Mejores Prácticas de Gobierno de TI en las Instituciones Financieras

XIV CONGRESO LATINOAMERICANO DE AUDITORIA INTERNA Y EVALUACION DE RIESGO

12 al 14 de Mayo 2010 • Hotel Marriott Panamá
Ciudad de Panamá, República de Panamá

Francisco de Assis **Fernandes**
Brasil

Gobierno y Gestión del Riesgo de TI

- “IT risk is business risk” (ITGI).

- El ITGI considera que el Gobierno de TI no es una disciplina aislada. Es parte integrante del Gobierno Corporativo.

- La práctica de administración de riesgos busca:

  - clasificar los riesgos.
  - evaluar el tamaño de su impacto.

- Según el ITGI el Gobierno de TI está relacionado fundamentalmente a dos eventos:

  - Entrega de valor de TI para el negocio (alineando TI con la estrategia del negocio).
  - Mitigación de riesgos de TI (estructurada por la política interna de la empresa).

Objetivos de la administración

- Alineamiento de las funciones de TI con el negocio: estratégicamente y tácticamente;

- Evaluando la relación costo/beneficio, en el cual el costo en TI está claramente relacionado con el valor que él agrega a la organización;

- La excelencia operativa, que es la entrega de proyectos de TI y servicios con alta calidad, alta eficiencia y con niveles de servicio preestablecidos.

POPPER, C.
Holistic framework for IT governance. Program on Information Resources Policy.
Harvard University, Ene 2000

Administración Global y Amplia

- Alineamiento Estratégico: mantener a razón entre las soluciones de TI y el negocio de la empresa.

- Valor de TI: optimizar los costos de las inversiones en TI y el retorno de las mismas.

- Administración de riesgo: asegurar la protección de los activos de TI, posibilitando la recuperación de informaciones en caso de desastres y mantener la continuidad de la operación de los servicios de TI.

- Administración de Recursos: optimizar el conocimiento y la infraestructura de TI.

- Medidas de Desempeño: acompañar la entrega de los proyectos de TI y monitorear los servicios de TI.

IT GOVERNANCE INSTITUTE

Fiscalización del Banco Central de Brasil

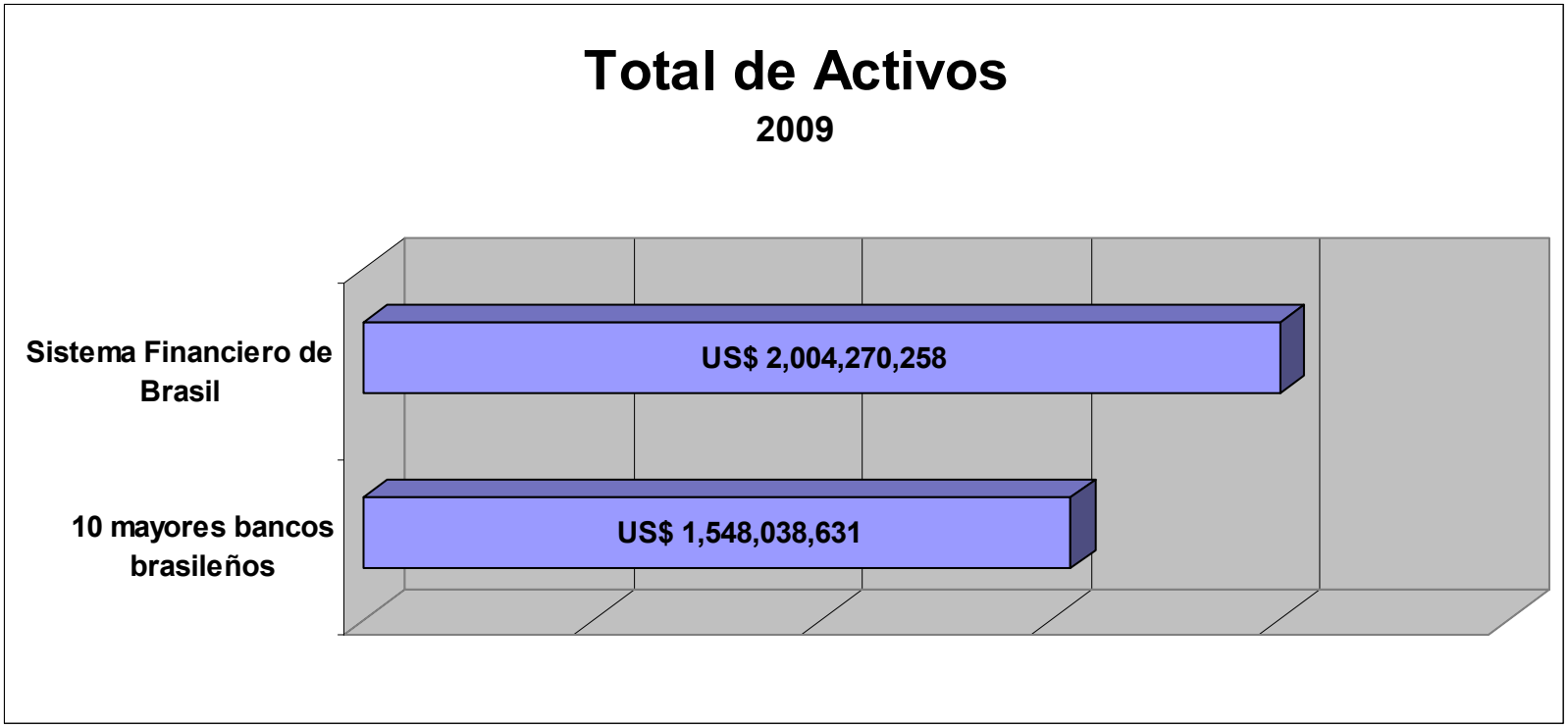
- Creación de los equipos especializados: tecnología de la información, entre otros.

- Sistema de evaluación de las instituciones financieras (*rating*), buscando realizar una evaluación detallada de la institución. Define incluso la frecuencia de las inspecciones del Banco Central.

- Adopción, a partir del 2º semestre de 1999, del **Cobit** en los trabajos de revisión de los ambientes de informática de los bancos. Tal metodología, está siendo muy utilizada satisfactoriamente en los trabajos del Departamento de Supervisión en los últimos años.

BANCO CENTRAL DE BRASIL, Dirección de Fiscalización
Informe de Actividades: 1995 a 2002

El sistema financiero en Brasil



FEBRABAN – Federación Brasileña de Bancos

FEBRABAN

O Setor Bancário em Números

Rede de Atendimento

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2008/07	2009
Agências	16.396	16.841	17.049	16.829	17.260	17.627	18.087	18.572	19.142	*3,1%*	20.046
Postos tradicionais (1)	9.495	10.241	10.148	10.054	9.856	9.985	10.220	10.555	11.661	*10,5%*	12.131
Postos eletrônicos	14.453	16.748	22.428	24.367	25.595	30.112	32.776	34.669	38.710	*11,7%*	41.472
Correspondentes não bancários	13.731	18.653	32.511	36.474	46.035	69.546	73.031	95.849	108.074	*12,8%*	149.507
Total de pontos de atendimento	54.075	62.483	82.136	87.724	98.746	127.270	134.114	159.645	177.587	*11,2%*	223.156

Fonte: Banco Central do Brasil

(1) Inclui Postos de Atendimento Bancário (PAB), Postos de Arrecadação e Pagamentos (PAP), Postos Avançados de Atendimento (PAA), Postos de Atendimento Cooperativivo (PAC), Postos de Atendimento ao Microcrédito, Postos Avançados de Crédito Rural (PACRE),

Enquanto, desde o ano 2000, o número de agências bancárias instaladas no País cresce ao ritmo de 2% a.a. até 2008, a quantidade de postos eletrônicos amplia-se em cerca de 13% a.a. Os correspondentes não bancários evoluíram quase 30% ao ano nesse período, superando as 100 mil unidades, garantindo, assim, o acesso a serviços bancários a todos os recantos do Brasil.

O Setor Bancário em Números

FEBRABAN

Número de contas e Internet Banking *(em milhões)*

	2000	2001	2002	2003	2004	2005	2006	2007	2008	2008/07	2009
Contas correntes	63,7	71,5	77,3	87,0	90,2	95,1	102,6	112,1	125,7	*12,1%*	133,6
Clientes com contas de poupança	45,8	51,2	58,2	62,4	67,9	71,8	76,8	82,1	92,0	*12,1%*	91,1
Contas de *Internet Banking*	8,3	8,8	9,2	11,7	18,1	26,3	27,3	29,8	32,5	*9,1%*	35,4 (*)
Pessoas Físicas								25,3	27,7	*9,5%*	30,1 (*)
Pessoas Jurídicas								4,5	4,8	*6,7%*	5,3 (*)

Fontes: Banco Central do Brasil; Abecip - Associação Brasileira das Entidades de Crédito Imobiliário e Poupança; Febraban.

(*) estimativa

No período de oito anos (2000/2008), o número de contas correntes e de poupança dobrou. Ou seja, registrou um crescimento médio de 9% a.a. Ao final de 2008, eram cerca de 32,5 milhões o total de contas de Internet Banking. Esta cifra deve ser comparada aos 43 milhões de internautas maiores de 16 anos (IBOPE / NetRatings). Mais importante ainda é a diversificação crescente das operações que podem ser realizadas nos sites dos bancos que atuam no Brasil, certamente um cenário privilegiado em relação a qualquer outro país.

FEBRABAN

O Setor Bancário em Números

Recursos Computacionais dos Bancos

Instalados em centrais, departamentos e pontos de atendimento.

Equipamento	Unidade	2003	2004	2005	2006	2007	2008	2008/07
Mainframes	MIPS	164.608	228.701	272.442	349.441	403.128	510.934	*27%*
Servidores UNIX / LINUX centralizados	Unidades	1.835	2.241	2.347	2.530	2.874	4.668	*62%*
Servidores UNIX / LINUX em pontos de atendimento	Unidades					5.719	9.025	*58%*
Servidores Windows centralizados	Unidades	12.428	11.863	10.302	13.727	13.492	14.947	*11%*
Servidores Windows em pontos de atendimento	Unidades					16.698	16.204	*-3%*
Terminais de Caixa	Unidades	131.773	120.015	119.233	131.719	133.385	141.170	*6%*
Estações de trabalho / PC's / Notebooks	Unidades	373.537	378.184	447.567	478.982	510.847	515.296	*1%*
PDAs / Smartphones/ Assemelhados	Unidades			1.902	8.360	12.206	16.304	*34%*
Fitotecas robotizadas	Unidades	135	139	143	167	188	227	*21%*
Discos	Terabytes	2.074	1.914	2.628	5.213	7.010	9.554	*36%*

Fonte: FEBRABAN

A multiplicidade de usos dos computadores pelos bancos, seja para ampliar a prestação de serviços aos seus clientes, seja para atender às necessidades de gestão de suas áreas internas, aliada à proliferação de dados a serem processados e a armazenados, bem como à crescente sofisticação das aplicações desenvolvidas, fazem do segmento financeiro um dos mercados mais importantes para a comercialização de hardware, software e serviços. Isso fica bastante evidente ao observarmos o quadro acima. Outro fato a registrar é a crescente utilização de equipamentos UNIX / LINUX.

Banco Central de Brasil – Adopción del CobiT

- En Brasil tenemos 156 instituciones financieras (bancos comerciales, múltiplos y Caixa Econômica – Posición en abril/2010).

- En razón del Banco Central de Brasil utilizar el **CobiT** como referencia técnica para las actividades de supervisión y fiscalización, las estructuras de TI y la auditoría interna de los bancos brasileños también lo utilizan fuertemente.

"La utilización del CobiT como modelo para Gobierno de TI y referencia para el Banco Central en la actividad de supervisión bancaria de las instituciones del sistema financiero brasileño"

Autora: Elaine Cristina Suetsugu
FIA – Fundación Instituto de Administración

Entrevista con representante del Banco Central de Brasil
Realizada en noviembre/2008
Contacto: Francisco José Barros de Figueiredo – Supervisor de Fiscalización
Departamento de Supervisión de Bancos y Conglomerados Bancarios
División de Equipos Especializados – Tecnología de la Información

Partes más importantes de la entrevista

"La fiscalización bancaria en el área de TI antes del **CobiT** era realizada con base en metodología propia. Había versiones propias y diferentes de equipo en equipo, y estas muchas veces cuestionaban y discutían sobre los procesos de control que eran definidos para evaluación".

"Con el **CobiT** el problema de actualización y el cuestionamiento en cuanto a los procesos de controles definidos fueron subsanados".

"El objetivo es verificar si los procesos y procedimientos del área de TI son adecuados, se buscan minimizar los riesgos de incidentes en los recursos de TI, de forma de prevenir que los negocio de las instituciones financieras sean afectadas debido a problemas con recursos de TI".

"El cuestionario que el BACEN utiliza para relevamiento de informaciones está estructurado en el mismo orden que los procesos de control del **CobiT**".

"La nota de la evaluación del ambiente de TI es una de las que componen la nota general de *rating* de la institución".

Encuesta Académica con Bancos Brasileños

“Gobierno de TI en las instituciones financieras en Brasil: Una evaluación de tendencias”

Maestría en Tecnología

Autora: Edméa Pujol Cantón
Centro Estadual de Educación Tecnológica Paula Souza
Mayo/2008

Encuesta con 58 bancos brasileños

Distribución de los bancos participantes de la Encuesta

		Origem			Porte				
		Privado	Público	Total	Pequeno	Médio	Grande	Pequeno M.	Total
		Resp	Resp	Resp	Resp	Resp	Resp	Resp	Resp
Naturalidade	Nacional	30	1	31	11	12	5	3	31
	Nacional participação estrangeira	4		4		2	2		4
	Nacional controle estrangeiro	3		3	2		1		3
	Estrangeiro	13	1	14	4	4	6		14
	Estadual		3	3	1	1	1		3
	Federal		3	3		1	2		3
	Total	50	8	58	18	20	17	3	58
Tipo	Múltiplo	32	6	38	12	13	11	2	38
	Comercial	3	1	4	2	1	1		4
	Caixa								
	Investimento	7	1	8	3	2	2	1	8
	Leasing								
	Financeira	8		8	1	4	3		8
	Total	50	8	58	18	20	17	3	58

Cantón, Edméa Pujol

Governança deTI nas instituições financeiras no Brasil: uma avaliação de tendências / Edméa Pujol Cantón. - São Paulo: CEETEPS, 2008.

Resultado – Escenario Actual (2008)

1ª	A instituição atende aos requisitos regulatórios para atender a regulamentações governamentais.
2ª	Há na instituição Segurança da Informação implantada com políticas, área dedicada e normas.
3ª	A instituição reconhece que as exigências regulatórias representam uma oportunidade para aumentar o valor ao negócio.
4ª	Há na instituição uma área responsável para a Gestão de Riscos (permanente).
5ª	Há implantação de uma Cultura de Compliance.
6ª	Existe informação regular à diretoria sobre os riscos aos quais a instituição é exposta.
7ª	Há na instituição um PCN - Plano de Continuidade de Negócios implantado.
8ª	Há implantação de uma Cultura de Controles Internos.
9ª	Há na instituição práticas de Governança Corporativa.
10ª	Há na instituição práticas de Governança de TI.
11ª	Há um plano que avalia a vulnerabilidade da instituição a novas tecnologias.
12ª	Há planos padronizados para gerenciamento de serviços de terceiros.

Resultado – Escenario Futuro (2010)

1ª	Há na instituição uma área responsável para a Gestão de Riscos (permanente).
2ª	Há na instituição Segurança da Informação implantada com políticas, área dedicada e normas.
3ª	Há na instituição um PCN - Plano de Continuidade de Negócios implantado.
4ª	Há implantação de uma Cultura de Controles Internos.
5ª	A instituição atende aos requisitos regulatórios para atender a regulamentações governamentais.
6ª	Há implantação de uma Cultura de Compliance.
7ª	Existe informação regular à diretoria sobre os riscos aos quais a instituição é exposta.
8ª	A instituição reconhece que as exigências regulatórias representam uma oportunidade para aumentar o valor ao negócio.
9ª	Há na instituição práticas de Governança de TI.
10ª	Há na instituição práticas de Governança Corporativa.
11ª	Há um plano que avalia a vulnerabilidade da instituição a novas tecnologias.
12ª	Há planos padronizados para gerenciamento de serviços de terceiros.

Resultado – Prioridad de los procesos del CobiT

		Prioridade	Processos
Planejar e Organizar	Atual	Maior	PO5 - Gerenciar o Investimento em TI PO6 - Comunicar Metas e Diretrizes Gerenciais
		Menor	PO8 - Gerenciar Qualidade
	2010	Maior	PO6 - Comunicar Metas e Diretrizes Gerenciais
Adquirir e Implementar	Atual	Maior	AI3 - Adquirir e Manter Infra-estrutura Tecnológica
		Menor	AI6 - Gerenciar Mudanças
	2010	Maior	AI7 - Instalar e Homologar Soluções e Mudanças
Entretgar e Suportar	Atual	Maior	DS4 - Assegurar Serviço Contínuo
			DS5 - Assegurar Segurança dos Sistemas
			DS12 - Gerenciar o Ambiente Físico
		Menor	DS1 - Definir e Gerenciar Níveis de Serviço
			DS7 - Educar e Treinar Usuários
	2010	Maior	DS4 - Assegurar Serviço Contínuo
Monitorar e Avaliar	Atual	Maior	ME3 - Assegurar Aderência aos Regulamentos
		Menor	ME4 - Prover Governança de TI
	2010	Maior	ME3 - Assegurar Aderência aos Regulamentos

La Auditoría Interna necesita actuar

- Con el aumento de la sensibilidad al tema en las corporaciones, la función de auditor interno obtuvo nuevas dimensiones.

- El objetivo de los trabajos de auditoría interna está desplazándose de las áreas más operativas hacia las áreas estratégicas.

- De los auditores internos se espera la evaluación y anticipación de la probabilidad de los riesgos.

- Más aún: es necesario verificar si las áreas de la empresa tienen controles adecuados para mitigarlos.

La Auditoría Interna necesita considerar

- Es necesario que esté muy bien definido lo que será hecho en caso de que un riesgo se concrete.

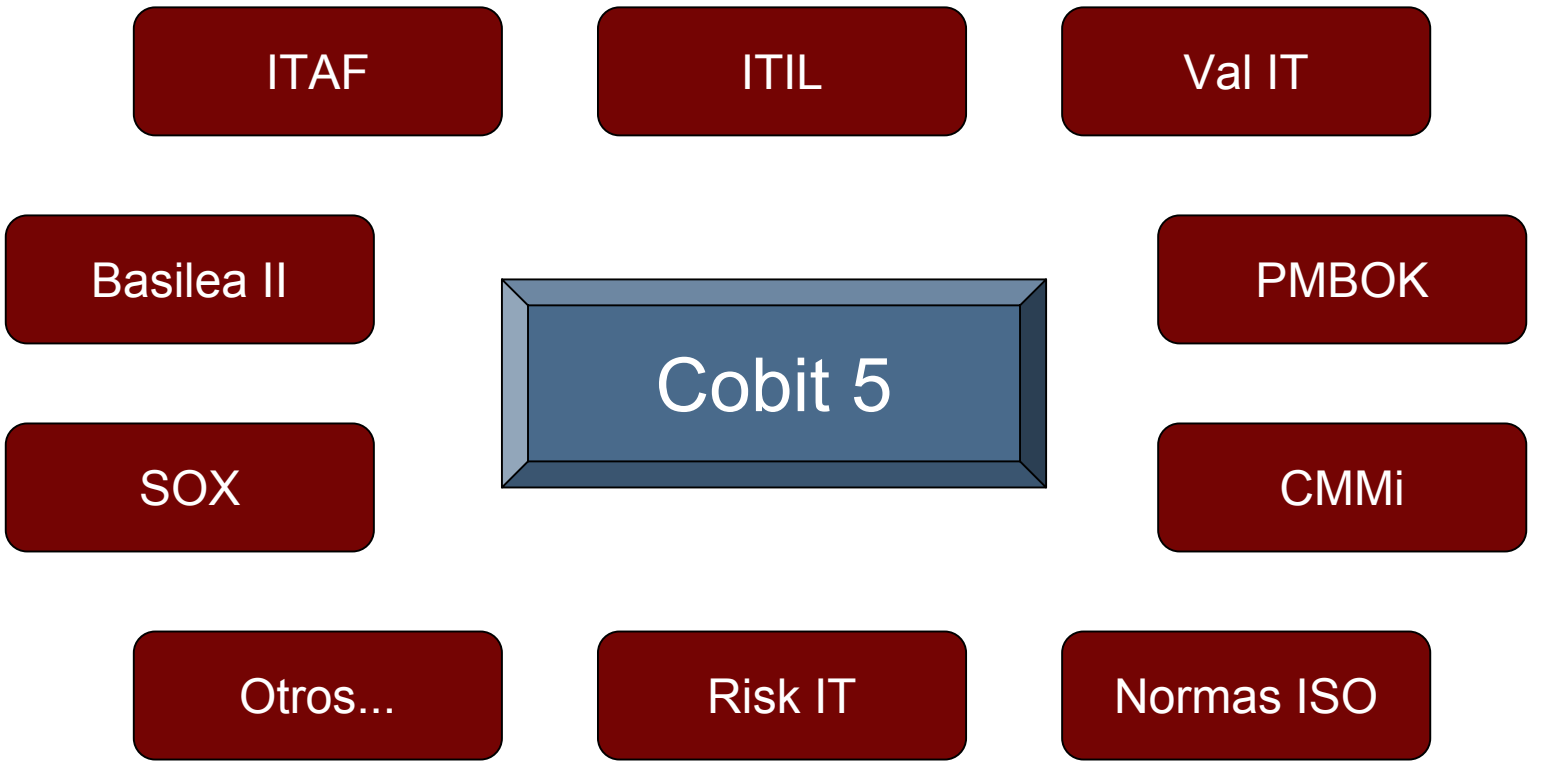
- No basta depositar toda la confianza de la perennidad de la organización, en profesionales calificados. Ellos mismos pueden no estar disponibles en alguna contingencia.

- Gobierno de TI presupone acciones factibles y transparencia.

- El Gobierno de TI determina cuáles decisiones deben ser tomadas y quién debe tomar esas decisiones. Además de eso, el Gobierno de TI involucra la decisión de quién será responsable por tomar las decisiones o contribuir para ellas: Caso típico de la participación de la Auditoría de TI.

Niveles de Control Interno

Cobit 5 – Enfocado en su misión



"Cuando inversores compran acciones, cirujanos realizan operaciones, ingenieros proyectan puentes, empresarios abren sus negocios y políticos compiten a cargos electivos, el riesgo es un asociado inevitable. No obstante, sus acciones revelan que el riesgo no precisa ser hoy tan temido: administrarlo se hizo sinónimo de desafío y oportunidad".

(PETER BERNSTEIN – "Desafío a los dioses: la fascinante historia del riesgo")

¡Gracias!

Francisco de Assis **Fernandes**
Banco Safra
FEBRABAN
Brasil

francisco.fernandes@safra.com.br

(+55 11) 3175-7521