Ciencias de la Información Vol. 45, No. 1, enero - abril, pp. 11 - 17, 2014

Modelo para la compartimentación de la información en las organizaciones.

Oiner Gómez Baryolo
René Rodrigo Bauta Camejo
Vivian Estrada Sentí

Este artículo propone un modelo que refleje y describa los principales conceptos que deben modelarse para lograr la compartimentación de la información, para fortalecer la seguridad de los sistemas de información de gran envergadura, que gestionen procesos críticos dentro de un entorno organizacional. La solución propuesta brinda la posibilidad de definir los elementos necesarios para lograr la compartimentación de la información a partir de criterios y reglas basadas en las características de los recursos y de esta forma lograr mayor nivel de granularidad en el establecimiento de políticas de control de acceso. A partir de las restricciones de negocio existentes, los administradores de sistemas tienen la posibilidad de establecer niveles de acceso a la información de forma dinámica, sin necesidad de realizar modificaciones en el código de las aplicaciones.

***Palabras Clave**: seguridad informática, control de acceso, sistemas de información, acceso a la información, compartimentación de información.*

RESUMEN

ABSTRACT

This article proposes a model that reflects and describes the principal concepts that must be modeled to achieve the compartmentalization of the information, to strengthen the safety of the information systems of big importance, which manage the critical processes inside an organizational environment. The proposed solution offers the possibility of defining the necessary elements to achieve the compartmentalization of the information from criteria and rules based on the characteristics of the resources and of this form to achieve major granularity level in the establishment of politics of access control. From the existing business restrictions, the system managers have the possibility of establishing levels of access to information of dynamic form, without need to realize modifications in the code of the applications.

***Keyword**: computer safety, control of access, information systems, access to information, compartmentalization of information.*

Introducción

Desde la década de los ´80, la gestión de información ha tenido un lugar importante hasta llegar a ser vital para la actividad del hombre y su impacto en las organizaciones, principalmente para las que tienen como misión la investigación, el desarrollo de nuevos horizontes tecnológicos y la producción de bienes o servicios para la sociedad (Ponjuán, 2011). Refiriéndose al concepto de "información", McGee y Prusak expresaron lo siguiente: "La información no se limita a los datos recopilados; en verdad, la información se refiere a datos recopilados, organizados, ordenados, a los cuales se les atribuye significado y contexto. La información representa datos en uso, y ese uso implica un usuario" (McGEE, 1995).

El desarrollo de las Tecnologías de la Información y las Comunicaciones (TIC) y su utilización en los espacios científicos y empresariales, obligan a las organizaciones a mantenerse actualizado en el uso de las

TIC para aumentar el nivel competitivo en el área en la que se desarrollan.

Como parte del desarrollo de las TIC y la necesidad de mejorar la eficiencia y efectividad en la gestión de la información, surgen los Sistemas de Información (SI) (Cui Na, 2010; Ponjuán, 2008). Según Laudon y Laudon un SI es: "un conjunto de componentes interrelacionados que reúne (uobtiene), procesa, almacena y distribuye información para apoyar la toma de decisiones y el control en una organización" (Kosciuk, 2006).

En la actualidad los SI constituyen una parte importante dentro de la proyección estratégica de las organizaciones. Las más competitivas dedican gran parte de sus inversiones a las TIC con el objetivo de mejorar la gestión de sus procesos de negocio y apoyar la toma de decisiones. Entre los sistemas más utilizados para informatizar y mejorar la gestión de los procesos en las organizaciones se encuentran los sistemas de Planificación de Recursos Empresariales (ERP, siglas en inglés), sistemas de Gestión de Cadena de Suministros (SCM, siglas en inglés) y sistemas de Gestión de la Relación con los Clientes (CRM, siglas en inglés), entre otros. Estas soluciones tienen como objetivo, gestionar la información de las diferentes áreas, con el fin de lograr el cumplimiento de sus objetivos estratégicos (Ding-YueHua, 2009; Gao Hua, 2010; Tarantilis, 2008).

Hoy día las organizaciones dependen de la integridad, confidencialidad y disponibilidad de estas soluciones de gestión para generar ingresos, conectando clientes, proveedores, empleados y socios de forma ininterrumpida. Sin embargo, los ataques a estos sistemas aumentan cada día, a pesar de seguir apareciendo nuevos requisitos de cumplimiento de normativas sobre la seguridad de la información (Micro, 2008). Según un reporte realizado por Infosecurity Europe en que participaron un grupo de grandes y medianas empresas que utilizan SI para gestionar sus procesos, el 90% y el 74% de las grandes y medianas empresas respectivamente fueron objeto de ataques informáticos en el 2009 (Potter, 2010). Los temas relacionados con la seguridad se torna más crítico en la medida que aumenta el nivel de conectividad en el entorno organizacional. Como resultado de esta creciente interconectividad, la información está expuesta a un número cada vez mayor de amenazas y vulnerabilidades (McDaniel, 2011). Atendiendo a los riesgos de seguridad a los que se enfrentan los SI, es necesario implementar un control de acceso eficiente que proteja la confidencialidad, integridad y disponibilidad de la información.

El control de acceso es el proceso de restringir o registrar el acceso de usuarios a objetos tales como ficheros, direcciones, información, entre otros recursos. Está basado en tres conceptos fundamentales: autenticación, autorización y auditoría que han fomentado el desarrollo de múltiples soluciones con el objetivo de garantizar la seguridad en los SI. El control de acceso proviene de la interacción entre un sujeto y un objeto que forman un flujo de información de uno al otro.

El sujeto es la entidad que recibe o modifica los datos contenidos en los objetos, puede ser un usuario, programa, proceso, entre otros. Este proceso incluye autenticar la identidad de los usuarios, autorizar el acceso a la información y almacenar las trazas o log que permiten realizar auditorías para identificar violaciones (Karp, 2009). El presente trabajo se centra en el proceso de autorización, haciendo énfasis en los niveles de compartimentación de la información. La compartimentación no es más que la división lógica de la información atendiendo a diversos criterios o atributos que ayuden a diferenciar una de otra a la hora de concederle privilegios al usuario para acceder a ella.

Atendiendo a los riesgos de seguridad a los que se enfrentan los SI, la comunidad científica relacionada con el tema ha dirigido sus esfuerzos a crear modelos, normas, guías, estándares y metodologías que contribuyan a fortalecer el control de acceso a la información en las organizaciones que utilicen los SI para gestionar sus procesos. A continuación se realiza un análisis de las principales soluciones existentes en la bibliografía para desarrollar aplicaciones informáticas con el fin de disminuir las brechas de seguridad que atentan contra la seguridad de la información en las organizaciones.

El Control de Acceso Discrecional (DAC), es una forma de acceso basada en los sujetos y grupos a los que pertenece un objeto. Se dice que es discrecional en el sentido de que un sujeto puede transmitir sus permisos a otro sujeto. El hecho de que los dueños (sujetos) de los objetos tengan los privilegios necesarios para decidir quién puede realizar acciones sobre él representa una vulnerabilidad crítica para los SI en la actualidad (Downs, está destinado fundamentalmente para los sistemas operativos y en los últimos años ha disminuido su utilización por las limitaciones y brechas de seguridad que presenta.

El Control de Acceso Obligatorio (MAC), brinda mayor seguridad que DAC y se basa en un conjunto de reglas de autorización (políticas) las cuales determinan si una operación sobre un objeto realizada por un sujeto está o no permitida basándose en los atributos de ambos. En este caso las políticas están centralizadas y no pueden ser sobrescritas por un sujeto. MAC define niveles para ubicar los sujetos y los objetos atendiendo a sus privilegios y criticidad respectivamente (Fan, 2009). Entre las limitaciones más importantes que se pueden destacar se encuentra el hecho de que sólo se establecen criterios enfocados a la confidencialidad, dejando al descubierto la integridad. Todos los usuarios que se encuentran en un nivel determinado pueden acceder a toda la información de los niveles inferiores sin restricción, esto provoca que no se puedan establecer diferencias entre usuarios del mismo nivel. La información se organiza y se filtra por un único criterio relacionado con su clasificación, esto restringe la posibilidad de compartimentar la información atendiendo a otros parámetros como el usuario, la empresa, entre otros.

El modelo de Control de Acceso Basado en Roles (RBAC), es un enfoque para implementar políticas de control de acceso basado en el concepto de rol, que actualmente es considerado como uno de los modelos más utilizados para desarrollar soluciones de control de acceso en el mundo. La calidad de RBAC permite constatar que es superior a MAC y DAC y que brinda conceptos innovadores en el ámbito de la seguridad (Ferraiolo, 2007). A pesar de la calidad de este modelo, presenta deficiencia en varios aspectos de diseño y su escalabilidad se ve limitada a la hora de establecer

acceso a la información entre los usuarios que desempeñan un mismo rol. En su descripción no provee ningún mecanismo que permita establecer criterios para compartimentar la información y sobre ellos establecer reglas que restrinjan las operaciones y el nivel de acceso a la información (Li, 2007).

En la bibliografía existen una serie de extensiones realizadas al modelo RBAC entre las que se encuentra el Control de Acceso Basado en Atributos (ABAC), el Control de acceso Basado en Políticas (PBAC), el Control de Acceso Basado en Casos de Uso (UBAC), el Control de Acceso Orientado a Objeto (OBAC), el Control de Acceso Basado en la Autorización, entre otras soluciones (Chandersekaran, 2010; Karp, 2009). Estas propuestas están dirigidas a solucionar problemas relacionados con el control de acceso en diferentes dominios, la gestión del acceso orientado a objetos y la asignación de privilegios atendiendo a políticas o atributos. En ninguno de los casos se hace referencia a la necesidad de compartimentar la información por los criterios que defina la organización según sus procesos de negocio.

Teniendo en cuenta las limitaciones existentes en esta área, el objetivo de la presente investigación es proponer un modelo que refleje y describa los principales conceptos que deben modelarse para lograr la compartimentación de la información. De esta forma se brindará la posibilidad de establecer niveles de accesos y reglas de filtrado atendiendo a los diferentes atributos que caracterizan la información que se desea compartimentar. Las reglas deben constituir un mecanismo dinámico que posibilite establecer políticas de control de acceso a la información con un alto nivel de granularidad y de esta forma evitar ataques que violen la disponibilidad, confidencialidad e integridad de la información. El caso de estudio que se provee describe la aplicación del modelo en un escenario real para facilitar su comprensión y análisis.

Materiales y métodos

La información clave para la toma de decisiones, es aquella que forma parte del sistema integrado de información de una organización. En la sociedad del conocimiento, donde el capital más preciado es el ser humano, cada día es mayor el número de organizaciones que planifican sus productos en función de la gestión de información y del conocimiento y de la viabilidad para su obtención. Con el surgimiento de la teoría de la organización, se acentuó la importancia de la información. Una organización es un sistema conformado por personas, recursos materiales e información. El uso de SI que soporten la gestión de los procesos de negocio en las organizaciones ha aumentado. De esta misma forma han crecido las pérdidas económicas por ataques informáticos, lo que demuestra la necesidad de evitar las brechas de seguridad en los SI. La seguridad es un aspecto muy difícil de lograr en los SI, producto del acelerado desarrollo de las TIC y con ellas las herramientas para ejecutar ataques.

Por esta razón la seguridad no puede ser un proceso empírico que sea implementado por los desarrolladores y que su calidad dependa totalmente de su inventiva. Es necesario establecer y cumplir con normas que guíen y regulen el desarrollo de estas soluciones para evitar ataques que afecten la confidencialidad, integridad y disponibilidad de la información. Una forma importante para proteger la información es compartimentarla atendiendo a los diferentes criterios que establezca la organización para restringir el acceso a ella. Con este objetivo se propone un modelo compatible con otros modelos como RBAC, que guía el desarrollo de soluciones para compartimentar la información gestionada en las organizaciones y de esta forma aumentar su seguridad. La Figura 1 ilustra los conceptos fundamentales que conforman el modelo y la relación entre ellos.

Para facilitar la comprensión del modelo, a continuación se describen cada uno de los conceptos que lo integran.

• **Sujeto:** Es el usuario, rol o sistema que intenta acceder a los recursos almacenados.

• **Permisos:** Son privilegios definidos (Insertar, Modificar, Visualizar, Ejecutar, entre otros) para restringir el acceso de los sujetos a los recursos.

• **Recursos:** Son los activos lógicos y físicos (ficheros, bases de datos, tablas,

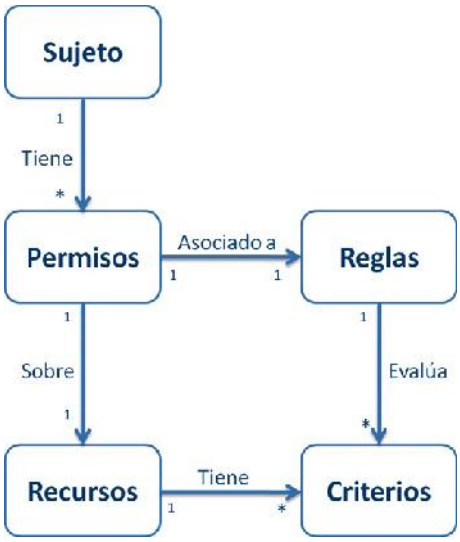

Figura 1. Modelo para la compartimentación de la información.

información, entre otros) con que cuenta una organización.

• **Criterios:** Son atributos que caracterizan al recurso (identificador, nombre, estado entre otros) y que se utilizan para almacenarlo e identificarlo.

• **Reglas:** Son restricciones preestablecidas por la organización para filtrar las peticiones de acceso a los recursos a través de su evaluación

.

A partir de este momento se utilizarán los términos definidos para hacer referencia a los conceptos que agrupan en el ámbito de la seguridad y de esta forma no restringir su aplicación solo al control de acceso de los usuarios a la información.

Como parte de la gestión interna o externa de una, surge la necesidad de establecer criterios para diferenciar los recursos y de esta forma poder crear diferentes niveles de acceso a ellos. Los niveles de acceso brindan la posibilidad de proteger los recursos de una empresa, área o persona de violaciones de confidencialidad, integridad y disponibilidad aunque todos se encuentren almacenados en un mismo lugar. De esta forma dentro de un mismo equipo de trabajo donde todos cumplen el mismo rol, se le puede asignar permisos especiales a uno de ellos para que además de su trabajo, supervise el de los demás sin que ellos puedan hacer lo mismo. La importancia de la compartimentación de los recursos aumenta en los entornos

multientidad, donde los recursos de varias entidades se encuentran almacenados en un mismo lugar y su gestión y seguridad se controla de forma centralizada. En este tipo de escenarios es necesario poder identificar a qué organización pertenece la información y quienes tienen acceso a realizar acciones sobre ella. Si no se establecen estas políticas un sujeto podría ver, modificar y borrar los recursos de todas las organizaciones que formen parte de ese entorno.

La planificación de actividades es un ejemplo típico donde se necesita definir claramente los privilegios de los usuarios sobre las tareas asignadas. En estos casos las tareas se pueden crear en un nivel superior de la estructura organizacional y asignarse a un usuario que pertenezca a una entidad o área inferior. De esta forma la tarea puede subir y bajar en la estructura organizacional dependiendo de su estado de cumplimiento y en todo momento se necesita garantizar su confidencialidad, integridad y disponibilidad. Ejemplos como este se pueden encontrar en las diferentes esferas de la sociedad donde se gestionan recursos críticos para las organizaciones utilizando los SI. La Figura 2 muestra la especificación del modelo propuesto para un entorno empresarial, utilizando conceptos conocidos en estos escenarios.

En la especificación del modelo propuesto se puede apreciar que existen dos sujetos con privilegios distintos sobre los recursos "Comprobante de operaciones". El sujeto "Auditor" solo puede ver los "Comprobante de operaciones" pertenecientes a su entidad y que esté en estado asentado. Las reglas y los criterios desempeñan un papel determinante en la protección de los recursos. A través de estos conceptos es posible filtrar las peticiones realizadas por los sujetos y de esta forma evitar que se ejecuten permisos no asignados sobre los recursos, que pongan en riesgo la disponibilidad, confidencialidad e integridad y de los bienes de una o varias organizaciones. El sujeto "Contador" tiene privilegios para realizar mayor cantidad acciones sobre los recursos, pero cuenta con más restricciones que disminuye el número de "Comprobante de operaciones" sobre los que puede actuar. Las limitaciones están dadas por el aumento de la cantidad de criterios establecidos para el filtro, en este caso el sujeto sólo podrá acceder a la información creada por él o por determinados usuarios de su entidad.

La compartimentación de la información utilizando criterios, permite establecer distintas clasificaciones a la hora de almacenar la información. Esto brinda la posibilidad de establecer una división lógica en el origen de datos. De esta forma, aunque en un mismo centro de datos se encuentre la información de varias organizaciones, es posible establecer reglas para que un sujeto solo pueda ejecutar acciones sobre la información a la que tiene acceso. Si no se aplica esta política, no es posible gestionar de forma centralizada los procesos de varias entidades sin que los usuarios tengan la posibilidad de acceder a toda la información almacenada. La utilización del modelo en el diseño de las soluciones de seguridad para los SI, permite establecer las restricciones necesarias para que el trabajador de un área acceda solo a la información de su área, el director acceda a la de la entidad y el ministro a la de todas las entidades que conforman el ministerio.

Para validar la calidad del modelo, se aplicó en el desarrollo de una solución de control de acceso para el sistema ERP Cedrux, desarrollado en la Universidad de las Ciencias Informáticas (UCI) obteniéndose buenos resultados. La solución provee los mecanismos necesarios para consolidar y desglosar información de varios procesos en todo el país, garantizando la confidencialidad, integridad y disponibilidad en todos los niveles organizacionales. A continuación se describe un caso de estudio que refleja con mayor claridad las posibles formas de aplicación del modelo y las ventajas que reporta.

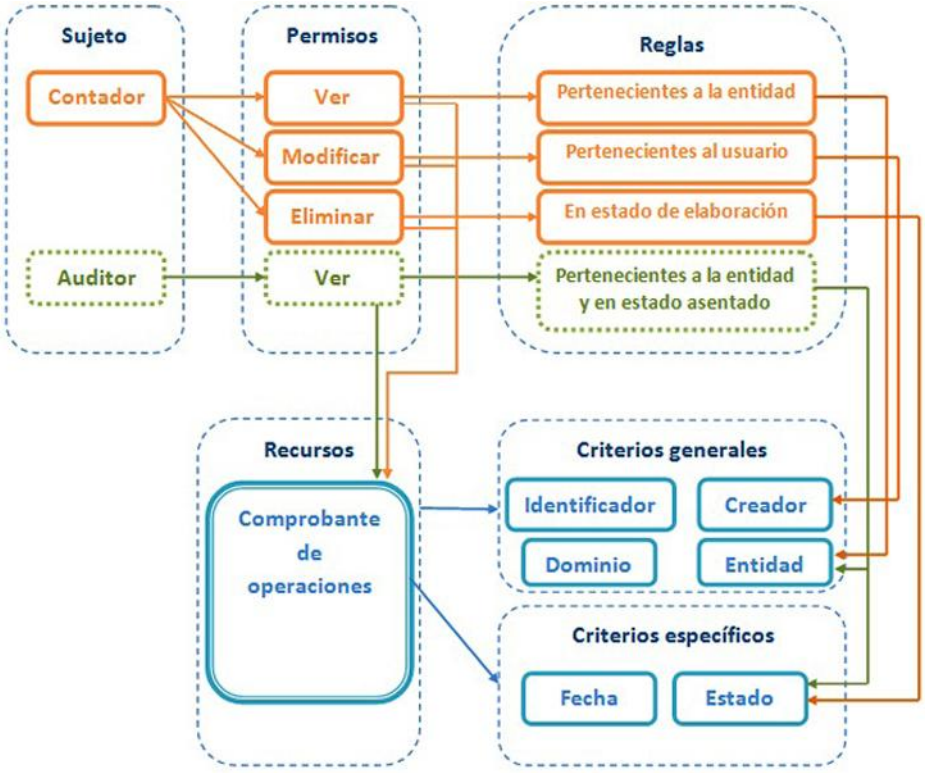

Figura 2. Descripción del modelo para la compartimentación de la información.

Resultados y discusión

En esta sección se muestra un caso de estudio, donde se aplica el modelo propuesto en el desarrollo de un módulo de control de acceso para un sistema ERP. El principal valor práctico radica, en la utilización del modelo como referencia para el desarrollo de sistemas de control de acceso para SI que requieran de una seguridad robusta, escalable y confiable como el sistema ERP Cedrux. El mismo está formado por varios subsistemas, diseñados para gestionar la información de diversas entidades simultáneamente y donde los recursos viajan constantemente de un punto a otro de la red. Como se había mencionado anteriormente, la importancia de la compartimentación de los recursos aumenta en los entornos multientidad. En estos escenarios se requiere de un mecanismo que brinde la posibilidad de gestionar la estructura organizacional del dominio

donde se enmarca el despliegue del SI. La estructura organizacional adopta la forma de un árbol y permite definir el sentido de la consolidación, el desglose, la réplica, entre otros procesos que implementan los SI.

Para crear la estructura organizacional es necesario que con anterioridad se hayan definido los conceptos que van a formar parte de los diferentes niveles estructurales, sus atributos y la relación de dependencia entre ellos. Las dependencias entre los conceptos desempeñan un papel determinante a la hora de crear las restricciones que mantienen la consistencia de la estructura. Concluida la definición de los conceptos, atributos y relación entre los niveles estructurales, es posible iniciar la creación de la estructura organizacional donde se va a desplegar el SI. En la Figura 3 se ilustra un ejemplo de este proceso donde se crean las estructuras ministerio, grupo empresarial, entidad, área y cargo. La definición de la jerarquía de estructuras forma la base para la compartimentación de los recursos entre las organizaciones y la asignación de privilegios a los usuarios para acceder a ellos.

El proceso descrito anteriormente solo permite restringir el acceso desde el punto de vista organizacional. Paralelo a este proceso es necesario gestionar los privilegios sobre la estructura o funcionalidades del sistema, con este objetivo se implementó lo descrito por el modelo RBAC. La creación de la estructura organizacional y la agrupación de permisos utilizando el concepto rol, convergen a la hora de asignarle los privilegios a un usuario sobre ambas estructuras. La gestión de este proceso permite definir los roles de un usuario y en qué estructuras de la jerarquía los va a desempeñar. Como es posible apreciar en la Figura 4 este proceso cuenta con dos partes, en la primera se selecciona el rol de sistema que se desea asignar y en la segunda se selecciona las estructuras de las jerarquías donde cumplirá el rol.

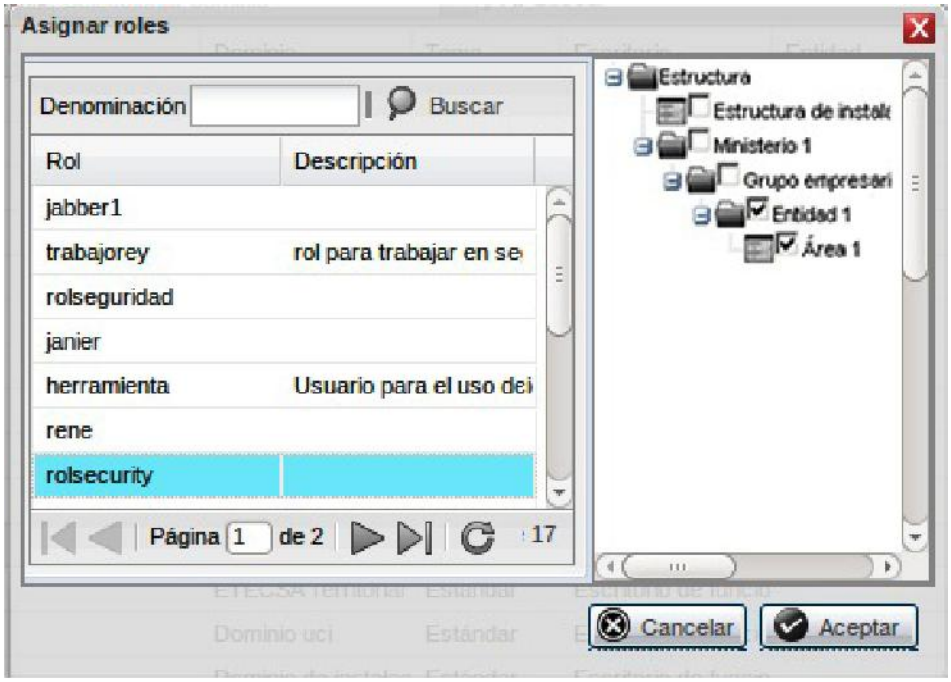

Figura 4. Interfaz para asignar roles a los usuarios.

Hasta el momento se ha implementado lo propuesto en el modelo RBAC, incluyéndole algunos conceptos importantes como la gestión de la estructura organizacional. La definición de esta estructura representa la base para establecer los permisos a los diferentes niveles en el dominio de despliegue del SI. En los entornos multientidad donde se aplican sistemas como el ERP Cedrux, el control de acceso hasta este nivel no es suficiente. Por esta razón es necesario brindar la posibilidad de profundizar en la configuración de los filtros que restringen el acceso a los recursos. El modelo propuesto brinda la posibilidad de establecer criterios para compartimentar los recursos en el momento de almacenarlos y de esta forma poder establecer reglas para filtrar las peticiones de acceso. En la Figura 5. se refleja un ejemplo de interfaz que permite configurar los permisos a nivel de rol y de usuario sobre la base de la compartimentación de los recursos, en este caso información relacionada con los comprobantes de operaciones de una entidad. En la parte inferior izquierda se seleccionó el sujeto de tipo rol para iniciar la configuración. Por esta razón se muestran los roles existentes (Contador y Auditor) y para cada uno de ellos los permisos que poseen sobre el recurso "Comprobante de operaciones", atendiendo a las reglas establecidas.

Para crear una configuración es necesario seleccionar los permisos que tendrá el sujeto, sobre qué recurso y bajo qué reglas.

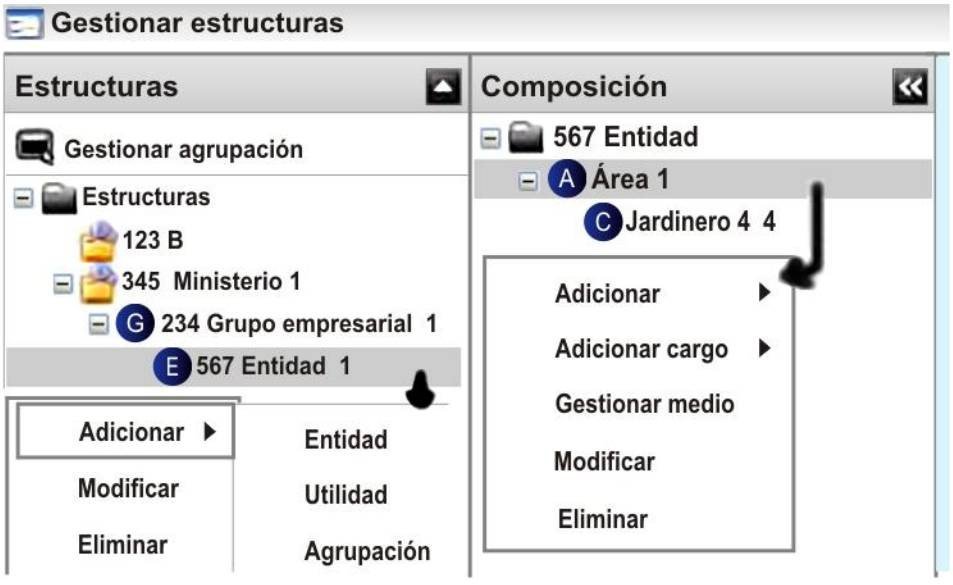

Figura 3. Gestionar estructuras.

Figura 5. Configurar permisos de acceso a los recursos.

Las reglas están compuestas por criterios que se asocian con valores que caracterizan al recurso. En la Figura 6 se presenta un ejemplo de configuración que establece un permiso (Ver) y dos criterios (Entidad y Estado) para filtrar las peticiones sobre el recurso "Comprobante de operaciones", aplicando la regla "Perteneciente a la entidad en estado asentado".

A partir de este momento el usuario se encuentra en condiciones de autenticarse en el SI para obtener la jerarquía de estructuras a las que tiene acceso. La Figura 7 muestra la interfaz que se brinda al usuario una vez autenticado correctamente. Para acceder al sistema, el usuario debe seleccionar la estructura a la que desea acceder para realizar las operaciones, lo cual condiciona los roles y por ende los sistemas, recursos u operaciones a las que puedeacceder. Cuando un usuario accede a una estructura se asume que todas las operaciones que realice quedarán registradas en ella. Para realizar operaciones sobre otra estructura de su dominio, el usuario tiene la facilidad de cambiar de estructura aunque esté dentro del sistema.

La descripción de los principales procesos que inciden directamente en la compartimentación de los recursos, permite dimensionar la importancia y complejidad que representa su gestión. La complejidad aumenta en la medida que se necesite aumentar las restricciones y el número de organizaciones involucradas.

La compartimentación y acceso a los recursos es un tema que se debe tener en cuenta desde el inicio del proceso de desarrollo de los SI. Esta decisión permite que se adopte un diseño correcto para el almacenamiento de los recursos y se tengan en cuenta los criterios que van a caracterizar a cada uno de ellos. Las reglas que se apliquen en el filtrado de las peticiones dependen de los criterios establecidos y de la profundidad de las restricciones de acceso. La confidencialidad, integridad y disponibilidad de los recursos depende de la solución tecnológica que se implemente para gestionar el proceso de autorización. Un ataque que afecte uno de estos aspectos pondría en riesgo la estabilidad de las organizaciones involucradas. La aplicación del modelo en el desarrollo del sistema ERP Cedrux constituye un aporte considerable, teniendo en cuenta la responsabilidad que representa mantener la confidencialidad, integridad y disponibilidad de la información que debe gestionar este sistema. Si a esto se le añade la complejidad de un despliegue nacional con las características de un entorno multientidad, el reto para lograr la seguridad es cada vez mayor.

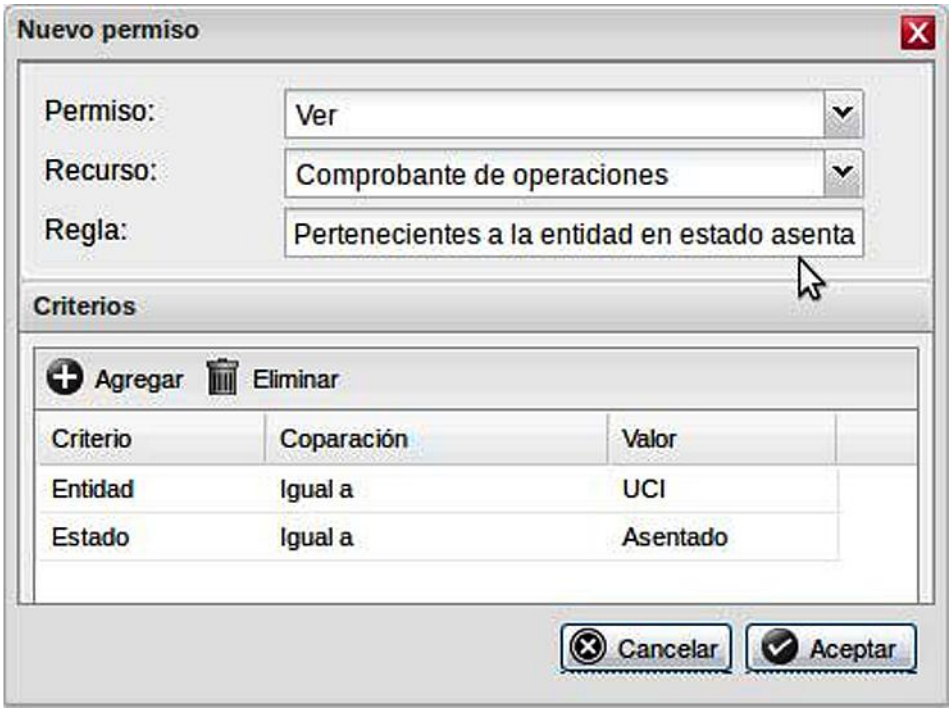

Figura 6. Registrar permisos.

Conclusiones

El desarrollo experimentado por las Ciencias de la Información y sus manifestaciones interdisciplinarias, como los Sistemas de Información, se ha identificado que las organizaciones que utilizan este tipo de soluciones para desarrollar una adecuada cultura de gestión de información y conocimiento logran convertirse en entidades de avanzada. La gestión del conocimiento ha cambiado la forma en que las organizaciones gestionan sus procesos, debido a la necesidad de poder contar con información confiable, íntegra y oportuna en todo momento que contribuya al cumplimiento de sus objetivos estratégicos.

El crecimiento acelerado de los ataques informáticos y las pérdidas ocasionadas por ellos, demuestran que se debe crear una conciencia organizacional que fomente la aplicación de medidas de seguridad a todos los niveles en los SI que utilizan. La implementación de estándares resulta vital para disminuir las brechas de seguridad que puedan ser aprovechadas para ejecutar ataques que pongan en riesgo los recursos de las organizaciones. Los estándares más utilizados en este sentido no cuentan con el nivel de especificación escalabilidad necesario para ser aplicado

en entornos multientidad. Las soluciones más robustas como el caso de RBAC restringen el control de acceso hasta nivel de rol, esto constituye una limitante en el caso que se necesite establecer restricciones entre usuarios que desempeñen el mismo rol. Otra de las limitaciones importantes es que soportan sus configuraciones sobre la base de objetos y operaciones sin profundizar en los criterios y reglas que permiten establecer diferencias entre los objetos.

Las limitaciones detectadas constituyen los antecedentes que dieron origen a la presente investigación. En la misma se presentó un modelo que profundiza en el control de acceso a los recursos haciendo énfasis en sus características para lograr su compartimentación en las diferentes tecnologías de almacenamiento. La solución propuesta introduce la utilización de reglas para aumentar el filtrado en las peticiones de acceso a los recursos. El modelo se aplicó en el desarrollo de un sistema de seguridad denominado Acaxia. Esta solución tiene la responsabilidad de preservar la confidencialidad, integridad y disponibilidad de los recursos que gestiona el sistema ERP Cedrux. El trabajo en un futuro inmediato involucra otros procesos como la autenticación y auditoría para completar el flujo dentro del control de acceso en SI.

Bibliografía

Chandersekaran, C. S. S., William R. (2010). Use Case Based Access Control. IIIS, 1-6. Disponible en http://www.iiis.org/CDs2010/CD2010SCI/CITSA_2010/PapersPdf/IA091CX.pdf.

Cui Na, L. Y., An Haizhong, Wang Yue. (2010). A value-added service model of mining right information. Paper presented at the International Conference on E-Business and E-Government, Beijing, China.

Ding-YueHua, X.-R., Yi-Kui. (2009). Design of VSS Software Configuration Management Database for WEB Application Project. IEEE Computer Society, 1. Disponible en http://csdl.computer.org/dl/proceedings/paccs/2009/3614/00/3614a567.pdf

Downs, D. D. R., Jerzy R.; Kung, Kenneth C.; Jordan, Carole S. (1985). Issues in Discretionary Access Control (DAC). IEEE Computer Society, 208. Disponible en http://csdl.computer.org/dl/proceedings/sp/1985/0629/00/06290208.pdf

Fan, Y. H., Zhen; Liu, Jiqiang; Zhao, Yong. (2009). A Mandatory Access Control Model with Enhanced Flexibility. Paper presented at the International Conference on Multimedia Information Networking and Security, Hubei, China Disponible en http://csdl.computer.org/dl/proceedings/mines/2009/3843/01/3843a120.pdf

Ferraiolo, D. F. K., D. Richard, handramouli, Ramaswamy. (2007). Role-Based Access Control. Disponible en http://www.iberlibro.com/9781596931138/Role-Based-Access-Control-Ferraiolo-David-1596931132/plp.

Gao Hua, X. x. s. (2010). Fuzzy omprehensive Appraisal of ERP Selection. Paper resented at the International Conference on Electrical and Control Engineering. Disponible en http://csdl.computer.org/dl/proceedings/icece/2010/4031/00/4031c780.pdf

Karp, A. H. H., Harry; Davis,Michael H. (2009). From ABAC to ZBAC: The Evolution of Access Control Models. USA. Disponible en http://www.hpl.hp.com/techreports/2009/HPL-2009-30.pdf

Kosciuk, N. H. (2006). Resumen del libro Sistema de Información Gerencial. El Libro Libre, 3.

Li, N. B., Ji-Won; Bertino, Elisa. (2007). A Critique of the ANSI Standard on Role Based Access Control. USA: Purdue University. Disponible en http://www.cs.purdue.edu/homes/ninghui/papers/aboutRBACStandard.pdf

McDaniel, P. S., Sean W. . (2011). Data Provenance and Security. IEEE Security & Privacy, 83-85. Disponible en http://sdl.computer.org/dl/mags/sp/2011/02/msp2011020083.pdf

Tassara, G. (2005). Una mirada lingüística a la sentencia judicial. Trabajo presentado en XVI Congreso de la Sociedad Chilena de Lingüística.

McGEE, J. P., L. (1995). Gerenciamento estratégico da informação. Rio de Janeiro: Campus.

Micro, T. (2008). Web Application Security: Trend Micro. Disponible en http://es.trendmicro.com/imperia/md/content/es/products/datasheets/ds01was_081111es.pdf

14. Ponjuán, G. D. (2008). Gestión de información: Precisiones conceptuales a partir de sus orígenes. Informação & Informação, 12, 26-38. Disponible en http://www.uel.br/revistas/uel/index.php/informacao/article/download/1830/1544

15. Ponjuán, G. D. (2011). La gestión de información y sus modelos representativos. Valoraciones. Ciencias de la Información, 42(2), 11-17 Disponible en http://cinfo.idict.cu/index.php/cinfo/article/download/300/95

Potter, C. B., Andrew. (2010). Information Security Breaches Survey 2010: Technical report. Earl's Court, London: Infosecurity Europe. Disponible en www.7safe.com/breach_report

Tarantilis, C. D. K.C.T. ; Theodorakopoulos, N. D.(2008). A Web-based ERP system for business services and supply chain management Application to real-world process scheduling. European Journal of Operational Research, 1310-1326.

Recibido: 22 de mayo de 2013.
Aprobado en su forma definitiva:
27 de diciembre de 2013

Oiner Gómez Baryolo
Universidad de las Ciencias Informáticas. Cuba
Correo-e.: oinergb@gmail.coml

René Rodrigo Bauta Camejo
Universidad de las Ciencias Informáticas.Cuba
Correo-e.:rrbauta@uci.cu

Vivian Estrada Sentí
Universidad de las Ciencias Informáticas.Cuba
Correo-e.:vivian@uci.cu