Business Intelligence**
- **Governança e gestão de TI**

SOFTWARE

- Software é a parte lógica de um sistema computacional. Quando digo “sistema computacional”, refiro-me a todo equipamento capaz de processa informação.
- É como se os softwares fossem nossos pensamentos: você não consegue pegar o pensamento, mas você sabe que ele existe e que está dentro de você e, muitas vezes, é o que faz as coisas concretas acontecerem. Da mesma forma, o software existe, mas você não consegue pegá-lo; você sabe que ele está lá, mas é abstrato; e, muitas vezes, você vê criando coisas concretas, como uma impressão no papel ou um objeto impresso em impressora 3D, por exemplo.

SOFTWARE (CICLO DE VIDA)

- O Ciclo de Vida de um Software é uma estrutura que indica processos e atividades envolvidas no desenvolvimento, operação e manutenção de um software, abrangendo de fato toda a vida do sistema.
- Neste ciclo, existem modelos que definem como o software será desenvolvido, lançado, aprimorado e finalizado.

SOFTWARE (CICLO DE VIDA)

- Existem 3 fases básicas:

1) DEFINIÇÃO: Conhecer a situação atual e fazer a identificação do problema para buscar uma resolução do mesmo. É na definição que você fará a modelagem dos processos e a análise do sistema.

2) DESENVOLVIMENTO: Envolve as atividades relacionadas a design, prototipagem, codificação, testes, entre outras atividades que forem necessárias, como por exemplo, a integração com outro sistema.

3) OPERAÇÃO: Nesta etapa o software já estará em produção e você dará o devido suporte aos usuários e, claro, corrigir possíveis bugs que possam aparecer.

TIC'S

- Tecnologias de Informação e Comunicação. São as "tecnologias utilizadas para tratamento, organização e disseminação de informações" (TAKAHASHI: 2000, 176).
- "As Tecnologias da Informação e Comunicação correspondem a todas as tecnologias que interferem e medeiam os processos informacionais e comunicativos dos seres. Ainda, podem ser entendidas como um conjunto de recursos tecnológicos integrados entre si, que proporcionam, por meio das funções de *hardware*, *software* e telecomunicações, a automação e comunicação dos processos de negócios, da pesquisa científica e de ensino e aprendizagem."

COMUNICAÇÃO UNIFICADA

- A comunicação unificada é uma nova arquitetura tecnológica na qual as ferramentas de comunicação são integradas para que tanto empresas quanto indivíduos possam gerenciar todas as suas comunicações em uma única interface em vez de separadamente.
- Tudo que está a serviço da comunicação pode ser integrado, como por exemplo:

- Serviços de mensagem unificadas e multimídia;
- Comunicação em tempo real;
- Serviços de dados
- Transações.

COMUNICAÇÃO UNIFICADA

- **Como podem ser úteis? (Exemplos)**
- Os funcionários que dependem da mobilidade em conexão podem permanecer conectadas com seus smartphones ou telefones IP sem fio mesmo quando estão fora do escritório ou em casa;
- As empresas podem reduzir consideravelmente os custos incorridos para acomodar os trabalhadores em escritórios, permitindo que eles trabalhem de casa. Além disso, o recurso humano de outras localidades pode ser aproveitado sem aumento de custo e sem os atrasos normais devido à distância geográfica;
- A TI não precisará monitorar sistemas múltiplos de comunicação, realizando apenas o gerenciamento de uma interface, o que permite aumentar a produtividade;
- As chamadas via Web e videoconferência permitirão melhor interatividade e produtividade reduzindo, assim, o custo de viagens e telecomunicações;
- A empresa terá menos registros e contas para se preocupar, já que poderá ter todos os seus serviços de um único provedor e um único contato para cada um de seus funcionários.

BANCOS DE DADOS

- Coleção de dados relacionados;
- É um conjunto de dados integrados que tem o intuito de atender uma comunidade de usuários;
- Fatos conhecidos que podem ser registrados e possuem significado implícito;
- Coleção lógica e coerente de dados;
- Representam algum aspecto do “mundo real”;
- Construído para uma finalidade específica;
- Manual ou informatizado;
- Complexidade variável e qualquer tamanho.

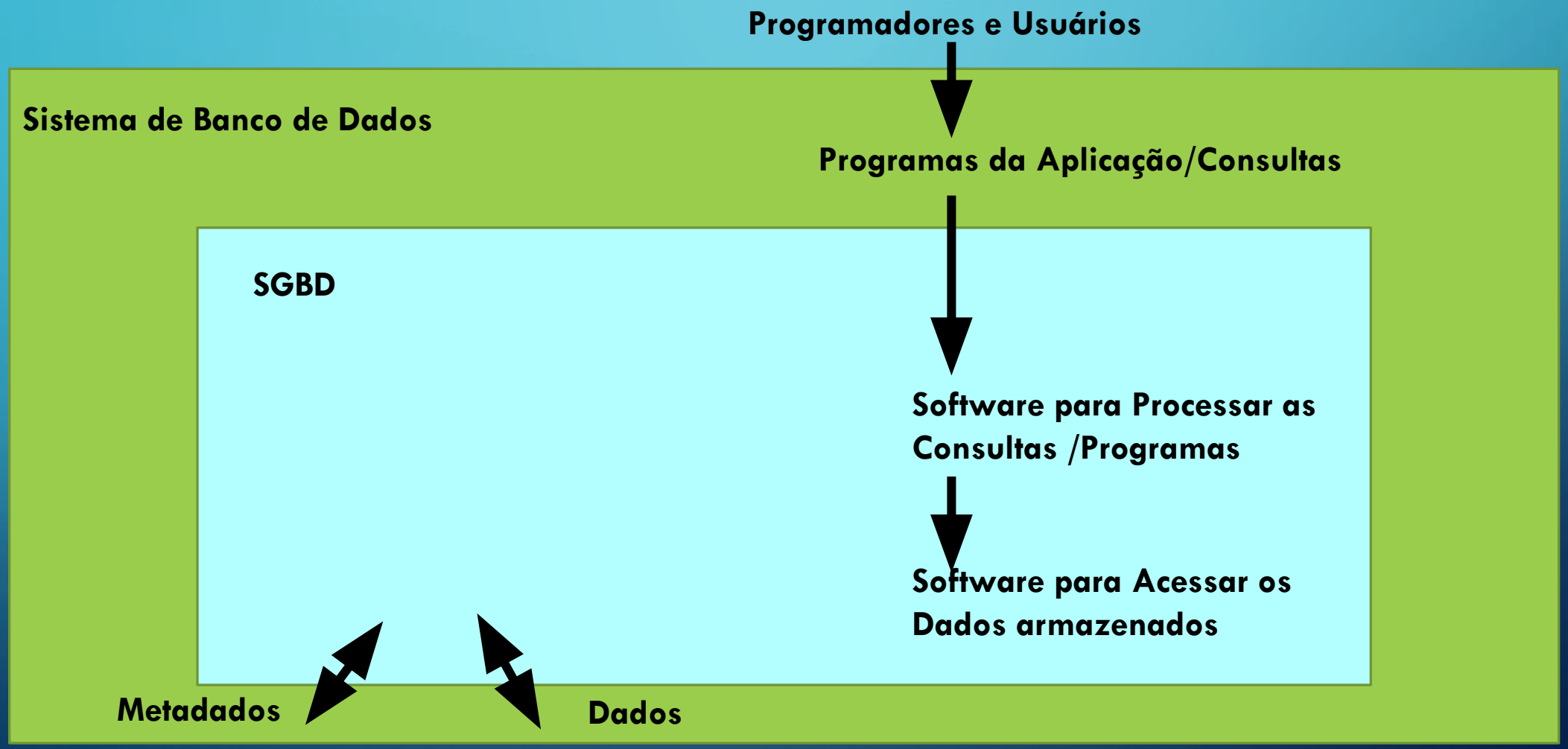
SGBD – SISTEMA DE GERENCIAMENTO DE BANCO DE DADOS

- Ou DBMS (DataBse Management Systems);
- Coleção de programas
- Permitem aos usuários criar e manter um banco de dados;
- Software de propósito geral que possibilita a DEFINIÇÃO, CONSTRUÇÃO E MANIPULAÇÃO de banco de dados;
- É dependente de Tecnologia;
- Incorpora as funções de definição, recuperação e alteração de dados em um banco de dados;

SGBD – SISTEMA DE GERENCIAMENTO DE BANCO DE DADOS

- Definir um BD envolve os tipos de dados, as estruturas e as restrições para os dados que serão armazenados;
- Construir o BD é o processo de armazenar os referidos dados em algum meio de armazenamento que seja controlado por um SGBD;
- Manipular o BD inclui funções recuperação e atualização de dados;

AMBIENTE DE SISTEMAS DE BANCO DE DADOS



CARACTERÍSTICAS DE TECNOLOGIA SGBD

- **Múltiplas visões:** Cada usuário pode acessar a diferentes visões do banco de dados, as quais descrevem somente os dados de interesse do usuário;
- **Controle de Redundância:** No SGBD, cada item lógico do dado é armazenado num único lugar. Pode haver redundância controlada, para ganhos de performance.
- **Controle de Concorrência:** O SGBD deve incluir um software de controle de concorrência para garantir consistência das informações contidas no BD do acesso quando do acesso dos usuários.

CARACTERÍSTICAS DE TECNOLOGIA SGBD

- **Segurança:** Restrição de acesso não autorizado dos dados. O SGBD prover mecanismos de autenticação de usuários;
- **Backup e Recovery**: Possibilidade de cópia de segurança e recuperação de falhas de hardware e software;
- **Múltiplas interfaces para diferentes tipos de usuários:** Linha de comando.
- **Manutenção de Restrições de Integridade no Banco de Dados:** Capacidade de definir e impor restrições;

SEGURANÇA EM BANCO DE DADOS

- O SGBD fornece técnicas que possibilitem que certos usuários ou grupos de usuários acessem apenas partes selecionadas de um banco de dados, sem obter ao restante do banco de dados.
- O SGBD inclui subsistema de autorização e segurança de banco de dados, que é responsável por garantir a segurança de partes de um banco de dados, criando mecanismos de segurança.
- Mecanismos de segurança em banco de dados são aplicáveis contra diversos tipos de ameaças.
- A criação de esquemas para prover privilégios de acesso a usuários autorizados, de modo a fornecer e revogar privilégios.

SEGURANÇA EM BANCO DE DADOS

- SIGILO: usuários não devem acessar dados aos quais não possuem permissão. Exemplo: Um correntista acessar os dados da conta bancária de outro correntista.
- INTEGRIDADE: Usuários não devem modificar dados sem permissão. Exemplo: Somente o professor pode alterar a nota da prova do aluno.
- DISPONIBILIDADE: O dado deve estar disponível sempre que preciso. Exemplo: O Banco de Dados precisa estar disponível quando determinado usuário devidamente autorizado necessitar realizar uma operação.

MEDIDAS DE SEGURANÇA EM BANCO DE DADOS

- Define uma política de segurança que especifica quais são os usuários que possuem autorização e acesso ao BD, e com que finalidade.
- Existem dois mecanismos de segurança no nível do SGBD:

 Discricionário: Usados para conceder privilégios aos usuários, como os modos de acesso a arquivos ou registros de dados (leitura, inserção, exclusão ou atualização);

 Obrigatório: Usados para impor segurança de acordo com o nível no qual determinados dados e usuários foram classificados.

NORMA ISSO/IEC 17799:2005

- Trata da Gestão da Segurança da Informação
- Agora, substituída pela ISSO/IEC 27002.
- Segurança da informação é a proteção da informação de vários tipos de ameaças para **garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio.**
- **É obtida através da implementação de um conjunto de controles adequados: políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware.** ataques de denial of service

SEGURANÇA DA INFORMAÇÃO

- Quais são **as ameaças** à Segurança da Informação?
- Fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação (acidentes naturais) – ameaças externas
- Danos causados por códigos maliciosos (malwares), hackers e ataques de denial of servisse (DoS) (Ataques de navegação de serviço) – ameaças internas
- **Principais ameaças** (exemplos mais cobrados): erro humano, funcionário insatisfeito, **engenharia social, ferramentas de software (cavalo de troia).**

SEGURANÇA DA INFORMAÇÃO – RISCOS + COBRADOS

Worms (vermes): parecidos com vírus, mas que são capazes de se programarem automaticamente através de redes, enviando cópias de si mesmo.

Bots (robôs): programa capaz de propagar automaticamente, explorando vulnerabilidades ou falhas existentes na configuração de um software instalado.

Trojan Horse (Cavalo de Troia): Aparentemente um programa inofensivo (exemplo uma apresentação, foto) e que quando executado abre as portas de comunicação do seu computador para ser invadido.

Trackware: rastreiam a atividade do sistema e reúnem informações do sistema ou hábitos do usuário.

PRINCIPAIS GOLPES - INTERNET

PHISHING: Tipo de fraude projetada para roubar informações particulares que sejam valiosas.

SPEAR PHISHING: Golpe de e-mail direcionado com o objetivo único de obter acesso não autorizado aos dados sigilosos (diferente do PHISHING, foca em um grupo ou organização específica).

PHARMING: técnica que utiliza o sequestro de um servidor para levar o usuário a um site falso, alterando DNS do site de destino.

ENGENHARIA SOCIAL: destinada a induzir os usuários a enviar dados confidenciais, infectar seus computadores ou abrir links infectados.

SIG OU ERP

- SIG (Sistema Integrado de Gestão) ou ERP (Enterprise Resource Planning)
- É um sistema de informação com módulos integrados que dão suporte a diversas áreas operacionais, tais como vendas/marketing;
- Os sistemas integrados podem reunir todos os principais processos de uma organização em um único software que permite que a informação flua sem descontinuidade.
- Sem um ERP implantado, a informação é processada individualmente em cada área da organização, **gerando assim retrabalho, erros, alto custo, redução de lucros e perda de produtividade.**

BUSINESS INTELLIGENCE

- Sistemas e processos integrados para transformar os dados coletados em grandes quantidades em informações mais fáceis de ler pelo nível estratégico da empresa, gerando mais praticidade no estabelecimento de planos de negócios para a instituição.

GOVERNANÇA CORPORATIVA

- É o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo as práticas e os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle. As boas práticas de Governança Corporativa convertem princípios em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor da organização, facilitando seu acesso ao capital e contribuindo para a sua longevidade.
- (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2010).

GOVERNANÇA CORPORATIVA - PRINCÍPIOS

- TRANSPARÊNCIA: mais do que obrigação, é desejo de informar para gerar um clima de confiança interna e externamente à organização.
- EQUIDADE: não só entre sócios de capital, mas também com todas as partes interessadas.
- PRESTAÇÃO DE CONTAS: quem recebe um mandato tem o dever de prestar contas de seus atos.
- RESPONSABILIDADE CORPORATIVA: visão de longo prazo, considerações de ordem social e ambiental.

GOVERNANÇA CORPORATIVA X GESTÃO DE TI

- A Governança de TI funciona como um mecanismo que visa à proteção da empresa. Ela estabelece políticas que indicam e fiscalizam as regras estabelecidas para setor de tecnologia da informação.
- Já a Gestão de TI está relacionada à rotina da TI na organização. Seu objetivo é entregar os melhores serviços e elevar o desempenho do negócio. O papel da gestão de TI inclui o estabelecimento e manutenção dos processos para que o ciclo de funcionamento permaneça bem.

PRINCIPAIS FRAMEWORKS PARA GESTÃO DE TI

Os frameworks (um guia de boas práticas) precisam ser estudados e aplicados conforme as necessidades da equipe de TI.

Vamos conhecer os principais frameworks para gestão de TI:

- ITIL
- COBIT
- MOF
- SCRUM
- PMBOK

ITIL

ITIL é a sigla para *Information Technology Infrastructure Library*, um *framework* amplamente conhecido e utilizado por cerca de 180 países.

O ITIL **é organizado em cinco livros para auxiliar a equipe de TI quanto às boas práticas referentes aos projetos**. Os livros são classificados e direcionados a:

- Estratégia;
- Transição;
- Desenho;
- Operação;
- Melhoria contínua.

O ITIL tem destaque por ser uma das certificações mais importantes, uma vez que é focado no planejamento e na execução dos projetos de TI.

COBIT

- O foco do COBIT (*Control Objectives for Information and Related Technologies*) é a**uxiliar nos processos de governança e gestão de TI**, ainda que seja mais voltado à governança.
- *É importante destacar a principal diferença em relação ao ITIL:enquanto este busca ajudar a equipe durante o planejamento e execução dos serviços, o COBIT é mais voltado para a gestão dos processos, papel da governança.*
- Por isso, é interessante que ambos os *frameworks* trabalhem de forma conjunta.
- Os princípios do COBIT são:
- Ser um *framework* integrado;
- Fazer uma distinção clara entre governança e gestão;
- Abordagem holística;
- Visão da empresa como um todo;
- Atender às demandas dos colaboradores

MOF

- O MOF, sigla correspondente à *Microsoft Operations Framework*, é centralizado nos **princípios, práticas e atividades que asseguram a confiabilidade dos serviços e soluções de TI**.
- A base do MOF é um formulário com perguntas direcionadas ao que é necessário para o presente — o atual momento da empresa.
- Também é válido destacar que esse *framework* fornece comandos necessários para todas as etapas necessárias para o suporte dos serviços de TI: a criação, a organização e a operação.
- O grande objetivo do MOF é fornecer um ambiente proativo capaz de aumentar a eficiência entre os colaboradores da TI.

SCRUM

- O SCRUM é um *framework* aplicado ao **rápido desenvolvimento** da gestão de TI.
- A principal característica do SCRUM é que ele surgiu como uma forma de as equipes evitarem o excesso de documentação e burocracia nos projetos web.
- A necessidade excessiva de documentar os processos pode resultar em perda de tempo no andamento das atividades do setor.
- Esse *framework* também apresenta vantagens como a flexibilidade a mudanças durante as etapas de execução de um projeto, além de constantes *feedbacks* internos.
- O SCRUM também é caracterizado por reuniões regulares da equipe para a discussão dos *sprints* — pequenas partes de um projeto maior.
- Assim, o SCRUM objetiva conferir maior agilidade sem comprometer o resultado final do projeto.

PMBOK

PMBOK significa *Project Management Body of Knowledge* e integra o PMI (*Project Managment Institute*).

- Esse *framework* **contempla dez áreas de conhecimento, que são úteis para a administração das etapas de um projeto.**
- O PMBOK, ao contrário do SCRUM, é caracterizado pelo **excesso de documentação** e planejamento, o que, para alguns profissionais de TI, é uma barreira.
- A grosso modo, no entendimento da maioria dos profissionais de TI, os projetos devem prezar pela agilidade e ação, retirando o foco de aspectos mais burocráticos como a documentação. Ainda assim, vale a pena dizer que é o PMBOK que se responsabiliza pela **padronização do ciclo de vida dos projetos e por tornar a comunicação mais eficiente, melhorando o controle e a visualização das atividades.**
- O PMBOK é composto por cinco processos, que são:
- Iniciação;
- Planejamento;
- Execução;
- Monitoramento;
- Controle e encerramento.