



ESTRATÉGIA DE INTEGRAÇÃO, INFORMAÇÕES E TECNOLOGIA NA ADMINISTRAÇÃO DOS RISCOS

Francisco Camargo
CLM Software
&
Celso H. Leite
BINDERS Business Integration

www.clm.com.br/risco

INTEGRAÇÃO DE ESTRATÉGIA, INFORMAÇÕES E TECNOLOGIA NA ADMINISTRAÇÃO DOS RISCOS

AD
PO



- RISCO OPERACIONAL
- DESAFIOS
- REDUZINDO O RISCO OPERACIONAL
- SISTEMA MONITOR
- INTEGRAÇÃO NO AMBIENTE DE NEGÓCIOS
- INTEGRAÇÃO VIABILIZANDO O R.O.I.
- PLATAFORMA DE INTEGRAÇÃO
- PLANEJAMENTO DA INTEGRAÇÃO



Risco Operacional



- Comitê de Basileia – 2001:
 - “É o risco de perdas diretas ou indiretas, resultante de uma inadequação ou uma falha atribuível aos processos internos, pessoas, sistemas informáticos ou eventos externos”.





- O RISCO OPERACIONAL:

- Permeia todas as atividades humanas.
- É originado em erros e enganos, intencionais ou não, cometidos pelos diversos agentes dos processos.
- É aleatório, tanto quanto à incidência, quanto à perda.

- ABRANGÊNCIA

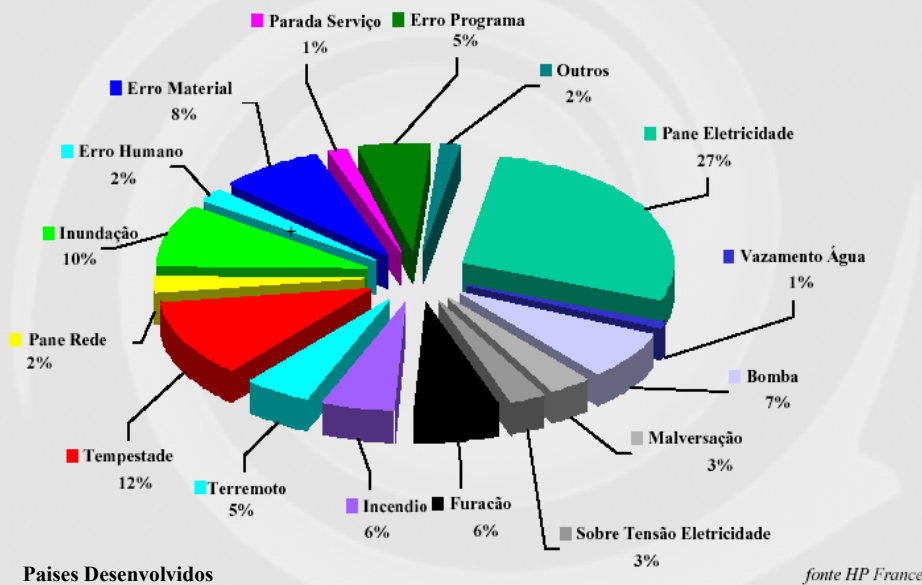
- O Risco Operacional vai muito além do Risco das Operações, sendo disperso geográfica e funcionalmente.

- O Risco Operacional pode provocar perdas econômicas e não econômicas a uma instituição, devido a:

- ✓ Fraudes internas e externas
- ✓ Erros humanos
- ✓ Falhas nos sistemas (Hardware e Software)
- ✓ Deficiência nos procedimentos e controles.



Principais causas de sinistros



Desafios



• RISCO OPERACIONAL

- O BIS (*Bank for International Settlements*), após ter estabelecido os critérios para a MENSURAÇÃO dos Riscos de Crédito e de Mercado, passou a estudar o Risco Operacional e os meios para a sua medição.
- Este é um grande desafio, pois o tipo e a incidência desse tipo de Risco são únicos para cada Banco:
 - ✓ Cada banco atende a um tipo de mercado
 - ✓ Está organizado de maneira única, em termos administrativos e de tecnologia
 - ✓ Tem maneiras próprias de efetuar os Controles Internos

• PRESERVAÇÃO DE HISTÓRICO

- Por ser único, em termos de Risco Operacional, cada Banco deve ter um histórico particular dos erros cometidos e das conseqüências financeiras e reputacionais desses erros, para propiciar a adoção das medidas corretas.
- Preservação do histórico é medida essencial, para suporte à quantificação e monitoração do Risco Operacional.

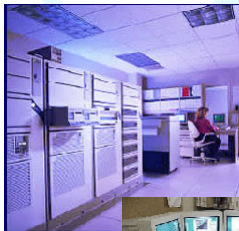


• OUTROS DESAFIOS

- Estabelecer PADRÕES para o gerenciamento dos riscos em toda a Instituição.
- Disponibilizar dados em TEMPO REAL, para possibilitar análise contínua, alinhada com a dinâmica do mercado e das operações do Banco.
- Identificar “GAPS” de dados, para garantir que as informações necessárias aos cálculos dos Riscos estejam disponíveis.
- Construir uma infra-estrutura AUDITÁVEL, para permitir que, a qualquer momento, seja analisada a origem dos dados de riscos e suas implicações, para possibilitar a tomada de medidas de correção.

- Os critérios de Basiléia II mostram como MEDIR e ALOCAR capital, em função do Risco Operacional.
- O que eles não ensinam é como REDUZIR esse tipo de Risco.
- É verdade que o que não se consegue medir, não se consegue controlar.

Basiléia II é apenas o primeiro passo.



A maior parte dos Bancos tem dois tipos de processos:

- Os “*mainstreams*”, isto é, processos diários, relativos à operação principal do Banco e geralmente tratados em SISTEMAS DE GRANDE PORTE;
- As operações “especiais”, cujo ciclo não é diário, são tratadas por FERRAMENTAS INFORMÁTICAS DE “APOIO”.

Reduzindo o Risco Operacional



- Eventuais erros ocorridos no “*mainstream*” afetam milhares de clientes e transações; historicamente, esses erros são raros, pois os sistemas foram concebidos e construídos de forma a reduzi-los.
- A exceção são os erros intencionais, isto é, as FRAUDES.

Reduzindo o Risco Operacional



- Nas “operações especiais”, a situação é outra, por ser muito mais dependente de processos “humanos”.
- A experiência prova que, nessa área, é muito maior a probabilidade de ocorrência e que o dano pode ser muito maior.

Onde está o verdadeiro RISCO?



Exemplo: Perdas em conflito do Exército americano

	<i>II Guerra 1942-45</i>	<i>Coréia 1950-53</i>	<i>Vietnam 1965-72</i>	<i>Iraque 1990-91</i>
<i>Acidentes</i>	56% 1.007.704	44% 77.108	54% 270.608	75% 1.406
<i>Fogo Amigo</i>	1% 15.839	1% 1.943	1% 4.678	5% 86
<i>Ação Inimiga</i>	43% 776.105	55% 97.198	45% 229.239	20% 366



15

Sistema Monitor para a Redução do Risco Operacional



- O que se propõe é a criação de um sistema do tipo IDS (Detecção de Intrusos) ou Firewall.
- Esses sistemas de Monitoração e Análise ficam, em tempo real, analisando cada pacote que passa pela rede, tentando identificar se é um evento de ataque ou não.
- Cada pacote é interpretado contra um conjunto de regras, disponíveis no sistema, que evoluem no tempo, em função do conhecimento adquirido quanto a novas ameaças ou vulnerabilidades.



16

Sistema Monitor para a Redução do Risco Operacional



- A exemplo de um IDS, um Sistema Monitor analisaria em Tempo Real e/ou Diferido a totalidade das transações do Banco.
- Cada transação seria analisada, no contexto, contra as regras existentes no Monitor, detetando a ocorrência de certos eventos relacionados com:
 - ✓ Fraudes
 - ✓ Erros e Falhas
 - ✓ Lavagem de Dinheiro
 - ✓ Atrasos e irregularidades
 - ✓ Oportunidades de negócio



17

Sistema Monitor para a Redução do Risco Operacional



- O Sistema Monitor poderia, segundo cada caso:

- | | |
|--|--|
| • Evitar sua ocorrência: | Sistema de defesa
Sistema de Autorizações |
| • Informar e dar alarme oportunamente: | Sistema de Alarmes |
| • Diminuir as perdas: | Workflow |
| • Tomar as ações correspondentes: | Workflow |
| • Armazenar os dados: | Data warehouse |



18

Sistema Monitor para a Redução do Risco Operacional



- O Monitor seria construído ao redor de três núcleos: uma plataforma de integração, um DataWarehouse (DW) e uma Central de Comunicações.
- Cada transação (evento) seria analisada e armazenada por um certo tempo no DW.
- Seria analisada contra o histórico do cliente e contra o histórico do funcionário do banco que a realizou ou aprovou, à procura de padrões de comportamento que traduzam a possibilidade de erro ou fraude.



19

Sistema Monitor para a Redução do Risco Operacional



- As transações, objeto de suspeita, seriam assinaladas para quem de direito, através da Central de Comunicações.
- Seriam objeto de uma INVESTIGAÇÃO a posteriori, que seria armazenada no DataWarehouse, ocasionando ou não mudanças de Regras.

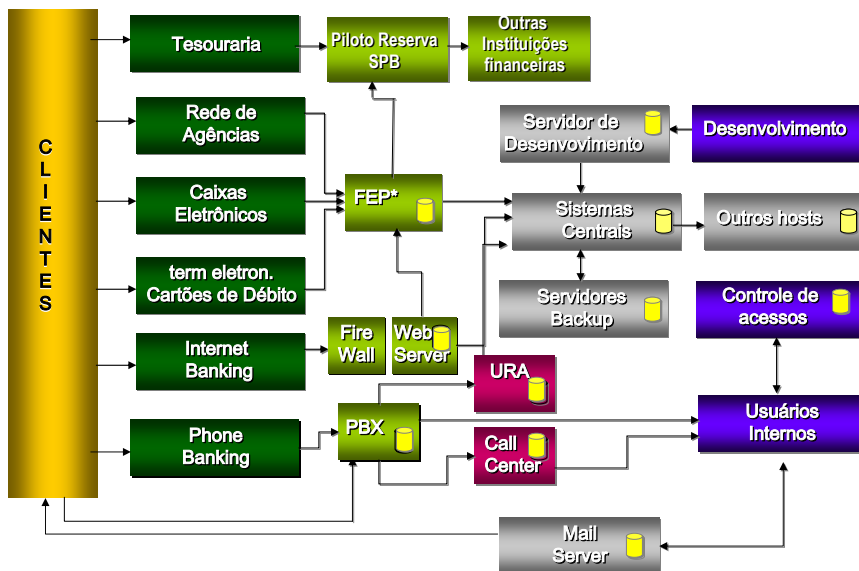


20

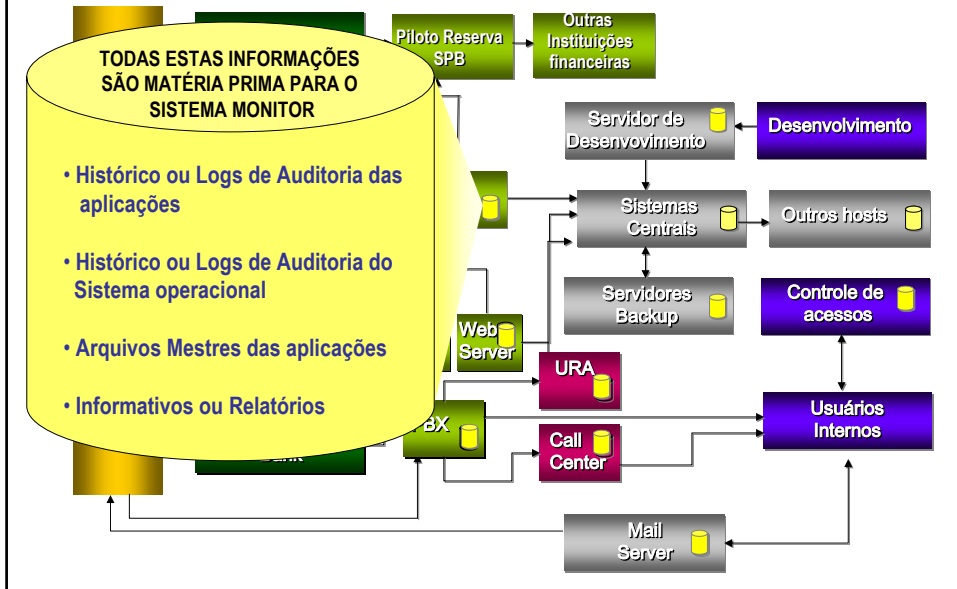
Ciclo do Sistema Monitor



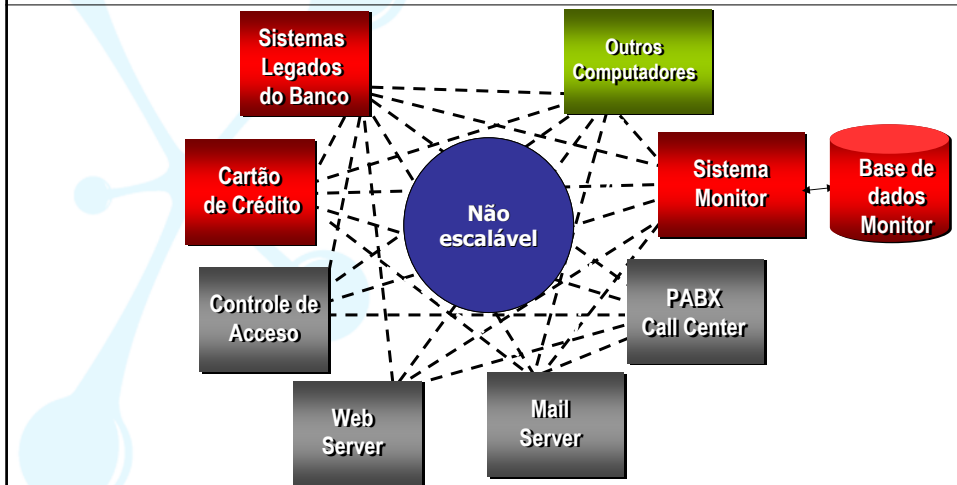
Esquema Típico de Sistemas



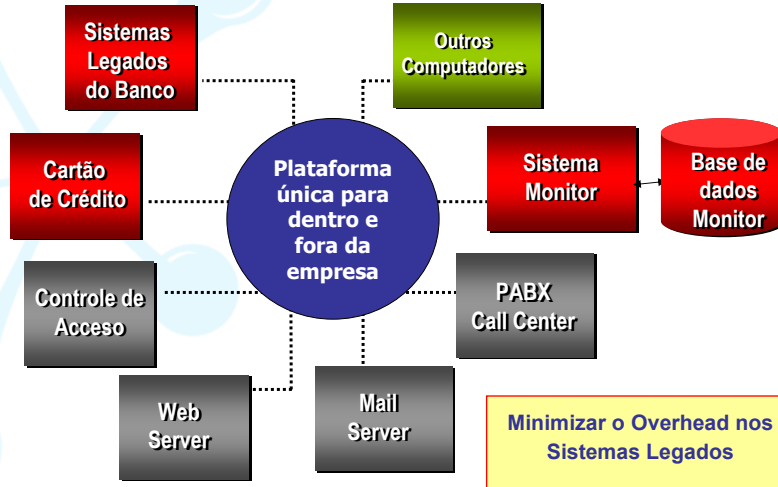
Esquema Típico de Sistemas



Integração / Sistema Monitor



Integração / Sistema Monitor



25

Integração no Ambiente de Negócios



26



Organizações no mundo todo dependem, em média, de 50 aplicações corporativas para conduzir seus negócios, sendo que cerca de 33% dos orçamentos para TI são gastos com a integração dessas aplicações

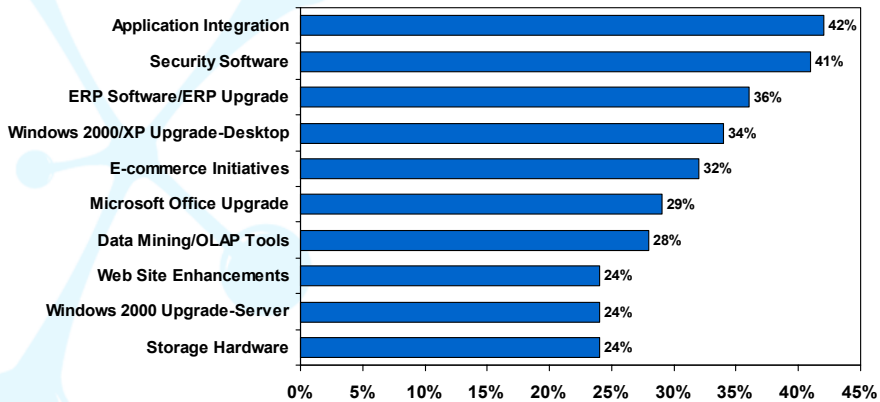
- META Group

- Os CIOs precisam gerenciar as demandas contrárias de baixar os custos, aumentar a segurança, melhorar o gerenciamento do risco e acelerar a inovação.

Desafio: calibrar as expectativas da empresa com o orçamento reduzido



Integração no Ambiente de Negócios



Fonte: Morgan Stanley CIO Survey, Agosto 2002



29

Integração Viabilizando ROI



Redução de Despesas

Redução de Custos Operacionais
Front Office
Back Office
Redução do custo total de TI
Redução da complexidade de TI
Redução do Índice de Perdas
Melhorias nos Processos de Gestão

Aumento de Receitas



Fidelidade de Clientes
Crescimento da Carteira de Clientes
Elevação da Receita por Cliente
Crescimento do Market Share

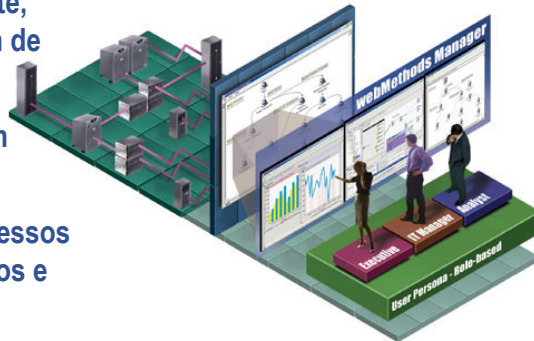
Ganhos nos Resultados



30

• Visualização Global do Negócio

- Visão global de cada cliente, fornecedor, projeto, ordem de compra, ativo, etc.
- Acesso às informações em Tempo Real
- Controle de todos os processos de negócio, sistemas, dados e informações



Plataforma de Integração

DIAGNÓSTICO

- Provê uma única fonte de dados sobre as atividades do negócio
- Possibilita a otimização de processos-chave

GERENCIAMENTO

- Cria um ponto central de gerenciamento
- Propicia ações corretivas e preventivas



IDENTIFICAÇÃO

- Identifica os componentes de integração
- Apresenta-os para a gerência

MONITORAÇÃO

- Status em tempo real
- Alertas

Plataforma de Integração



Uma plataforma de integração permite que as empresas atendam a todas as suas necessidades de integração com uma só infraestrutura escalável, permitindo que fluxos de trabalho colaborativo sejam automatizados.

Esta plataforma deve aproveitar os padrões abertos do mercado, para integrar fontes de informação dispersas e conectar clientes e fornecedores, provendo:

- Integridade transacional
- Segurança
- Confiabilidade



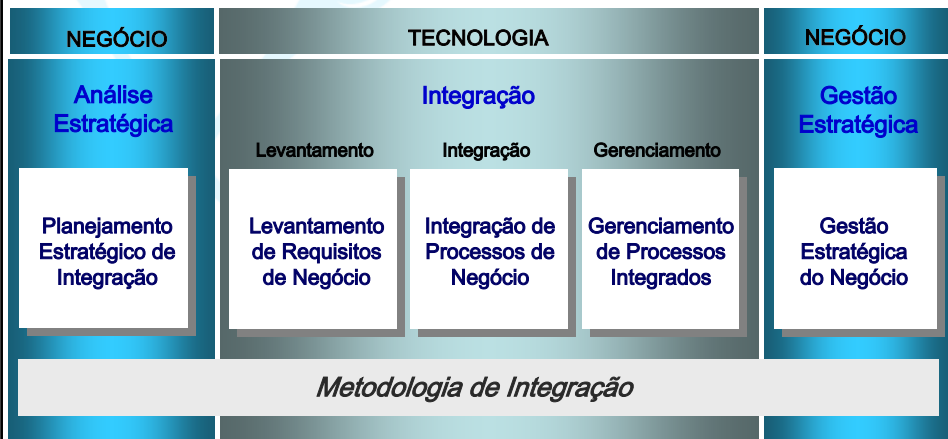
33

Plataforma de Integração



34

Planejamento da Integração



Planejamento da Integração



Planejamento Estratégico de Integração

Alinhamento Estratégico

Levantamento dos Processos

Priorização das Mudanças

Plano de Ações

Definição da Plataforma

Retorno do Investimento



Planejamento da Integração



Levantamento dos Requisitos de Negócio

Entendimento dos Requisitos

Levantamento dos Processos

Priorização das Mudanças

Modelo Canônico de Dados

Desenho da Arquitetura

Planejamento dos Testes



37

Planejamento da Integração



Integração dos Processos de Negócio

Preparação dos Ambientes

Desenvolvimento

Execução de Testes

Deployment



38

Planejamento da Integração



Gerenciamento dos Processos Integrados

Monitoração dos Processos

Tratamento de Exceções

Resolução de Problemas

Equipe Especializada



39

Planejamento da Integração



Gestão Estratégica do Negócio

Análise dos Resultados

Avaliação do Retorno

Revisão dos Processos

Levantamento do Impacto

Plano de Melhorias



40



INTEGRAÇÃO DE ESTRATÉGIA, INFORMAÇÕES E TECNOLOGIA NA ADMINISTRAÇÃO DOS RISCOS

Francisco Camargo – fcamargo@clm.com.br - (11) 5052-4733

Celso H. Leite – celso.leite@binders.com.br - (11) 5506-9446

www.clm.com.br/risco