45º JORNADAS ARGENTINAS DE INFORMÁTICA - JAIIO
Simposio de Informática en el Estado (SIE 2016)
Tema: Seguridad de la Información

"AUDITORIA CONTINUA: PISTAS DIGITALES EFICACES A PARTIR DEL LOG DE TRANSACCIONES"

Lic. Héctor Rubén MORALES[1], Dra. Cecilia Beatriz DÍAZ[2], Dr. Ricardo Justo CASTELLO[3]
Facultad de Ciencias Económicas–Universidad Nacional de Córdoba
[1]hruben.morales@gmail.com, [2]cdiaz@eco.unc.edu.ar, [3]castello@eco.unc.edu.ar

Resumen: En el ámbito de los sistemas de información computarizados el auditor advierte como problema, que de los tres componentes de un sistema de información: Entrada, Procesamiento, y Salida; la fase correspondiente al Procesamiento, pasó a ser para él una "caja negra".
Esa incertidumbre del auditor surge a partir de la escasez de pistas de auditoría confiables para su tarea de control.
A partir de la Ley Sarbanes-Oxley se focaliza la atención sobre cómo los datos son procesados y usados dentro de las empresas; y se aboga por mejorar el sistema de control interno con reportes en tiempo real, fomentando el desarrollo de técnicas de auditoría continua, igual las Normas Internacionales de Auditoría (NIAs).
Este trabajo busca delinear las bases de un modelo de monitoreo continuo, basado en pistas de auditoría a partir del log de transacciones del motor de base de datos, con control del auditor, resulte de aplicación genérica y reduzca el riesgo de auditoría.

Palabras Clave: pistas – datos – transacción – log - control.

1. Introducción

El enfoque de la Auditoría Continua, surge a partir del avance tecnológico, siendo la Auditoría de Sistemas la disciplina que considera la dinámica planteada por los sistemas computarizados. En este ámbito el auditor advierte como problema que de los componentes del sistema de información, esto es: Entrada de datos, Procesamiento, Salida de datos y Almacenamiento o Base de datos, la fase del Procesamiento, pasó a ser para él una "caja negra" donde desconoce lo que ocurre dentro, al igual que desconoce sobre la confianza e integridad de la información contenida en la Base de datos (BD).

Las metodologías de auditar evolucionaron en los últimos años con varias técnicas. Surgieron alternativas de controles "dentro del procesamiento", casos teóricos y desarrollos puntuales. Una de ellas, se refiere a "agregar módulos de auditoría" conectados en puntos determinados del aplicativo de procesamiento de transacciones monitoreando en tiempo real una amplia variedad de procesos y transacciones, y capturando errores y/o violación de controles. Otra técnica, es la "de extracción de datos–pistas desde el procesamiento", son sistemas independientes que monitorean en forma continua extrayendo transacciones hacia otro ambiente que comparan con estándares para detectar desvíos respecto a lo esperado.

Si bien ello sirvió para reducir la incertidumbre del auditor, el problema de fondo aún persiste. La bibliografía especializada así lo afirma y considera que en la actual etapa, la mayoría de las técnicas desarrolladas actúan sobre el software mismo o capa de aplicación.

En efecto, estas técnicas testean principalmente el Procesamiento, pero no afrontan la capa más profunda e importante que es la BD del sistema, donde impactan todas las acciones que acontecen. Estas acciones pueden tratarse de operaciones no captadas por las técnicas o procesos de auditoría sobre el procesamiento, o bien operaciones que no fluyen previamente por este al ser efectuadas directamente sobre la BD. Esto último podría conformar desde ingresos, modificaciones o eliminaciones de datos informales o no autorizados, hasta casos que denoten irregularidades o acciones dolosas, en cuyo caso, el auditor debería estar advertido y no desconocer.

Lo expresado ha contribuido para determinar la escasez o bien una calidad laxa y, a la vez, riesgosa de los datos y pistas de auditoría que dispone el auditor para su tarea. Esta percepción, es tanto en una auditoría contable, como hasta en una investigación por fraude donde se debe aportar evidencias con efectos legales (auditoría forense). Si la información controlada no es suficiente y confiable, el auditor trabajará con información distorsionada, haciendo un diagnóstico erróneo de su control, que lo hará extensivo a su conclusión u opinión final.

Estas pistas deberían permitir al auditor seguir el flujo de las transacciones procesadas por los aplicativos de gestión. Esto es, que ante una verificación, pueda reconstruir el flujo de esa transacción a partir del último dato que está observando y, de allí hacia atrás, conocer todas las huellas o modificaciones que sufrió ese registro en la BD, incluso contar con aquellos datos eliminados e información adicional, tales como: hora del evento, usuario, terminal y tipo de operación.

1.1. Antecedentes

A partir de la Ley Sarbanes-Oxley (SOX, 2002), la más importante regulación surgida luego de los escándalos financieros en Estados Unidos a fines de 2001, se focaliza la atención sobre cómo los datos son procesados y usados dentro de las empresas; y se aboga por mejorar el sistema de control interno con reportes en tiempo real, fomentando el desarrollo de técnicas de auditoría continua. En la misma línea, se enmarcan las Normas de Auditoría Internaciones (NIAs).

Ante ello surgieron varios modelos teóricos desarrollados para auditar transacciones en forma continua. Estos pueden agruparse en dos metodologías (1):

- Módulos Embebidos de Auditoría -Embebed Audit Modules o EAMs(2): módulos de software puestos en puntos predeterminados del sistema de gestión para obtener información sobre las transacciones o eventos procesados.
- Sistemas independientes: monitorean extrayendo datos desde el sistema auditado. Comparan los datos extraídos de transacciones con estándares para monitorear el sistema y detectar anormalidades; son conocidos como "Continuous Process Auditing System (CPAS)".

Un caso de estudio de referencia de este último modelo es el trabajo "Continuous Monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemmens" (3), donde se describe una implementación piloto -denominada CMBPC- de monitoreo continuo sobre los controles aplicados a los procesos de negocio atendidos por el sistema de gestión (ERP SAP R/3) de Siemmens.

Este caso, uno de los primeros estudios publicados, demostró las potencialidades para la auditoría de las técnicas de Auditoría Continua y también destaca las dificultades y limitaciones para ponerlas en práctica. Básicamente, el foco de este estudio fue analizar mecanismos de monitoreo en tiempo real sobre los controles usados en algunos de los procesos del sistema de gestión seleccionados especialmente para este caso de estudio. Gráficamente, el modelo de este prototipo fue el siguiente:

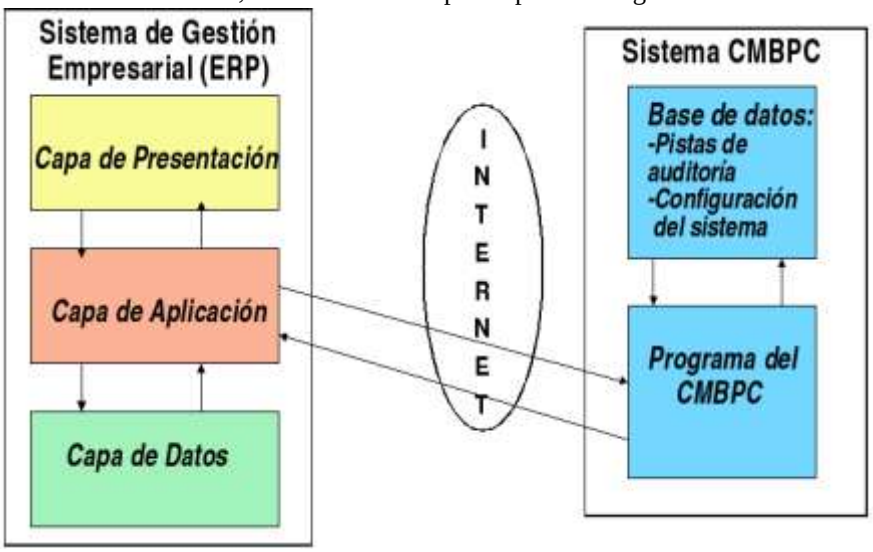

Grafico N°1: Prototipo del Continuous Monitor Business Process Control (CMBPC)

Como puede observarse el CMBPC (2) de Alles y Vasarhelyi, corresponde a la categoría de CPAS y opera monitoreando flujos de información sobre la Capa de Aplicación del ERP. Sin embargo, los citados autores consideran que lo óptimo sería implementar un CPAS monitoreando la Capa de Datos. Esto

permitiría monitorear directamente las operaciones sobre la BD que registran las transacciones procesadas por la aplicación, es decir, nos ubicaríamos en la línea de inicio, en la cual el dato u operación tiene su origen e impacta en la BD. Esta opción fue descartada por los autores a causa del tamaño (más de 20.000 tablas) y complejidad del esquema de la BD del caso bajo estudio.

A una conclusión similar llega el estudio de Debreceny (2), al describir que el sistema cuenta tiene aproximadamente 10.000 tablas con 100.000 atributos y observar como dificultosa la tarea de mapear los conocimientos de los procesos de negocio, y determinar exactamente qué atributos monitorear.

2. Modelo propuesto: Servidor de Auditoría

En el año 2007, comenzamos el desarrollo de un prototipo de monitoreo continuo, denominado "Servidor de Auditoría", en el marco de un proyecto de investigación conducido por investigadores de la Facultad de Ciencias Económicas de la Universidad Nacional de Córdoba y el área de Auditoría Interna de la Empresa Provincial de Energía de Córdoba (EPEC). La arquitectura de este prototipo se basó en monitorear la Capa de Datos del sistema de gestión comercial y el objetivo del trabajo fue desarrollar un mecanismo para obtener Pistas de Auditoría Digitales.

Se partió de la hipótesis de que una de las mayores dificultades para la auditoría de sistemas de información es la escasez de pistas de auditoría que permitan seguir el flujo de las transacciones procesadas por los aplicativos de gestión y, además, permitir al área de Auditoría Interna contar con una fuente complementaria de datos para contrastar con los reportes brindados por el sistema de gestión. Utilizando como modelo el Gráfico N°1, la arquitectura de esta propuesta fue la siguiente:

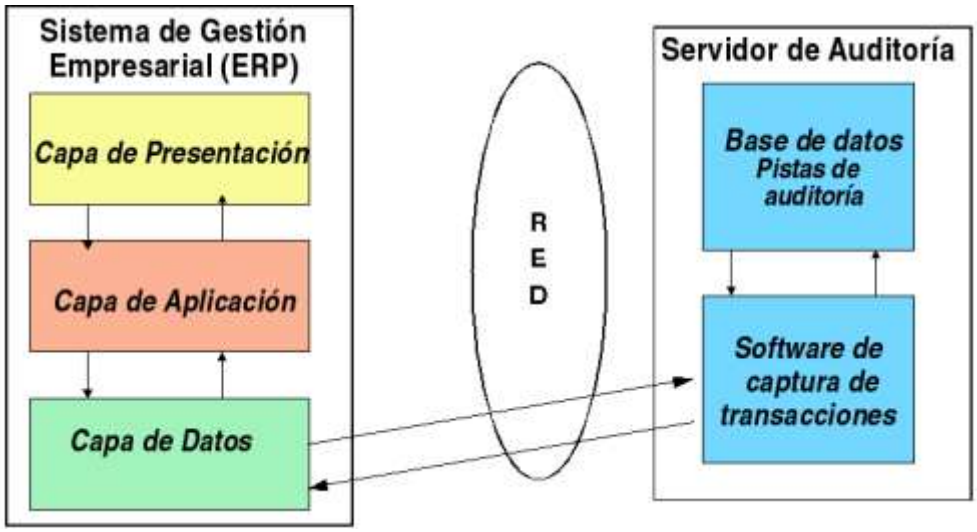

Grafico N°2: Prototipo del Servidor de Auditoría

La descripción de la implementación y los resultados del proyecto es el objeto de este trabajo. A continuación, desarrollamos el Modelo Conceptual que lo sustenta y luego los resultados del Prototipo implementado.

2.1 Modelo conceptual

El modelo de sistema de Auditoría Continua que se propone en este estudio está basado en la arquitectura de procesamiento vigente: servidores especializados por funciones atendiendo los requerimientos de la red de computadoras de la entidad. Concretamente, el aporte de esta propuesta es desarrollar un servidor específico para la función de auditoría conectado a la red donde corre el sistema de gestión. El Servidor de Auditoría es, entonces, un computador independiente, un CPAS, destinado a colectar los datos de todas las operaciones procesadas por el sistema de gestión y que se deseen preservar de cambios no autorizados.

En la figura siguiente (Gráfico N° 3) se representa el modelo de arquitectura de procesamiento actual: servidores especializados por funciones, a la que se agrega el Servidor de Auditoría (actualmente un servidor virtual).

Gráfico N° 3 – Esquema de una red de procesamiento con un Servidor de Auditoría

2.2. Recolección de datos

En el citado estudio de Hui Du y Saeed Roohani (1), los autores señalan que para ejecutar un monitoreo continuo, el sistema auditor debe ser capaz en forma continua de seleccionar, extraer y evaluar datos desde el sistema auditado sin importar la variedad de programas de aplicación y el formato de los datos utilizados, sugiriendo tecnologías de data warehouse o data mart para almacenar y procesar los datos de las transacciones traídas desde el sistema auditado.

En este caso, el primer desafío cuando se implementó el prototipo del Servidor de Auditoría fue seleccionar la tecnología para colectar los datos generados por las transacciones procesadas por el sistema de gestión (sistema auditado), para ello, se consideraron las siguientes alternativas:

- Utilizar agentes inteligentes (EAMs).
- Utilizar motores colectores de datos, en un procedimiento similar a la tecnología utilizada por los data warehouse.
- Utilizar los datos almacenados en el Log de Transacciones de la BD.

Esta última tecnología fue considerada inicialmente como la más adecuada para desarrollar el prototipo, el argumento más importante en la decisión de su elección fue que la mayoría de los paquetes ERP utilizan motores de bases de datos y éstos cuentan con un Log de Transacciones destinado originalmente para contingencias (recuperar información por fallas). Esta alternativa ofrecía como principal ventaja evitar modificar la programación del sistema auditado.

La figura siguiente (Gráfico N° 4) presenta un esquema del modelo propuesto para colectar los registros de las operaciones procesadas por el sistema de gestión y copiarlas desde el Log de Transacciones al Servidor de Auditoría:

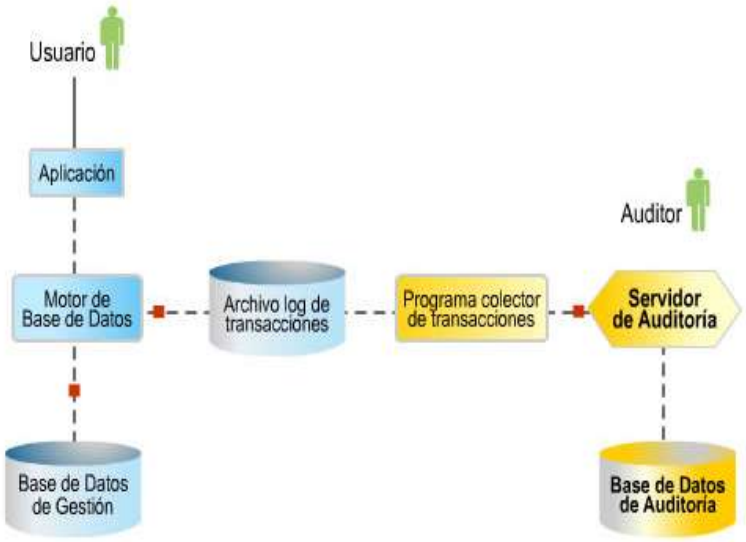

Gráfico N° 4 – Modelo colector a partir del Log de Transacciones

La elección de priorizar el monitoreo de la Capa de Datos se basó en considerar a este eslabón como el lugar donde terminan impactando todas las operaciones procesadas por el sistema auditado.

En el Log de Transacciones queda reflejado todo el historial de las transacciones procesadas, informándo si se trató de operaciones de ingreso, modificación o eliminación de datos (INSERT, UPDATE o DELETE). El Log de Transacciones también permite reconstruir la secuencia de las acciones llevadas a cabo internamente en la BD, es decir, llegar a conocer los rastros o huellas de una operación hacia cualquier sentido desde el punto en que se esté analizando.

2.3. Etapas para implementar el prototipo

Previo a la puesta en producción del prototipo Servidor de Auditoría se desarrolló una metodología para "mapear" los procesos de negocio en la estructura de la BD y seleccionar las tablas esenciales y campos a capturar. Para ello es requisito que el auditor conozca el esquema de la BD, el diagrama entidad/relación y los procesos que desea controlar. Sintéticamente las etapas llevadas a cabo fueron:

1. Relevamiento de las operaciones a colectar y de las estructuras de datos asociadas.
2. Diseño del modelo de datos para el Servidor de Auditoría.
3. Desarrollo de los procedimientos y del software para colectar datos desde el sistema de gestión, transferirlos al Servidor de Auditoría y grabarlos en el mismo.
4. Desarrollo de los procedimientos y software para recuperar las operaciones a controlar desde el Servidor de Auditoría y realizar procesos propios de auditoría.

2.4. Descripción del prototipo

En el año 2007 se desarrolló la primera versión del prototipo Servidor de Auditoría para el área Auditoría Interna de la Empresa Provincial de Energía de Córdoba (EPEC). La empresa disponía de una red compleja atendida por servidores de aplicación y bases de datos Sun/Solaris de gran porte, servidores departamentales Intel/Windows de menor rango y servidores virtuales de conectividad (mail, webserver) Intel/Windows; el software de BD es Oracle.

El prototipo desarrollado colecta los datos en tiempo diferido (del día anterior) y utiliza como tecnología fuente para colectar los datos del Log de Transacciones del gestor de base de datos Oracle.

Para desarrollar el prototipo se usaron productos de software libre: sistema operativo Linux, motor de base de datos MySQL, lenguaje PERL para los programas colectores de transacciones y de consultas a la BD de auditoría. El hardware destinado es servidor virtual de 1 TB de almacenamiento en disco, suficientes para guardar las transacciones seleccionadas correspondientes a casi un año de operaciones del

sistema auditado: los archivos Log de Transacciones obtenidos desde el sistema de gestión y la base datos propia con la información requerida por el Área de Auditoría.

3. Registro y control de las operaciones a partir del Log de transacciones

Como se dijo, a partir del Log de Transacciones de la BD, el Servidor de Auditoría registra todas y cada una de las operaciones generadas desde la aplicación y también aquellas ejecutadas directamente sobre la BD. A su vez, discrimina para cada transacción las sucesivas operaciones previas que efectuó hasta alcanzar el estado actual.

Es precisamente el registro de los pasos sucesivos previos que realiza "internamente" el sistema, desde que se inicia una transacción hasta que registra el resultado final donde reside la mayor utilidad que brinda esta propuesta al auditor.

Recordemos los momentos de una operación y cómo impactan las operaciones que se procesan sobre una BD:

Gráfico N° 5 – Impacto de las operaciones sobre una base de datos

Es decir, sintéticamente, los pasos de una transacción típica pueden enumerarse en los siguientes:

1. Ingreso de datos al computador ya sea desde la aplicación o bien directamente sobre la BD.
2. El sistema (aplicación) genera las operaciones que impactarán en la BD como altas (INSERT), eliminaciones o bajas (DELETE), o modificaciones (UPDATE), referenciadas a cada uno de los registros y/o campos específicos de las diferentes tablas en que impacta la operación.
3. El Log de Transacciones guarda cada una de estas operaciones internas y el dato que existía anteriormente; éste último es llamado técnicamente UNDO y se genera por cada operación que modifique el contenido de la BD.
4. El dato nuevo (llamado REDO) -consecuencia de una operación de alta, baja o modificación- será la información obtenida por el usuario cuando efectúe una consulta a la BD.

En este esquema, los interrogantes para el auditor son los siguientes:

- Si el dato final que observa tiene correspondencia con el dato original ingresado y es el resultado de un proceso correcto o, por el contrario, este dato fue manipulado luego de ingresado, ya sea desde la aplicación o desde un acceso directo a la BD.
- Si el dato fue ingresado desde la aplicación por el usuario habitual y autorizado y/o resulta de un proceso interno normal; o fue ingresado en forma directa sobre la BD sin las debidas autorizaciones.

En ambos casos las respuestas están contenidas en el Log de Transacciones dado que:

- Mantiene los rastros de las transacciones procesadas en la BD, guardando toda la información: dato anterior (UNDO), hora, fecha, terminal de operación, usuario (si fue desde la aplicación), o si la modificación se hizo en forma directa sobre la BD.
- Muestra los rastros que indican si el dato fue directamente registrado (INSERT) en la BD, cuando debió ser el resultado de un proceso normal del sistema de gestión; o si hay inconsistencias que denotan un ingreso irregular del dato, como por ejemplo: fecha y hora del ingreso efectivo del dato, no coincide con la fecha de la operación que registra la BD de gestión.

4. Resultados

Una primera comprobación, luego de pruebas iniciales, fue que la totalidad de las operaciones procesadas y que impactaron sobre la BD del sistema auditado quedaron reflejadas en los correspondientes tablas y campos de la BD del Servidor de Auditoría. De esta forma se logró contar en el Servidor de Auditoría con la información necesaria y suficiente para obtener la "evidencia informática" requerida para demostrar ante terceros las acciones llevadas a cabo en el sistema de gestión.

La evidencia informática (pistas de auditoría) que se logra a partir del log de transacciones y almacenada en las tablas del Servidor de Auditoría contiene los siguientes datos:

- Fecha y hora (hh:mm:ss) de la operación
- Origen de operación: desde la aplicación o directamente sobre la BD
- Nombre del usuario
- Terminal desde la cual operó
- Identifica el archivo log que contiene la operación
- Detalla la tabla y los campos operados con sus respectivos valores actuales
- Los valores anteriores de los campos operados (llamado Undo).
- El valor del ROWID (dato alfanumérico para identificar el registro modificado), se aplica en los casos de UPDATE o DELETE y sirve para obtener información complementaria del resto de los campos que no formaron parte de la operación.
- Eventos de desconexión-conexión de triggers, informando el nombre del procedimiento, hora-fecha de desconexión y de conexión. Esto permite al auditor investigar las operaciones efectuadas durante la desconexión.

A partir de los resultados satisfactorios en las pruebas iniciales el prototipo del Servidor de Auditoría se puso en producción en forma permanente. Actualmente la BD del Servidor de Auditoría cuenta con 88 tablas, aquellas consideradas más "sensibles" a los fines de auditoría y control, sobre un total de 1.349 tablas pertenecientes a dos aplicativos monitoreados.

En el ambiente de trabajo provisto por servidor de auditoría, el auditor puede realizar diariamente los siguientes reportes generales:

- De cada tabla aquellas operaciones que significan cambios en datos permanentes, es decir, aquellos datos que una vez generados no pueden ser cambiados, por ejemplo: identificación de los clientes, número de un comprobante, etc..
- Existencia de operaciones de UPDATE o DELETE sobre tablas de auditoría del sistema auditado, cuyos datos se generan por la acción de triggers. Este control parte de la premisa que las tablas de auditoría sólo deben contener operaciones de INSERT.
- Identificación de las operaciones ejecutadas directamente (por el DBA) sobre la BD.
- Operaciones ejecutadas durante la desconexión de los triggers.
- Reportes de operaciones ejecutadas en forma aislada e individual, cuando deberían resultar de procesos masivos y automáticos. Ejemplo: liquidación de sueldos.

5. Aportes del Servidor de Auditoría y log de transacciones

El prototipo desarrollado de Servidor de Auditoría a partir del log de transacciones cuenta con su propio sistema operativo, software de gestión de bases de datos (DBMS), herramientas de monitoreo de red y programas de análisis de datos específicos para las funciones de análisis y control; estando su administración bajo responsabilidad del área Auditoría Interna.

Entre los aportes del modelo propuesto en este estudio, identificamos:

- Brinda un ambiente específico y propio de procesamiento al área de Auditoría Interna de la organización, independiente del control e intervención del área Sistemas. Virtualmente contiene los datos de todas las operaciones procesadas por los sistemas de gestión, generando las correspondientes datos duplicados (pistas de auditoría digitales); todo bajo la responsabilidad y control del área Auditoría Interna.
- Independiza el trabajo del auditor de los condicionamientos impuestos por la operatoria del sistema de gestión. Actualmente el trabajo de los auditores debe subordinarse a las prioridades fijadas por quienes administran el sistema de gestión.
- Permite mejorar el sistema de control interno de la empresa, al proveer una nueva fuente de información adicional para corroborar los datos brindados por el sistema de gestión comercial.

- Reduce a su mínima expresión el riesgo asociado a la alteración de la información que utilizará el auditor para sus tareas de control, logrando el objetivo primordial de mantener la integridad de los datos.
- Brinda un tablero de control para funciones de auditoría y control. A partir de herramientas de consulta a la BD del Servidor de Auditoría se desarrollan opciones de consultas para el auditor en forma automática y con la frecuencia apropiada, a manera de tablero de comandos, que genere reportes para detectar presuntas irregularidades asociadas al manipuleo de la información contenida en la BD de gestión.
- Unifica en una BD específica para la función de auditoría la información derivada de las operaciones críticas procesadas por los sistemas de gestión de la organización.

6. Conclusiones

La propuesta se basó en la incorporación de un nuevo dispositivo -Servidor de Auditoría- a la red de procesamiento de datos de una empresa. Este nuevo servidor tiene la función de recoger y procesar toda la información que necesita el área Auditoría Interna de la empresa sobre las operaciones procesadas, conservando pistas de auditoría digitales derivadas del sistema auditado.

Según el mencionado estudio de Hui Du y Saeed Roohani(1), un modelo de monitoreo continuo debe enfatizar dos criterios principales: a) el sistema auditor debe ser un sistema separado para mantener la independencia del auditor, y b) debe existir una efectiva interacción y comunicación con el sistema auditado en forma permanente. Creemos que este desarrollo cumple ambos requisitos: genera un ambiente de trabajo separado para Auditoría Interna y asegura el monitoreo completo de todas las transacciones procesadas por el sistema auditado.

En síntesis, esta alternativa proporciona un ambiente exclusivo y seguro para los auditores, administrado por ellos e independiente de cualquier condicionamiento e ingerencia por parte de otras áreas de la empresa, destacando los siguientes aportes:

- *Base de datos propia:* en efecto, al contar con una base de auditoría propia, que ha sido definida con tablas y datos que hacen a la esencia de las transacciones económicas y financieras de la empresa, se facilita la obtención de listados y reportes necesarios para los controles habituales.
- *Independencia*: en tal sentido, y reafirmando lo expresado más arriba, no sólo no depende del Área de Sistemas para obtener información, sino que por el contrario el acceso al Servidor de Auditoría queda restringido al personal de Auditoría Interna.
- *Duplicación de datos claves*: facilita un control adicional de importante valor agregado, toda vez que permite efectuar controles cruzados entre las bases de auditoría y la de gestión.
- *Control de la actividad de los administradores de la base de datos*: El esquema basado el log de transacciones aporta un registro detallado de todas las operaciones que realizan los Administradores de bases de datos (DBA) en forma directa. Relacionado con ello también se cuenta con el reporte de operaciones de desconexión-conexión de triggers.

En general se considera que los resultados alcanzados han posibilitado a la empresa contar con una herramienta de auditoría continua, permitiendo un monitoreo diario, específico y detallado de la totalidad de los datos correspondientes a las tablas controladas (las consideradas más sensibles y significativas para el control) y que hacen a la esencia del negocio. De esta manera, al disponer de una BD de auditoría, los auditores pueden hacer controles cruzados y validaciones propias sobre los datos capturados, y a su vez, un monitoreo general del resto de la información complementaria permitiendo rearmar desde un punto cualquiera el flujo de una transacción y hacia cualquier dirección.

En tal sentido, la información obtenida de la BD de auditoría permite conocer en detalle toda la evidencia informática necesaria para el caso de que la misma sea requerida por terceros; al contener sobre cada evidencia registrada: a) datos propios de la operación (fecha y hora, usuario, terminal, número del archivo log, acciones de los triggers) , b) información o valor actual de los campos de la BD de gestión sobre los que actuó la operación, c) información o valor anterior de dichos datos (producto de UPDATE o DELETE).

Referencias Bibliograficas:

(1) Hui Du y Saeed Roohani, “Meeting Challenges and Expectations of Continuous Auditing in the Context of Independent Audits of Financial Statatments”, International Journal of Auditing, 11: 133-146, 2007.

(2) Debreceny, R., Gray, G, Jun-Jin, J, Lee, K y Yau, W. – "Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Funcionality" – Journal of Information Systems, Vol.19 N° 2, 2005.

(3) Alles, Michael; Vasarhelyi, Miklos y otros, "Continuous Monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemmens*",* 2005.

(4) Alles, Michael; Alexander Kogan, Vasarhelyi, Miklos. "Continuous Data Level Auditing: Business Process Based Analytic Procedures in an Unconstrained Data Environment". 2007. Rutgers University.

Bibliografía:

1. Alles, Michael; Vasarhelyi, Miklos y otros (2005), *"Continuous Monitoring of business process controls: A pilot implementation of a continuous auditing system at Siemmens"*.
2. Alles, Michael; Alexander Kogan, Vasarhelyi, Miklos (2007), *"Continuous Data Level Auditing: Business Process Based Analytic Procedures in an Unconstrained Data Environment"*. Rutgers University.
3. Alles, M, Kogan, Alexander y Vasarhelyi, Miklos (2000), "*Accounting in 2015"*, The CPA Journal, November.
4. Alles, M, Kogan, Alexander y Vasarhelyi, Miklos (2004), *"Restoring auditor credibility: tertiary monitoring and logging of continuous assurance systems".* International Journal of Accounting Information Systems 5.2.183-202.
5. Alles, M., Tostes, F., Vasarhelyi, M. y Riccio, E. (2006) "*Continuous auditing: The USA experience and considerations for its implementation in Brazil*, Journal of Information System and Technology Managment, V. 1, 2.
6. Debreceny, R., Gray, G, Jun-Jin, J, Lee, K y Yau, W. (2005), *"Embedded Audit Modules in Enterprise Resource Planning Systems: Implementation and Funcionality"* – Journal of Information Systems, Vol.19 N° 2.
7. Hui Du y Saeed Roohani (2007), *"Meeting Challenges and Expectations of Continuous Auditing in the Context of Independent Audits of Financial Statatments"*, International Journal of Auditing, 11: 133-146.
8. O'Really, Anthony, (2006) "*Continuous auditing: wave of the future?",* The Corporate Board. Sept/Oct. p.24-26.
9. Vasarhelyi, Miklos and Halper, Fern – (1991) *"The Continuous Audit of Online Systems"*, Auditing: A journal of Practice & Theory, Vol 10, N° 1.
10. Vasarehelyi, Milkos and Lombardi, D (2010), "*The future of audit: A Modified Delphi Approach, Working paper",* Rutgers Accouting Research Center.
11. Voarino, G. P. and Vasarhelyi, M (2001)*, "Contiunous Perfomance and Control Monitoring at BIPOP"*, Working paper, Rutgers University, Dep.. of Accouting.