Referência para citação:
FERNANDES, L. G.; JANISSEK-MUNIZ, R. AUDITORIA DE SISTEMAS BASEADA NO RISCO: estruturação do conhecimento para dar suporte à análise e planejamento de auditorias. In: CONGRESSO INTERNACIONAL DE GESTÃO DA TECNOLOGIA E SISTEMAS DE INFORMAÇÃO (CONTECSI), 5º, 2008, São Paulo. **Anais...** São Paulo: FEA/USP, 2008.

SYSTEMS AUDIT BASED ON RISK: structuring of knowledge in order to support the analisys and planning the audit

Liliam Grieger Fernandes (Universidade de Caxias do Sul, RS, Brasil) - liliamgrieger@gmail.com

Raquel Janissek-Muniz (Universidade Federal do Rio Grande do Sul, RS, Brasil) - rjmuniz@ea.ufrgs.br

Abstract: Financial institutions as well as most organizations do not survive without information systems. Indispensable, they must be subject to risk management. The internal controls are an important part in this management, and that's why the Systems Audit department has the obligation to verify the effective execution of these controls. But, faced with a large number of systems, it is necessary to evaluate what is most critical to prioritize the audits. It is proposed a methodology to evaluate the systems using data from audits to create a hierarchy of relevance and risk. With the focus on the most critical systems it is possible to audit the systems more susceptible to the risks. This makes the task of annual planning audits much faster because it is based on indicators of risk and relevance of systems. Moreover, identifying and measuring the improvements made in controls systems as audits occur, promotes the standardization of audits and the creation of a knowledge base of the systems. **Keywords:** Knowledge Management, Audit of Information System, Risk Analysis, Information Security, Corporate Governance.

AUDITORIA DE SISTEMAS BASEADA NO RISCO: estruturação do conhecimento para dar suporte à análise e planejamento de auditorias

Resumo: As instituições financeiras, assim como a maioria das organizações, não sobrevivem sem os sistemas de informação. Indispensáveis, eles precisam ser objeto de gerenciamento de riscos. Tendo os controles internos papel importante nesse gerenciamento, cabe à Auditoria de Sistemas verificar o efetivo cumprimento destes, minimizando riscos. Diante de diversos sistemas, é necessário avaliar os mais críticos para priorizar auditorias. Neste contexto, é proposta uma metodologia para avaliar os sistemas utilizando dados de auditorias para criar uma hierarquia de relevância e de risco. Com foco nos sistemas críticos, é possível auditar prioritariamente aqueles mais suscetíveis aos riscos. Assim, torna a tarefa de planejamento anual de auditorias mais rápida, respaldada nos indicadores de risco e relevância dos sistemas. Também permite identificar e mensurar melhorias realizadas nos controles de sistemas, promove a padronização de auditorias e criação de base de conhecimento sobre os

sistemas. **Palavras-chave:** Gestão do Conhecimento, Auditoria de Sistemas de Informação, Análise de Risco, Segurança da Informação, Governança Corporativa.

1 Introdução

Fatos ocorridos em 2001 mudaram definitivamente o cenário de gestão de risco nas organizações. Um deles, o atentado terrorista de 11 de setembro em Nova Iorque, mostrou o quão vulneráveis são as organizações e a urgência de um plano de continuidade dos negócios. Outro fato significativo foi o escândalo seguido do pedido de concordata da empresa de energia norte-americana, a Enron. Este último, somado a diversos outros escândalos financeiros, levou a promulgação da Lei Sarbanes Oxley, cuja premissa é estimular a eficiência e transparência para promover uma rígida conduta de Governança Corporativa, com base em um efetivo gerenciamento de risco (SERMOND, 2007).

O princípio do gerenciamento de risco para promover a Governança é que quanto menor o risco que uma organização corre mais confiável ela é. Assim, além do desafio de promover a Segurança da Informação, deve haver a integração entre estratégia de negócios, operação, *compliance* e finanças (SERMOND, 2007).

A Governança Corporativa é capaz de gerar valor quando aplicada e quando se tem também um negócio de qualidade, lucrativo e bem administrado. Neste caso, a boa governança permitirá uma administração ainda melhor, em benefício de todos os acionistas e daqueles que lidam com a empresa. Os protagonistas do processo de Governança são os acionistas, conselheiros, executivos e auditores, que garantem a mútua prestação de contas (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2007).

A Auditoria de Sistemas, como parte da Auditoria Interna, possui papel importante na promoção da Governança Corporativa, pois, através dela é possível controlar a eficácia e a eficiência dos controles, assessorando a administração quanto ao desempenho das atribuições definidas para cada área da empresa (FERNANDES, 2007). Também é papel da Auditoria de Sistemas avaliar a aplicação da Segurança da Informação – confidencialidade, integridade, disponibilidade, não repúdio, entre outros.

No âmbito de sistemas de informação, deve-se garantir que a informação seja armazenada, processada e ao final se obtenha uma saída íntegra e confiável, independente do sistema utilizado. Além disso, para o cliente e investidor, é importante a garantia de sigilo dos seus dados e confiabilidade das informações, oriundas em sua maioria dos sistemas de informação.

Quando se fala de Segurança da Informação, é importante considerar que o negócio de muitas organizações depende das informações contidas nos seus sistemas, como é o caso das instituições financeiras, que possuem as informações como matéria-prima e produto final. Assim, é necessário proteger este importante ativo, minimizando a exposição das informações aos diversos riscos existentes e garantindo a continuidade do negócio.

Considerando uma realidade onde, apesar dos avanços crescentes em termos de segurança, os sistemas e informações estão expostos a riscos internos e externos – como, por exemplo, acesso indevido, mau uso da informação, falhas e erros os quais colocam em risco a integridade e a confiabilidade dos dados – torna-se necessário auditar os sistemas e os processos envolvidos no acesso e na manipulação das informações.

A Auditoria de Sistemas, embora realize trabalhos periódicos, abrange sistemas em desenvolvimento, produção, manutenção, microinformática, ambientes, e outros recursos da tecnologia da informação, cujas características são distintas, bem como os prazos de execução. Diante disso, há dificuldade em definir as prioridades para o planejamento de auditorias, pois mesmo sendo grande a quantidade de trabalho a ser normalmente executada pela Auditoria de Sistemas, a disponibilidade de recursos humanos é inferir a demanda. Outro aspecto a ser considerado, é a necessidade de auditar de forma alinhada com os objetivos da organização (FERNANDES, 2007).

Com o entendimento que a melhor alternativa para planejar auditorias de sistemas em produção é através da análise de risco, este artigo propõe uma forma de priorizar auditorias, operacionalizada através da identificação e mensuração de riscos, permitindo, assim, a hierarquização dos sistemas. No contexto deste estudo, foi considerada a relevância dos sistemas para a organização, identificando àqueles mais suscetíveis aos riscos e que podem gerar maior impacto ao negócio, priorizando, dessa forma, as auditorias.

Com a preocupação de criar a teórica para a prática, este estudo utilizou a pesquisa-ação, umas das técnicas de pesquisas qualitativas. Partindo dos conhecimentos adquiridos pelos auditores de sistemas e apoiados por um modelo de estruturação deste conhecimento, foram formalizados e padronizados aspectos importantes a serem avaliados nos sistemas, em um modelo de roteiro de auditorias.

Uma breve explanação dos assuntos relacionados se encontram nos capítulos 2, 3 e 4. Os procedimentos metodológicos são descritos no capítulo 5, seguido da análise dos resultados. No capitulo 7 são realizadas as considerações finais.

2 Como utilizar a Gestão do Conhecimento para aprender sobre riscos?

A Gestão do Conhecimento é conceituada por Zabot e Silva (2002) como a capacidade de relacionar informações estruturadas e não estruturadas com regras constantemente modificadas e aplicadas pelas pessoas na empresa. E como o conhecimento é um emaranhado de significados que são construídos ao longo da vida, com a fixação de cada explicação e relacionando-a com outras, é possível transformar os acontecimentos em uma forma de aprendizado e montar uma construção sem fim.

Nesta linha de pensamento, pode-se dizer que a Gestão do Conhecimento auxilia no aprendizado sobre riscos, pois estes, embora muitas vezes pareçam, não são

aleatórios. Como o grau de incerteza é diretamente proporcional ao grau de desconhecimento a respeito do evento, é fundamental que as pessoas estejam em contínuo aprendizado, realizando a integração dos conhecimentos – tácitos (conhecimento subjetivo, criado a partir da vivência e das experiências do indivíduo) e explícitos (conhecimento formalizado) – e dos processos, pois as experiências de cada um são repensadas, de forma a criar uma aptidão para o aprendizado sobre riscos (APGAR *apud* LOREA; GRACIANI, 2007).

Mas é necessário criar um modelo que auxilie no processo de estruturação das informações, permitindo criar, armazenar, disseminar e proteger os conhecimentos adquiridos pelos auditores. Assim, os conhecimentos isolados sobre os sistemas, seus controles e riscos, criam o conhecimento organizacional.

3 Qual a relação de controles e análise de riscos?

O risco é definido por Paula (1999) como condições ou fatos significativos que podem criar uma situação de impossibilidade para a continuidade dos objetivos estabelecidos. Sob o foco das instituições financeiras, o risco “pode ser tudo o que impacta o capital, podendo ser oriundo de eventos, esperados ou não” (SPECCHIO *apud* KNECHT, 2003, p.61). Portanto, os ativos que possuem maiores possibilidades de prejuízos são vistos como mais arriscados que os ativos com menor possibilidade de prejuízos.

Embora as instituições financeiras apresentem diversos riscos, o operacional é o mais atuante deles (SILVA, 2006). Isto porque todos os processos podem apresentar erros e falhas que podem vir a ocasionar outros riscos, como o de imagem, legal, de crédito e mercado. Assim, é necessário estabelecer controles adequados e monitoramento de atividades críticas.

Para tal, existem os Controles Internos, instrumentos da organização destinados à vigilância, fiscalização e verificação administrativa, e que permitem prever, observar, dirigir ou governar os acontecimentos que são verificados dentro da empresa e que produzem reflexo no patrimônio, conforme a definição dada por Jund (2002). O autor destaca que, embora, o fato de um adequado sistema de controle interno ter por finalidade a prevenção de ocorrência de erros e falhas, ele não constitui uma garantia absoluta. Porém, objetiva minimizar a exposição dos bens da organização a possíveis erros e fraudes que possam ocorrer ou facilitar a sua identificação quando já ocorridas.

Silva (2006) argumenta que a finalidade dos controles internos é a gestão de riscos, e que a sua aplicação deve ser uma cultura da organização e não um procedimento isolado. Mas, os controles internos só serão eficazes se os riscos estiverem identificados. Para identificá-los deve-se considerar que os principais ativos das instituições financeiras são as informações, e, ainda, que estas se encontrem em sua maioria nos sistemas. Muito embora existam em diversas outras formas – impressa, escrita em papel, falada – é fato que estão expostas a um crescente número e variável de ameaças e vulnerabilidades. Assim, devem

ser identificados os riscos relacionados com as informações e os sistemas de informação, para assegurar proteção adequada.

4 A Segurança da Informação no processo de auditoria de sistemas

A área de conhecimento que trata da proteção das informações é chamada de Segurança da Informação e, conforme a NBR ISO/IEC 17799, abrange a informação, os processos, sistemas e redes. Portanto, a Segurança da Informação não é alcançada apenas por meios técnicos, mas também apoiada por uma gestão e por procedimentos apropriados de identificação de controles e associados à análise e avaliação de riscos.

Os princípios básicos de Segurança da Informação – confidencialidade, integridade e disponibilidade – permitem adotar controles e medidas de proteção à informação, reduzindo os riscos de vazamento e divulgação não autorizada da informação, fraudes financeiras, apropriação indevida de informações e reputação da imagem da instituição (FEBRABAN *apud* KNECHT, 2003).

Como a maior parte das informações estão armazenadas nos sistemas, e sendo a Auditoria responsável pela verificação da aplicação dos Controles Internos e pela salvaguarda dos ativos da organização, a verificação da Segurança da Informação deve fazer parte do escopo das auditorias de sistemas.

Cabe lembrar que para a efetiva Governança deve haver controles e monitoramento que garantam o atendimento dos objetivos da organização, bem como transparência para clientes e investidores. Porém, em muitos casos, as medidas de proteção recomendadas pela Auditoria de Sistemas acarretam em queda da capacidade de processamento, em função do acréscimo de verificações e procedimentos de segurança inseridos nos sistemas.

Assim, Beal (2004, p.55) sugere a elaboração e a documentação de análise de riscos dos recursos informacionais e de TI a serem protegidos, com a escala de riscos a que estão sujeitos e as conseqüências para o negócio, caso esses recursos venham a ser comprometidos. Dessa forma, facilita o convencimento da alta direção de que a prevenção não somente é o caminho mais responsável, mas também o mais barato a longo prazo.

Com intuito de auditar os sistemas, avaliando a aplicação dos controles internos e a Segurança da Informação, o planejamento de Auditorias de Sistemas é fundamentado na análise de risco dos sistemas. A descrição dos procedimentos metodológicos e as etapas do trabalho estão descritas no próximo capítulo.

5 Metodologia

O estudo partiu de uma abordagem qualitativa que, conforme argumenta Roesch (1999), apresenta métodos de coleta e análise de dados apropriados para uma fase exploratória da pesquisa, quando se trata de melhorar a efetividade de um

programa. Para completar a escolha do método, utilizou-se a pesquisa-ação, definida como uma técnica apropriada para construir teoria para a prática (ROESCH, 1999).

Com a reunião dos conhecimentos tácitos e explícitos dos auditores de sistemas, foi modelado um roteiro para estruturar os dados, que em sua maioria foram coletados através da técnica de pesquisa documental. Também foram utilizadas técnicas de questionário e reunião.

5.1 Roteiro de Auditoria de Sistemas em Produção

Como parte da metodologia, foi desenvolvido um roteiro de Auditoria de Sistemas em Produção, com objetivo de ser um dos papéis de trabalho, ou seja, ferramenta utilizada para documentar os testes e verificações no decorrer da auditoria. O roteiro, adaptado com base na NBR ISO/IEC 17799, é composto de 10 controles macros, classificados com a propriedade de Segurança da Informação mais atuante em cada controle, recebendo um peso para compor a pontuação total dos sistemas, conforme mostra o Quadro 1:

Nº	Controle Macro	Propriedade Seg. Informação	%	
1	Avaliação da situação cadastral de acesso e segregação de função	Confidencialidade	25%	60%
2	Avaliação da segurança de acesso	Confidencialidade		
3	Análise de trilhas de auditoria	Não Repúdio	10%	
4	Análise de documentação do sistema	Disponibilidade	25%	
5	Avaliação da contingência	Disponibilidade		
6	Verificação de ocorrências e manutenções sistêmicas	Integridade	40%	40%
7	Avaliação das rotinas de crítica de entrada e consistência de dados	Integridade		
8	Avaliação de rotinas de processamento e interfaces	Integridade		
9	Avaliação da base de dados	Integridade		
10	Avaliação dos dados de saída	Integridade		

Quadro 1: Ponderação dos controles do roteiro
Fonte: Resultado do estudo

Cada controle macro é composto de pontos de controle, e estes, por sua vez, apresentam um conjunto dinâmico de testes e verificações, bem como as normas, leis, resoluções ou melhores práticas associadas. Os testes e verificações aplicados são descritos e apresentam, ainda, a situação encontrada, que conseqüentemente está relacionada com um grau de risco. A Figura 1 apresenta a estrutura do roteiro, que permite a formalização dos testes aplicados, a situação encontrada, bem como possíveis recomendações.

1 - AVALIAÇÃO DA SITUAÇÃO CADASTRAL DE ACESSO E SEGREGAÇÃO DE FUNÇÃO

Ponto de Controle	Teste/Verificação	Comentários	Situação	Normas Associadas	Recomendações
1.1 Verificar se existe procedimento formal para cadastramento e descadastramento de acesso de usuários no sistema, tendo por objetivo o controle da concessão de direitos de acesso.	Descrição Teste 1.1.1	Verificando os formulários existentes....		ISO 17799 9.2.1, IN 32 Títulos 51.3.3 e 51.3.10.	
	Descrição Teste 1.1.2	O teste realizado, com a solicitação de cadastramento do usuário Bxxxxx comprovou...			
	Descrição Teste 1.1.3	Analisando X formulários, selecionados através de amostragem, ...			Recomenda-se a utilização de....
	Descrição Teste 1.1.4	Conforme auditoria nº XXX, que avaliou...			
	Descrição Teste 1.1.5	Verificou-se que			
1.2 Analisar os usuários cadastrados no sistema quanto a necessidade do acesso, com a finalidade de controlar e permitir o acesso somente àqueles que necessitam para o devido desempenho na atual função.	Descrição Teste 1.2.1	Verificou-se através de ...		ISO 17799 item 9.2.1, IN 32 Títulos 51.3.3 e 51.3.10.	
	Descrição Teste 1.2.2	A análise realizada...			
	Descrição Teste 1.2.3	Em análise dos N usuários cadastrados no sistema ...			Recomenda-se que ....
	Descrição Teste 1.2.4				
	Descrição Teste 1.2.5				
1.3 Analisar os usuários cadastrados quanto à situação atual, verificando se os funcionários exonerados, aposentados, com contrato encerrado e impedidos, foram removidos do sistema.	Descrição Teste 1.3.1			ISO 17799 item 9.2.1, IN 32 Títulos 51.3.3 e 51.3.2.	
	Descrição Teste 1.3.2				
	Descrição Teste 1.3.3				
1.4 Analisar	Descrição Teste 1.4.1			ISO 17799 item 9.2.1, IN 32 Títulos 51.3.3 e 51.3.2.	
	Descrição Teste 1.4.2				
	Descrição Teste 1.4.3				
	Descrição Teste 1.4.4				

Capa de Apresentação | 1. Cadastro e Segregação | 2.Segurança de Acesso | 3.Trilhas de Auditoria (logs) | 4.Documentação | 5.Contingência | 6. C

Figura 1: Vinculação de pontos de controle e testes nos controles macros
Fonte: Adaptação do roteiro de Auditoria de Sistemas em Produção de uma instituição financeira

5.2 Identificando o grau de risco

Considerando as situações possíveis definidas para os testes, e o fato que mesmo com o controle existente e aplicado o risco existe, e, ainda, com base no grau de risco definido por Cassarro (1997), estabeleceu-se as seguintes relações para os testes:

- **Atendido – risco baixo:** a situação do teste ou verificação está plenamente atendido;
- **Parcialmente atendido – risco médio:** há controle aplicado na maioria das vezes;
- **Não atendido – risco alto:** constatou-se que não se encontra atendido;
- **Avaliado em outra auditoria - risco conforme estabelecido na outra auditoria:** deve ser repetida a situação encontrada na auditoria que avaliou o ponto;
- **Fora do escopo – risco alto:** o ponto de controle não está no escopo de avaliação;
- **Não se aplica** – **sem risco associado:** controle não necessário.

5.3 Avaliando a relevância do sistema

Além de atribuir o risco que cada ponto de controle pode apresentar, é necessário avaliar e mensurar a importância dos sistemas. Assim, deve-se classificar o sistema quanto a sua função, havendo três possibilidades:

- **Operacional**: classificação dada para um sistema de informação que trata as informações rotineiras da organização;
- **Gerencial**: é o sistema de informação que agrupa dados provenientes das operações da organização de forma a facilitar a tomada de decisão pelos gestores;
- **Genérico**: sistema que não existe por si só, foi criado para outros sistemas utilizarem, unificando informações e processos repetidos e necessários para diversos outros sistemas.

Se o sistema for classificado como operacional ou gerencial, é necessário avaliar, ainda, se o sistema:

- É de vital importância operacional para a instituição;
- Conduz/controla ativos e/ou passivos financeiros;
- Dá suporte a processos corporativos (com impacto nas agências da rede);
- É de ordem legal (BACEN, CVM etc);
- Terá impacto em outros sistemas já operacionais.

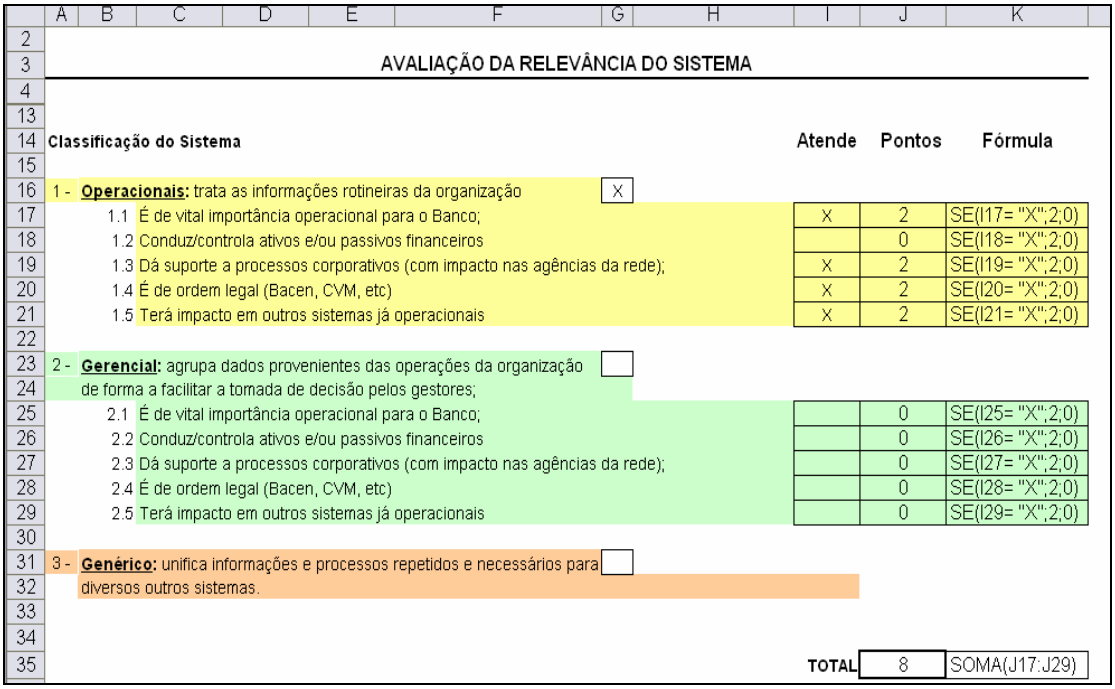
5.4 Indicadores de risco e relevância

Coletadas as informações dos sistemas e estruturadas no roteiro, é possível hierarquizar o risco e relevância de cada sistema. Para tanto, foram definidas formas de mensuração do risco e da relevância, com a criação de indicadores.

Para obter o indicador de relevância do sistema, é considerada a quantidade de afirmações verdadeiras que o sistema atende, dentro da sua classificação. Para cada afirmação que o sistema se enquadra, é somado 2 (dois) pontos, conforme mostra Figura 2.

O indicador de risco do sistema é resultante da situação dos testes e verificações, que obtém a pontuação conforme o grau de risco:

- Risco baixo = 1 ponto;
- Risco médio = 5 pontos;
- Risco alto = 10 pontos;
- Não se aplica = 0 ponto.

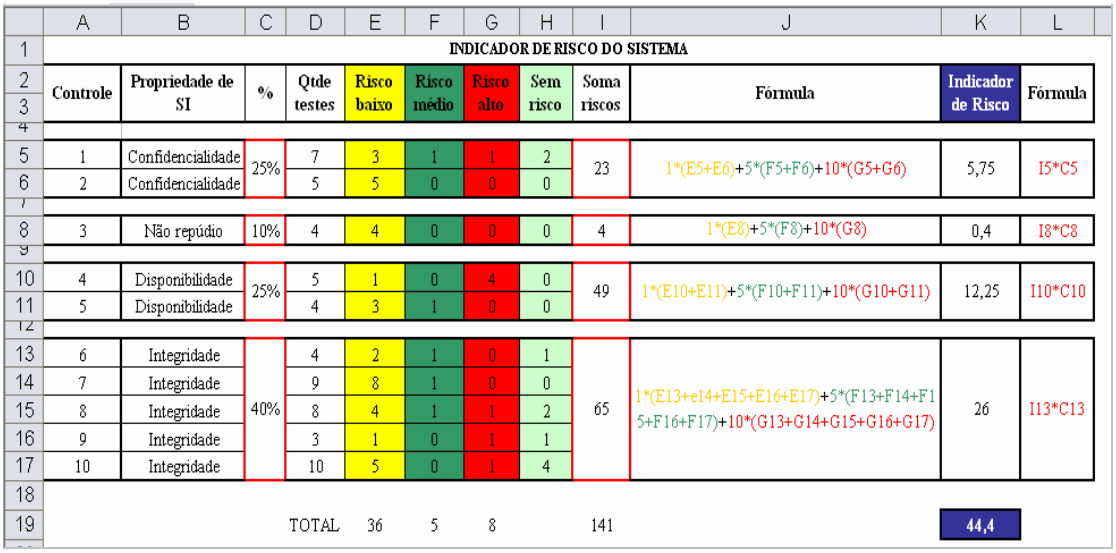


AVALIAÇÃO DA RELEVÂNCIA DO SISTEMA

Classificação do Sistema	Atende	Pontos	Fórmula
1 - **Operacionais:** trata as informações rotineiras da organização	X		
1.1 É de vital importância operacional para o Banco;	X	2	SE(I17= "X";2;0)
1.2 Conduz/controla ativos e/ou passivos financeiros		0	SE(I18= "X";2;0)
1.3 Dá suporte a processos corporativos (com impacto nas agências da rede);	X	2	SE(I19= "X";2;0)
1.4 É de ordem legal (Bacen, CVM, etc)	X	2	SE(I20= "X";2;0)
1.5 Terá impacto em outros sistemas já operacionais	X	2	SE(I21= "X";2;0)
2 - **Gerencial:** agrupa dados provenientes das operações da organização de forma a facilitar a tomada de decisão pelos gestores;			
2.1 É de vital importância operacional para o Banco;		0	SE(I25= "X";2;0)
2.2 Conduz/controla ativos e/ou passivos financeiros		0	SE(I26= "X";2;0)
2.3 Dá suporte a processos corporativos (com impacto nas agências da rede);		0	SE(I27= "X";2;0)
2.4 É de ordem legal (Bacen, CVM, etc)		0	SE(I28= "X";2;0)
2.5 Terá impacto em outros sistemas já operacionais		0	SE(I29= "X";2;0)
3 - **Genérico:** unifica informações e processos repetidos e necessários para diversos outros sistemas.			
TOTAL		8	SOMA(J17:J29)

Figura 2: Indicador de relevância dos sistemas
Fonte: Simulação de dados

Multiplicando a pontuação do risco pela quantidade de cada grau de risco, agrupados pelas propriedades da Segurança da Informação, obtém-se a soma de riscos. A soma é multiplicada pelo percentual correspondente da propriedade e o resultado de cada propriedade é somado, obtendo-se o indicador de risco do sistema, conforme a Figura 3:



INDICADOR DE RISCO DO SISTEMA

Controle	Propriedade de SI	%	Qtde testes	Risco baixo	Risco médio	Risco alto	Sem risco	Soma riscos	Fórmula	Indicador de Risco	Fórmula
1	Confidencialidade	25%	7	3	1	1	2	23	1*(E5+E6)+5*(F5+F6)+10*(G5+G6)	5,75	I5*C5
2	Confidencialidade		5	5	0	0	0				
3	Não repúdio	10%	4	4	0	0	0	4	1*(E8)+5*(F8)+10*(G8)	0,4	I8*C8
4	Disponibilidade	25%	5	1	0	4	0	49	1*(E10+E11)+5*(F10+F11)+10*(G10+G11)	12,25	I10*C10
5	Disponibilidade		4	3	1	0	0				
6	Integridade	40%	4	2	1	0	1	65	1*(E13+e14+E15+E16+E17)+5*(F13+F14+F15+F16+F17)+10*(G13+G14+G15+G16+G17)	26	I13*C13
7	Integridade		9	8	1	0	0				
8	Integridade		8	4	1	1	2				
9	Integridade		3	1	0	1	1				
10	Integridade		10	5	0	1	4				
		TOTAL		36	5	8		141		44,4	

Figura 3: Indicador de risco
Fonte: Simulação de dados

Com objetivo de testar a metodologia desenvolvida, foram selecionadas 12 auditorias já ocorridas, que tiveram as informações analisadas e estruturadas no roteiro. Os resultados obtidos estão descritos no próximo capítulo.

6 Análise de Resultados

Para realizar a análise dos resultados, inicialmente, foram comparados os indicadores de risco e relevância, e depois realizadas simulações com base na quantidade de testes dos sistemas selecionados e as possibilidades do risco associado para cada teste. Também se identificou, através de análises, outras aplicações dos resultados desta metodologia.

6.1 Análise da hierarquia dos indicadores

Para analisar a adequação dos resultados dos indicadores, os sistemas foram agrupados por tipo, e, os indicadores inseridos em uma planilha, com as informações ordenadas de três formas: pela soma dos indicadores, pelo risco e pela relevância. Na Figura 4 são apresentadas as comparações entre os sistemas, sendo que o cabeçalho em letra vermelha indica o critério de ordenação.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Sistemas Operacionais					Sistemas Operacionais					Sistemas Operacionais			
2	Sistema	Relevância	Risco	Soma		Sistema	Relevância	Risco	Soma		Sistema	Relevância	Risco	Soma
3	YHN	10	70,1	80,1		YHN	10	70,1	80,1		YHN	10	70,1	80,1
4	WDF	10	63,15	73,15		WAL	6	64,5	70,5		WDF	10	63,15	73,15
5	WAL	6	64,5	70,5		WDF	10	63,15	73,15		FVN	8	44,4	52,4
6	POL	6	62,25	68,25		POL	6	62,25	68,25		ASX	8	32,5	40,5
7	FVN	8	44,4	52,4		FVN	8	44,4	52,4		MQW	8	30	38
8	RFT	4	44,35	48,35		RFT	4	44,35	48,35		PTO	8	25,05	33,05
9	ASX	8	32,5	40,5		ASX	8	32,5	40,5		WAL	6	64,5	70,5
10	MQW	8	30	38		MQW	8	30	38		POL	6	62,25	68,25
11	PTO	8	25,05	33,05		PTO	8	25,05	33,05		RFT	4	44,35	48,35
12														
13														
14	Sistemas Gerencias					Sistemas Gerencias					Sistemas Gerencias			
15	Sistema	Relevância	Risco	Soma		Sistema	Relevância	Risco	Soma		Sistema	Relevância	Risco	Soma
16	CFD	6	65	71		CFD	6	65	71		KEW	8	31,2	39,2
17	GJK	4	41	45		GJK	4	41	45		CFD	6	65	71
18	KEW	8	31,2	39,2		KEW	8	31,2	39,2		GJK	4	41	45
19														
20														

Figura 4: Comparação de hierarquização
Fonte: Resultados da pesquisa. As siglas dos sistemas foram alteradas.

Como pode ser visto, nenhum dos sistemas selecionados para a coleta de informações foi classificado como sistema genérico, 3 são gerenciais e 9 operacionais.

Basicamente, foram comparados os sistemas conforme as ordenações resultantes, bem como a mudança de posição em relação ao critério de ordenação. Como exemplo, observou-se o sistema YHN, que se encontra no topo independente do critério de ordenação. Já o WDF, que da segunda posição na ordenação por soma e relevância, cai para a terceira em função do risco. Já o sistema PTO, na nona posição pelas ordenações de soma e risco, sobe para sexta colocação em função da relevância.

Após análise e discussão dos resultados dos indicadores, conclui-se que a hierarquização se mostra adequada e da forma que foi apresentada, cabe direcionar o foco individual – risco ou relevância – ou o consolidado – soma. Cabe lembrar que o conhecimento tácito dos auditores foi fundamental para a validação dos resultados, bem como a análise de ocorrências ou não com os sistemas.

6.2 Simulação para descoberta de padrões

Ainda que a metodologia desenvolvida para indicar os sistemas a serem priorizados no planejamento de auditorias tenha se mostrada adequada, ela foi realizada pela comparação entre os sistemas. Objetivando identificar faixas de risco dos indicadores, ou seja, se o do sistema apresenta um indicador de risco alto ou não, foram realizadas algumas simulações.

A primeira simulação considerou todos os testes válidos, de todos os controles com risco alto, a segunda com risco médio e a terceira com risco baixo. Partindo das simulações, foram realizadas algumas análises e identificou-se o menor número de testes aplicados, o maior e a média. Consequentemente foram identificadas faixas de valores as quais os indicadores de risco se enquadram em função do risco estabelecido.

Na Figura 5 é apresentado um comparativo do indicador real obtido para os sistemas com as simulações dos testes válidos com cada grau de risco.

	P	Q	R	S	T	U	V
246							
247			real	simulação			
248	sistemas	testes válidos	indicador risco	risco baixo	risco médio	risco alto	
249	MQW	41	30	12,2	61	122	
250	RFT	42	44,35	13,5	67,5	135	
251	POL	44	62,25	14,9	74,5	149	
252	KEW	45	31,2	14,25	71,25	142,5	
253	ASX	48	32,5	15,15	75,75	151,5	
254	PTO	48	25,05	15,3	76,5	153	
255	FVN	49	44,4	15,55	77,75	163,5	
256	WDF	50	63,15	15,35	76,75	153,5	
257	WAL	50	64,5	15,8	79	158	
258	GJK	54	41	16,35	81,75	163,5	
259	CFD	57	65	16,8	84	168	
260	YHN	66	70,1	21,15	105,75	211,5	

Figura 5: Descoberta de padrões
Fonte: Resultados da pesquisa

Observa-se que mesmo com igual quantidade de testes, sistemas ASX e PTO, o indicador resultante nas simulações foi diferente, pois a variação de testes está nos controles que compõem uma propriedade de Segurança da Informação. Assim, como o valor do risco é multiplicado pelo percentual que corresponde àquela propriedade, os valores serão diferentes, porém com pouca variação.

Nas simulações realizadas, pôde ser visto que a quantidade de testes variou de 41 a 66, porém a faixa do indicador de risco fica de 12,2 a 21,15 quando considerado o grau de risco baixo para todos os testes. Para testes com grau de risco médio o indicador variou de 61 a 105,75, ficando quase próximo do indicador com risco alto, de 122 a 211,5.

Com essa forma de apresentar os dados, conclui-se que, embora exista variação na quantidade de testes realizados, existe um padrão em relação à faixa de valores. Dessa forma, pode-se dizer que o sistema MQW apesar de ser o que possui menor quantidade de testes, tem a maior parte deles com grau risco baixo. Pois, considerando que apresentou grau de risco real 30, e pelos parâmetros da simulação de risco baixo para o próprio sistema de 12,2 e médio 61, e ainda, o maior resultado para testes do risco baixo como 21,15 e o menor de risco médio 61, pode-se dizer que no grupo, está com grau de risco baixo. Da mesma forma, o YHN, que apresentou indicador de risco real 70,1 e possui o maior número de testes, pode ser considerado como um sistema com indicador de grau de risco médio. Já o PTO com 48 testes, está com risco baixo, pois apresenta indicador menor que o MQW.

Assim, mesmo considerando que as auditorias podem apresentar quantidades de testes diferentes, o que altera o indicador de risco do sistema, é possível classifica-lo em função da média do indicador.

6.3 Escopo de auditorias

A metodologia desenvolvida para hierarquizar os sistemas pode contribuir, também, para definição de escopo de auditorias, pela comparação da aplicação de controles. Conforme apresentado na Figura 6, foram aplicados 18 testes para a verificação de confidencialidade, e destes, 11 apresentam risco alto.

RISCO DO SISTEMA									
Nº Controle	Propriedade de SI	%	Qtde testes	Risco baixo	Risco médio	Risco alto	Sem risco	Soma riscos	Indicador de Risco
1	Confidencialidade	25%	10	3	1	6	0	125	31,25
2	Confidencialidade		8	2	1	5	0		
3	Não repúdio	10%	4	4	0	0	0	4	0,4
4	Disponibilidade	25%	5	4	0	0	1	16	4
5	Disponibilidade		3	2	0	1	0		
6	Integridade	40%	7	6	0	0	1	44	17,6
7	Integridade		5	3	1	0	1		
8	Integridade		4	4	0	0	0		
9	Integridade		7	5	1	0	1		
10	Integridade		4	1	1	1	1		
			TOTAL	34	5	13		189	53,25

Figura 6: Análise dos controles para definição de escopo de auditorias
Fonte: Simulação de dados

Mesmo considerando que o sistema não apresenta um indicador de risco tão expressivo, poderá ser priorizado no planejamento de auditorias, porém com escopo menor. Dessa forma, a auditoria é realizada em curto espaço de tempo com foco apenas nestes controles mais frágeis.

7 Considerações finais

Com a utilização do roteiro como papel de trabalho, vinculado com a metodologia proposta, é possível, ao finalizar o preenchimento do roteiro, quantificar os riscos presentes no sistema objeto da auditoria e paralelamente avaliar a importância do sistema para a organização.

Ainda há a possibilidade de realizar análise comparativa da situação dos controles para diversos sistemas. Ao analisar as informações obtêm-se diversos conhecimentos que poderão ser aplicados para definição de escopo das auditorias, ou ainda para identificar que um processo, semelhante em diversos sistemas, está falho. Esta comparação entre sistemas é muito útil, pois permite quantificar e demonstrar, de forma resumida a situação que os controles se encontram nos sistemas. Mas deve-se lembrar que a relevância do sistema sempre deve ser considerada.

Destacam-se, também, as vantagens de manter os conhecimentos formalizados, estruturados, sem demandar esforço para a coleta dos dados específicos para avaliar os sistemas e realizar planejamento de auditorias, e avaliação contínua dos riscos. Acrescenta-se, ainda, que a organização estará se adequando à tendência e as regulamentações de trabalhar com foco na gestão dos riscos.

Porém, é importante haver um roteiro padronizado de pontos de controles, testes e verificações, bem como conceitos e definições bem claras para todos os auditores. Além, disso, o ideal é ter um repositório único dos roteiros, de forma a finalizar o seu preenchimento e já ter o sistema sendo comparado com os demais, bem como o mesmo sistema em outro período, avaliando as melhorias realizadas.

Assim, pode-se dizer que esta metodologia apresenta diversas vantagens indo além da aplicação no planejamento anual de auditorias. Ela é capaz de ser uma ferramenta de agregação de conhecimento, pois as informações são disponibilizadas permitindo diversas análises da situação dos controles nos sistemas. E com uma base maior de informações dos sistemas, acredita-se que outras descobertas de conhecimento possam ser realizadas. Porém, é importante formalizar estes conhecimentos, para a disseminação e posterior internalização do conhecimento pelos indivíduos. Assim, este ciclo de criação de conhecimento organizacional não tem fim.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799: Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da Informação.** Apresentação. Rio de Janeiro, 2005.

BEAL, Adriana. **Gestão Estratégica da Informação: como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações.** São Paulo: Atlas, 2004.

CASSARRO, Antonio Carlos. **Controles Internos e segurança de sistemas: prevenindo fraudes e tornando auditáveis os sistemas.** São Paulo: LTr, 1997.

FERNANDES, Liliam Grieger. **Gestão do Conhecimento Aplicada ao Planejamento de Auditoria de Sistemas com Ênfase na Análise de Riscos.** 2007. 87 f. Monografia (conclusão do curso) – Universidade de Caxias do Sul, Pró-Reitoria de Pós Graduação e Pesquisa, Caxias do Sul.

INSTITUTO BRASILEIRO DE GOVERNAÇA CORPORATIVA. Disponível em <http://www.ibgc.org.br>. Acesso em: 16 dez. 2007.

JUND, Sergio. **Auditoria: conceitos, normas técnicas e procedimentos.** Rio de Janeiro: Impetus, 2002.

KNECHT, Genise Maria. **Metodologia de Avaliação de Riscos de sistemas Informatizados para Planejamento das Atividades de Auditoria.** 2003. 149 f. Monografia (conclusão de curso) – Pontifícia Universidade Católica do Rio Grande do Sul – Faculdade de Administração, Contabilidade e Economia – Curso de Ciências Contábeis, Porto Alegre.

LOREA, Eduardo; GRACIANI, Marcos. **Obras do acaso: Apesar da natural aversão a perdas, a maioria dos empresários brasileiros ainda não aderiu à gestão de risco com ferramentas capazes de mitigar o poder do acaso nos acidentes.** Amanhã, Edição 229 de mar. 07. Disponível em <http://amanha.terra.com.br/edicoes/229/capa01.asp>. Acesso em: 29 mar. 2007.

PAULA, Maria Goreth Miranda Almeida. **Auditoria Interna: embasamento conceitual e suporte tecnológico.** São Paulo: Editora Atlas, 1999.

ROESCH, Sylvia Maria Azevedo. **Projetos de estágio e de pesquisa em administração: guias para estágio, trabalhos de conclusão, dissertações e estudos de caso.** São Paulo: Editora Atlas, 1999.

SERMOND, Graça. **Quem se arrisca?** Risk Report, São Paulo, Ano 1, n.2, p.3, set./out. 2007.

SILVA, Antonio Luiz Scorsi. **Controles Internos**. FEDERAÇÂO BRASILEIRA DOS BANCOS, 2006.

ZABOT, João Batista M.; Silva, L.C. Mello. **Gestão do conhecimento: aprendizagem e tecnologia: Construindo a Inteligência Coletiva.** São Paulo Atlas, 2002.