ARTÍCULO

Modelo de gestión de log para la auditoría de información de apoyo a la toma de decisiones en las organizaciones

Model log management for the audit information, to support decision making in the organizations

MSc. Oiner Gómez Baryolo, Dra. C. Vivian Estrada Sentí, Ing. René Rodrigo Bauta Camejo, Dra. C. Isabel García Rodríguez

Universidad de las Ciencias Informáticas. La Habana, Cuba.

RESUMEN

En los últimos años, la auditoría de información ha aumentado en importancia como resultado de su impacto en la prevención o detección de violaciones que afecten la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos de una organización. La auditoría de información es un componente importante de la auditoría informática y depende en gran medida de la expresividad de los log de eventos para garantizar la calidad de los resultados. El estándar XES y el marco de trabajo Auditing, constituyen las soluciones más novedosas enfocadas en la gestión de log de eventos. El análisis de estas y otras soluciones arrojó como resultado que existen limitaciones relacionadas con la formalización de la estructura de los log de eventos, las cuales impactan de forma negativa en la calidad del resultado de los análisis. Estas deficiencias dificultan la toma de decisiones relacionadas con la seguridad, el funcionamiento de los sistemas de información y su impacto en los procesos de negocio de la organización. A partir de la problemática existente, la principal contribución de este trabajo se enmarca en la concepción de un modelo de gestión de log de eventos para la auditoría de información de apoyo a la toma de decisiones en las organizaciones con diferentes objetivos. En él se describen los conceptos necesarios para integrar de forma coherente los procesos de negocio, los actores, los sistemas de información y demás aspectos asociados a la aplicación. El modelo se aplicó en el desarrollo de varios sistemas de información, y se obtuvieron buenos resultados.

Palabras clave: Sistema de información, auditoría de información, auditoría informática, log de eventos, XES, Auditing.

ABSTRACT

In recent years, the information audit has increased in importance due to its impact on the prevention or detection of violations that affect the confidentiality, integrity, availability and traceability of the organization resources. The information audit is an important component of the informatics audit depends largely on the expressiveness of the event log to ensure the quality of results. The standard XES and Auditing framework are the most innovative solutions focused on managing the event log. The analysis of these and other solutions, showed there are limitations related to the structure of the event log formalization, which impact negatively on the quality of the analysis results. These deficiencies hinder decision making related to security, information systems operation and their impact on business processes of the organization. From the problematic existing, the main contribution of this work is the design of a model event log management for the audit information, to support decision making in organizations with different goals. It describes the needed concepts to integrate, in a consistently way, the business processes, actors, Information Systems and other aspects associated with the application environment. The model was applied in the development of different information systems, having good results.

Key words: information system, audit information, informatic audit, event log, XES, Auditing.

INTRODUCCIÓN

En la actualidad, las organizaciones que desarrollan una cultura de gestión de información y conocimiento logran convertirse en entidades de avanzada. La gestión del conocimiento (GC) es un nuevo enfoque gerencial que se basa en el reconocimiento y la utilización del valor más importante de las organizaciones: los recursos humanos, su conocimiento y su disposición a colocarlos a su servicio. Los resultados de una adecuada GC contribuyen a una mejor toma de decisiones y a trazar estrategias para el desarrollo y el aprendizaje organizacional. La GC ha cambiado la forma en que las organizaciones gestionan sus procesos, por la necesidad de poder contar con información confiable, íntegra y oportuna en todo momento que contribuya al cumplimiento de sus objetivos estratégicos. En los últimos años, las tecnologías de la información y las comunicaciones (TIC) evolucionaron para dejar de ser un componente básico del negocio y convertirse en un elemento crítico para la ejecución de las estrategias en este ámbito.[1]

La materia prima para el cumplimiento de los objetivos estratégicos de las organizaciones y el proceso de toma de decisiones es el empleo adecuado de la información y el conocimiento acumulado a lo largo de su historia. Lo que hace que el conocimiento sea valioso para las organizaciones es la capacidad de mejorar las decisiones y medidas adoptadas sobre la base de su uso. El análisis de los datos históricos permite tomar decisiones más acertadas sobre cómo dirigir la organización para alcanzar mayor eficiencia y eficacia y mantenerla en un lugar competitivo en el mercado. Según un estudio realizado por el Reino Unido, el 90 y el 63 % de las organizaciones de mayor y menor tamaño, respectivamente, dependen del acceso a sus sistemas de información (SI) para lograr una gestión eficiente de sus procesos.[2]

Las organizaciones de hoy día dependen de la disponibilidad de soluciones de gestión, como los sistemas de planificación de recursos empresariales (ERP), sistemas de gestión de cadena de suministros (SCM) y sistemas de gestión de la relación con los clientes (CRM), entre otros. Estos SI permiten generar ingresos, conectar clientes, proveedores, empleados y socios de forma ininterrumpida.[3] Sin embargo, los ataques a estos sistemas aumentan cada día, a pesar de que no dejan de surgir nuevos requisitos de cumplimiento de normativas sobre la seguridad de la información.[4] En el caso de los SI aplicados en el área de la salud resulta fundamental la AI para prevenir ataques que puedan ocasionar riesgos para los pacientes, pérdida de confidencialidad en la información y otras afectaciones que atenten contra la calidad en la toma de decisiones.

Dado los riesgos de seguridad a los que se enfrentan los SI, cada día cobra mayor importancia el control interno en las organizaciones.[5] Una parte importante del control interno lo constituye la auditoría informática,[6,7] destinada a evaluar el cumplimiento de normativas, la gestión de los recursos, el funcionamiento y seguridad de los SI, entre otros elementos relacionados con el uso de las TIC en las organizaciones. Para esto se apoya fundamentalmente en la auditoría de la información (AI) con el objetivo de realizar análisis sobre la información que generan los SI, como resultado de la ejecución automática de procesos internos o la interacción con otros sistemas o usuarios.[8] La AI es un examen crítico que se realiza sobre la información que generan los SI, con el fin de evaluar la eficacia y la eficiencia de un proceso, un sistema, una persona, una organización u otro concepto que forme parte del entorno.[9-11] Los log de eventos constituyen una fuente importante de información dentro de cualquier organización para realizar AI.[12] Un log de eventos es una evidencia de los acontecimientos que ocurren dentro de los SI y las redes de una organización. Los log están compuestos por eventos de entrada y cada entrada contiene información relacionada con una acción u operación específica que se ha ejecutado en un sistema.

El problema que se pretende resolver con el presente trabajo es la falta de estructuración, información y expresividad en los log de eventos para soportar la AI con diferentes objetivos. Entre los objetivos fundamentales se encuentra la posibilidad de realizar análisis para prevenir, detectar, predecir, evaluar y recomendar acciones relacionadas con la seguridad, el funcionamiento y la gestión de los procesos de negocio en los escenarios de desarrollo o de despliegue de los SI.

El análisis de las principales normas, guías, modelos, estándares y metodologías existentes en la bibliografía para la AI permitió dividir estas soluciones en dos grupos fundamentales según su nivel de descripción, objetivos y limitaciones:

- El primer grupo está compuesto por el informe del Comité de Patrocinadores de la Comisión Treadway (COSO), la Biblioteca de Infraestructura de Tecnologías de la Información (ITIL), los Criterios de la Comisión de Control de Canadá (CoCo), el modelo de Objetivos de Control para tecnología de la información y relacionada (COBIT) y la norma ISO/IEC 27002:2005.[13] Estas soluciones se limitan a establecer políticas y recomendaciones en función de la auditoría de los recursos para lograr los objetivos de negocio de las organizaciones.

- El segundo grupo lo integra el flujo de eventos extensibles (XES) y el marco de trabajo Auditing. En ellos se proponen soluciones a un nivel más bajo que aumentan sus posibilidades de aplicación. Este grupo si provee especificaciones técnicas, pero no conciben de forma integrada los procesos de negocio y los SI. Esto trae consigo que se limiten muchos análisis importantes para las organizaciones relacionados con el funcionamiento del sistema en la ejecución de los diferentes procesos. Entre los puntos de reutilización identificados en estas

soluciones se encuentran los conceptos y definiciones de XES orientadas al registro de eventos y parámetros relacionados con los procesos y los análisis orientados a la mejora y el descubrimiento de procesos del marco de trabajo Auditing.[14,15]

A pesar de los avances mostrados en los últimos tres años en el ámbito de la AI, la conceptualización, integración y escalabilidad de las soluciones relacionadas con la gestión de log de eventos constituyen un reto en la actualidad. Las limitaciones identificadas impactan de forma negativa en la GC existente en los log de eventos, para el apoyo a la toma de decisiones en las organizaciones, con diferentes perspectivas.

El objetivo de la presente investigación es proponer un modelo que refleje y describa los principales conceptos que deben modelarse para obtener un registro eficiente de todos los eventos que se ejecuten en un SI, su relación con los elementos que forman parte del entorno y los procesos de negocio que informatiza. El registro de los eventos permitirá analizar el comportamiento de los parámetros que afecten en alguna medida la robustez, escalabilidad y seguridad del sistema y de los datos. También brindará la posibilidad realizar análisis para detectar patrones, anomalías o predecir comportamientos y descubrir modelos relacionados con la gestión de los procesos de negocio de las organizaciones.

MODELO DE GESTIÓN DE LOG

Cada vez se hace mayor el número de procesos que se informatizan en las organizaciones con el fin de obtener los beneficios que genera el uso de las TIC. Los propios cambios ocurridos en el tratamiento informático han introducido transformaciones sustanciales sobre el concepto tradicional de AI. La GC provee un conjunto de herramientas para lograr la eficacia en la realización de las AI de los procesos de negocio y los SI en las organizaciones. Es necesario concebir de forma integrada el diseño de los procesos de negocio y su ejecución en el SI para garantizar que los log de eventos contengan la información necesaria sobre el funcionamiento del SI y los procesos que él informatiza en la organización. La figura 1 muestra el modelo conceptual general para el registro y análisis de los log de eventos generados por el SI, como resultado de la ejecución de los procesos de negocio.

El modelo concibe la AI con tres objetivos fundamentales, orientada a la seguridad y al funcionamiento del SI y a la mejora de procesos. Es aplicable tanto a los SI desarrollados orientados a procesos como a los que no fueron concebidos desde el inicio bajo esta filosofía; de ahí sus mayores posibilidades de aplicación. Su concepción incorpora la gestión integrada de los log de eventos referentes al funcionamiento y seguridad del SI, la ejecución de los procesos de negocio y los usuarios que ejecutan dichos procesos. Además incluye aspectos relacionados con el almacenamiento y el análisis de los log de eventos para apoyar la toma de decisiones en el entorno de desarrollo y de despliegue de los SI. Estos elementos son de vital importancia para las organizaciones que requieren modos sistemáticos para la gestión de información y la identificación y conversión de las habilidades, conocimientos y experiencias individuales en conocimiento de la organización.

En el *Nivel de negocio* se agrupan los procesos y actividades que fueron modelados inicialmente para ejecutarse en el SI. En este nivel se especifica si la actividad puede ser ejecutada por uno o varios roles, o solo por algunos usuarios que cumplen dichos roles. Además se puede establecer si los roles o usuarios ejecutan

la actividad en una o varias estructuras de la jerarquía definida. La relación entre estos niveles permite identificar qué usuarios o roles realizaron cierta actividad y en qué nivel de la jerarquía la ejecutaron. La especificación de la estructura donde se va a ejecutar la actividad, garantiza que los datos se puedan agrupar por estructura, lo cual resulta útil para lograr la compartimentación de la información y con esto evitar violaciones de confidencialidad, integridad o disponibilidad.

El *Nivel de Sistema* contiene la estructura del SI que puede contener uno o varios subsistemas. Para lograr la integración entre el modelo de proceso de negocio y el SI es necesario especificar la acción del sistema que ejecuta cada una de las actividades atómicas que conforman el proceso de negocio a informatizar. De esta relación se puede obtener los privilegios que tienen los roles y usuarios sobre las diferentes partes del sistema y estructuras de la jerarquía. La integración del *Nivel de Sistema* con los niveles anteriores forma la base para el registro coherente de las acciones del SI en relación con las actividades que conforman un proceso de negocio.

Concluida la integración entre los niveles anteriores, el sistema se encuentra en condiciones de ejecutar la secuencia de actividades que conforman un proceso, sin violar las reglas del negocio establecidas. Una parte importante de los sistemas de información lo constituye la arquitectura de datos. El marco de trabajo Auditing, propuesto por *Van der Aalst*,[14] define en su arquitectura una base de datos denominada *Datos actuales (Current data)*. En esta base de datos se encuentran los procesos que no han concluido. Sobre ellos se proponen un conjunto de análisis para predecir comportamientos, detectar violaciones y recomendar acciones que fomenten la mejora de proceso. Al completarse la ejecución de cada instancia de un proceso, todo lo relacionado con ella pasa a una base de datos denominada *Datos históricos (Historic data*) para ser objeto de otros tipos de análisis.

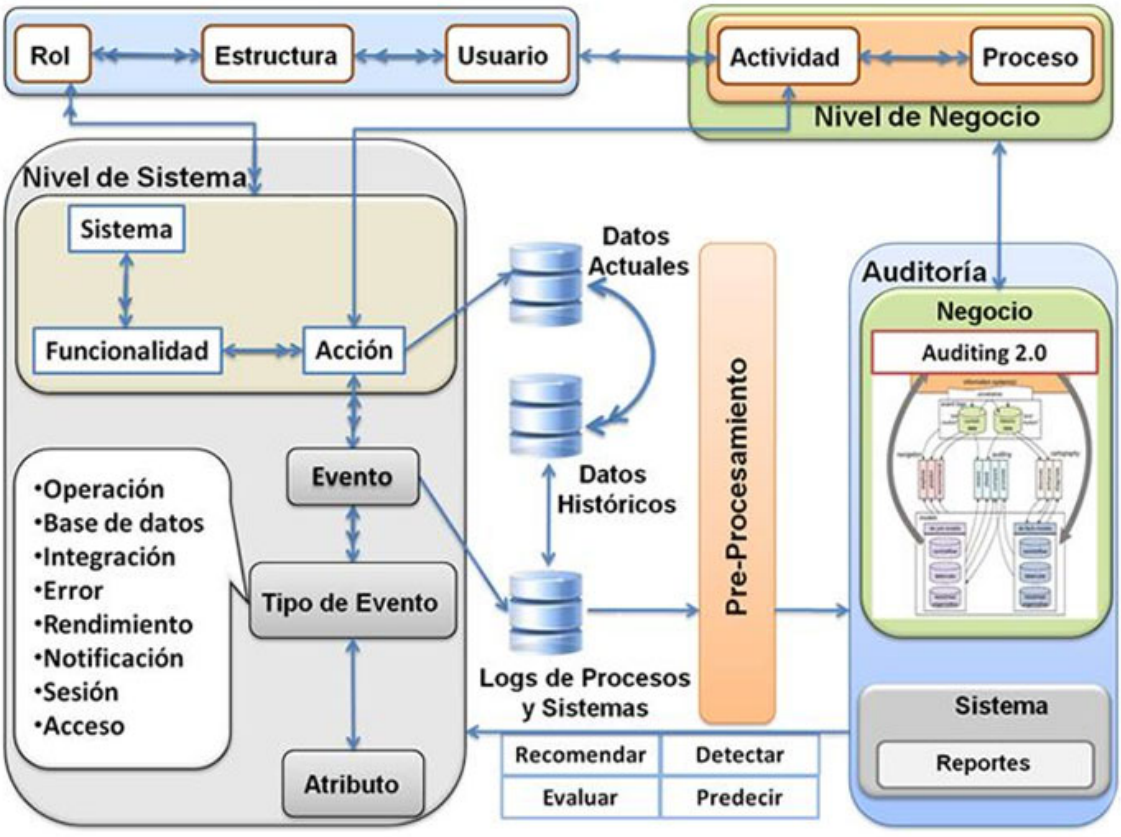


Fig. 1. Modelo de gestión de log.

En la arquitectura de datos del modelo (fig. 1) se define una base de datos perteneciente al SI denominada *Datos Actuales*. En ella solo se modelan los conceptos y atributos que soportan la gestión de los datos del proceso a informatizar. No incorpora las entidades y parámetros asociados al modelo de proceso (instancia, actividad, rol, entre otros). Todas las operaciones que se ejecutan en la base de datos del sistema se replican siempre a una base de datos denominada *Datos Históricos*. La base de datos de histórico mantiene la misma estructura que la de *Datos Actuales*; solo se le debe incorporar a cada tabla un nuevo identificador para evitar los conflictos de llaves. Estos conflictos pueden surgir porque en la base de datos que contiene los datos actuales solo se encuentran los últimos valores del objeto, mientras que en la base de datos de históricos se encuentran los actuales y los anteriores.

En los escenarios descritos, el usuario puede ejecutar una acción en el sistema, que representa una actividad dentro del proceso de negocio. La acción en el sistema puede desencadenar una operación (INSERT, DELETE, UPDATE) en la base de datos que contiene los datos actuales, esta se replicará inmediatamente en la base de datos de históricos. Por esta razón cada instancia de un objeto existente en la base de datos del sistema está relacionada con una o varias instancias en la base de datos históricos. Las acciones del sistema, aparte de ejecutar operaciones en la base de datos, pueden desencadenar un conjunto de eventos que constituyen información básica para la AI. Los eventos se dividen por tipos para disminuir el crecimiento de la información, facilitar su análisis y mantener la escalabilidad de la solución. Los eventos más comunes identificados hasta el momento por los autores, y que forman parte del modelo, se resumen a continuación:

- *Operación*: evento que registra los atributos generales relacionados con la estructura del sistema donde se ejecutó la acción y a qué actividad y proceso de negocio responde. Incluye, además, información sobre quién la ejecutó, en qué estructura de la jerarquía y desde que dirección IP. Los demás eventos que se definen a continuación incluyen atributos de este tipo de evento e incorporan otros relacionados con su gestión.

- *Base de datos*: está encargado de registrar los atributos relacionados con el nivel de base de datos. Se ejecuta si una acción realiza alguna operación en la base de datos.

- *Integración*: se refiere al que se ejecuta si, como resultado de una acción en el sistema, se consume un servicio para complementar alguna actividad del negocio.

- *Error*: es el que se desencadena producto de un error en la ejecución de una acción del sistema. Pueden generarse por un error en la codificación o en las tecnologías que soportan el sistema. Mayormente son errores no controlados; de ellos se registra información relacionada con su origen.

- *Excepciones*: los que se producen como consecuencia de la violación de reglas impuestas por el negocio o por las restricciones tecnologías del entorno.

- *Rendimiento*: es el que se activa si se quiere registrar información relacionada con el consumo de memoria, tiempo de respuesta y demás parámetros relacionados con la acción ejecutada.

- *Notificación*: se ejecuta como resultado de reglas definidas que traen consigo el envío de una alerta o aviso. Las notificaciones se activan si se ejecuta una acción que contenga alguna de ellas y pueden enviarse por correo, teléfono, sistema, entre otras vías.

- *Validación*: se desencadena en el momento que se activa la validación de una acción ejecutada en el sistema. Se establecen con el fin de regular la ejecución de ciertas acciones a través de condiciones. De este tipo de evento se registra la

validación ejecutada y si fructificó o no. En caso que no fructifique se incluye la justificación del resultado.

- *Acceso*: el que se activa en el momento que se ejecuta o se trata de ejecutar una acción no autorizada en el sistema. Registra información relacionada con la violación para identificar brechas de seguridad y posibles responsables.

El registro de los eventos descritos anteriormente debe proveer la información necesaria para realizar análisis sobre el funcionamiento del SI y sobre los procesos de negocio que él informatiza. Con este objetivo, la arquitectura de datos del modelo propuesto incorpora una nueva fuente de datos denominada *Logs de Procesos y Sistemas*. En esta fuente de datos se almacena todo lo referente a las acciones que se ejecutan en el sistema. Si el sistema está orientado a procesos, se le incorporan parámetros como el identificador del proceso, de la instancia y de la actividad relacionada con la acción ejecutada en el sistema. En caso de que la acción traiga consigo operaciones en la base de datos (*Datos Actuales*), se registrará un evento de tipo *Base de Datos* que contiene el identificador del objeto afectado. Este identificador está relacionado con la instancia del objeto almacenada en los *Datos Históricos* donde se encuentran los demás atributos asociados a él. De esta forma se relacionan las acciones ejecutadas en el sistema con las actividades y procesos modelados. Esta relación hace posible que se puedan identificar todas las operaciones a nivel de sistema y de base de datos ejecutadas sobre un objeto y su relación con las actividades que forman parte de la instancia del proceso en ejecución.

La base de datos de *Logs de Procesos y Sistemas* contiene las instancias de procesos en ejecución y las completadas. Por esta razón es necesario realizar un pre-procesamiento de los datos para garantizar las entradas requeridas por Auditing, incluido en el modelo propuesto para el análisis orientado a proceso. Este marco de trabajo necesita dos entradas fundamentales, las instancias en ejecución y las instancias completadas; ambas entradas se garantizan con el pre-procesamiento de los datos del modelo propuesto. Al asumirse Auditing se incorporan todas las ventajas que proporcionan los análisis que realiza en función de la mejora de proceso. El registro de los eventos a nivel de sistema y de base de datos, apoyado por el pre - procesamiento, constituye un factor importante para el descubrimiento de procesos en los sistemas que no fueron concebidos con este propósito desde el inicio. El descubrimiento de procesos puede ser un punto de partida muy útil para iniciar la informatización de un proceso o simplemente mejorarlo.

AUDITORÍA DE INFORMACIÓN ENFOCADA EN LA SEGURIDAD Y EN EL FUNCIONAMIENTO DE LOS SISTEMAS

La seguridad, robustez y escalabilidad de los SI son aspectos que deben garantizarse desde el inicio del proceso de desarrollo. Un punto importante para lograr este objetivo lo constituye el registro y análisis de las acciones ejecutadas en el sistema y los eventos desencadenados por cada una de ellas.

Las soluciones de registro y análisis de eventos constituyen una herramienta esencial para llevar un control estricto de las acciones que se ejecutan en los SI, con el objetivo de detectar o predecir violaciones de seguridad, cuellos de botella, así como problemas de rendimiento producto de un mal diseño e implementación del sistema o limitaciones de las tecnologías. El modelo propuesto permite desarrollar soluciones que ayuden a determinar qué acciones o servicios son los más críticos y así extremar las medidas para lograr su correcto funcionamiento.

Permite identificar los sistemas o subsistemas, funcionalidades o acciones que más excepciones producen además de su origen. La detección inmediata de estas anomalías permite dedicar el tiempo y los recursos necesarios para erradicarlas con la mayor brevedad posible y de esta forma evitar atrasos en el cronograma acordado. Otro de los parámetros que se debe garantizar es el rendimiento del sistema. Con este objetivo, se debe proveer una solución que permita el control y seguimiento del tiempo de respuesta y uso de memoria de todas las actividades que se ejecutan en el sistema. El análisis de esta información puede apoyar la decisión de corregir el análisis e implementación de las actividades implicadas para mejorar estos parámetros y, de esta forma, garantizar la robustez del sistema en escenarios de bajas prestaciones tecnológicas.

Los SI de mayor calidad existentes en la actualidad están desarrollados sobre arquitecturas orientadas a servicios para lograr la integración entre sus módulos o con sistemas externos. Las afectaciones que puede provocar la falla de alguno de estos servicios demuestra la necesidad de llevar un control estricto de su utilización, para detectar errores que pueden atentar contra la disponibilidad de una parte o la totalidad del sistema. El registro de estos eventos permite determinar cuáles son los servicios más críticos de la arquitectura y la cantidad de servicios que se consumen como parte de una acción. Los resultados obtenidos apoyan la toma de decisiones para reducir la cantidad de servicios utilizados para obtener un dato, evitar cuellos de botellas y las violaciones de seguridad.

Todos los análisis descritos hasta el momento, enfocados en la mejora del SI, están soportados por diferentes reportes, los que pueden estar encaminados a detectar, predecir, evaluar o recomendar aspectos relacionados con el SI:

- *Detectar*: se logra a partir de los análisis que se realizan con el fin de detectar violaciones, errores, inconsistencias, entre otros aspectos negativos o positivos en el sistema.
- *Predecir*: se logra a través del análisis de los diferentes eventos desencadenados en el sistema. Se puede predecir el comportamiento del sistema bajo ciertos parámetros; ejemplo: el rendimiento con una cantidad de operaciones ejecutadas concurrentemente.
- *Evaluar*: constituye un aspecto importante para determinar la robustez, seguridad y escalabilidad del sistema en los diferentes entornos. Los reportes que se obtienen de la base de datos *Logs de Procesos y Sistemas* permiten evaluar la criticidad de las fallas, servicios, violaciones, entre otros aspectos que se originaron en el sistema.
- *Recomendar*: basado en los análisis anteriores se pueden recomendar cambios en el sistema para erradicar las violaciones, fallas o posibles limitaciones futuras. No solo se recomiendan acciones para solucionar eventos que tuvieron lugar; también es posible recomendar acciones para lograr mejores resultados en un flujo en ejecución.

CASO DE ESTUDIO

Actualmente en Cuba se desarrollan varios sistemas de información como parte del proceso de informatización de la sociedad, con el objetivo de aumentar la eficiencia y la efectividad de los procesos. Uno de estos sistemas es el ERP Cedrux, desarrollado sobre herramientas y tecnologías libres. Cedrux tiene la responsabilidad de soportar la planificación, protección y distribución de los recursos del país de forma eficiente. Por la importancia e impacto de este sistema, fue necesario

establecer una política eficiente de gestión de log de eventos que permitiera obtener los beneficios que reporta la AI, en función de mejorar la seguridad, el funcionamiento y la gestión de los procesos de negocio en Cedrux. Para lograr este objetivo se decidió aplicar el modelo propuesto, en el desarrollo de un componente de gestión de log de eventos integrado a Cedrux, que garantice los requisitos identificados. Con este objetivo se utilizaron las tecnologías y herramientas libres que se muestran en el cuadro.

Cuadro. Tecnología y herramientas utilizadas

Tecnologías	Herramientas
▪ ExtJs 2.2 (JavaScript) ▪ Zend Framework 1.11 (PHP) ▪ ORM Doctrine 1.2 (PHP)	▪ PostgreSQL 8.3 ▪ Apache 2.0 ▪ Mozilla Firefox 2.2

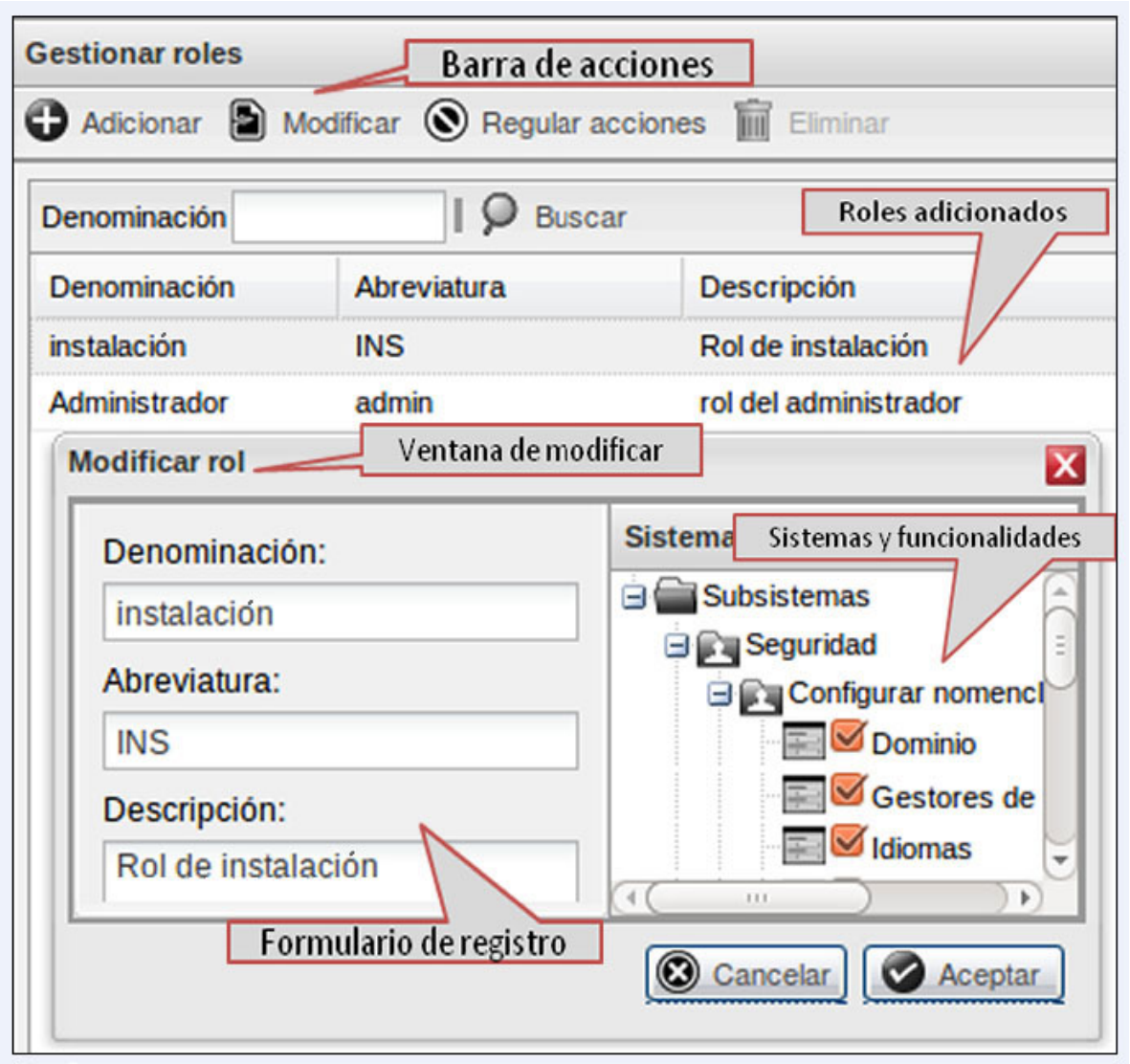


Fig. 2. Interfaz para la relación entre estructuras.

La efectividad del registro y la AI que se logre con un componente de gestión de log de eventos, depende en gran medida de la calidad de la implementación del modelo propuesto. La configuración inicial de los procesos y eventos que se desean auditar influyen en la expresividad final de los log de eventos; por esta razón es necesario que en esta etapa se definan las diferentes estructuras que caracterizan el dominio organizacional, los actores del negocio y el SI. Concluida la configuración, se pueden establecer las relaciones entre los procesos y estructuras del nivel de aplicación y de datos del sistema. La figura 2 muestra la interfaz que permite establecer dicha relación. A la izquierda se muestran los procesos existentes, en el centro la estructura del sistema a nivel de aplicación y a la derecha la estructura del sistema a nivel de datos. La relación se inicia con la selección del proceso que se desea configurar. Posteriormente se selecciona la acción que pertenece a este proceso y se especifica con qué objetos del nivel de base de datos interactúa. La gestión orientada a proceso permite definir los procesos críticos y decidir si se van a registrar todos los eventos que se produzcan en ambos niveles como resultado de la ejecución de una actividad, para realizar análisis posteriores.

En las organizaciones donde se utilizan SI para gestionar sus procesos, las responsabilidades se agrupan por roles. Estas responsabilidades se traducen en privilegios en el sistema, por esta razón, el concepto rol es uno de los más importantes dentro del control de acceso. La figura 3 refleja los componentes fundamentales que debe contener una interfaz de gestión de roles. Para la creación de un rol es necesario especificar los parámetros relacionados con su identificación como concepto y los privilegios sobre las diferentes estructuras del sistema.

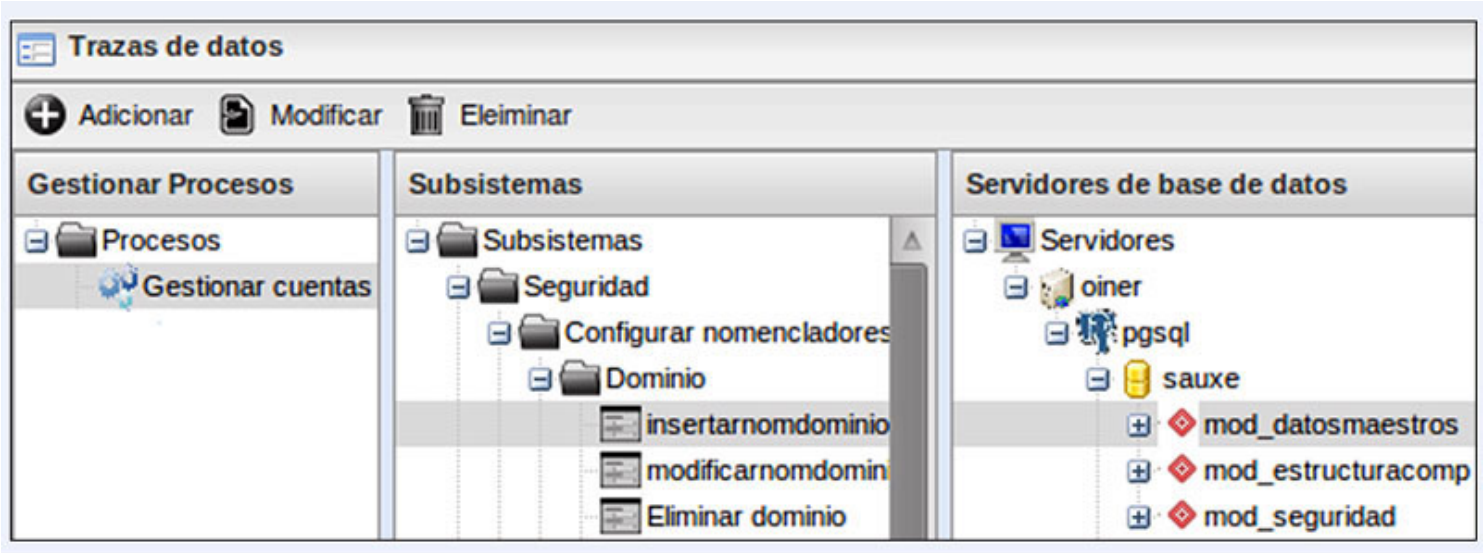


Fig. 3. Interfaz para la gestión de roles.

Al asignarle privilegios a un rol sobre los sistemas, la solución de control de acceso construye dinámicamente un rol de base de datos sin permisos de conexión, pero con privilegios para realizar las operaciones definidas en la configuración de la integración entre las estructuras de ambos niveles. Concluido el proceso de gestión de roles, se debe decidir qué tipo de escenario se va a adoptar. En función del escenario definido se crea un rol con los mismos privilegios que el padre, pero con permiso de conexión y se le asigna por sistema, por rol o usuario del nivel de aplicación.

Concluido el proceso de configuración y asignación de privilegios, la herramienta de gestión de log de eventos tiene los elementos necesarios para registrar todas las actividades que se realicen en el sistema. El registro de las actividades da las posibilidades de realizar análisis con fines específicos en los diferentes entornos. La figura 4 muestra un reporte que evidencia el comportamiento de los sistemas en cuanto al atributo rendimiento. El reporte de rendimiento está compuesto por una serie de atributos, alguno de los cuales se describen a continuación:

- *Categoría*: está relacionado con el objetivo que se persigue al realizar el análisis. Puede ser para evaluar la arquitectura, la seguridad, los sistemas, entre otros.

- *Proceso*: se refiere al que pertenece la acción ejecutada.

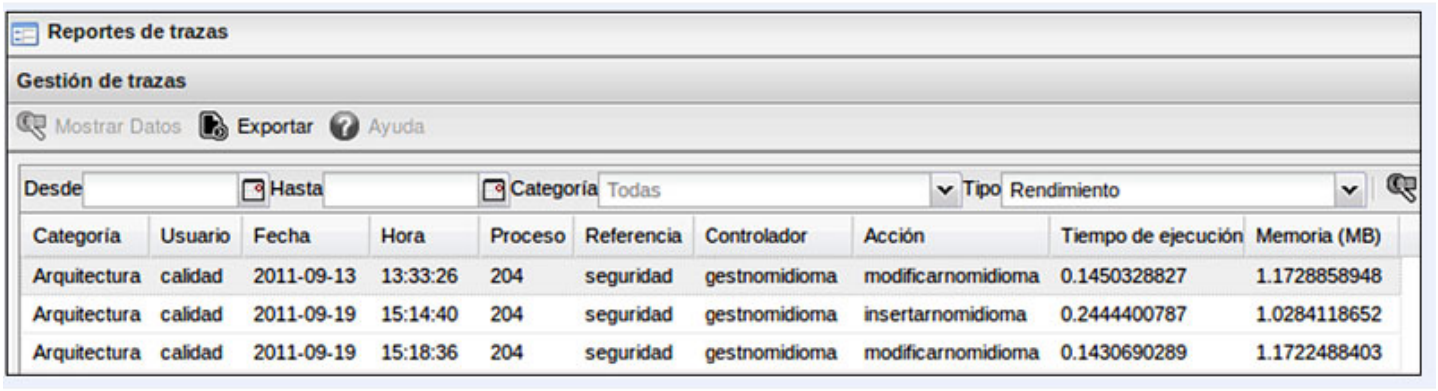
- *Referencia*: sistema o subsistema al que pertenece la acción.

- *Controlador*: objeto responsable de ejecutar la acción.

- *Acción*: es la operación o evento que se ejecuta en el nivel de aplicación.

- *Tiempo de ejecución*: es el tiempo que demora el sistema para darle la respuesta al usuario.

- *Memoria*: Uso de memoria del sistema para ejecutar la acción solicitada.



Categoría	Usuario	Fecha	Hora	Proceso	Referencia	Controlador	Acción	Tiempo de ejecución	Memoria (MB)
Arquitectura	calidad	2011-09-13	13:33:26	204	seguridad	gestnomidioma	modificarnomidioma	0.1450328827	1.1728858948
Arquitectura	calidad	2011-09-19	15:14:40	204	seguridad	gestnomidioma	insertarnomidioma	0.2444400787	1.0284118652
Arquitectura	calidad	2011-09-19	15:18:36	204	seguridad	gestnomidioma	modificarnomidioma	0.1430690289	1.1722488403

Fig. 4. Reporte de rendimiento.

La información que refleja este reporte permite hacer un análisis del rendimiento por sistema, procesos y actividades o acciones. Con este análisis se pueden identificar y tomar decisiones en cuanto a los riesgos y vulnerabilidades del diseño, la implementación y las prestaciones de la infraestructura tecnológica.

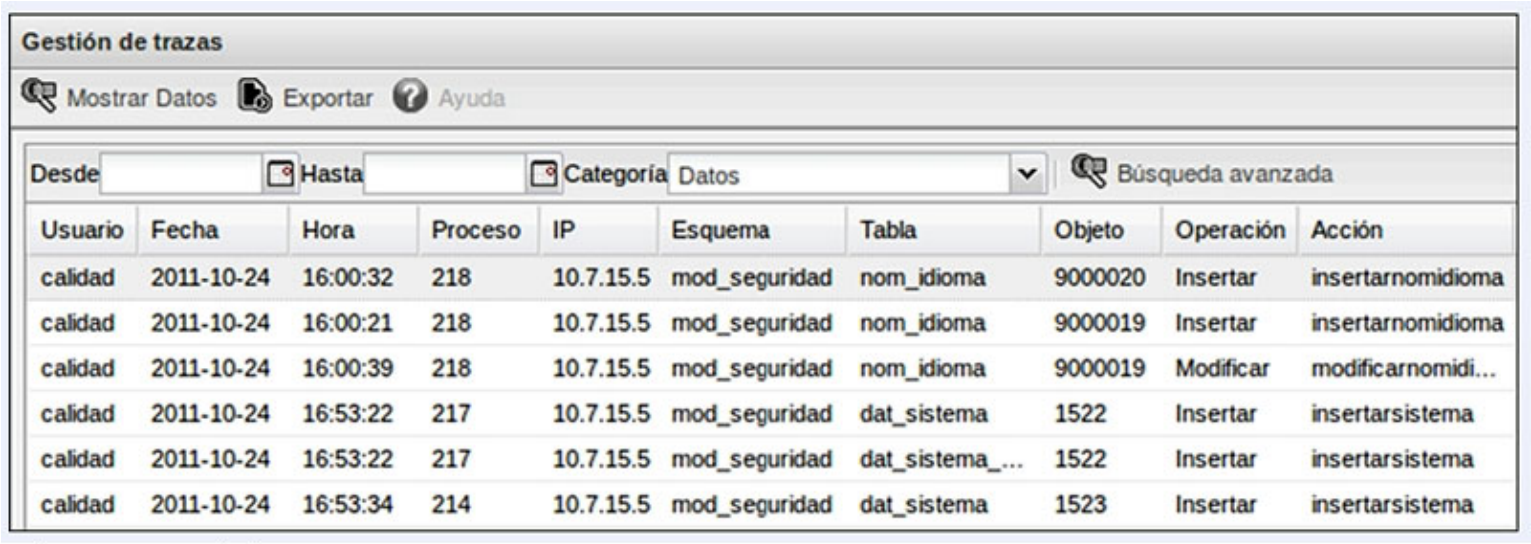
Al concluir la etapa de desarrollo e iniciar el despliegue en las organizaciones, en la mayoría de los casos surgen situaciones no concebidas que ponen en riesgo el correcto funcionamiento del sistema. Por esta razón es necesario mantener por algún tiempo el registro y seguimiento del sistema para evaluar su funcionamiento en el escenario real donde se despliegue. En los entornos reales aparecen nuevas amenazas relacionadas con las violaciones de seguridad. En este sentido es necesario incorporar un conjunto de reportes que reflejen la información necesaria para realizar este tipo de análisis. La figura 5 muestra un ejemplo de reporte con el fin de realizar análisis que permitan detectar las violaciones y los posibles responsables. En los log de eventos pueden existir atributos que son genéricos para todos los tipos de eventos.

- *Esquema*: tipo de objeto que incorpora el gestor PostgreSQL para crear agrupaciones dentro de las bases de datos.

- *Tabla*: tipo de objeto que presenta la mayoría de los SGBD para almacenar los datos.

- *Objeto*: se refiere al objeto de negocio sobre el que se realizó la operación (una cuenta, una persona, entre otras).

- *Operación*: la que se ejecutó en el nivel de datos (SELECT, INSERT, DELETE, entre otras).



Usuario	Fecha	Hora	Proceso	IP	Esquema	Tabla	Objeto	Operación	Acción
calidad	2011-10-24	16:00:32	218	10.7.15.5	mod_seguridad	nom_idioma	9000020	Insertar	insertarnomidioma
calidad	2011-10-24	16:00:21	218	10.7.15.5	mod_seguridad	nom_idioma	9000019	Insertar	insertarnomidioma
calidad	2011-10-24	16:00:39	218	10.7.15.5	mod_seguridad	nom_idioma	9000019	Modificar	modificarnomidi...
calidad	2011-10-24	16:53:22	217	10.7.15.5	mod_seguridad	dat_sistema	1522	Insertar	insertarsistema
calidad	2011-10-24	16:53:22	217	10.7.15.5	mod_seguridad	dat_sistema_...	1522	Insertar	insertarsistema
calidad	2011-10-24	16:53:34	214	10.7.15.5	mod_seguridad	dat_sistema	1523	Insertar	insertarsistema

Fig. 5. Reporte de datos.

La aplicación del modelo en el desarrollo del sistema de AI descrito en el caso de estudio, evidencia la necesidad de establecer un conjunto de configuraciones iniciales que garanticen la descripción e integración coherente de los conceptos del entorno que se desea auditar. Se recomienda utilizar la programación orientada a aspectos con el objetivo de activar solo los tipos de eventos que se desean auditar y, de esta forma, evitar el crecimiento innecesario de los log de eventos y las afectaciones de rendimiento en el SI. Concluido el proceso de configuración, el SI está en condiciones de registrar la información relacionada con los eventos activos en el momento que se ejecuten. Los reportes que se muestran en las figuras 4 y 5, reflejan algunos de los análisis que se pueden realizar y que cuentan con una fuente de log de eventos con calidad. El primero de ellos se enfoca en el comportamiento del rendimiento del SI ante las acciones ejecutadas y el segundo en la trazabilidad de los diferentes estados, sujetos y actividades por las que pasa un objeto. Se puede afirmar que la calidad de los log de eventos es directamente proporcional a la calidad de la GC y los beneficios que pueden aportar a las organizaciones.

CONCLUSIONES

En este artículo se presenta un modelo de gestión de log de eventos que provee una estructura genérica para estandarizar el registro de los diferentes tipos de eventos que se producen en los SI. Los conceptos incluidos en el modelo permiten adicionar de forma dinámica los atributos que caracterizan a cada tipo de evento

para lograr mayor expresividad en los log de eventos. La calidad de la información contenida en los log de eventos condiciona la efectividad de la AI y las decisiones que se puedan tomar a partir de los análisis realizados.

La interacción de los usuarios con los SI, genera una fuente importante de conocimiento a lo largo de su historia. Por esta razón es necesario aplicar una política de gestión de log de eventos eficiente que garantice su almacenamiento y expresividad para posteriores análisis. Para lograr mayor calidad y expresividad en los log de eventos es necesario concebir e integrar de forma coherente los procesos y actores del negocio, los SI y la estructura organizacional. La integración de los elementos mencionados permite realizar AI para predecir, evitar, detectar, evaluar y recomendar acciones relacionadas con la seguridad y funcionamiento del SI o con la ejecución de los procesos de negocio en la organización.

El análisis de información en las bases de datos *Datos Actuales* que utilizan los SI para ejecutar sus operaciones de negocio, influye de forma negativa en la seguridad y rendimiento del sistema. Por esta razón es recomendable contar con una base de datos que contenga todas las operaciones realizadas sobre un objeto a través de su historia.

La aplicación del modelo en desarrollo de un componente de gestión de log de eventos, permite estandarizar el registro de eventos y propiciar la AI con múltiples objetivos, en función de las características y necesidades del escenario de aplicación.

La robustez y flexibilidad del componente garantiza su integración y reutilización en varios sistemas como el ERP Cedrux y el Sistema para la Distribución de Medicamentos de la entidad QUIMEFA, entre otros sistemas. En todos los casos se alcanzan buenos resultados, sustentados por los avales y cartas de aceptación emitidos por los clientes.

REFERENCIAS BIBLIOGRÁFICAS

1. Morris S, Christodoulides M, Cornwell Jones LR. UK Security Breach Investigations Report. UK: 7Safe; 2010:1.

2. PricewaterhouseCoopers. Information Security Breaches Survey 2010:technical report. Infosecurity Europe. 2010:2-7.

3. Hendricks KB, Singhal VR, Stratman JK. The impact of enterprise systems on corporate performance: A study of ERP, SCM, and CRM system implementations. Operations Management. Journal of Operations Management 2007;25:6582.

4. Micro T. Web Application Security. Trend Micro; 2008:1.

5. Sánchez AA. Análisis técnico por ventas de una distribuidora de celulares. Ingeniería en Auditoría y Control de Gestión. Quito, Ecuador: Escuela Superior Politécnica de Litoral; 2007:19-20.

6. Nicho M, Cusack B. A metrics generation model for measur in the control objectives of information systems audit. 40th Hawaii International Conference on System Sciences. Waikoloa, HI: IEEE Computer Society; 2007:235.

7. Ciurea C. The Informatics Audit A Collaborative Process. The Informatics Audit A Collaborative Process. 2010;14:119-27.

8. Botha H, Boon JA. The Information Audit: Principles and Guidelines. Libri. 2003;53:2338.

9. Aalst WMPvd, ed. Process Mining Discovery, Conformance and Enhancement of Business Processes. Germany: Springer; 2010.

10. González SS, Lluch MZ. Auditoría de la información, punto de partida de la gestión del conocimiento. El profesional de la información. 2003;12:290-7.

11. Aumatell CSi. Auditoría de la información, punto de partida de la gestión del conocimiento. El profesional de la información. 2003;12:261-8.

12. Sabbaghi AM. Fariborz establishing an efficient and searchable encrypted log using record authenticator. International Conference on Computer Technology and Development. Qazvin, Irán: IEEE; 2009.

13. Sahibudin M, Ayat M. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Organizations. Second Asia International Conference on Modelling & Simulation. Asia: IEEE; 2008:749-753.

14. Aalst WMPvdH KM, Werf JM, Verdonk M. Auditing 2.0: Using Process Mining to Support Tomorrow's Auditor. IEEE 2010.

15. Günther CW. Extensible Event Stream. 2009:1-22.

Recibido: 18 de enero de 2012.
Aprobado: 26 de marzo de 2012.

MSc. *Oiner Gómez Baryolo.* Universidad de las Ciencias Informáticas. Carretera a San Antonio Km. 2 y ½, La Habana, Cuba. oiner@uci.cu