

UNIVERSIDADE LUTERANA DO BRASIL

ULBRA – *CAMPUS* GUAÍBA

CURSO DE SISTEMAS DE INFORMAÇÃO



**METODOLOGIA PARA VALIDAÇÃO DE
EVIDÊNCIAS EM AUDITORIA DE SISTEMAS**

RELATÓRIO DO ESTÁGIO CURRICULAR

MIGUEL ÂNGELO CHAGAS NEUMANN

Guaíba, junho de 2007.

Local de Estágio: Banco do Estado do Rio Grande do Sul SA

Supervisor na Empresa: Genise Knecht

Endereço: Rua Caldas Júnior, 108, 5 andar CEP 90018900

Porto Alegre, RS

E-mail: genise_knecht_ofc@banrisul.com.br

Fone(s): (51) 32152930

SUMÁRIO

1	INTRODUÇÃO.....	5
2	APRESENTAÇÃO DA EMPRESA	7
3	FUNDAMENTAÇÃO TEÓRICA.....	8
4	SOLUÇÃO IMPLEMENTADA	12
5	CONCLUSÕES E RESULTADOS ALCANÇADOS	19
6	REFERÊNCIAS BIBLIOGRÁFICAS	20

ÍNDICES DE ILUSTRAÇÕES

ILUSTRAÇÃO 1 - VALIDAÇÃO DA EVIDÊNCIA	14
ILUSTRAÇÃO 2 - DIMENSÕES PARA VALIDAÇÃO DA TÉCNICA DE AUDITORIA	14
ILUSTRAÇÃO 3 - DESCRIÇÃO DA EVIDÊNCIA	17
ILUSTRAÇÃO 4 - DESCRIÇÃO DA EVIDÊNCIA COMENTADA.....	18

ÍNDICES DE TABELAS E QUADROS

TABELA 1 - BANCO DO ESTADO DO RIO GRANDE DO SUL	7
TABELA 2 - O BANRISUL EM NÚMEROS	7
TABELA 3 - O BANRISUL EM NEGÓCIOS	7
TABELA 4 - QUADRO DOS ITENS A REGISTRAR POR TÉCNICA DE AUDITORIA	15
TABELA 5 - QUADRO DOS ITENS POR DIMENSÃO	16

1 INTRODUÇÃO

A rede de relacionamentos constituída atualmente impõem que organizações implementem padrões e melhores práticas em tecnologia da informação e comunicações.

Crises em determinada entidade, além de afetar os colaboradores internos e parceiros, podem atingir organismos separados econômica, administrativa ou politicamente.

Nesse sentido, padrões como CMMI, PMI, COBIT, ITIL, SOX, COSO, ISOs e Basiléia são cada vez mais utilizados e em algumas situações, impostos pela legislação ou pelo mercado.

Eventualmente, trabalhos de auditoria de sistemas possuem conseqüências, tais como alterações contratuais, redefinições de requisitos e demissões, que são passíveis de contestação judicial. Portanto, ao realizarmos nossas considerações sobre os pontos de auditoria, devemos ter presente o esgotamento do uso de subsídios técnicos e jurídicos.

Com o presente estudo, pretendo possibilitar que os trabalhos de auditoria possuam a devida eficácia jurídica, baseando-os em métodos e técnicas válidos, já utilizados em forense computacional.

A ISO17799:2005, 13.2.3 Coleta de evidências, diz: *“Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas, armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição(ões) pertinente(s)”*.

As Normas Brasileiras de Contabilidade, emitidas pelo CFC, título 12.1.2 – Procedimentos da Auditoria Interna, definem:

“12.1.2.1 – Os procedimentos de auditoria interna são os exames, incluindo testes de observância e testes substantivos, que permitem ao auditor interno obter provas suficientes para fundamentar suas conclusões e recomendações.

12.1.2.2 – Os testes de observância visam a obtenção de uma razoável segurança de que os controles internos estabelecidos pela administração estão em efetivo funcionamento, inclusive quanto ao seu cumprimento pelos funcionários da Entidade.

12.1.2.3 – Os testes substantivos visam à obtenção de evidência quanto à suficiência, exatidão e validade dos dados produzidos pelos sistemas de informações da Entidade.

12.1.2.4 – As informações que fundamentam os resultados da auditoria interna são denominadas de "evidências", que devem ser suficientes, fidedignas, relevantes e úteis, de modo a fornecerem base sólida para as conclusões e recomendações.”

O título 3.3.21 Conformidades a Serem Analisadas pela Auditoria Interna, da Instrução Normativa 55 (Política de Segurança da Informação do Banrisul SA) define: “Devem ser elaborados procedimentos e instruções de trabalho que garantam que estão sendo geradas evidências adequadas, em caso de necessidade, para apoiar um processo jurídico contra uma pessoa ou organização.”.

Ou seja, os processos de gestão adequada de evidências, possuem obrigação normativa, inclusive interna, para implementação no Banrisul.

2 APRESENTAÇÃO DA EMPRESA

O Banrisul é uma empresa focada na promoção do desenvolvimento econômico e social do Estado do Rio Grande do Sul. Como banco múltiplo, opera nas áreas comercial, de desenvolvimento e social, atendendo a todos os segmentos da sociedade gaúcha.

Banco do Estado do Rio Grande do Sul

Espécie	Sociedade de Economia Mista, constituída sob forma de Sociedade Anônima
Foco de atuação	Região Sul do Brasil
Data de fundação	12 de setembro de 1928
Perfil dos clientes	Pessoas físicas, micro, pequenas, médias e grandes empresas
Ramo de atividade	Instituição financeira, bancária, atuando como banco múltiplo nas carteiras: comercial, crédito financiamento e investimento, crédito imobiliário, desenvolvimento, arrendamento mercantil e investimento
Número de colaboradores	8.967

Tabela 1 - Banco do Estado do Rio Grande do Sul

O Banrisul em números

	2005	2006
Cobertura no Estado	77% dos municípios	78% dos municípios
Número de Agências	401	415
Postos de Atendimento	290	286
Banrisul Eletrônico	351	361

	2004	2005	2006
Número de clientes	2,8 milhões	2,9 milhões	2,9 milhões

Tabela 2 - O Banrisul em números

Resultado positivo

Em 2006, o Banrisul registrou lucro líquido de R\$ 361,7 milhões, o que correspondeu a uma rentabilidade de 27,9% sobre o patrimônio líquido final de R\$ 1,3 bilhão.

O Banrisul em negócios

	2005	2006
Conveniados Banricompras	34,7 mil	41,3 mil
Agência Virtual (transações)	69 milhões	69,5 milhões
Transações Eletrônicas	262 milhões	275,8 milhões
Lucro Líquido	R\$ 351,9 milhões	R\$ 361,7 milhões
Patrimônio Líquido	R\$ 1,1 bilhão	R\$ 1,3 bilhão

Tabela 3 - O Banrisul em negócios

3 FUNDAMENTAÇÃO TEÓRICA

Controles Internos

Os controles internos são parte do processo administrativo. São formas de gerenciar o risco, incluindo políticas, procedimentos diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal [ISO17799].

Compõe um plano de organização e todos os métodos e medidas coordenadas, adotados numa empresa para:

- salvaguardar os ativos de prejuízos decorrentes de fraudes ou erros não intencionais;
- incrementar a eficiência operacional e promover a obediência às normas estabelecidas pela administração.

Auditoria de Sistemas

Um dos itens que compõe os Controles Internos é a Auditoria[Res BACEN 2554], constituída pelo conjunto de procedimentos técnicos que tem por objetivo examinar a integridade, adequação e eficácia dos controles internos[Res CFC 986/03].

Ao objeto reconhecidamente importante para análise no trabalho de auditoria, chamamos de Ponto de Controle. O ponto de controle pode ser um banco de dados, uma coluna de tabela, um item de conformidade, uma rotina de software, algo que sofrerá um teste de conformidade.

O trabalho de auditoria é executado com uma metodologia, utiliza técnicas e ferramentas para realizar os exames necessários e é documentado através de papéis de trabalho.

As Auditorias podem ter origem:

- Externa – realizada por instituição externa e independente da empresa auditada;
- Interna – realizada por departamento interno, independente e ligado ao órgão máximo de decisão interno;
- Mista – realizada em conjunto por auditorias interna e externa.

No caso de Auditoria Interna, os trabalhos são executados conforme o Planejamento Anual da Auditoria e situações que necessitem averiguações específicas são realizadas através de verificações especiais.

Com o avanço dos sistemas computacionais, que passaram a realizar todos os principais processos corporativos, o auditor necessitou se especializar em sistemas de informação. Surgiu então, a Auditoria de Sistemas, que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais de uma determinada entidade.

Como o ambiente de informática possui características bastante particulares, o auditor de sistemas utiliza metodologia, técnicas, ferramentas e papéis de trabalho próprios.

Dentre as principais técnicas de auditoria de sistemas, podemos citar:

- Questionário – Conjunto de perguntas para verificar um ponto de controle. Pode ser via rede, formulário impresso, in loco etc;
- Simulação de dados – Submissão de um conjunto de dados de teste no sistema;
- Visita in loco – Visita do auditor às instalações físicas do auditado;
- Mapeamento estatístico – Verificar rotinas mais utilizadas, desativadas etc;
- Rastreamento – Listar o caminho de uma transação durante a execução de um programa(debug);
- Entrevista – Visita ao auditado visando verificar pontos de controle;
- Análise de relatório / tela – Verificar adequação às regras de negócio, usabilidade, eficácia etc;
- Simulação paralela – Utilização de dados de produção em ambientes que simulam as funções do sistema para verificar os resultados obtidos;
- Análise de log – Verificar se os registros de log contém as informações necessárias à trilha de auditoria;
- Checklist – Lista de itens a serem verificados em ação do auditor;
- Análise de programa fonte – “Leitura” dos comandos do código fonte, análise dos fluxos e diagramas, identificação de vícios de programação;
- Snapshot – Fotografia de determinado momento de execução do sistema para verificar variáveis, processos etc.

De acordo com o objeto auditado, as Auditorias de Sistemas podem ser classificadas em:

- Auditoria de Rede – Comunicação, servidores, switches etc;
- Auditoria de Microinformática – Estações de trabalho, aplicativos, suítes de escritório etc;
- Auditoria de Sistemas em Desenvolvimento – Metodologias, ferramentas, padrões etc;
- Auditoria de Sistemas em Produção – Conformidade, adesão ao negócio, controles internos etc;
- Auditoria de Sistemas em Manutenção – Avaliar correção de rotinas, implementação de funcionalidades novas etc;
- Auditoria em Produtos – Avaliar softwares de fornecedores terceirizados;
- Auditoria em Processos – Verificar se os processos estão desenhados conforme as necessidades de negócio, legais etc;
- Auditoria em Ambientes – Verificação onde o objeto auditado abrange várias plataformas ou sistemas que, superficialmente, não possuem associação. Por exemplo o ambiente anti-vírus de uma empresa.

Dentre as principais atividades dos Auditores de Sistemas podemos elencar: revisão de sistemas aplicativos em produção, revisão de desenvolvimento e manutenção de sistemas aplicativos, redesenho de processos, revisão de *data centers*, revisão da eficiência de TI, revisão de segurança em redes corporativas, revisão de segurança em gerenciamento de banco de dados, planos de contingência, revisão de aderência à política de segurança, interfaces EDI, planos de continuidade de negócios, auxílio à auditoria externa, revisão de trilhas de auditoria e auxílio à auditoria interna operacional.

O resultado do trabalho do auditor é o relatório de auditoria, documento no qual constam as avaliações e recomendações de auditoria.

Evidências de auditoria

Para verificar os controles, o auditor utiliza informações coletadas por ele mesmo ou fornecidas por terceiros, muitas vezes pelo próprio auditado.

Ocorre que muitas auditorias e verificações especiais, resultam em processos judiciais, o que cria a necessidade de garantir a autoria e integridade na utilização, armazenamento, transporte de informações e das conclusões apresentadas sobre as evidências analisadas.

As constatações do auditor podem ter origem:

- i. De observações do ambiente – o auditor realiza suas constatações verificando o ambiente;
- ii. De extração de documentos – as constatações são extraídas diretamente de arquivos recebidos;
- iii. Do auditado ou de terceiros – as informações são recebidas de outros;
- iv. De análises do auditor – as constatações são originadas por cálculos, interpretações e comparações do auditor.

Documento

As evidências são originadas a partir de arquivos e documentos acessados pelo auditor.

Existem vários significados para a palavra documento. Dentre eles podemos citar:

“Unidade de registro de informações qualquer que seja o suporte ou formato.”

Dicionário Brasileiro de Terminologia Arquivística, do Arquivo Nacional

“1 Instrumento escrito que, por direito, faz fé daquilo que atesta; escritura, título, contrato, certificado, comprovante. 2 Escrito ou impresso que fornece informação ou prova. 3 Qualquer fato e tudo quanto possa servir de prova, confirmação ou testemunho.”

DICMAXI Michaelis

A utilização combinada dos significados acima, define o conceito de documento no atual momento tecnológico.

Resta-nos garantir a autoria e autenticidade do documento e de seu conteúdo.

4 SOLUÇÃO IMPLEMENTADA

Para validar as evidências, podem ser utilizadas informações que identifiquem as ações e objetos. Dentre elas podemos citar:

Assinatura – A punho ou digital.

PKI – Infra-estrutura de chave pública. Mecanismo utilizado para gerar códigos(chaves) para utilização assinaturas digitais, por exemplo.

Assinatura Digital - assinatura digital é uma modalidade de assinatura eletrônica, resultado de uma operação matemática que utiliza criptografia e permite aferir, com segurança, a origem e a integridade do documento.

Ata notarial - instrumento público autorizado por notário competente, a requerimento de uma pessoa com interesse legítimo e que, fundamentada nos princípios da função imparcial e independente, pública e responsável, tem por objeto constatar a realidade ou verdade de um fato que o notário vê, ouve ou percebe por seus sentidos, cuja finalidade precípua é a de ser um instrumento de prova em processo judicial, mas que pode ter outros fins na esfera privada, administrativa, registral, e, inclusive, integradores de uma atuação jurídica não negocial ou de um processo negocial complexo, para sua preparação, constatação ou execução. Lei 8.935, de 18/11/1994.

Checksum - um número de bits transmitido com os dados para que o dispositivo receptor possa verificar a precisão dos dados recebidos. Se o número de bits que chega é o mesmo enviado, a transmissão é considerada concluída.

Estatística – Utilização de procedimentos estatísticos para prospecção de informações.

Mactimes – datas de criação, alteração e acesso dos arquivos.

Proprietário – usuário que criou o arquivo ou diretório.

Cabeçalho do e-mail – campos do e-mail que contém informações como origem, destinatário, assunto etc.

Id do e-mail – identificador da mensagem.

URL - Universal Resource Locator (URL) é o endereço de um recurso ou ficheiro disponível na Internet.

As evidências podem ser validadas em quatro dimensões:

- i. No conteúdo dos dados/informações de origem(arquivos)

Verificar se houve alteração dos dados.

- ii. No canal de acesso do auditor aos dados de origem

Verificar se o meio pelo qual os dados/informações chegaram ao auditor são confiáveis. Verificar origem e destino.

- iii. Nos procedimentos de geração das evidências

Validar se as técnicas utilizadas pelo auditor não desvirtuam os dados/informações. Conciliar as evidências geradas.

- iv. Na apresentação das conclusões

Validar se a apresentação das conclusões é pertinente com as evidências e se as ações realizadas podem ser reconstruídas.

Para validarmos uma evidência, necessitamos analisar a técnica de auditoria quanto à sua origem e a origem quanto às quatro dimensões apresentadas.



Ilustração 1 - Validação da Evidência

Dimensões para Validação da Técnica de Auditoria

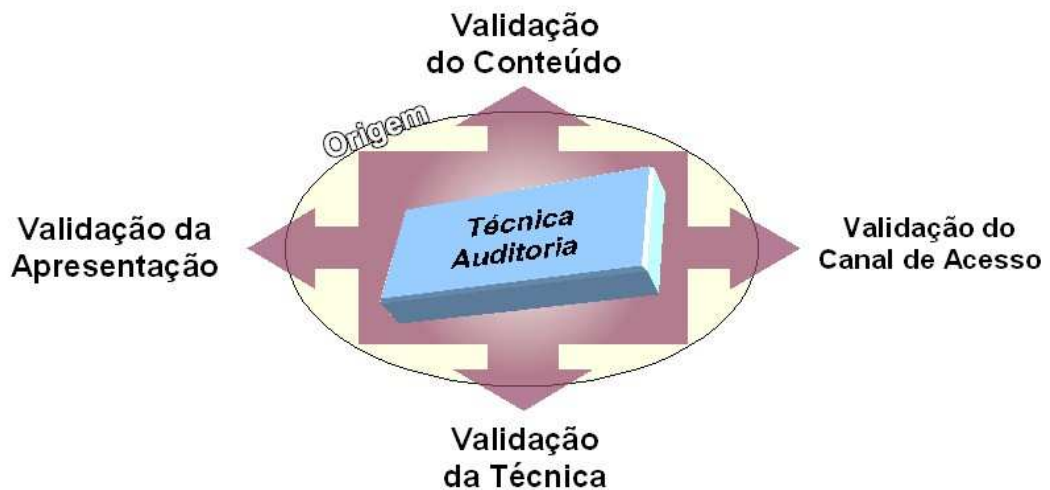


Ilustração 2 - Dimensões para Validação da Técnica de Auditoria

Quadro descritivo dos itens a registrar na execução das Técnicas de Auditoria

Técnica	Origem				Itens para registrar
	De observações do ambiente	De extração de documentos	Do auditado ou de terceiros	De análises do auditor	
Questionário			X		Assinatura do auditor Assinatura do questionado
Simulação de dados				X	Ações Assinaturas Atores Estatística Registro dos momentos de início e fim Registros Massa de testes Resultados
Visita in loco	X				Ações Assinaturas Atores Check List Registro dos momentos de início e fim
Mapeamento estatístico				X	Captura de memória Captura de tráfego Estatística Listagem de processos Listagem de variáveis
Rastreamento				X	Captura de memória Captura de tráfego Debug Estatística Listagem de processos Listagem de variáveis Logs Trilhas de auditoria
Entrevista			X		Assinatura do auditor Assinatura do entrevistado Registro do local Registro dos momentos de início e fim
Análise relatório / tela				X	Ações Assinaturas Atores Estatística Registro dos momentos de início e fim
Simulação paralela				X	Ações Assinaturas Atores Registro dos momentos de início e fim
Análise de log				X	Ações Assinaturas Atores Estatística Registro dos momentos de início e fim Registros
Checklist	X				Assinaturas Atores Registro dos momentos de início e fim
Análise de programa fonte				X	Ações Assinaturas Atores Registro dos momentos de início e fim
Snapshot				X	Ações Assinaturas Atores Captura de memória Captura de tráfego Debug Listagem de processos Listagem de variáveis Registro dos momentos de início e fim

Tabela 4 - Quadro dos itens a registrar por Técnica de Auditoria

Quadro descritivo dos itens a registrar conforme a dimensão do dado/informação analisada

Dimensão	Origem				Forma de Validação
	De observações do ambiente	De extração de documentos	Do auditado ou de terceiros	De análises do auditor	
Conteúdo		X	X	X	Assinatura Ata notarial Checksum Estatística Mactimes Proprietário
Canal de Acesso			X		Assinatura Ata notarial Cabeçalho do e-mail Checksum Data/Hora Id do e-mail URL
Procedimentos	X	X	X	X	Assinatura Ata notarial Checksum Data/Hora Estatística Log
Apresentação	X	X	X	X	Assinatura Log

Tabela 5 - Quadro dos itens por dimensão

De posse dos quadros acima, torna-se possível estabelecer alguns testes para validação das técnicas de auditoria e definir o formulário DESCRIÇÃO DA EVIDÊNCIA, para anexar aos papéis de trabalho.

Além dos relacionamentos acima, devemos adicionar ao formulário DESCRIÇÃO DA EVIDÊNCIA um campo para registrar a movimentação da informação, que em forense computacional, trata-se de **cadeia de custódia**.

Descrição da Evidência

Nº e Assunto da Auditoria: _____
Descrição dos Dados/Informação: _____
Formato da Evidência: _____
Data de geração: _____ Data de entrega: _____

Técnica de Auditoria utilizada

<input type="checkbox"/> Análise de log	<input type="checkbox"/> Questionário
<input type="checkbox"/> Análise de programa fonte	<input type="checkbox"/> Rastreamento
<input type="checkbox"/> Análise relatório / tela	<input type="checkbox"/> Simulação de dados
<input type="checkbox"/> Checklist	<input type="checkbox"/> Simulação paralela
<input type="checkbox"/> Entrevista	<input type="checkbox"/> Snapshot
<input type="checkbox"/> Mapeamento estatístico	<input type="checkbox"/> Visita in loco
<input type="checkbox"/> Outra _____	

Validação da Evidência

<u>Dimensão</u>	<u>Forma de Validação</u>
<input type="checkbox"/> Conteúdo	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Ata notarial _____ <input type="checkbox"/> Checksum _____ <input type="checkbox"/> Mactimes _____ <input type="checkbox"/> Proprietário _____ <input type="checkbox"/> Outra _____
<input type="checkbox"/> Canal de Acesso	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Cabeçalho do e-mail _____ <input type="checkbox"/> Checksum _____ <input type="checkbox"/> Data/Hora _____ <input type="checkbox"/> Id do e-mail _____ <input type="checkbox"/> URL _____ <input type="checkbox"/> Outra _____
<input type="checkbox"/> Procedimentos	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Ata notarial _____ <input type="checkbox"/> Checksum _____ <input type="checkbox"/> Data/Hora _____ <input type="checkbox"/> Log _____ <input type="checkbox"/> Outra _____
<input type="checkbox"/> Apresentação	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Log _____ <input type="checkbox"/> Outra _____

Cadeia de Custódia

Origem: _____
Área da Origem: _____
Justificativa: _____
Destinatário: _____
Área do Destinatário: _____

Ilustração 3 - Descrição da Evidência

Dados da Auditoria

Descrição da Evidência Data de acesso do auditor à informação
 Nº e Assunto da Auditoria
 Descrição dos Dados/Informação:
 Formato da Evidência:
 Data de geração: **Data de entrega:**
 Formato no qual a esta a Informação. Ex.: arquivo eletrônico .doc
 Data de geração da Informação.
 Técnica de auditoria utilizada

Técnica de Auditoria utilizada

<input type="checkbox"/> Análise de log <input type="checkbox"/> Análise de programa fonte <input type="checkbox"/> Análise relatório / tela <input type="checkbox"/> Checklist <input type="checkbox"/> Entrevista <input type="checkbox"/> Mapeamento estatístico <input type="checkbox"/> Outra _____	<input type="checkbox"/> Questionário <input type="checkbox"/> Rastreamento <input type="checkbox"/> Simulação de dados <input type="checkbox"/> Simulação paralela <input type="checkbox"/> Snapshot <input type="checkbox"/> Visita in loco
--	--

Validação da Evidência

Dimensão	Forma de Validação
<input type="checkbox"/> Conteúdo	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Ata notarial _____ <input type="checkbox"/> Checksum _____ <input type="checkbox"/> Mactimes _____ <input type="checkbox"/> Proprietário _____ <input type="checkbox"/> Outra _____
<input type="checkbox"/> Canal de Acesso	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Cabeçalho do e-mail _____ <input type="checkbox"/> Checksum _____ <input type="checkbox"/> Data/Hora _____ <input type="checkbox"/> Id do e-mail _____ <input type="checkbox"/> URL _____ <input type="checkbox"/> Outra _____
<input type="checkbox"/> Procedimentos	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Ata notarial _____ <input type="checkbox"/> Checksum _____ <input type="checkbox"/> Data/Hora _____ <input type="checkbox"/> Log _____ <input type="checkbox"/> Outra _____
<input type="checkbox"/> Apresentação	<input type="checkbox"/> Assinatura _____ <input type="checkbox"/> Log _____ <input type="checkbox"/> Outra _____

Forma de validação utilizada.

Cadeia de Custódia

Origem: _____
 Área da Origem: _____
 Justificativa: _____
 Destinatário: _____
 Área do Destinatário: _____

Rotulo de trânsito da informação

Ilustração 4 - Descrição da Evidência comentada

5 CONCLUSÕES E RESULTADOS ALCANÇADOS

O processo implementado utiliza técnicas de forense computacional e estatística na construção das recomendações do auditor, o que possibilita a validação das mesmas.

Um dos principais mecanismos para comprovação, seria a utilização de uma estrutura de PKI, que não existe atualmente no Banrisul e, portanto, não pudemos validar.

Salientamos que nem sempre teremos certeza absoluta da validação, mas que mesmo assim, a concatenação de vários indicadores podem construir um cenário de difícil contestação. Tal qual o próprio exame de DNA, onde pode-se afirmar com 99,9999% de certeza que o suposto pai é o pai da criança, ou com 100% de certeza se o suposto pai não é o pai da criança.

A demonstração pública das ações realizadas, possibilita a transparência do trabalho do auditor, gerando maior confiança nas recomendações, bem como, capacidade de correção de eventuais erros cometidos.

Uma conseqüência da implementação, é um registro mais apurado dos trabalhos executados, permitindo a transmissão do conhecimento entre os profissionais de auditoria.

6 REFERÊNCIAS BIBLIOGRÁFICAS

- [SIS04] Rômulo de Oliveira, Alexandre Carissimi, Simão Toscani. *Sistemas Operacionais* 3 Ed. Porto Alegre: Sagra Luzzatto, 2004, 259p.
- [OLI04] F. C. Oliveira, Paulo Henrique. *Amostragem Básica*. Rio de Janeiro: Ciência Moderna, 2004, 260p.
- [TCP05] Luciano Palma, Rubens Prates. *TCP/IP Guia de Consulta Rápida*. São Paulo: Novatec, 2005, 128p.
- [EXP05] Jargas, Aurélio Marinho. *Expressões Regulares Guia de Consulta Rápida*. São Paulo: Novatec, 2005, p.
- [RSL05] Morimoto, Carlos. *Redes e Servidores Linux*. Porto Alegre: Sulina, 2005, p.
- [LFT05] Morimoto, Carlos. *Linux: Ferramentas Técnicas*. Porto Alegre: Sul Editores, 2005, 311p.
- [JOA03] Lima, João Paulo. *Administração de Redes Linux*. Goiânia: Gráfica Terra Ltda., 2003, 448p.
- [DAN06] Dan Farner, Wietse Venema. *Perícia Forense Computacional Teoria e Prática Aplicada*. São Paulo: Pearson Prentice Hall, 2006, 190p.
- [AND06] Rodrigues de Freitas, Andrey. *Perícia Forense Aplicada à Informática – Ambiente Microsoft*. São Paulo: Brasport, 2006, 215p.
- [RUF01] Rufino, Nelson Murilo de O. *Segurança Nacional Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores*. São Paulo: Novatec, 2001, 248p.
- [DIA00] Dias, Cláudia. *Segurança e Auditoria da Tecnologia da Informação*. São Paulo: Axcel Books, 2000, 218p.
- [INS93] Instituto dos Auditores Internos do Brasil. *Procedimentos de Auditoria Informática*. São Paulo: Câmara Brasileira de Auditoria Informática, 368p.
- [ISO05] Associação Brasileira de Normas Técnicas. *ABNT NBRISO/IEC 17799:2005*. Rio de Janeiro: 2005, 120p.
- [COM04] FEBRABAN. *Compliance e Auditoria de Sistemas nas transações de e-Commerce*. São Paulo: 2004, 84p.
- [MET04] FEBRABAN. *Metodologia de Auditoria Interna com Foco em Riscos*. São Paulo: 2004, 133p.
- [NOV04] FEBRABAN. *Novos Conceitos de Auditoria de Sistemas em Bancos*. São Paulo: 2004, 80p.
- [BAC98] BACEN. *RESOLUCAO 2.554*. Brasília: 1998, 3p.
- [BAC06] BACEN. *RESOLUCAO 3.380*. Brasília: 2006, 4p.