Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

Tipo de artículo: Artículo original
Temática: Seguridad informática
Recibido: 17/06/2015 | Aceptado: 06/11/2015

PCAECM: Modelo para la Planificación y Control de las Auditorías en Entornos Cubanos Multidominios

PCACME: model for Planning and Control Audit in Cuban Multi-domains Environments

Yasser Azán Basallo[1*], Oiner Gómez Baryolo[2]

[1] Centro de Telemática. Universidad de las Ciencias Informáticas, Carretera a San Antonio de los Baños, km 2 ½, Torrens, Boyeros, La Habana, Cuba. CP.: 19370. Correo: yazan@uci.cu
[2] Facultad de Ingeniería en Sistemas Computaciones y Telecomunicaciones. Universidad Tecnológica Ecotec, Juan Tanca Marengo Km. 2, Guayaquil, Ecuador. Correo: ogomez@ecotec.edu.ec

[*] Autor para correspondencia: yazan@uci.cu

Resumen

En el presente trabajo se describen las necesidades de la Contraloría General de la República de Cuba (CGRC) para informatizar los procesos de planificación y control de las auditorías. Uno de los problemas más fuertemente presentados para realizar la planificación es la compartimentación de las acciones de control asignados a los supervisores, para aumentar el nivel de restricción de acceso al plan anual de auditoría. Por eso en este trabajo se describe un modelo siguiendo un Esquema de Seguridad Multidominio para un sistema de planificación y control. Se muestran los resultados arrojados de una comparación con otras aplicaciones que implementan otros modelos de seguridad a través de indicadores proporcionados por expertos. De esta forma demostrar el fortalecimiento de la seguridad con las mejoras en el control de acceso a través del modelo propuesto y por consiguiente de la confidencialidad de la información.

Palabras clave: Auditoría, control, planificación, modelo

Abstract

In this paper are described the needs of the Comptroller General of the Republic of Cuba (CGRC) to computerize planning and control audits. One of the hardest problems presented for planning and control actions are the partitioning of information assigned to supervisors to increase the level of restriction of access to the annual audit plan. Therefore, in this work is described a model following a Multidomain Security Scheme for planning and control system. The results obtained are show from a comparison with other applications that implement other security models using indicators provided by experts. Thus are demonstrating the strengthening of security improvements in access control through the proposed model and therefore the confidentiality of the information.

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

Keywords: *Audit, control, planning, model*

Introducción

El fraude corporativo es un problema global. Si bien los hallazgos difieren levemente a nivel regional, la mayoría de los resultados son consistentes con respecto a las tipologías, las características de los defraudadores y los controles para detectarlos, independientemente del lugar donde ocurra el fraude. El informe de la Asociación de Examinadores de Fraude Certificados (siglas en inglés: ACFE) sobre el fraude corporativo del año 2014, contiene un análisis de 1,483 casos de fraude profesional que ocurrieron en más de 100 países que fueron reportados por Certified Fraud Examiners (siglas en inglés: CFEs) estima que: de las tres categorías primarias de fraude profesional, la malversación del recurso es por mucho el más común, ocurriendo en más de 85% de casos analizados; sin embargo, también es típicamente el más costoso de los tres tipos, causando una pérdida media de $130,000. En el contraste, el fraude de la declaración financiero ocurre frecuentemente mucho menos, mientras respondiendo de 9% de los casos en nuestro último estudio, pero causa el más gran impacto financiero de las tres categorías por lejano, con una pérdida del medio de $1 millón. La corrupción tiende a desplomarse el medio por lo que se refiere a frecuencia y la pérdida del medio (Examiners 2014).

En Cuba no está exenta de este problema, el 34 por ciento de las 234 entidades estatales auditadas en el 2012 por la Contraloría General de Cuba presentó un "saldo negativo", según lo publicado en el sitio Cubadebate (Cubadebate 2013).

Por estos motivos se creó el 25 de abril del 2001 por el Decreto Ley No. 219 del Consejo de Estado, el Ministerio de Auditoría y Control (MAC), actualmente la Contraloría General de la República de Cuba (CGRC). El mismo es el Organismo de la Administración Central del Estado (OACE) encargado de dirigir, ejecutar y controlar la aplicación de la política del estado y el gobierno en cuanto a: prevenir, detectar y enfrentar los actos de corrupción administrativa mediante la realización de la Auditoría Gubernamental, Fiscalización y Control Gubernamental. También tiene las funciones de regular, organizar, dirigir y controlar metodológicamente, el Sistema Nacional de Auditoría.

La estructura básica de la Contraloría General de la República de Cuba está conformada por contralorías provinciales en cada una de las provincias del país y por diversas direcciones, en la sede central en La Habana, entre las cuales se encuentra las Direcciones Integrales de Auditoría, Supervisión y Control (DIASC). La DIASC es la encargada de realizar la planificación anual de todas las acciones de control a partir de los resultados del año anterior, teniendo en

cuenta las directivas trazadas para el año siguiente. Ejerce el seguimiento a la realización de dicho plan a través de los controles de cumplimento. La CGRC no es la única entidad del país que planifica las auditorías, todas las Unidades Centrales de Auditoría Interna (UCAI) de los Organismos de la Administración Central del Estado (OACE) planifican y concilian con la CGRC el plan de auditoría del organismo al cual pertenecen.

Por lo que se está en presencia de un entorno multidominio: donde múltiples organizaciones distribuidas interoperan cada uno con sus propias políticas de seguridad (Shafiq 2006). Este concepto permite la interoperabilidad de los sistemas informáticos.

En las DIASC y en las UCAI de los OACE, gran parte del proceso de planificación se realiza de forma manual o con programas que no completan el proceso de planificación como lo dicta la Resolución 091/08 de la CGRC. Una de las herramientas existentes en esta dirección es GEPE: para la planificación de auditorías en empresas que se encuentren en perfeccionamiento empresarial. También se encuentran RAUDIT: para gestionar solamente el registro de las órdenes de trabajo de cada auditoría planificada. Los sistemas: Registro de Auditores y PHD realizan los procesos de gestión del Registro de auditores de la República de Cuba y de gestionar el registro de presuntos hechos delictivos respectivamente.

Las tecnologías informáticas actuales con las que cuenta la CGRC, no son capaces de compartimentar la información del plan de auditoría entre los usuarios del dominio de la CGRC y de las 41 UCAI existentes en el país, para conciliar y realizar un seguimiento del cumplimiento del plan anual de auditorías de sus organismos. Estos sistemas además no son capaces de establecer una diferenciación entre usuarios con el mismo rol, dentro de un mismo dominio. Debido a estas insuficiencias no se pueden establecer las políticas necesarias para limitar el acceso a la información del Plan Anual de Auditoría conformado por la CGRC, ni siquiera dentro de un mismo dominio. Estas deficiencias ponen en riesgo la confidencialidad de la información.

Esta investigación tiene como objetivo presentar una propuesta de modelo para consolidar la confidencialidad de la información manejada en las DIASC según los problemas señalados.

Materiales y métodos o Metodología computacional

El principal objetivo del modelo RBAC (Tao Wang 2006) es prevenir que los usuarios no autorizados tengan libre acceso a la información de la organización. La definición básica de RBAC establece que los usuarios son asignados a roles, los permisos son asociados a roles y los usuarios adquieren permisos siendo miembros de roles. Las asignaciones usuario-rol y permiso-rol pueden ser muchos-a-muchos, por lo que un usuario puede pertenecer a

muchos roles y un rol puede poseer muchos usuarios. De manera similar un permiso puede ser asociado a muchos roles y un rol puede tener asociado muchos permisos (WANG Tao 2010). El RBAC también incluye el concepto de sesión, que permite la activación y desactivación selectiva de roles, posibilitando que un usuario pueda ejercer los permisos de varios roles simultáneamente (Ali E. Abdallah 2008; Jason Crampton 2009).

A pesar del control del acceso que permite el RBAC, este modelo presenta dificultades que los mismos autores señalan (Li Ma 2009; Kuhn 2010; Xuexiong 2010):

- La herencia de roles genera una serie de conflictos que propician las violaciones de las restricciones establecidas.
- Para la asignación de roles no se tienen en cuenta las características del entorno organizacional donde se despliega el sistema.
- La gestión de privilegios tiene que ser centralizada para que los administradores mantengan la fortaleza del control de acceso.
- La ausencia de un mecanismo para establecer diferencias entre los usuarios que desempeñan un mismo rol.
- Las restricciones solo se establecen a nivel de roles, sin tener en cuenta que para una determinada operación pueden existir restricciones en función de las características o atributos del recurso.

Las limitaciones mencionadas anteriormente evidencian porque el modelo no puede ser usado para la solución del problema de investigación planteado.

Debido a las limitaciones presentadas por el modelo RBAC, se propone el modelo PCAECM. Es una extensión del modelo RBAC dirigido al proceso de planificación y control de auditorías en entornos cubanos multidominios. Los entornos multidominios es en donde múltiples organizaciones distribuidas interoperan cada uno con su propias políticas de seguridad (Shafiq 2006).

Se propone una solución para el control del acceso a la información generada a partir de la planificación y control de las auditorías en entornos cubanos multidominios y de esta forma preservar la confidencialidad de la información. La figura 1 ilustra los conceptos y relaciones que conforman el modelo PCAEMC.

El núcleo del modelo PCAECM

Para la planificación y control de las auditorías, a los usuarios se le asignan roles con los permisos que van a en su propio dominio, así como en los dominios externos a su entidad. El dominio: Una entidad lógica con una red interconectada, y puede representar una subred consistente de un conjunto de elementos de red (1994).

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

En el concepto permiso se incluyen las operaciones que están presentes en el proceso de planificación y control en el país. El Plan constituye el recurso o la información que necesita ser protegida a través de los permisos.

En el concepto dominio se agrupan en un mismo conjunto, un determinado número de entidades que pueden ser: ministerios, sociedades anónimas, empresas y otros tipos de entidades para la cual se quiere planificar las auditorías. Los dominios son jerárquicos porque un dominio como los OACE, tienen subordinadas un número de entidades, pero a su vez se subordinan a la CGR, en los procesos de planificación y control de las auditorías. Con la asignación de usuarios a un dominio, se logra restringir el acceso a los recursos, en este caso al plan. Según el dominio al cual pertenezca un usuario, será el fragmento del plan al cual tendrá acceso. De esta forma se logra compartimentar la información contenida en el objeto Plan.

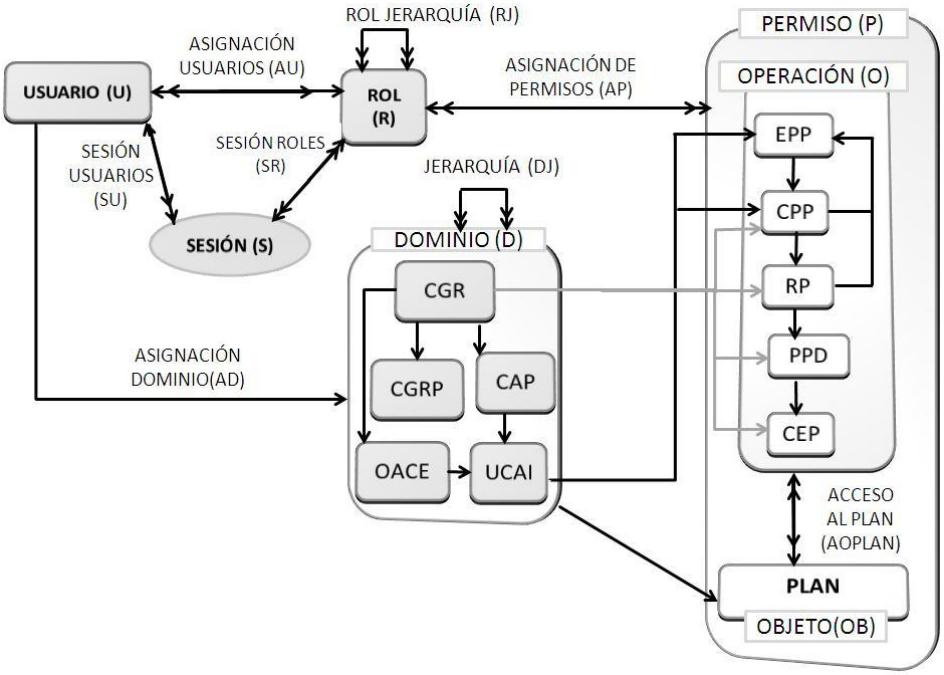

Figura 1: Modelo PCAECM.

Formalización del modelo

Las políticas RBAC (PL) consisten en (Gail-Joon Ahn 2000; Yue Zhang 2007):

- R es un conjunto de roles.
- U es un conjunto de usuarios.
- P es un conjunto de permisos.

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

- S es un conjunto de sesiones.
- AU es la asignación de roles a usuarios
- AU ⊆ U×R es una relación de muchos roles a un singular usuario.
- AP ⊆ P×R es una relación de asignación de permisos a roles de muchos a muchos.
- RJ ⊆ R×R. La jerarquía de roles es organizada en un orden parcial, en un mayor igual que, de esta forma si x es mayor que y, entonces x hereda los permisos del rol y. Los miembros de x son implícitamente miembros de y.

Un usuario puede ser miembro de múltiples roles y cada rol puede tener muchos usuarios. Del mismo modo, un rol puede tener muchos permisos y al mismo tiempo los permisos pueden ser asignados a muchos roles (Gail-Joon Ahn 2000).

Definiciones adicionales

- D es un conjunto de dominios.
- Plan es el objeto contenedor de la información del plan de auditoría.
- es un conjunto de operaciones que están definidos en los permisos P.
- AD ⊆ U×D es una relación de asignación de dominios a usuarios de muchos a muchos.
- US ⊆ U×S es una relación de asignación de sesiones a usuarios de muchos a muchos.
- DJ ⊆ D×D. La jerarquía de dominio es organizada en un orden parcial, en un mayor igual que. De esta forma si a es mayor que b, entonces a contiene las entidades del dominio b. Los miembros del dominio de b son implícitamente miembros del dominio de a.
- AOPLAN ⊆ O×PLAN es una relación de muchos a muchos entre las operaciones y el objeto Plan.
- CGRP ⊆ CGR. El dominio CGRP es un subconjunto del dominio CGR.
- CAP ⊆ CGR. El dominio CAP es un subconjunto del dominio CGR.
- OACE ⊆ CGR. El dominio OACE es un subconjunto del dominio CGR.
- UCAI ⊆ OACE. El dominio UCAI es un subconjunto del dominio OACE.OACE ≠ CAP. Un dominio de tipo OACE es distinto a un CAP porque un dominio del primer tipo comprende a un conjunto de entidades que están distribuidos en todo el territorio nacional, mientras que el segundo dominio está restringido a un conjunto de dominio que pertenecen a una misma provincia. Además, el CAP no es un subdominio del OACE porque agrupa otras entidades que no pertenecen a una OACE determinada o a ninguna.

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

Para el trabajo con las operaciones definidas, se trabaja de forma especializada, donde para una operación le corresponde un permiso. De esta forma se puede tener un usuario con permiso sobre una sola operación y tenga solamente alcance sobre la porción de la información sobre el plan anual de auditoría de país, sobre el cual trabaja el usuario y solo necesita conocer y de esta forma se restringe el acceso a la información confidencial.

Resultados y discusión

El resultado que se presenta a continuación es una comparación con otras instancias de modelos de autorización, para demostrar el fortalecimiento de la seguridad con las mejoras en el control de acceso a través del modelo propuesto y por consiguiente de la confidencialidad de la información.

Selección de indicadores para la comparación

Para la selección de indicadores se analizaron las normas, estándares, controles, resoluciones y guías más relevantes según la bibliografía consultada, entre las que se destacan las siguientes: ISO 27001 del 2005, ISO/IEC 17799 del 2005, controles sp800-53 del 2009 que recomienda el NIST, guía OWASP del 2008 y la Resolución 127 de 2007 del MIC (Adrian Wiesmann 2005; IEC 2007; ITGI 2007; MIC 2007; ITGI, ISACA et al. 2008; Gallagher and Locke 2009). En la tabla 1se encuentran los indicadores definidos para el proceso Autorización. Se definieron indicadores además para el proceso de Identificación y Autenticación y para el de Auditoría. Pueden ser los indicadores para estos dos últimos procesos, consultados en la tesis doctoral (Baryolo 2012).

Tabla 1: Definición de los indicadores.

Procesos	**No.**	**Indicadores**
Autorización	In_{11}	Solución de autorización
	In_{12}	Implementa algún estándar para la asignación de privilegios y el intercambio de mensajes de autorización
	In_{13}	Gestión de privilegios basado en roles
	In_{14}	Gestión de privilegios a nivel de usuario
	In_{15}	Gestión de las estructuras del nivel de base de datos y su relación con los sistemas
Autorización	In_{16}	Gestión de privilegios a nivel de base de datos
	In_{17}	Gestión de privilegios utilizando criterios o propiedades que identifican a los recursos (objetos, datos, URL, entre otros) para aplicar reglas sobre ellos

	In 18	Gestión de privilegios a nivel de funcionalidades
	In 19	Gestión de privilegios teniendo en cuenta las estructuras y los dominios organizacionales (entornos multidominios)
	In 20	Gestión centralizada de privilegios en entornos multisistemas
	In 21	Mínimo privilegio
	In 22	Administración de cuentas
	In 23	Federación de privilegios entre dominios
	In 24	Administración de sesiones de usuarios

Selección de los sistemas

Para llevar a cabo las pruebas, se seleccionaron varios sistemas que implementan módulos de control de acceso. Los mismos están basados en los modelos más empleados en la actualidad para el desarrollo de soluciones de control de acceso. Para la selección de los sistemas que formaron parte de la muestra, se establecieron cuatro criterios fundamentales:

1. Que implementaran alguno de los procesos del control de acceso basado en los modelos, estándares y protocolos más aplicados de la literatura. De esta forma se garantiza que los sistemas seleccionados implementan estándares, modelos o protocolos que fueron creados con el mismo objetivo que el modelo propuesto, este es, fortalecer el control de acceso.
2. Que los sistemas fueran de gran envergadura y que informatizaran procesos críticos del entorno organizacional o centrado en alguno de los procesos del control de acceso. Este criterio brinda la posibilidad de contar con sistemas críticos para la gestión de los procesos en el entorno organizacional y por tanto la fortaleza del control de acceso debe ser mayor. También puede conllevar a la selección de sistemas especializados en uno de los procesos del control de acceso.
3. Que contaran con evaluaciones de seguridad de entidades nacionales o clientes externos. Lo cual constituye un aval que respalda que los sistemas seleccionados cumplen con los requisitos de seguridad establecidos por las entidades internas y externas.
4. Que tuvieran buenos resultados en la aplicación en entornos reales, reflejando que los sistemas cumplieron satisfactoriamente los requisitos de seguridad establecidos en entornos reales de aplicación.

En la muestra se encuentran sistemas desarrollados sobre los marcos de trabajo más utilizados en la actualidad para el desarrollo de SI, que cumplen los requisitos establecidos. En la tabla 2 se especifica el nombre de los sistemas, su

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

descripción, los procesos del control de acceso que implementan, bajo qué modelos fueron desarrollados y la entidad que realizó la evaluación de seguridad en caso que proceda.

Tabla 2. Descripción de los sistemas seleccionados.

Sistemas	Descripción	Nombre del Proceso	Soluciones que implementan	Entidad evaluadora
ERP Universitario	Sistema para gestión de los procesos sustantivos del entorno universitario	Autorización	ABAC (Yuan 2005)	Calisoft
SIGEP	Sistema para la gestión de información penitenciaria en Venezuela	Autorización	RBAC	Cliente en Venezuela
SUIN	Sistema para la gestión de identidades de las personas en Cuba	Autorización	RBAC	MININT
SIGEL	Sistema para la gestión del proceso electoral en Cuba	Autorización	RBAC y ABAC	Calisoft y MININT
SIIPOL	Sistema para la gestión de los procesos policiales en Venezuela	Autorización	RBAC y ABAC	Cliente en Venezuela
SIGAC	Sistema para la planificación y control de Auditorías	Autorización	PCAECM	

Diseño experimental

El pre-experimento tiene como objetivo observar, en un entorno básico, la instancia del modelo PCAECM (SIGAC) presenta un nivel de fortaleza igual o mayor que los demás sistemas. Para ello es necesario evaluar la fortaleza del control de acceso de cada sistema a partir del nivel de cumplimiento de los indicadores seleccionados. Para el experimento se toma como entradas los indicadores, la criticidad de cada uno de ellos y los sistemas seleccionados, entre ellos se encuentran algunos desarrollados en la UCI y otros libres desarrollados por organizaciones extranjeras. La evaluación se debe realizar para el proceso Autorización que es el analizado.

- Sistemas desarrollados en la UCI: los indicadores fueron aplicados por los arquitectos y líderes de proyectos que participaron en su desarrollo.

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

- Sistemas libres desarrollados por organizaciones extranjeras: los indicadores fueron aplicados por especialistas con experiencia en el trabajo con estos sistemas.

La Tabla 2 muestra el diseño del pre-experimento realizado como parte del proceso de validación.

Tabla 2: Diseño experimental propuesto.

		Sistema 1 (Modelo 1)		**…**	**Sistema n (Modelo n)**	
In	**C (No normalizado)**	**E**	**EF**	**…**	**E**	**EF**
In_1	P_1	E_{11}	$P_1 xE_{11}$	…	E_{1n}	P_1xE_{1n}
In_2	P_2	E_{21}	$P_2 xE_{21}$	…	E_{2n}	P_2xE_{2n}
…	…	…	…	…	…	…
In_m	P_m	E_{m1}	$P_m x E_{m1}$	…	E_{mn}	P_mxE_{mn}

A continuación, se describen los conceptos utilizados en el pre-experimento:

- **Indicadores (In):** son los indicadores seleccionados por cada uno de los procesos para realizar las evaluaciones.
- **Criticidad (C):** se refiere al peso asignado por los expertos a cada uno de los indicadores atendiendo a su nivel de criticidad. La criticidad final de cada indicador se obtendrá a partir del cálculo del promedio (P) entre todos los valores emitidos por los expertos en las encuestas. El valor de criticidad para cada indicador se encuentra entre el rango de uno a cinco, siendo el valor uno de menor y el cinco de mayor valor de criticidad.
- **Sistema:** sistemas seleccionados para ser evaluados en cada uno de los procesos a través de la aplicación de los indicadores.
- **Modelo implementado:** representa el modelo que implementa cada uno de los sistemas en el proceso evaluado.
- **Evaluación (E):** representa el nivel de cumplimiento de los indicadores que tiene cada uno de los sistemas.
- **Evaluación final (EF):** constituye la evaluación final que obtienen los sistemas en cada uno de los indicadores, obtenida de la multiplicación de los Pm x Emn.

La evaluación de los indicadores puede tomar valores entre cero y cinco en función del nivel de cumplimiento que tenga el sistema en el indicador evaluado. La evaluación final de cada sistema en un indicador se calcula multiplicando la evaluación recibida en el indicador (ejemplo: E11) por el promedio de criticidad (ejemplo: P1).

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

Donde el cinco es el mejor valor de evaluación del indicador y el cero donde no se encuentra indicio de cumplimiento del indicador en el sistema analizado.

El procesamiento de los resultados de los experimentos se usó el programa estadístico SPSS (siglas de Statistical Package for the Social Sciences) versión 13.0. Con este diseño experimental se procede a la aplicación del pre-experimento.

Aplicación del pre-experimento

La aplicación del pre-experimento tiene como objetivo valorar el nivel de fortaleza que presenta la instancia de PCAECM (SIGAC) en comparación con las demás instancias que forman parte de la muestra, en cada uno de los procesos del control de acceso. Para ello fue necesario evaluar la fortaleza del control de acceso de cada instancia a partir del nivel de cumplimiento de los indicadores seleccionados. Las evaluaciones de los sistemas en cada uno de los indicadores no se incluyeron en los anexos para no comprometer su seguridad, por esta razón solo se realizan los análisis en función de los porcientos de cumplimiento de los indicadores en cada proceso.

Al proceso de Autorización se le aplicaron los indicadores (indicadores del In11 al In24) definidos para este proceso. Las evaluaciones obtenidas permitieron identificar los siguientes elementos:

Los estándares más utilizados para implementar este proceso son los modelos RBAC y ABAC.

- Existen deficiencias relacionadas con la implementación de estándares para el intercambio de mensajes de autorización.
- La gestión de privilegios sobre los recursos del nivel de sistema y los recursos del nivel de base de datos se realiza de forma independiente.
- Todas las soluciones cumplen con el principio de mínimo privilegio.
- Se evidencia la necesidad de fortalecer la administración de las sesiones de los usuarios.
- A pesar de excluir las evaluaciones relacionadas a los entornos multidominios, el sistema SIGAC presenta mayor nivel de seguridad que los demás sistemas.

La figura 2 refleja el porciento de cumplimiento de los indicadores asociados a este proceso por cada uno de los sistemas que forman parte de la muestra.

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

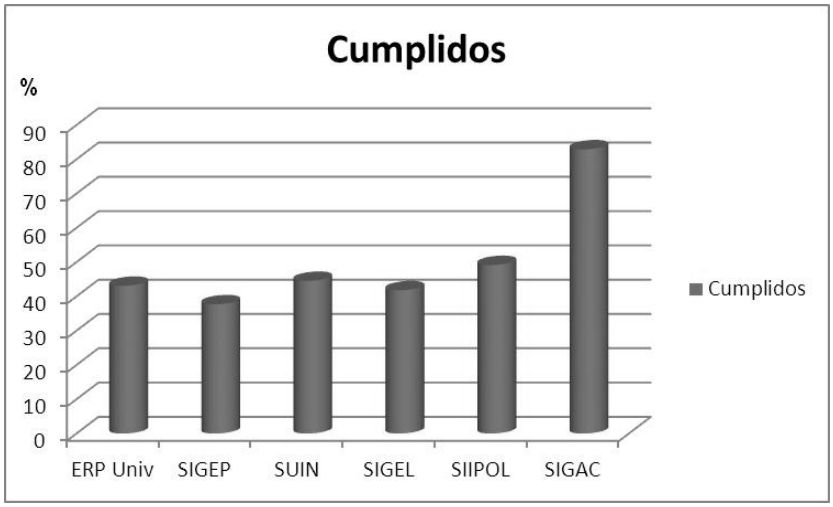

Figura 2: Cumplimiento de los indicadores de autorización.

Para verificar si existen diferencias significativas entre las evaluaciones proporcionadas por los especialistas de cada uno de los sistemas, se aplicó el test de Kruskal-Wallis. Se utilizó esta prueba no paramétrica porque su distribución no puede ser definida a priori, pues los datos observados son los que la determinan, las estadísticas no se basan en ninguna suposición en cuanto a la distribución de probabilidad a partir de la que fueron obtenidos los datos. Esta prueba permitió observar que existen diferencias significativas (significación menor a 0.05) entre las evaluaciones de los indicadores establecidas para cada uno de los sistemas. Los detalles de esta prueba se pueden encontrar en la tabla 3.

Tabla 3: Significación obtenida entre todas las muestras en el proceso de autorización.

			Indicadores
Chi-Square			17,807
Df			5
Asymp. Sig.			,003
Monte Carlo Sig.	Sig.		,002(a)
	99% Intervalo de confianza	Límite inferior	,001
		Límite superior	,003

a Basado en 10000 tablas incluidas en la muestra a partir de a partir de 2000000.
b Kruskal Wallis Test
c Variables agrupadas por: Sistemas

Partiendo de los resultados obtenidos, es necesario demostrar que existen diferencias significativas entre SIGAC y los demás sistemas a través de la comparación por pares. Con este objetivo se seleccionaron los tres sistemas con mayor rango medio, entre los tres sistemas se encuentran SIGAC, SIIPOL y SIGEL como se muestra en la tabla 4. Los

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

sistemas están enumerados del 1 al 6. Con el siguiente orden: ERP Universitario, SIGEP, SUIN, SIGEL, SIIPOL y SIGAC.

Tabla 4: Rango medio de las evaluaciones de cada uno de los sistemas en el proceso de autorización por el test de Kruskall-Wallis.

Sistemas		N	Rango medio
ERP Univ.	1,00	14	37,07
SIGEP	2,00	14	33,54
SUIN	3,00	14	37,21
SIGEL	4,00	14	37,46
SIIPOL	5,00	14	43,18
SIGAC	6,00	14	66,54
	Total	84	

Para realizar las comparaciones entre SIGAC y los otros dos sistemas se aplicó el test de Mann-Whitney. Se utilizó esta prueba no paramétrica por las mismas razones que la anterior. El análisis de los resultados de esta prueba permitió constatar que existen diferencias significativas (significación menor a 0.05) entre la evaluación de los indicadores correspondiente a SIGAC y las de los otros dos sistemas de mayor rango medio. Ver las tablas 5 y 6.

Tabla 5: Significación obtenida en la comparación por pares de las evaluaciones de SIGAC y el sistema SIGEL

			Indicadores
Mann-Whitney U			31,500
Wilcoxon W			136,500
Z			-3,076
Asymp. Sig. (2-tailed)			,002
Exact Sig. [2*(1-tailed Sig.)]			,001(a)
Monte Carlo Sig. (2-tailed)	Sig.		,001(b)
	99% Intervalo de confianza	Límite inferior	,000
		Límite superior	,002
Monte Carlo Sig. (1-tailed)	Sig.		,001(b)
	99% Intervalo de confianza	Límite inferior	,000
		Límite superior	,002

a No corregidos para los lazos.
b Basado en 10000 tablas incluidas en la muestra a partir de a partir de 334431365.
c Variables agrupadas por: Sistemas

Tabla 6: Significación obtenida en la comparación por pares de las evaluaciones de SIGAC y el sistema SIIPOL.

	Indicadores
Mann-Whitney U	49,500
Wilcoxon W	154,500

Revista Cubana de Ciencias Informáticas
Vol. 10, No. 1, Enero-Marzo, 2016
ISSN: 2227-1899 | RNPS: 2301
http://rcci.uci.cu
Pág. 245-260

Z			-2,253
Asymp. Sig. (2-tailed)			,024
Exact Sig. [2*(1-tailed Sig.)]			,024(a)
Monte Carlo Sig. (2-tailed)	Sig.		,025(b)
	99% Intervalo de confianza	Límite inferior	,021
		Límite superior	,029
Monte Carlo Sig. (1-tailed)	Sig.		Sig.
	99% Intervalo de confianza	Límite inferior	,010
		Límite superior	,015

a No corregidos para los lazos.
b Basado en 10000 tablas incluidas en la muestra a partir de a partir de 1502173562.
c Variables agrupadas por: Sistemas.

Los resultados de las pruebas permiten afirmar que SIGAC presenta mayor fortaleza en el proceso de autorización que los demás módulos de control de acceso.

De esta forma se demuestra que el componente de autorización del modelo PCAECM, fortalece en mayor medida el control de acceso que los modelos implementados en este proceso por los demás sistemas. Por tanto, se deriva que la confidencialidad de la información es mayor con el modelo propuesto que con los comparados.

Conclusiones

En el transcurso de la investigación se llegaron a las siguientes conclusiones:

- El modelo PCAECM como extensión del modelo RBAC incorpora varios conceptos que garantizan en su conjunto un nivel mayor de granularidad en el establecimiento de políticas de autorización en entornos cubanos multidominios con respecto al modelo RBAC.
- Los resultados del experimento realizado permitieron constatar que la instancia del modelo propuesto (SIGAC) preserva en mayor medida la confidencialidad de la información que las demás instancias que formaron parte de la muestra.
- Se proporciona una solución informática a los problemas de compartimentación de la información en entornos cubanos multidominios, la cual no estaban soportadas en las aplicaciones de planificación estudiadas y además que cumpliera con las normativas cubanas para la planificación y control de auditorías.

Referencias

AARON KERSHENBAUM, M. M.-Z., MARK WALL (1994). Network Management and Control. M. M. Ivan.T. Frisch, Shivendra S. Panwar. Nueva York, EUA, Plenum Press. **2**.

AdRIAN WIESMANN, A. V. D. S., MARK CURPHEY, RAY STIRBEI (2005). Una Guía para Construir Aplicaciones y Servicios Web Seguros. T. O. W. A. S. P. (OWASP). EUA. **2.0:** 1 - 311. Disponible en: <https://www.owasp.org/images/b/b312/OWASP_Development_Guide_312.310.311_Spanish.pdf> [Consultado 324/302/2012].

ALI E. ABDALLAH, H. T. (2008). Integrating Delegation with the Formal Core RBAC Model. The Fourth International Conference on Information Assurance and Security, Naples, Italia, IEEE Computer Society.

BARYOLO, O. G. (2012). CAEM: Modelo de Control de Acceso para sistemas de información en entornos multidominios. DEPARTAMENTO TECNOLOGÍA. La Habana, Universidad de las Ciencias Informáticas**:** 131.

CUBADEBATE (2013) "Cuba: Auditoría a un tercio de entidades estatales concluyó con saldo negativo." Cubadebate.com.

EXAMINERS, A. o. C. F. (2014). 2014 Report to the Nations. EUA, Association of Certified Fraud Examiners**:** 84.

GAIL-JOON AHN, R. S., MYONG KANGKAND JOON PARK (2000) "Injecting RBAC to Secure a Web-based Work ow System." The ACM Digital Library, 1 - 10 DOI: 10.1145/344287.344295.

GALLAGHER, P. D. AND G. LOCKE (2009). Recommended Security Controls for Federal Information Systems and Organizations. U. National Institute of Standards and Technology (NIST). EUA. **Special Publication 800-53:** 1 - 237. Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-253-Rev233/sp800-253-rev233-final.pdf> [Consultado 221/203/2012].

IEC, I. (2007). International Standard ISO/IEC 27002. ISO/IEC. Suiza. **ISO/IEC 17799:2005/Cor.1:2007(E)**.

ITGI (2007). Control Objectives for Information and related Technology (COBIT). I. G. Institute. EUA. **4.1:** 1 - 211. Disponible en: <http://www.isaca.org/COBIT/Pages/default.aspx> [Consultado 227/203/2011].

ITGI, ISACA, et al. (2008). Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa. I. ITGI, OGC, TSO. EUA. **2,7:** 1 - 130. Disponible en: <http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-134.131,-ITIL-v133-y-ISO-27002-en-beneficio-de-la-empresa-v27002,27007.pdf> [Consultado 27006/27010/22011].

JASON CRAMPTON, H. K. (2009). A Framework for Enforcing Constrained RBAC Policies. International Conference on Computational Science and Engineering, Washington, DC, USA, ACM Digital Library.

KUHN, D. R., COYNE, EDWARD J., WEIL, TIMOTHY R. (2010) "Adding Attributes to Role-Based Access Control." IEEE Computer Society **43**, 79-81.

LI MA, S. M., JIANGHUA LV, YUEFEI SUI (2009). A Dynamic Description Logic-based Formalism for RBAC. IEEE Computer Society, Washington, DC, USA, Fourth International Conference on Computer Sciences and Convergence Information Technology.

MIC (2007). Resolución No. 127 /2007. Oficina de Seguridad para las Redes Informáticas. M. d. l. I. y. l. C. d. l. r. d. Cuba. La Habana, Cuba. **127 /2007:** 1-24. Disponible en:

<http://ftur.uh.cu/intra/ftp/Resoluciones%20y%20Reglamentos/Resoluciones/R%20127-20107%20120Reglamento%20120de%20120Seguridad%20120Informatica.pdf> [Consultado 20128/20109/22011].

SHAFIQ, B. (2006) "ACCESS CONTROL MANAGEMENT AND SECURITY IN MULTI-DOMAIN COLLABORATIVE ENVIRONMENTS." The ACM Digital Library.

TAO WANG, W.-H. L., ZUN LIU (2006) "RBAC Permission Consistency Static Analysis Framework." IEEE Computer Society.

WANG Tao, L. W.-h., LIU Zun (2010). RBAC Permission Consistency Static Analysis Framework. International Conference on Multimedia Information Networking and Security, Nanjing, Jiangsu, China, IEEE Computer Society.

XUEXIONG, Y., W. QINXIAN (2010) "A Multiple Hierarchies RBAC Model." International Conference on Communications and Mobile Computing, 56-60.

YUAN, E. A. J. T. (2005) "Attributed Based Access Control (ABAC) for Web Services." International Conference on Web Services, 1-9.

YUE ZHANG, J. B. D. J. (2007). A Request-Driven Secure Interoperation Framework in Loosely-Coupled Multi-domain Environments Employing RBAC Policies. Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007. International Conference on, New York, EUA.