Auditoria de Transações Eletrônicas

Prevenindo a Fraude Bancária

FEBRABAN

Federação Brasileira de Bancos

- Conceitos
- Regra X Transação X Risco
- Ciclo Vicioso
- Papel de Trabalho
- Situações de Exposição a Risco
- Conclusões
- Outras Preocupações

Conceitos

- Transação Eletrônica
- Restrição de Acesso
- Restrição de Uso
- Regra de Negócio

Conceitos

Transação Eletrônica

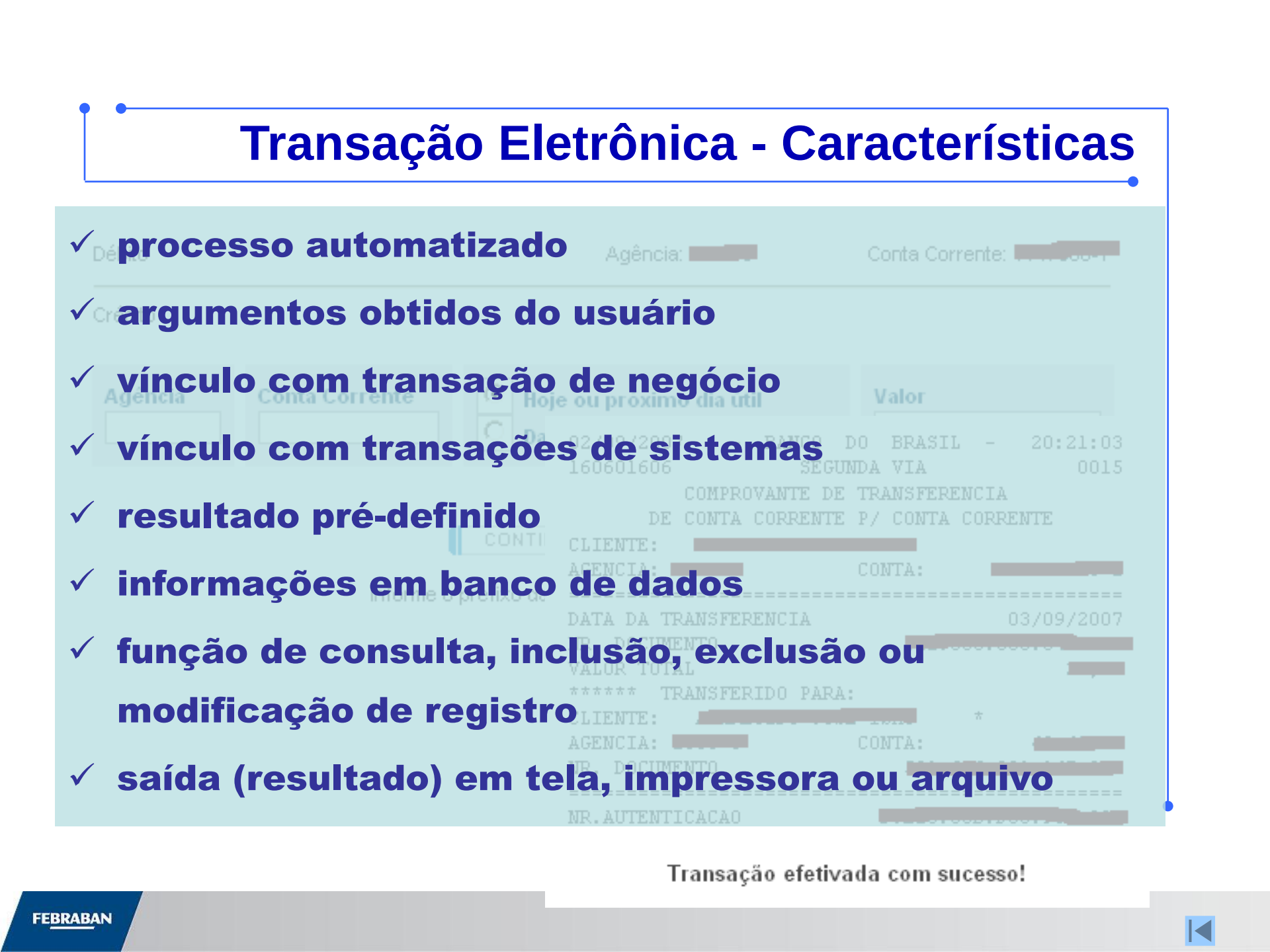
Conjunto de comandos programados para consultar, inserir, excluir ou alterar um ou mais registros em um banco de dados

(conceito da Auditoria Interna do BB)

A transação eletrônica (TE) não precisa/não deve ser considerada como o objeto específico de um trabalho de auditoria. Esse atributo pertence ao processo/negócio/atividade que a comporta.

Transação Eletrônica - Características

- ✓ processo automatizado
- ✓ argumentos obtidos do usuário
- ✓ vínculo com transação de negócio
- ✓ vínculo com transações de sistemas
- ✓ resultado pré-definido
- ✓ informações em banco de dados
- ✓ função de consulta, inclusão, exclusão ou modificação de registro
- ✓ saída (resultado) em tela, impressora ou arquivo



Conceitos

Restrição de Acesso

Mecanismo que restringe o acesso de usuários a redes, sistemas e transações mediante validação por senha, certificação digital e/ou identificação biométrica.

Conceitos

Restrição de Uso

Limitação imposta ao usuário, que afeta seu direito de acesso ou de uso de determinada transação ou sistema, ativada por parâmetros previamente catalogados e sistematizados

exemplo

Restrição de Uso - exemplo

A Polícia Federal pediu, e a Justiça autorizou, o acesso geral ao extrato de chamadas e ao cadastro dos clientes de oito empresas de telefonia...

...os dados são consultados pelos policiais por meio de senhas concedidas pelas companhias. Essa autorização não inclui escuta telefônica. Mas, como as senhas não têm restrição de uso, em tese os policiais poderiam mapear as ligações de qualquer cidadão.

A autorização... durou até agosto de 2008, quando a Justiça excluiu a possibilidade de acesso ilimitado ao histórico das ligações...

O juiz... defendeu que há controle do uso de senhas porque os nomes dos policiais usuários do mecanismo ficam registrados nos sistemas das empresas telefônicas.

Fonte: Folha On Line – 03.04.2009

Conceitos

Regra de Negócio

“Sentenças que definem ou restringem algum aspecto do negócio”

“Condições que governam os eventos do negócio de tal forma que eles ocorram de uma forma aceitável para o negócio”

(Von Halle)

Von Halle, Barbara. *Business Rules Applied: Building Better Systems* . New York: Wiley, 2001, 464 p.
BRG: http://www.businessrulesgroup.org/brghome.htm BRCommunity: www.brcommunity.com/
Manifesto: http://businessrulesgroup.org/brmanifesto.htm
Defining Business Rules: http://www.businessrulesgroup.org/first_paper/br01c0.htm

Regra X Transação X Risco

Situações de Exposição a Risco

A falta de restrição de acesso ou a sua aplicação inadequada possibilitam/facilitam:

- ✓ ***o uso de TE por usuários e dependências que não poderiam executar ou não estão autorizadas a executar a atividade onde inserida a TE***
- ✓ ***a disponibilização do uso de TE sem sua submissão a sistema de controle de acessos***
- ✓ ***a ocorrência de fraude por meio de captura ilícita de senhas***
- ✓ ***a ocorrência de fraude por meio de compartilhamento de senhas***

continua

Situações de Exposição a Risco

A falta de aplicação, nas transações eletrônicas, das regras de negócio (restrições de uso e outras) possibilitam / faciltam:

- ✓ ***que usuários internos alterem seus próprios cadastros e produtos***
- ✓ ***a efetivação de lançamentos manuais em contas privativas do sistema***
- ✓ ***a inserção de informações inválidas em bancos de dados***

- classificar um cliente menor de 16 anos como capaz, em desacordo com a legislação

- cadastrar "renda auferida" em valor incompatível com a "função exercida". Ex: R$ 200 mil para "auxiliar de serviços gerais"

continua

Situações de Exposição a Risco

A inexistência de trilha de auditoria de transações eletrônicas e de sistema eficiente de consulta de logs centralizada e parametrizada (por usuário, por dependência, por período, etc.) prejudica:

- ✓ ***a implementação de medidas preventivas (rotinas inteligentes)***

  as maiores fraudes não são detectadas pelas organizações porque ocorrem mediante uso sequenciado de transações e sistemas distintos, cujo grau de risco individual é considerado baixo

- ✓ ***a investigação de fraudes – produção de prova***

  QUEM acessou O QUÊ, QUANDO, ONDE e O QUE FEZ?

Conclusões

- ✓ *As restrições de acesso a transações eletrônicas por mecanismos simples (Ex: senha de seis dígitos) não supre quesitos básicos de segurança, uma vez que as falhas e fraudes perpetradas por usuários ocorrem mediante o acesso, legítimo ou não, às transações*
- ✓ *A inexistência de rotinas inteligentes em sistemas e transações eletrônicas contribui para o aumento das falhas e fraudes na instituição*
- ✓ *A implementação de rotinas de monitoramento e controles, tendo como objeto transações que não "carregam" regras de negócio em seu programa, são ineficazes e dispendiosas*
- ✓ *A definição de alçadas e aplicação de método para classificação de transações eletrônicas (parâmetros, vigência, nível de criticidade, categoria de acesso a dados, etc.) é fundamental no processo de ativação e acompanhamento das transações eletrônicas*

continua

Conclusões

- ✓ ***A existência de transações e rotinas em sistemas que não incorporam, de forma automatizada, as regras de negócio, pode indicar nível de controle inadequado na instituição***
- ✓ ***Aceitar a existência, completeza e disponibilidade da regra de negócio como sinônimo de controle pode condicionar o gestor de negócio a limitar a abrangência de sua responsabilidade e comprometer o sistema de controle da instituição***
- ✓ ***A inexistência de trilha de auditoria de transações eletrônicas (log) de forma unificada e disponível para consulta imediata pelos administradores, gestores e áreas de controle e segurança do Banco inviabiliza ações preventivas e dificulta as reativas***

Outras Preocupações

Funcionários admitem furtar dados ao deixar emprego, indica pesquisa MAGGIE SHIELS da **BBC News**

"Nosso estudo demonstrou que 59% das pessoas dirão 'vou levar alguma coisa de valor comigo quando eu sair'", concluiu Spinney. O Instituto Ponemon, uma empresa especializada em pesquisas nas áreas de gerenciamento e privacidade, fez sua enquete com 945 trabalhadores que foram demitidos ou pediram demissão do emprego nos últimos 12 meses. Todos os entrevistados tinham acesso a informações como dados sobre clientes, listas de contato, registros de funcionários, documentos confidenciais da empresa, programas de computador e outros tipos de propriedade intelectual.

Fonte: Folha On Line – 25.02.2009

Muito Obrigado!

Contato: rudinei@bb.com.br