
Gestão e Governança de TI

Fatec Zona Leste

Luciano Francisco de Oliveira

2023

Sumário

- Governança de TI
- SOX
- Basileia II e III
- Resoluções 3.380 e 4.457 Bacen
- Gestão de TI

Lembrando: Governança de TI

(Princípios segundo ISACA, ITGI)

- Alinhamento Estratégico;
- Entrega de Valor;
- Gestão de Recursos;
- Gestão de Riscos;
- Mensuração de Desempenho.



Lembrando: Desafio de TI

- Promover de forma eficaz e eficiente o seu alinhamento com o negócio (estratégias, diretrizes e promoção de valor).



Modelo de governança de TI

Alinhando às estratégias e compliance com dispostos legais respondendo as expectativas dos stakeholders.



Sarbanes-Oxley – SOX: resumido

Aderências:

- Avaliar a efetividade do sistema de controle sobre a emissão de relatórios financeiros;
- Comunicar as deficiências dos sistemas de controle interno que possam afetar a habilidade da organização em registrar, processar, sumarizar e comunicar informações financeiras;

[seção 302]



Sarbanes-Oxley – SOX: resumido

Aderências:

- A administração tem a responsabilidade de estabelecer e manter uma estrutura adequada de controle interno e procedimentos para relatórios financeiros;
- A administração deve avaliar a efetividade do sistema de controle interno sobre relatórios financeiros;
- Realizar auditoria externa específica sobre a avaliação interna da efetividade do sistema de controle interno feita pela administração.

[seção 404]

Sarbanes-Oxley – SOX: resumizado

Princípios para atender os requisitos da lei:

- O conteúdo da informação deve ser apropriado;
- A informação deve estar disponível no momento em que for necessária;
- A informação é atual ou pelo menos a última disponível;


Sarbanes-Oxley – SOX: resumizado

Princípios para atender os requisitos da lei:


- Os dados e as informações estão corretos;
- A informação é acessível aos usuários interessados;
- Há um sistema de controle interno sobre relatórios financeiros que garante todos os demais itens anteriores.



Sarbanes-Oxley – SOX: resumizado

Requisitos de qualidade da informação	Implicações da SOX
<p>O conteúdo da informação deve ser apropriado</p> 	<p>Proc. de desenvolvimento de requisitos de software; Processo de ger. de requisitos de software; Métodos de engenharia de software; Processos de verificação (teste); Processos de validação (aceite do usuário); Proc. de segurança da informação nos aplicativos; Processos de aceitação de produtos de terceiros; Processo de gestão da mudança e da configuração</p>
...	

Sarbanes-Oxley – SOX: resumizado

Requisitos de qualidade da informação	Implicações da SOX
<p data-bbox="416 392 909 611">A informação deve estar disponível no momento em que for necessária</p> 	<p data-bbox="944 392 2080 901">Disponibilidade de aplicativos; Disponibilidade da infraestrutura; Gerenciamento de Incidentes e problemas; Suporte aos usuários; Gestão de aplicativos e de ativos de TI; Processos de gerenciamento da infraestrutura; Segurança da infraestrutura; Gerenciamento da contingência; Gerenciamento de disponibilidade e desempenho.</p>
...	

Sarbanes-Oxley – SOX: resumido

Requisitos de qualidade da informação	Implicações da SOX
A informação é atual ou pelo menos é a última disponível	Processo de gerenciamento de dados; Planejamento e ger. da contingência e de desastres; Segurança da informação na infraestrutura.
Os dados e as informações estão corretos	Segurança da informação em aplicativos; Segurança da infraestrutura de TI; Teste de software; Controle da mudança e da configuração; Gerenciamento de dados; Gerenciamento de requisitos.
...	

Sarbanes-Oxley – SOX: resumido

Requisitos de qualidade da informação	Implicações da SOX
A informação é acessível aos usuários interessados	Segurança da informação referente a controle de acessos e privilégios; Controle de autorizações.
Há um sistema de controle interno sobre relatórios financeiros	Avaliação de riscos de TI; Gestão da qualidade; Plano de desastres e recuperação

Acordo de Basiléia II

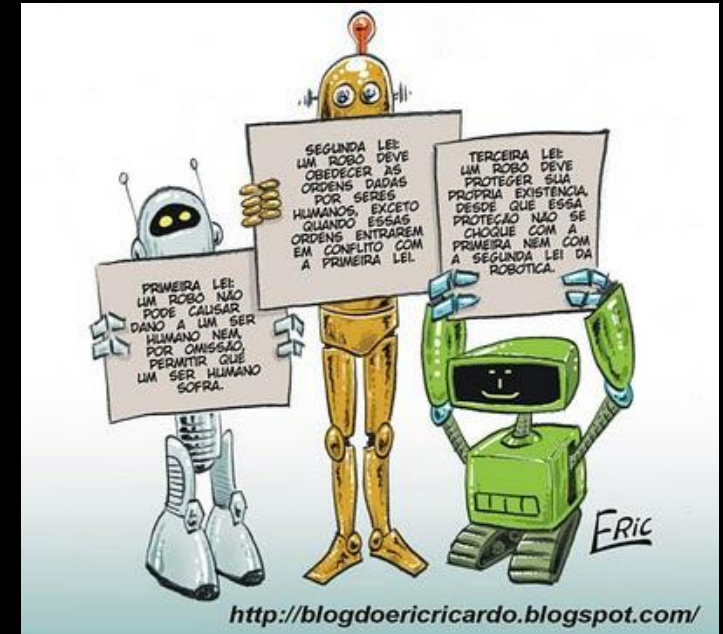
Estipula requisitos fiduciários mínimos para as instituições financeiras, em exposição dos riscos de créditos e operacionais.



Lembram:

Três Leis da Robótica:

- 1) um robô não pode ferir um humano ou permitir que um humano sofra algum mal;
- 2) os robôs devem obedecer às ordens dos humanos, exceto nos casos em que tais ordens entrem em conflito com a primeira lei; e
- 3) um robô deve proteger sua própria existência, desde que não entre em conflito com as leis anteriores.



Acordo de Basileia II

Seus 3 pilares, estabelecem:

- regras e procedimentos para o cálculo dos requisitos de capital, sobre os riscos de crédito e operacionais, com abordagens distintas de avaliação e mitigação de riscos.
- regras para que os Bancos Centrais de cada país executem auditorias nas instituições financeiras, visando avaliar a aplicação dos métodos de gestão de risco, a avaliação e mitigação de riscos de crédito e operacionais, e a emissão de informações ao mercado sobre a sua exposição de risco.
- regras à comunicação ao mercado, dos requisitos mínimos de capital, face os riscos e aos métodos e resultados de avaliações de riscos, conforme o 1º pilar.

Acordo de Basileia II

Principais impactos e riscos:

- Capacidade de armazenamento e mineração de dados do clientes;
- Integridade das informações;
- Segurança da informação;
- Contingenciamento para operações;
- Planejamento da capacidade;
- Planejamento de recuperação de desastres;
- Integridade do processo de emissão de relatórios.

Acordo de Basiléia III (Basel Comitee, 2010)

Objetivos do novo acordo. (Comitê do G20), destacam-se:

- Aumentar a qualidade do capital disponível de modo a assegurar que os bancos lidem melhor com as perdas;
- Diversificar a cobertura do risco, incorporando as atividades de trading, securitizações, exposições fora do balanço e derivativos;
- Introduzir uma taxa de alavancagem para o sistema e medidas sobre requerimentos mínimos de liquidez, tanto para o curto quanto para o longo prazo;

Acordo de Basiléia III (Basel Comitee, 2010)

Objetivos (cont.):

- O comitê propõe práticas para a gestão de liquidez, realização dos testes de estresse, governança corporativa e práticas de avaliação de ativos.
- Preocupação com a gestão e concentração de risco além da promoção de incentivos para que os bancos tenham uma melhor administração do risco e retorno orientados para o longo prazo.



Banco Central do Brasil (BCB)

resolução 3.380 de 2006.

- Determina que as instituições financeiras e demais instituições autorizadas a funcionar pelo BCB implementem sua própria estrutura de gerenciamento de risco operacional.
- Incluindo a falhas em sistemas e TI como risco operacional.
- Deve-se identificar, avaliar, monitorar, controlar e mitigar os riscos da instituição.



Banco Central do Brasil (BCB)

Resolução 4.557 de 2017.

- A Resolução BACEN 4.557 revoga os dispositivos anteriores (Resoluções do BACEN 3380/2006 entre outras) e apresenta como principal alteração a exigência de que os riscos de crédito, liquidez, operacional, de variação de taxas de juros e de mercado, além da estrutura de capital, sejam gerenciados de forma contínua e integrada, exigindo que as instituições financeiras concentrem tais atividades em um único Chief Risk Office (CRO).

Banco Central do Brasil (BCB)

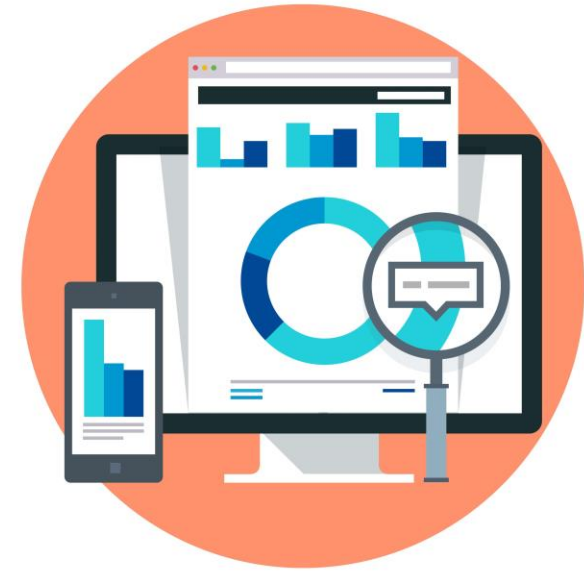
Resolução 4.557 de 2017.

No contexto brasileiro:

- Conselho Monetário Nacional (CMN) aprovou a Resolução 4557/2017 (BACEN, 2017b), que dispõe:
- sobre o gerenciamento integrado de riscos e de capital pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.
- Estabelece ainda que as instituições devem implementar a estrutura de gerenciamento contínuo e integrado de riscos e de capital, sendo facultada às instituições do sistema cooperativo de crédito.

Governança de TI

Governança de TI diz respeito à maneira como são tomadas as decisões relacionadas à TI em uma organização e aos mecanismos implementados para assegurar a sua efetividade no alcance dos resultados esperados pelos stakeholders.



Principais Decisões da Governança de TI

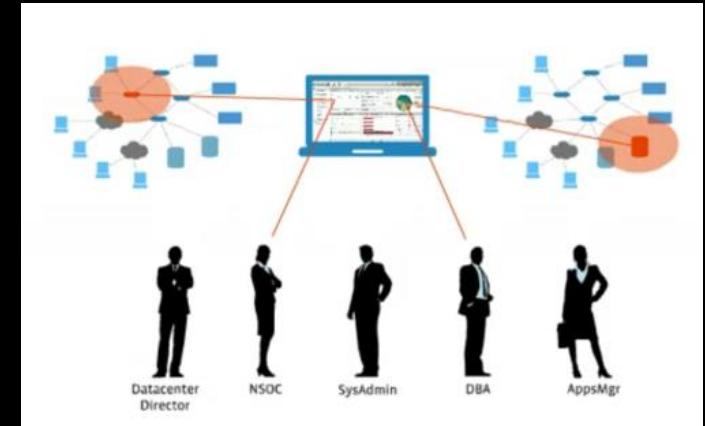
Weill e Ross (2006) contextualizam a avaliação de investimentos em TI como uma das cinco decisões interrelacionadas que devem ser tomadas no âmbito da governança de TI.

Decisões	Aspectos
Princípios de TI	Declarações de alto nível sobre a utilização da TI no negócio.
Arquitetura de TI	Organização lógica dos dados, aplicações e infraestrutura definidas a partir de políticas, relacionamentos e opções técnicas adotadas para padronização e integrações técnicas e de negócios desejadas.
Infraestrutura de TI	Serviços compartilhados de TI coordenados de maneira centralizada e provendo a base para o uso da TI aplicada.
Necessidades de Aplicações de Negócio	Especificação das necessidades de negócio para as aplicações de TI, adquiridas externamente ou desenvolvidas internamente.
Investimentos e Priorização de TI	Decisões sobre quanto e em o que investir, incluindo a aprovação e os métodos utilizados para justificá-los.

Fonte: Adaptado de Weill e Ross (2006)

Impactos da TI sobre as organizações

- Apoio administrativo
 - predominante no apoio administrativo com sistemas de informação ligados, principalmente, às rotinas administrativas e de controles, com pouca interação direta com os produtos e serviços da organização.
- Suporte ao negócio
 - com seus sistemas de informação ligados nas operações e uma grande parte das atividades de suporte ao negócio.



Impactos da TI sobre as organizações

- Estruturação do negócio
 - a TI passa a ser o meio principal na articulação na maior parte dos processos de negócios
- Fusão ao negócio
 - a TI tem papel integrante do negócio, além de estruturar as operações, atua na criação dos produtos e serviços.



Alinhamento estratégico

- Posturas quanto à inovação tecnológica
- O paradoxo da inovação tecnológica
- Riscos inerentes às diferentes posturas
- Posturas híbridas
- Caminhos alternativos

Paradoxo: pensamento, proposição ou argumento que contraria os princípios básicos e gerais que costumam orientar o pensamento humano. Contradição.

Alinhamento entre estratégias de negócio e de TI

- O conceito de tecnologia de informação (TI), trata muitos aspectos além de recursos tecnológicos (computadores, softwares e tecnologias de comunicação).
- Inclusive não trata apenas da estrutura voltada às atividades ligadas à tecnologia em uma organização de forma eficaz e eficiente, mas propõem atender às necessidades dos usuários dentro dos níveis de serviço acordados.

Investimentos em TI nas organizações

- A partir da valorização das informações que suportam os processos decisórios nas organizações, desde seu valor operacional ao seu valor estratégico da TI, gerando assim estímulos na consolidação de investir em TI, propiciando a geração de novas estratégias e geração de valor para o negócio.



Três dimensões dos investimentos em TI

- tecnologia, pessoas e gestão.
- Tecnologia diz respeito à escolha adequada do composto de recursos de hardware e software que serão utilizados pela organização.



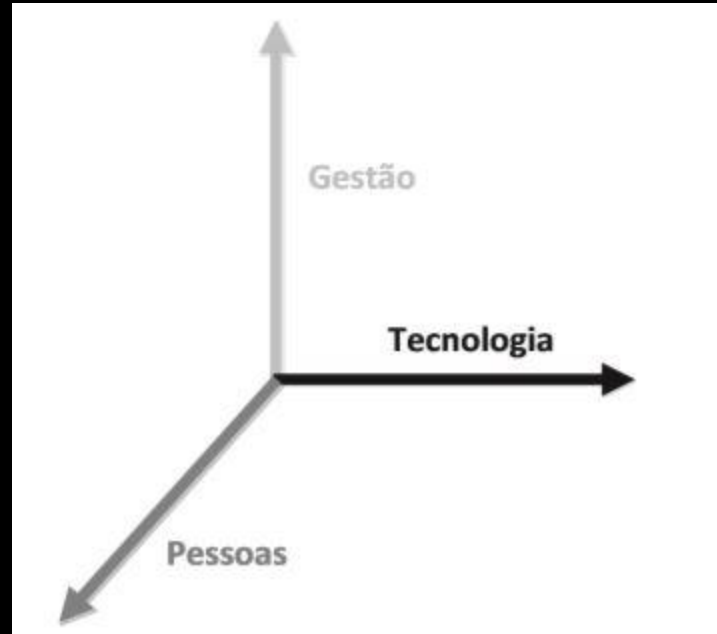
Três dimensões dos investimentos em TI

- tecnologia, pessoas e gestão.
- Investimentos em tecnologia (hardware, software, consultoria etc.) precisam ser acompanhados de investimento nas pessoas que conviverão com a inovação. Sem isto, pode-se facilmente cair num contexto em que, por falta de capacitação, as pessoas não usem os novos recursos em sua plenitude.

Três dimensões dos investimentos em TI

- tecnologia, pessoas e gestão.
- à gestão — o que abrange desde mudanças de processos até reflexões estratégicas, passando por estrutura organizacional, comunicação interna e externa etc. É muito comum que um projeto de TI possibilite mudanças substanciais nos processos: simplifica procedimentos, elimina tarefas etc.

Três dimensões dos investimentos em TI



Fonte: Di Serio e Leite (2003)

Aspectos sobre avaliação de investimentos em TI

- Contexto organizacional, os momentos e os tipos de avaliação e os níveis de análise são fundamentais para que os projetos sejam avaliados de forma adequada aos propósitos estabelecidos.
- A avaliação de TI deve ser compreendida no contexto que abrange tais investimentos na organização. Esta atividade está envolta em processos sociais e organizacionais e pode ocorrer de diversas formas e com critérios distintos, num contínuo que vai desde metodologias rigorosas até justificativas baseadas predominantemente na intuição.

Importância da avaliação de investimentos em TI

- Os montantes de capital envolvidos geralmente são representativos;
- Certos investimentos em TI não são associados diretamente à geração de lucro da organização;
- Todos os benefícios operacionais, táticos e estratégicos, bem como os custos, devem ser avaliados;
- Nem sempre há consenso sobre a necessidade, o valor ou o desempenho do investimento;

Importância da avaliação de investimentos em TI

- Há crescente insatisfação com o desempenho das funções de TI;
- Devem-se evitar ineficiências na tomada de decisões;
- Uso e importância crescentes da TI no negócio principal das organizações;
- Alinhamento de expectativas dos gestores de negócio e tecnológicos;
- cont...

Importância da avaliação de investimentos em TI

- Existência de vários projetos de investimento (em TI e em outros tipos de ativos) candidatos a receber capital; e
- Apresentação, por parte de alguns investimentos, de horizontes temporais de retorno muito longos e bastante incertos.



Frameworks de Governança em TI

Alguns frameworks que indicam boas práticas de governança de TI.



Referências

ABNT. **NBR ISO/IEC 27001**. Rio de Janeiro: ABNT, 2006.

_____. **NBR ISO/IEC 27002**. Rio de Janeiro: ABNT, 2005.

BEAL, A. **Segurança da Informação**. São Paulo: Atlas, 2008.

BRAGA FILHO, J. R. **Os dados da sua empresa estão seguros?** Rio de Janeiro: Brasport, 2004.

CAMPOS, A. **Sistema de segurança da informação: controlando os riscos**. 2ª ed. Florianópolis: Visual Books, 2007.

CORREIA NETO, Jocildo F.; LEITE, Jaci Corrêa. **Decisões de Investimentos em Tecnologia da Informação: vencendo os desafios da avaliação de projetos em TI**. Rio de Janeiro: Elsevier, 2015.

DAWEL, G. **A segurança da informação nas empresas: ampliando horizontes além da tecnologia**. Rio de Janeiro: Ciência Moderna, 2005.

DI SERIO, Luiz C.; LEITE, Jaci C. **Tecnologia e Competitividade no Brasil**. FGV-EAESP, Núcleo de Pesquisas e Publicações, Relatório de Pesquisa, nº 18, 2003.

FERREIRA, F. N. F.; ARAÚJO, M. T. de. **Política de segurança da informação: guia prático para elaboração e implementação**. 2ª ed. Rio de Janeiro: Ciência Moderna, 2008.

Referências

FONTES, E. **Segurança da informação: o usuário faz a diferença**. São Paulo: Saraiva, 2006.

_____. **Praticando a segurança da informação**. Rio de Janeiro: Brasport, 2008.

LIMA, P. M. F. **Crimes de computador e segurança computacional**. São Paulo: Atlas, 2011.

LYRA, M. R. Segurança e auditoria em sistemas de informação. Rio de Janeiro: Ciência Moderna, 2008.

MEIRELES, N. R. **Gestão estratégica do sistema de segurança: conceitos, teorias, processos e prática**. São Paulo: Sicurezza Editora, 2011.

MOREIRA, N. Stringasci. **Segurança mínima: uma visão corporativa da segurança de informações**. Rio de Janeiro: Axcel Books, 2001.

SHOSTACK, A.; STEWART, A. **A nova escola da segurança da informação**. Rio de Janeiro: Alta Books, 2008.