Auditoría de Transacciones Electrónicas

Prevención del Fraude Bancario

FEBRABAN

Federação Brasileira de Bancos

- Conceptos
- Regla X Transacción X Riesgo
- Ciclo Vicioso
- Papel de Trabajo
- Situaciones de Exposición al Riesgo
- Conclusiones
- Otras Preocupaciones

Conceptos

- Transacción Electrónica
- Restricción de Acceso
- Restricción de Uso
- Regla de Negocio

Conceptos

Transacción Electrónica

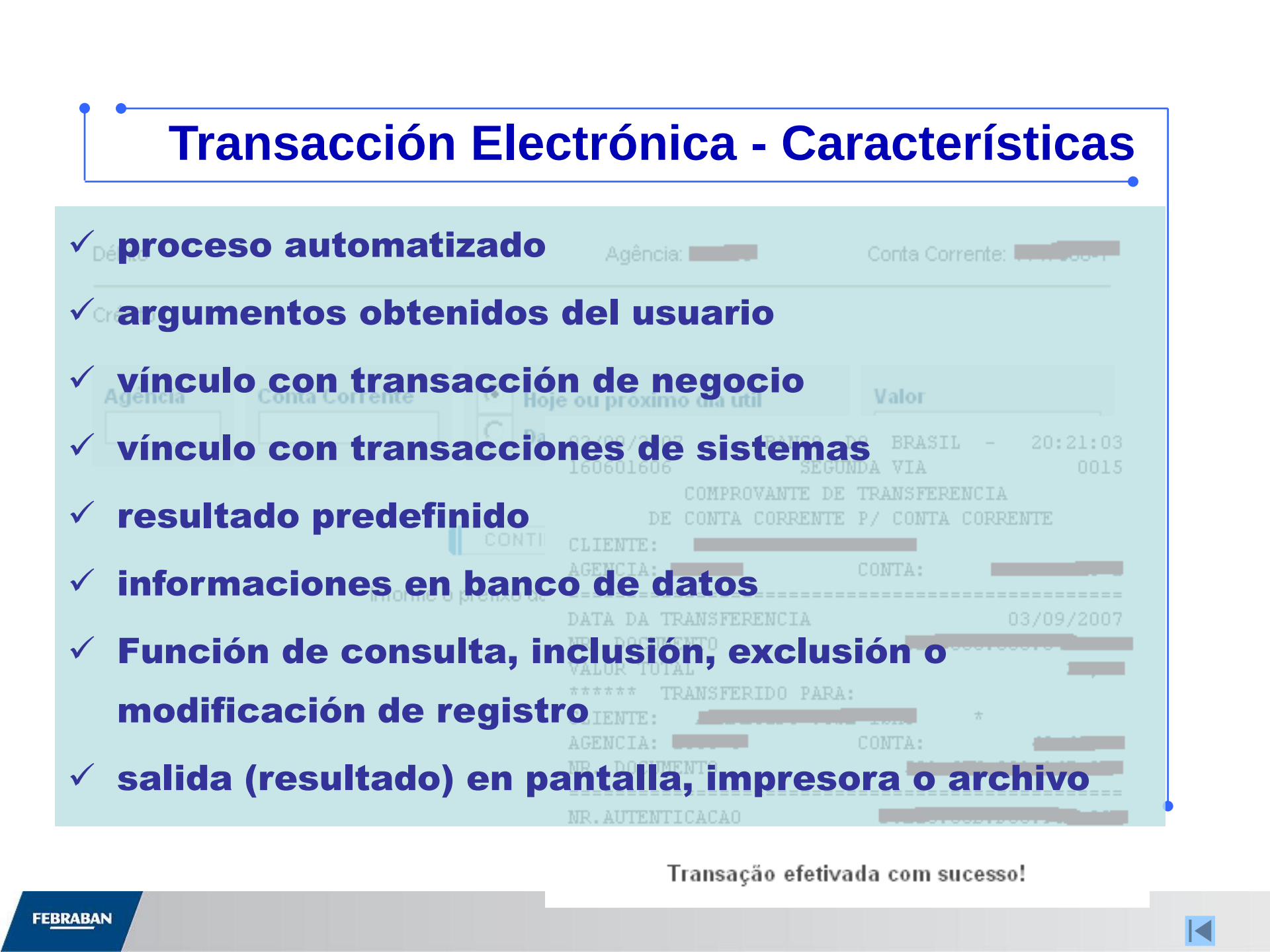
Conjunto de comandos programados para consultar, incluir, excluir o modificar uno o más registros en un banco de datos

(concepto de la Auditoría Interna del BB)

La transacción electrónica (TE) no precisa/no debe ser considerada como el objeto específico de un trabajo de auditoría. Ese atributo pertenece al proceso/negocio/actividad que la comporta.

Transacción Electrónica - Características

- ✓ proceso automatizado
- ✓ argumentos obtenidos del usuario
- ✓ vínculo con transacción de negocio
- ✓ vínculo con transacciones de sistemas
- ✓ resultado predefinido
- ✓ informaciones en banco de datos
- ✓ Función de consulta, inclusión, exclusión o modificación de registro
- ✓ salida (resultado) en pantalla, impresora o archivo



Conceptos

Restricción de Acceso

Mecanismo que restringe el acceso de usuarios a redes, sistemas y transacciones mediante validación por contraseña, certificación digital y/o identificación biométrica.

Conceptos

Restricción de Uso

Limitación impuesta al usuario, que afecta su derecho de acceso o de uso de determinada transacción o sistema, activada por parámetros previamente catalogados y sistematizados

ejemplo

Restricción de Uso - ejemplo

La Policia Federal solicitó, y la Justicia autorizó, el aceso general al extracto de llamadas y al registro de los clientes de ocho empresas de telefonia...

...los datos son consultados por los policias por medio de contraseñas otorgadas por las compañías. Esa autorización no incluye escucha telefónica. Pero, como las contraseñas no tienen restricciones de uso, en teoría los policias podrían mapear las llamadas de cualquier ciudadano.

La autorización... duró hasta agosto del 2008, cuando la Justicia excluyó la posibilidad de acceso ilimitado al histórico de llamadas....

El juez... lo defendió argumentando que hay control del uso de contraseñas porque los nombres de los policias usuarios del mecanismo quedan registrados en los sistemas de las empresas telefónicas.

Fonte: Folha On Line – 03.04.2009

Conceptos

Regla de Negocio

“Sentencias que definen o restringen algún aspecto del negocio”

“Condiciones que gobiernan los eventos del negocio de tal manera que ocurran de una forma aceptable para el negocio “

(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

Regla X Transacción X Riesgo

Situaciones de Exposición al Riesgo

La falta de restricción de acceso y su aplicación inadecuada posibilitan/facilitan:

- ✓ ***el uso de TE por usuarios y dependencias que no podrían ejecutar o que no están autorizados a realizar la actividad en donde está insertada la TE***
- ✓ ***la disponibilización del uso de TE sin someterse al sistema de control de accesos***
- ✓ ***el incidente de fraude por medio de captura ilícita de contraseñas***
- ✓ ***el incidente de fraude por medio del compartimiento de contraseñas***

continua

Situaciones de Exposición al Riesgo

La falta de aplicación, en las transacciones electrónicas, de las reglas de negocio (restricciones de uso y otras) posibilitan / facilitan:

- ✓ ***que usuarios internos modifiquen sus propios registros y productos***
- ✓ ***la efectivización de lanzamientos manuales en cuentas privadas del sistema***
- ✓ ***la inserción de informaciones incorrectas en bancos de datos***

- clasificar un cliente menor de 16 años como capaz, en desacuerdo con la legislación

- registrar "ingresos" en valor incompatible con la "función ejercida". Ex: R$ 200 mil para "auxiliar de servicios generales"

continua

Situaciones de Exposiciones a Riesgo

La inexistencia de una pista de auditoría de transacciones electrónicas y de un sistema eficiente de consulta de logs centralizada y parametrizada (por usuario, por dependencia, por período, etc.) perjudica:

- ✓ ***la implementación de medidas preventivas (rutinas inteligentes)***

  los mayores fraudes no son detectados por las organizaciones porque ocurren mediante el uso secuenciado de transacciones y sistemas distintos, cuyo grado de riesgo individual es considerado bajo

- ✓ ***la investigación de fraudes – producción de prueba***

  ¿QUIÉN accedió O QUÉ, CUANDO, DÓNDE y QUÉ HIZO?

Conclusiones

- ✓ ***Las restricciones de acceso a transacciones electrónicas por mecanismos simples (Ej: contraseña de seis dígitos) no cumplen con ítems básicos de seguridad, una vez que las fallas y fraudes perpetradas por usuarios ocurren mediante el acceso, legítimo o no, a las transacciones***
- ✓ ***La inexistencia de rutinas inteligentes en sistemas y transacciones electrónicas contribuye al aumento de las fallas y fraudes en la institución***
- ✓ ***La implementación de rutinas de monitoreo y controles, que tienen como objeto de transacciones que no "cargan" reglas de negocio en su programa, son ineficaces y costosas***
- ✓ ***La definición de alzadas y aplicación de método para clasificación de transacciones electrónicas (parámetros, vigencia, nivel de criticidad, categoría de acceso a datos, etc.) es fundamental en el proceso de activación y seguimiento de las transacciones electrónicas***

continua

Conclusiones

- ✓ ***La existencia de transacciones y rutinas en sistemas que no incorporan, de manera automatizada, las reglas de negocio, puede indicar un nivel de control inadecuado en la institución***
- ✓ ***Aceptar la existencia, complejidad y disponiblidad de la regla de negocio como sinónimo de control puede condicionar al gestor de negocio a limitar el alcance de su responsabilidad y comprometer el sistema de control de la institución***
- ✓ ***La inexistencia de pista de auditoría de transacciones electrónicas (log) de manera unificada y disponible para la consulta inmediata por los administradores, gestores y áreas de control y seguridad del banco no posibilita acciones preventivas y dificulta las reactivas***

Otras Preocupaciones

Funcionarios admiten robar datos al dejar el empleo, indica investigaciones MAGGIE SHIELS de la **BBC News**

"Nuestro estudio demostró que el 59% de las personas dirán "voy a llevar alguna cosa de valor conmigo cuando salga"", concluyó Spinney. El Instituto Ponemon, una empresa especializada en investigaciones en las áreas de gerenciamiento y privacidad, realizó una encuesta con 945 trabajadores que fueron despedidos o renunciaron a su empleo en los últimos 12 meses. Todos los entrevistados tenían acceso a informaciones como datos sobre clientes, listas de contacto, registros de funcionarios, documentos confidenciales de la empresa, programas de computadora y otros tipos de propiedad intelectual.

Fonte: Folha On Line – 25.02.2009

Muchas Gracias!

Contacto: rudinei@bb.com.br