UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

FACULTAD 2

CENTRO DE TELEMÁTICA

DEPARTAMENTO SEGURIDAD INFORMÁTICA

MODELO PARA LA PLANIFICACIÓN Y CONTROL DE LAS AUDITORÍAS EN ENTORNOS CUBANOS MULTIDOMINIOS

Trabajo final presentado en opción al título de

Máster en Informática Aplicada

Autor: Ing. Yasser Azán Basallo

Tutor: MSc. Oiner Gómez Baryolo

La Habana, 2012

AGRADECIMIENTOS

En especial deseo agradecer este trabajo a mí querida madre, Marilín Basallo Rodríguez y mi padre, Luis Azán Abreu; así como a mis amigos de la Universidad de las Ciencias Informáticas (UCI), quienes también contribuyeron a mi crecimiento profesional y humano.

También a quien le pertenece el corazón con el cual he logrado llegar a crear este trabajo de investigación, a mi novia Yanay Hernández Sosa, quien me ha acompañado y alentado a pesar de las adversidades y los tragos amargos.

DECLARACIÓN JURADA DE AUTORÍA

Declaro por este medio que yo Yasser Azán Basallo, con carné de identidad 83071610188, soy el autor principal del trabajo final de maestría: **Modelo para la planificación y control de las auditorías en entornos cubanos multidominios,** desarrollada como parte de la Maestría en Informática Aplicada y que autorizo a la Universidad de las Ciencias Informáticas a hacer uso de la misma en su beneficio, así como los derechos patrimoniales con carácter exclusivo.

Y para que así conste, firmo la presente declaración jurada de autoría en Ciudad de La Habana a los ____ días del mes de _____ del año 2012.

_____

<Firma del maestrante en tinta azul>

RESUMEN

El fraude corporativo es un problema global y nacional, por eso se creó primero el Ministerio de Auditoría y Control que luego pasó a ser La Contraloría General de la República de Cuba (CGRC). La CGRC está estructurada en diferentes direcciones y es el encargado de planificar, controlar y dirigir el Sistema Nacional de Auditoría del país.

En el presente trabajo se describen las necesidades presentadas por la CGRC a la Universidad de las Ciencias Informáticas (UCI) de informatizar los procesos de planificación y control de este organismo siguiendo un Esquema de Seguridad Multidominio. Se describe el modelo para la planificación y control en entornos cubanos multidominio y la solución informática dada a la CGRC y a las 41 Unidades Centrales de Auditoría Interna donde se instaló la solución computacional SIGAC.

Palabras claves: Auditoría, control, planificación, modelo.

ABSTRACT

Corporate fraud is a national and global problem, so he created first the Ministry of Audit and Control which later became Comptroller General of the Republic of Cuba (CGRC). The CGRC is structured in different directions and is responsible for planning, controlling and directing the National Audit of the country.

This paper describes the needs presented by the CGRC the University of Informatics Sciences (UCI) to automate the planning and control of this organism with Security *Scheme Multi-Domian*. Shows the *Multi-Domain* model and the computer solution for the process given above such as the 40 Central Internal Audit Units which was installed SIGAC computing solution.

Keywords: Audit, control, planning, model.

TABLA DE CONTENIDOS

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 2010, basado en 1.843 casos de fraude que fueron reportados por *Certified Fraud Examiners* (siglas en inglés: CFEs) estima que una organización típica pierde un 5% de sus ingresos anuales producto del fraude. Si se aplica este porcentaje al producto interno bruto global estimado para el 2009, se traduce en una pérdida potencial de más de 2,9 billones de dólares a nivel mundial [1].

Un estudio realizado por la KPMG[1] en América Latina las empresas que evalúan sus procesos internos pierden por año un 7% de sus ganancias por prácticas fraudulentas. Existe un 47% de las compañías en esta zona que no evalúan sus procesos internos. PriceWaterhouseCoopers[2] afirma que el 74% de las firmas sufren delitos y fraudes corporativos en el año. [2].

De las más de 750 entidades auditadas en Cuba en el año 2010, el 63% tuvo calificaciones satisfactorias y aceptables, mientras que el 37% fue evaluado deficiente o mal, según Gladys Bejerano Portela, Contralora General de la República de Cuba en el semanario Trabajadores [3].

---

[1] **KPMG** es una de las cuatro firmas más importantes del mundo de servicios profesionales junto a PricewaterhouseCoopers, Deloitte Touche Tohmatsu y Ernst & Young. Tiene presencia en 148 países. Es el resultado de la fusión en 1987 entre Klynveld Main Goerdeler (KMG) y Peat Marwick International.

[2] **PricewaterhouseCoopers** (PwC) es una firma de servicios profesionales con 169.000 personas en 153 países. Está organizada en tres grandes líneas de negocio: Auditoría, Consultoría de Negocio y Financiera y Asesoramiento Legal y Fiscal.

La grave situación existente en el mundo y en Cuba, resalta la importancia de incluir mecanismos o procesos en las entidades o empresas para evitar las violaciones mencionadas anteriormente. Por eso se crean las auditorías que no son más que "*un enfoque amplio que examina y critica el proceso administrativo, la división funcional y estructural, los planes, objetivos, procedimientos, controles, aspectos físicos y humanos, no solo los existentes, sino para detectar las omisiones*" [4]. Según Roberto Campo, especialista del Instituto Argentino de Auditoría Interna. "*Para las organizaciones siempre ha sido importante el cumplimiento de una normativa, verificar como se realizó, generar eficiencia y mitigar los riesgos que tiene la compañía*". Por estos motivos se creó la Contraloría General de la República de Cuba (CGRC). El mismo es el 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 las auditorías. Entre sus funciones de regular, organizar, dirigir y controlar metodológicamente, el Sistema Nacional de Auditoría [5].

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 la Dirección de Atención al Sistema Nacional de Auditoría, Supervisión y Control (DASNAC). La DASNAC 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 estamos en presencia de un entorno multidominio, donde diferentes organizaciones se interrelacionan usando sus propias políticas de seguridad [6]. Este concepto permite la interoperabilidad de los sistemas informáticos.

La planificación de la auditoría garantiza el diseño de una estrategia adaptada a las condiciones de cada entidad, tomando como base la información recopilada en la etapa de exploración previa. En este proceso se organizan las personas implicadas, las tareas a realizar por cada uno de los ejecutantes, los recursos necesarios, los objetivos y programas a aplicar entre otros [7].

En la DASNAC 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 presunto hechos delictivos respectivamente.

Las deficiencias mencionadas de las herramientas informáticas anteriores, provocan que se atrasen en la entrega de los informes de los controles de cumplimiento del Plan Anual de las Auditorías, por el volumen de datos que se manejan. Esta situación provoca que no estén los informes para el momento que se necesitan para la toma de decisiones.

Se cometen errores en el procesamiento manual de los datos. Este problema tiene lugar por las personas ya que no existe un sistema que realice las comprobaciones pertinentes para evitar los errores en la gestión de los datos. Un ejemplo es la planificación de varias auditorías en el mismo año a una misma organización, debido a su registro con diferentes nombres.

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.

Los problemas encontrados en los sistemas de planificación y control de auditoría existentes en la DASNAC, podrían estar condicionados por las deficiencias encontradas por los modelos existentes en la literatura. Entre los más aceptados para el control de acceso se encuentra el modelo RBAC**.** Este modelo es el más aplicado y consultado, pero sus propios creadores reconocen que no es aplicable a entornos multidominios, debido a que no tienen un mecanismo para establecer diferencias entre los usuarios que desempeñan un mismo rol.

El modelo RBAC ha sido extendido con diferentes objetivos. Entre los representativos están: el T-RBAC [8], el cual tiene como característica principal otorgar los permisos de acceso a las tareas; y el GEO-RBAC [9], que se centra principalmente en la asociación de roles con la extensión espacial y la activación y habilitación de roles en dependencia de la localización de los usuarios. Ninguno de estas restricciones resuelve el problema en su totalidad de la compartimentación de la información en entornos multidominio.

Partiendo de la problemática existente se definió el siguiente **problema de investigación:**

¿Cómo gestionar el proceso de planificación y control de las auditorías en entornos cubanos multidominios preservando la confidencialidad de la información?

El **objeto de estudio** está enmarcado en los procesos de planificación y control de las auditorías.

Para solventar el problema planteado se determinó como **objetivo general:**

Desarrollar un modelo de planificación y control de auditorías en entornos cubanos multidominios que cumpla con lo estipulado en la Resolución 091/08 de la CGRC e incorpore políticas de autorización para preservar la confidencialidad de la información.

Se desglosaron los siguientes **objetivos específicos** para lograr el objetivo general:

1. Construir el marco teórico conceptual de la investigación, relacionado con las soluciones existentes para la planificación y control de las auditorías y la definición de políticas de autorización.
2. Modelar el proceso de planificación y control de las auditorías en entornos cubanos multidominios.
3. Extender el modelo RBAC para que cubra los requisitos de autorización presentes en los entornos cubanos multidominio.
4. Aplicar el modelo propuesto en el desarrollo de un sistema informático para la planificación y control de las auditorías en entornos cubanos multidominio.
5. Validar el modelo propuesto.

Como **campo de acción** de la investigación se determinó:

Los modelos de planificación y control de las auditorías en entornos cubanos multidominios.

Al concluir el análisis de la literatura para conformar el marco teórico, se formuló la siguiente **hipótesis**:

Si se desarrolla un modelo de planificación y control de auditorías en entornos cubanos multidominio que cumpla con lo estipulado en la Resolución 091/08 de la CGRC e incorpore políticas de autorización, se logrará preservar la confidencialidad de la información.

CAPÍTULO I: FUNDAMENTACIÓN TEÓRICA DE LA INVESTIGACIÓN.

El proceso de auditoría de una organización es una de las principales etapas del ciclo de mejora continua de los procesos organizacionales. Aporta a la conformidad del sistema de gestión adoptado por la organización con las disposiciones planificadas.

El planeamiento de las auditorías organiza todo el trabajo: las personas implicadas, las tareas a realizar por cada uno de los ejecutantes, los recursos necesarios, los objetivos, los programas a aplicar entre otros. Se planifica para garantizar el éxito de la ejecución de la auditoría.

Según Salvador Mercado, planear es tan importante como organizar, dirigir o controlar, porque la eficiencia no se logra con la improvisación y si administrar es hacer a través de otros, se necesita hacer planes sobre la forma como esa acción se habrá de coordinar. El objetivo no se lograría si los planes no lo detallaron para ser alcanzado. Todo control sería poco efectivo si no se compara con un plan previo [10].

En este capítulo se puntualizan los conceptos, elementos y principios implicados en la planificación de auditorías. Se analizan los estándares y prácticas internacionales más difundidas para la práctica de auditoría y sus inconveniencias con respecto a la planeación en el país. Se analizan las herramientas informáticas encontradas que proporcionan una solución completa al proceso de auditoría.

1.1. Conceptos asociados al dominio del problema

La auditoría es el proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar la extensión en que se cumplen los criterios tomados como referencia [11].

La planificación de auditorías es una tarea común a todos los sistemas de gestión. En la planificación determinamos qué se va a auditar, cuándo y quién lo va a hacer. La

planificación ha de compatibilizar las necesidades de verificar que todo funciona bien, con la disponibilidad de la organización [11].

Confidencialidad: Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso [12].

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento [12].

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados [12].

Dominio: Una entidad lógica con una red interconectada, y puede representar una subred consistente de un conjunto de elementos de red [13].

Entornos multidominios: Con el aumento de la accesibilidad de la información y la necesidad de perfeccionar la gestión del conocimiento, existe una preocupación creciente por la confidencialidad, integridad, disponibilidad de los recursos en las organizaciones. En las grandes transnacionales corporativas, el acceso a la información no autorizada es uno de los principales problemas de seguridad. Numerosos estudios han demostrado que los accesos no autorizados, en particular, por los usuarios internos, representan una amenaza de seguridad importante para entornos empresariales distribuidos. Este problema es aún mayor en entornos multidominios, que abarcan varias organizaciones que colaboran para satisfacer sus necesidades de negocio [14]. Es en donde múltiples organizaciones distribuidas interoperan cada uno con su propias políticas de seguridad [6].

Un dominio de seguridad, en el contexto de un entorno de colaboración, es un grupo acotado de bienes protegidos y usuarios a los que se aplica una sola política de control de acceso ejecutada por un único administrador de seguridad. Un entorno multidominio es una estructura jerárquica compleja, que agrupa a varias organizaciones atendiendo

a un criterio común, para facilitar el acceso e interoperabilidad entre sus sistemas de información distribuidos de una forma segura [15].

El control de acceso: es un método que garantiza que solo tengan acceso a un sistema o a la información que éste contiene, aquellos debidamente autorizados para ello. Los mecanismos de control de acceso se implementan utilizando técnicas de hardware y software y por lo general incluyen: identificación y autenticación de usuarios; limitación de acceso, monitorización de las acciones de los usuarios y un sistema de auditoría [16].

1.2. Tipos de planificación

La planificación normativa o tradicional: Es un modelo de planificación que se rige por normas o parámetros previamente establecidos por el estado. Tiene una permanente capacidad para auto criticarse y evolucionar. Ha hecho el acopio de numerosas técnicas de análisis y predicción. Ha desarrollado todo un complejo sistema institucional y legal propio. Cuenta con una vastísima experiencia en los más diversos campos de aplicación. Su gran fortaleza es su familiaridad con los problemas propios del desarrollo económico – social visto desde el ángulo gubernamental. El planificador es -omnisciente-. Se subdivide en: Centralizada (Países socialistas) y Mixta, Pluralista, o Indicativa (países de Latinoamérica). Utiliza conceptos de políticas, proyectos, acciones y recomendaciones como proposiciones vagas de contenido de ejecución [17].

La planificación situacional: Es calcular, presidir y preceder las acciones para llevar una situación inicial a otras, hasta llegar a la situación que el actor pretende alcanzar. Otra de las definiciones que se puede encontrar en la literatura específica que este proceso es aquel que se genera por instancias de discusión, cálculos y análisis de los actores de una organización que construyen una situación objetiva de un determinado acto social. Tecnológicamente, aborda la anticipación simulada por la práctica. Planifica dentro de la realidad y coexiste con otros actores que también planifican. No tiene un

diagnóstico único, ni una verdad objetiva; sino una explicación situacional. Se articula lo político con lo económico pues su horizonte es político y el futuro es incierto. Es un proceso que no se agota en el tiempo, siempre está en acción. Entre la relación del -debe ser- y el -puede ser- tiene expresión "lo viable" que presenta aspectos económicos, institucionales, culturales y políticos. Concibe la norma como la orientación direccional entorno a la cual es necesario construir las condiciones para su cumplimiento; es decir, lo normativo tiene validez, pero no constituye de por sí el plan [17].

La planificación estratégica: A este tipo de planificación, Steiner la define como un proceso continuo y sistémico que relaciona el futuro con las decisiones actuales en el contexto de cambios situacionales y que se expresa en la formulación de un conjunto de planes interrelacionados. Permite establecer claramente la misión y valores de la organización, como principio rector. Tiene su origen en el ámbito empresarial y surge como fuente de consolidación de la llamada Planificación Tradicional. Para definir los elementos estratégicos, se parte del proceso de investigación sistemática interna y externa. Es un sistema que tiene la capacidad de auto-reproducción y organización. Es un proceso cíclico, permanente, participativo e interactivo. Su centro práctico es la coyuntura, y se refiere al cálculo que precede y preside la acción. Se centra más en el logro de metas y objetivos que en seguir normas y reglamentos. Reconoce la incertidumbre y que la realidad es un sistema complejo. Rechaza la posición reactiva para adoptar una posición pre-activa, aún con los riesgos que ello supone. Se sustenta en tres grandes pilares: el usuario, la propia organización y los competidores. Descansa en la formulación de tres tipos de planes fundamentales como son los planes estratégicos de largo plazo; los programas a mediano plazo, los planes operativos y presupuestos a corto plazo [17].

La planificación táctica operacional: Se refiere básicamente a la asignación previa de las tareas específicas que deben realizar las personas en cada una de sus unidades de operaciones. Se da dentro de los lineamientos de la planificación estratégica y la

planificación táctica. Es conducida o ejecutada por los ejecutivos del nivel medio. Trata con actividades normales programables. Se maneja información interna y externa. Sigue procedimientos y reglas definidas con toda precisión. Cubre períodos cortos. Está orientada hacia la administración de recursos. Sus parámetros principales son la efectividad y la eficiencia [17].

La planificación normativa es el tipo de planificación que se ajusta a la solución informática por sus características para dar respuesta al problema planteado.

1.3. Elementos de la planificación en general.

La planificación tiene los siguientes elementos: [17]

- Objetivos (¿Qué?)
- Problema que se resuelve con un objetivo (¿Para qué?)
- Las actividades (¿Cómo?)
- Recursos o medios para los ejecutores (¿Con qué?)
- Cronología, secuencia y tiempo (¿Cuándo o en cuanto tiempo?)
- En que cantidad, la meta (¿Cuánto?)
- Responsables y ejecutores (¿Quiénes?)
- En que lugar (¿Dónde?)

Teniendo en cuenta que la planificación normativa no es guiada por objetivos, sino por las normas de la resolución cubana 091/08, existen elementos de la planificación que no se van a ser cumplidas por la solución informática, estas son: objetivos, problema que se resuelve con un objetivo, recursos o medios para los ejecutores y la meta.

1.4. Principios de la planificación en general.

Racionalidad: Se requiere el establecimiento de objetivos claros y precisos encuadrados en el contexto de la realidad. Es la utilización de recursos para alcanzar no sólo una buena efectividad, sino una máxima eficiencia [18].

Previsión: En los planes debe presentarse los lapsos definidos en que se ejecutarán las diferentes actividades. Así mismo, se deberán prever y jerarquizar los recursos necesarios para su realización [18].

Utilidad: Los planes deben formar una integración orgánica, armónica y coherente a objeto de obviar la duplicidad de esfuerzos y el mal gasto de los recursos [18].

Flexibilidad: Los planes deben confeccionarse de manera tal que permitan su adaptabilidad a cualquier cambio que se suscite en el transcurso de su ejecución y más aún tratándose de planes relacionados con el hecho educativo, el cual se caracteriza por su intenso dinamismo [18].

Continuidad: Las metas jamás deben ser abandonadas, cumplidas unas, se perseguirán otras, de lo contrario iríamos en contra de los principios de racionalidad, eficiencia y planificación misma [18].

La racionalidad: Es un principio de la planificación que está vinculado con los objetivos por lo que no puede ser medido desde este punto de vista en la planificación normativa.

1.5. Resolución No. 091/08

La resolución surge por la necesidad de perfeccionar y actualizar el procedimiento para la elaboración y control del Plan Anual de Auditoría, Comprobaciones Especiales, Visitas de Supervisión e Inspecciones Gubernamentales e Información de su cumplimiento.

Tiene como objetivo definir las normas generales para la elaboración y control de los Planes de Auditorías, Comprobaciones Especiales, Visitas de Supervisión e Inspecciones Gubernamentales, así como la información de su cumplimiento. Además define quienes son las estructuras organizativas las cuales tienen las obligaciones de su cumplimiento.

Especifica los elementos que constituyen las bases para la confección del Plan, estas son [19]:

a) Plan de la Economía y el Presupuesto del Estado. Directivas del Gobierno para el ejecutado el año anterior y la obligación de su seguimiento.

b) Solicitudes realizadas por el Gobierno y el Partido.

c) Análisis de los resultados de las acciones de control, modo de operar, tendencias.

d) Situación y tendencias de las manifestaciones de corrupción.

e) Evaluación de la situación de control por sector, actividad u organización.

f) Resultados de las quejas y denuncias de la población.

En el figura 1.1 se encuentra modelado el proceso Plan Anual de las Acciones de Control según la Resolución No. 091/08 con IDEF0, un método diseñado para modelar decisiones, acciones y actividades de una organización o sistema.

Con este proceso se consigue llevar la planificación normativa para las auditorías que se realizan en Cuba y además el control y seguimiento de la planificación realizada. La planificación concebida en los estándares y modelos internacionales no va a poder orientar la planificación como se realiza en el país por el tipo de planificación concebida, que no tiene que ver con la que se sigue en el país. No quiere esto decir que una empresa cubana no pueda seguir uno de los siguientes estándares; pero la planificación anual a nivel de país, por lo menos no se va a poder realizarse con ninguna de ellas.

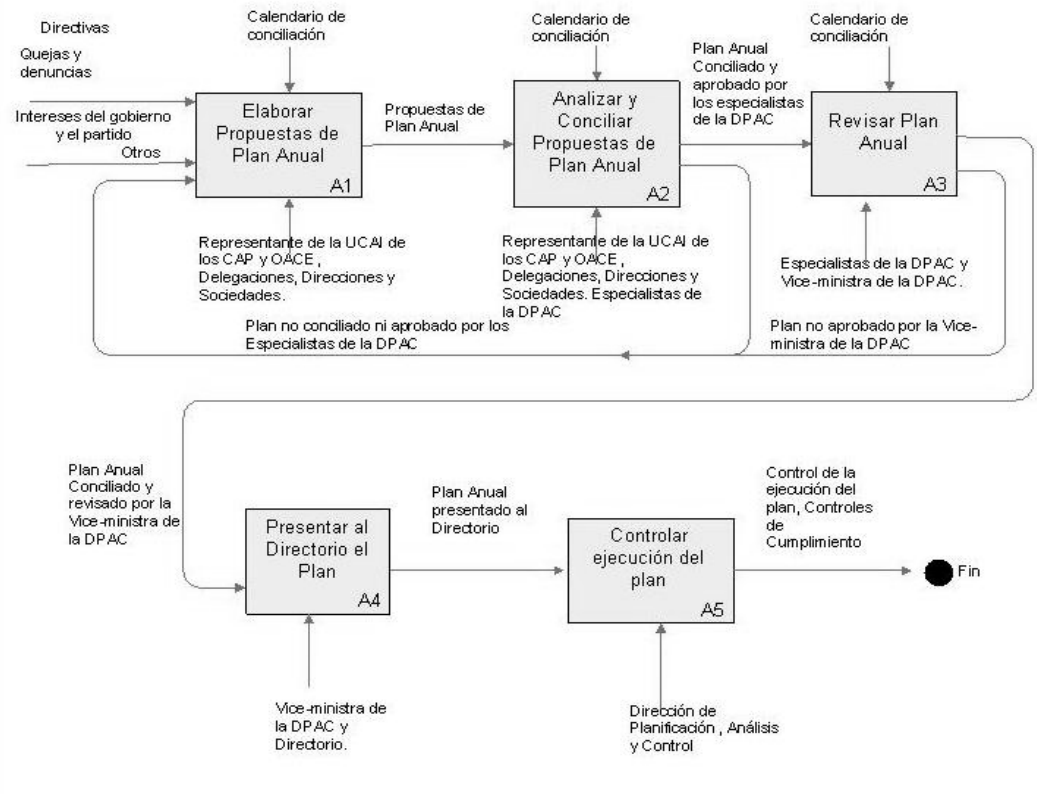


Figura 1.1: Proceso Plan Anual de Auditorías de Cuba Diagrama (Anexo 1, Tabla T1).

1.6. Modelos y estándares internacionales para el control interno y las auditorías

1.6.1. El Informe COSO

Son las siglas en inglés de: Comité de Organizaciones Patrocinadoras. Es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de Control Interno. Está diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías: [20]

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de la información financiera.
- Cumplimiento de leyes y normas que sean aplicables.

1.6.2. El Informe COCO

Son las siglas en inglés de: Criterios de la Comisión de Control. Es el producto de una profunda revisión sobre el reporte COSO y cuyo propósito fue hacer el planteamiento de un informe más sencillo y comprensible, ante las dificultades que en la aplicación del COSO enfrentaron inicialmente algunas organizaciones [21].

1.6.3. COBIT

Son las siglas en inglés de: Objetivos de Control para la Información y Tecnologías Relacionadas. Es un conjunto de mejores prácticas para el manejo de información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA), y el Instituto de Administración de las Tecnologías de la Información (ITGI) en 1992 [22].

1.6.4. ITIL

Son las siglas en inglés de: Biblioteca de Infraestructura de Tecnologías de la Información. Fue desarrollada al reconocer que las organizaciones dependen cada vez más de la Informática para alcanzar sus objetivos corporativos. Esta dependencia va en aumento como resultado de una necesidad creciente de servicios informáticos de calidad que se correspondan con los objetivos del negocio y que satisfagan los requisitos y las expectativas del cliente. A través de los años, el énfasis pasó de estar sobre el desarrollo de las aplicaciones TI a la gestión de servicios TI. La aplicación TI (a veces nombrada como un sistema de información) sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y, en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones [23].

1.6.5. ISO/IEC 27000

Es un conjunto de estándares desarrollados -o en fase de desarrollo por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical*

Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001 [24].

1.6.6. Valoración de los modelos y estándares internacionales control interno y las auditorías

Los actuales mecanismos internacionales orientan la confección de la planificación por objetivos para realizar las auditorías. Parten de la gestión de los riesgos como punto de partida de la planificación a diferencia de la resolución cubana, la cual parte de otros elementos para su elaboración mencionados en el epígrafe 1.2. ITIL es menos genérico que COBIT, ya que está enfocada a servicio. Las limitaciones presentes en los modelos y estándares estudiados impiden su aplicación para estandarizar el proceso de planificación de auditorías en la DASNAC y en las distintas UCAI del país.

El informe COSO en el componente Supervisión, define parámetros como son: El alcance de la evaluación, las actividades de supervisión continuadas existentes, las tareas de los auditores internos y externos, áreas o asuntos de mayor riesgo que no so parte del plan de las auditorías en Cuba. Además tiene otros elementos como son: el programa de evaluaciones, los evaluadores, la metodología y herramientas de control que son especificaciones en otros documentos que gestionan en la DASNAC pero no son datos propios del plan normado en la resolución cubana. Por estas diferencias no se ajusta a las condiciones cubanas el informe COSO a las necesidades del país.

Los estándares y modelos analizados guían la planificación estratégica por objetivos a diferencia de la planificación y control de las auditorías en Cuba, la cual se rige por las normas establecidas por el gobierno.

Por todo lo anteriormente expuesto, los estándares y modelos internacionales estudiados no pueden ser utilizados como pauta para la planificación y control de las auditorías en Cuba.

La Resolución 091/08 es una normativa de obligatorio cumplimiento para el entorno cubano. No se puede desviar de las regulaciones que esta indica, por lo que otra guía que indique procedimientos distintos a esta resolución no puede ser tomada aunque sean reconocidas internacionalmente.

1.7. Modelos de autorización

1.7.1. Modelo de Control de Acceso Basado en Atributos (ABAC)

En el modelo de Control de Acceso Basado en Atributos (en inglés Attribute Based Access Control, ABAC), los privilegios son establecidos en base a la colección de atributos que posee el usuario y una política que los determina. La representación de las políticas en ABAC es semánticamente más expresiva y posee una mayor granularidad ya que puede basarse en cualquier combinación de atributos de sujeto, de recursos y de entorno. En la infraestructura de gestión de políticas se utilizan certificados de atributos para asignar un conjunto de privilegios a cada usuario. El verificador comprueba en la política de control de acceso si el usuario tiene los privilegios suficientes para acceder al recurso solicitado [25]. La Figura 1.2 muestra los conceptos que integran la arquitectura propuesta por ABAC para el control de acceso.

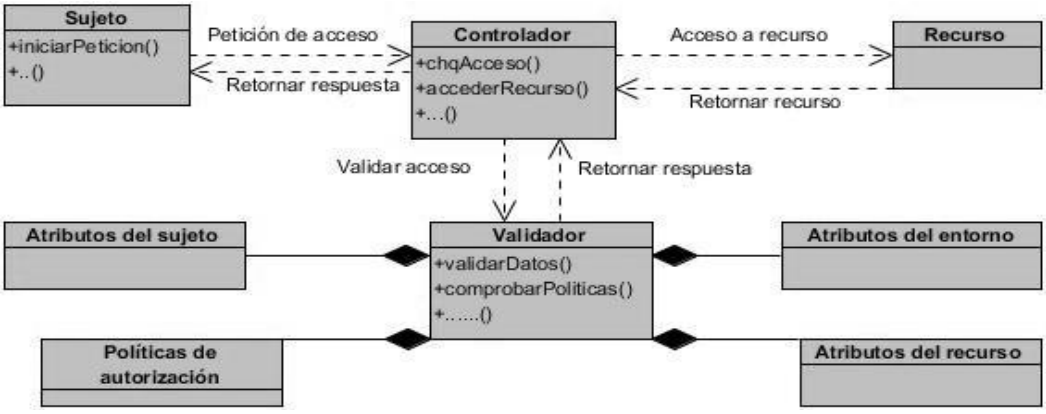


Figura 1.2. Modelo de control de acceso basado en atributos.

Las limitaciones de ABAC radican en la dificultad para definir los atributos de forma consistente en sistemas complejos desplegados en entornos multidominios [26]. La seguridad que proporciona ABAC depende del número de atributos y reglas que se establezcan. Este aspecto influye de forma negativa en el rendimiento del SI (Sistema Informático) a la hora de realizar las búsquedas para conceder o no el acceso. La ausencia del concepto rol en su definición, aumenta la complejidad de mantenimiento de las políticas en entornos heterogéneos y dinámicos [27-29].

1.7.2. Modelo de Control de Acceso Basados en Roles

El principal objetivo del modelo RBAC 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 [30]. 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 [31, 32].

Por otro lado, la Separación Dinámica de Deberes (en inglés, Dynamic Separation of Duty, DSD) al igual que la Separación estática de Deberes (en inglés, Static Separation of Duty, SSD), limitan los permisos que son disponibles para un usuario. Sin embargo DSD difieren de las SSD por el contexto en el cual estas limitaciones son impuestas. Las DSD limitan la disponibilidad de los permisos aplicando las restricciones sobre los roles que pueden ser activados durante una sesión de usuario. En otras palabras, un usuario puede ser activado para sólo uno de los dos roles distintos que le son asignados, mientras que su sesión de usuario siga activa [33, 34].

La Figura 1.3 muestra con mayor claridad los conceptos mencionados anteriormente y las relaciones que existen entre ellos.

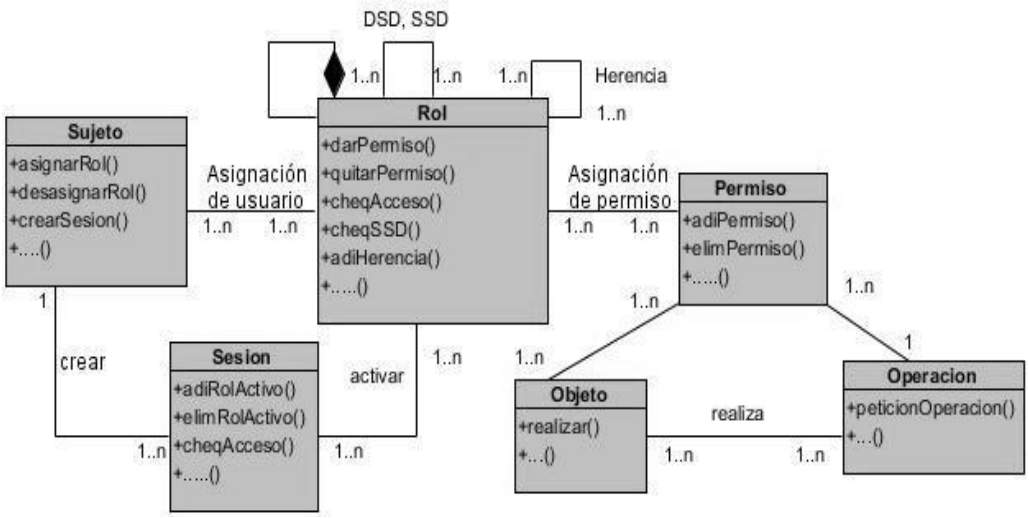


Figura 1.3. Modelo de Control de Acceso Basado en Roles (RBAC).

De este modelo surgieron varias variantes. A continuación se muestra en la figura 1.4 una tabla con 4 variantes del modelo RBAC.

El modelo RBAC y sus variantes permiten un control de los accesos de los usuarios a la información y por tanto regulan cuales usuarios pueden tener acceso a esta. Pero la limitación del modelo RBAC radica en poder delimitar el acceso a la información en entornos multidominio a usuarios que contengan un mismo rol, que es en parte el problema que trata la investigación presente.

A pesar del control del acceso que permite el RBAC, este modelo presenta dificultades que los mismos autores señalan [28, 35, 36]:

- 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.

RBAC0	Cada usuario tiene diferentes roles y cada rol lleva asociado algún permiso (no existen jerarquías ni restricciones).
RBAC1	Se introduce el concepto de *jerarquía de roles*, que se define como la autoridad de cada usuario para cumplir uno o varios roles. Los roles son las funciones que cada usuario tiene que cumplir. Por ejemplo, el usuario con mayor jerarquía dentro de una organización puede tener acceso a toda la información contenida en el sistema, incluso a la información del usuario con menor jerarquía, sin embargo no ocurre lo mismo al contrario.
RBAC2	Se introduce el concepto de *restricción*. El uso más frecuente de las restricciones es la separación de cargas dentro de una organización. Por ejemplo, una restricción es que un usuario en particular, debe cumplir solamente con un rol especificado, pero no puede efectuar funciones de otros roles (no existen jerarquías).
RBAC3	Las restricciones pueden ser impuestas sobre los roles jerárquicos dentro de una organización (existen jerarquías y restricciones, es el modelo más complejo).
Comparativa RBAC contra ACL	En grandes redes, el control de acceso basado en roles o **RBAC** (*Role Based Access Control*), tiene menos coste que las listas de control de acceso o **ACL**.
Comparativa RBAC contra MAC y DAC	El **RBAC** es más flexible que los modelos **DAC** (Control de Acceso Discrecional) y **MAC** (Control de Acceso Obligatorio).
Ejemplos de RBAC	• Venta de productos de entretenimiento *on line*. Los permisos de cada usuario se asignan por edad, por país del que proviene el usuario, etc. • Sector sanitario. Se establece una jerarquía de roles: el rol de médico tiene jerárquicamente mayor privilegio que el rol de enfermera y el de ésta, mayor privilegio que el de auxiliar de clínica.

Figura 1.4. Cuatro modelos de control de acceso basados en roles (RBAC) [12].

- 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.

1.7.3. Modelo de Control de Acceso Basado en Tareas y Roles (T-RBAC)

El T-RBAC, es un modelo mejorado para entornos empresariales, para la integración del modelo de Control de Acceso Basado en Roles (RBAC) y del modelo de Control de

Acceso Basado en Atributos (ABAC). La figura. 1.5 muestra en que consiste el T-RBAC. La mayor diferencia entre TRBAC y RBAC es que los permisos de acceso se asignan a las tareas en T-RBAC, en lugar de asignarse a los roles en el RBAC. En la actualidad, el usuario necesita los permisos de acceso para realizar tareas. Así la asignación de permisos de acceso a la tarea es razonable. En T-RBAC, las tareas se clasifican en tres categorías y son tratados de manera diferente. Las tareas de la clase W se utilizan para componer el flujo de trabajo. Crea las instancias de flujo de trabajo que son un conjunto de instancias de tareas. En la realidad, una empresa tiene muchos flujos de trabajo, pero suponemos un flujo de trabajo único para simplificar. Las tareas de clase S son para las de tipo de sesiones y las de clases P para las tareas privadas [8].

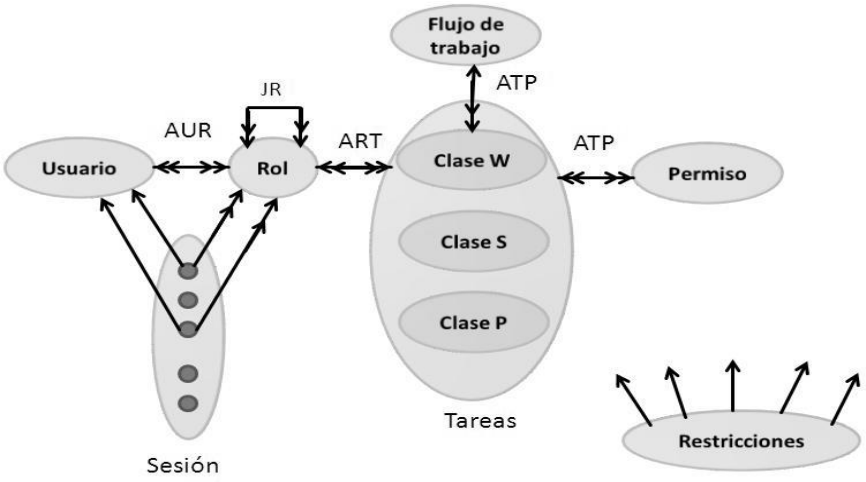


Figura 1.5. Modelo de Control de Acceso Basado en Tarea y Roles (T-RBAC) [8].

Este modelo es una extensión del modelo RBAC y en el estudio realizado no se le encontró un enfoque a entornos multidominio. Como está orientado a la asignación de permisos a las tareas, no es capaz de identificar ni a través de los roles, ni por las mismas tareas, a que dominio pertenece el usuario para poder diferenciar las restricciones que se le deben colocar al usuario sobre los recursos. Por esta causa no resuelve el problema de la investigación planteada.

1.7.4. Modelo de Control de Acceso Basado en la Localización (GEO-RBAC)

Este modelo es una extensión del RBAC, está guiado en el posicionamiento. La posición en este modelo puede ser real o lógica. La posición lógica puede ser adquirida a través de una tecnología de detección de ubicación. Mientras que la posición real, es un concepto semántico que es definido a un alto nivel de abstracción. Un rol espacial en Geo-RBAC es definido por el nombre y el rol extendido, que es un conjunto de posiciones lógicas. Los usuarios pueden pedir un rol solamente si su posición es lógicamente contenida dentro del rol extendido.

GEO-RBAC se centra principalmente en la asociación de roles con la extensión espacial y la activación y habilitación de roles en dependencia de la localización de los usuarios [9, 37]. La figura 1.6 muestra el núcleo del modelo.

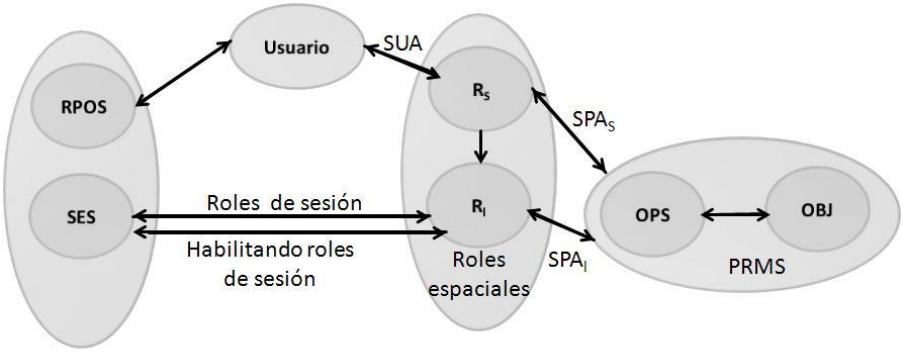


Figura 1.6. Modelo de Control de Acceso Basado en la Localización (GEO-RBAC) [9].

El estudio de este modelo arrojó que el modelo otorga la posibilidad de crear restricciones a los usuarios por el lugar o la localización, una restricción importante para la creación y el acceso a los planes de auditoría según el lugar donde se encuentre. Pero este modelo no ofrece una oportunidad de controlar el acceso de los usuarios que pertenezcan a diferentes organizaciones o que pertenezcan a diferentes dominios.

1.7.5. Modelo de Control de Acceso Basado en Roles Temporales (TRBAC)

El TRBAC es una extensión del modelo RBAC, con restricciones temporales sobre la activación/inhabilitación de roles. TRBAC apoya el rol de periódico de activar y desactivar y dependencias temporales entre tales acciones. Tales dependencias expresada por medio de roles disparadores (reglas activas que se ejecuten automáticamente cuando el acciones especificadas ocurrir) también se puede utilizar para restringir el conjunto de funciones que un usuario particular puede activar en un instante de tiempo dado. El disparo de un disparador puede causar a un rol a ser activado/desactivado, ya sea inmediatamente o después de una cantidad especificada de tiempo. Activar/Desactivar acciones pueden dar una prioridad que puede ayudar en la resolución de conflictos, tales como la activación simultánea y desactivación de una función. La acción con la prioridad más alta es ejecutada. [38]

Este modelo se basa en las funciones disparadores que existen en los gestores de bases para activar o desactivar los roles después de un periodo de tiempo determinado. Por tanto para otros sistemas que no están en un ambiente de gestión de bases de datos y no existan los disparadores, el modelo se queda sin efectividad. No quiere esto decir que un mecanismo de control de acceso con restricciones de caducidad por el tiempo, no se pueda implementar en otros tipos de sistemas. Para el problema de la investigación, podría aportar cierto grado de restricción, ya que es necesario restringir el acceso a los datos del plan y el control de las auditorías también por el tiempo. Esta posibilidad se debe a que los planes son elaborados anualmente. Una vez que el plan ha finalizado, el mismo no puede ser cambiado y por tanto es necesario delimitar el plan actual a los de años anteriores. Además no puede salir en la planificación del año en curso, la planificación de auditorías pasadas. Y para evitar estos problemas, es necesaria una política que brinde un mecanismo de acceso a la información que de mayor granularidad en este sentido. En este sentido, este modelo es efectivo, pero no brinda una solución completa, porque no aporta ningún tipo de restricción de permisos a los usuarios en entornos multidominio.

1.8. Soluciones informáticas para la administración de la planificación de auditorías.

1.8.1. Cura Auditoría

Es una solución informática de auditoría privativa que permite a las organizaciones estandarizar los documentos de trabajo, planificación de la auditoría, la ejecución y otros procesos de auditoría. Se integra con GRC Cura de la plataforma de software empresarial [39].

Proporciona la flexibilidad de soporte de extremo a extremo la funcionalidad de la gestión del ciclo de vida completo de auditoría, incluyendo: [39]

- Desarrollo de auditorías normalizadas y listas de verificación.
- Auditoría de la planificación y programación.
- Informes de auditoría y las recomendaciones.
- Los datos de campo de recogida.
- Examen de las recomendaciones de auditoría por los auditores.

1.8.2. RSA Archer para Gestión de Auditoría

Es un sistema informático que realiza el control del ciclo de vida completo de auditoría. Es una solución basada en tecnologías Web, con carácter privativo la cual proporciona una visión global de su programa de auditoría, incluyendo el seguimiento de la planificación, programación basada en el riesgo de prioridades, la dotación de personal, gestión de los procedimientos de auditoría y de los esfuerzos de remediación. A través de RSA Archer, la Dirección de Auditoría, puede transformar la documentación sobre papel en un programa de auditoría dinámica, mejorar el enfoque y la eficacia de las auditorías, llevar a cabo basado en el riesgo de alcance del universo de auditoría y se integran fácilmente con otras empresas de gobierno, riesgo y cumplimiento de los procesos [40].

1.8.3. APEX (Audit Planning and Execution)

Es una aplicación informática privativa la cual permite:

- La Gestión de Personal de Auditoría: Una vez definida la estructura de su organización, puede empezar a añadir los miembros del personal de auditoría a la estructura. Datos asociados, como el número de años de experiencia, área de especialización (Auditoría, Auditoría de Seguridad, etc.) e incluso una fotografía se puede añadir. Todos estos datos serán de utilidad en el desempeño de asignación de personal a las auditorías.
- APEX le permite trabajar con una estructura jerárquica para los auditados. El módulo de Auditoría del Sistema Auditado APEX es lo suficientemente flexible como para adaptarse a sus necesidades. Puede crear varios tipos de entidad como la empresa de auditoría del ministerio (en el caso de la auditoría gubernamental), departamento o proceso y vincularlos entre sí.
- Evaluación de riesgos: APEX proporciona una forma de gestionar los riesgos de las entidades auditadas. Usa los riesgos para crear auditorías de riesgo, o utilizar los programas de auditoría incorporado para realizar auditorías convencionales, o una combinación de ambas cosas [41].
- Generación del Plan: Una vez que el sistema contiene las entidades auditadas y el personal de auditoría, puede generar un plan de auditoría para un período determinado. Incluyen los auditados, auditores y crear equipos para realizar las auditorías. Un código de color de Gantt interfaz que ayuda en la planificación y le dice inmediatamente de la situación de las auditorías en curso [41].

1.8.4. MetricStream Audit Management

Es un módulo del sistema privativo Audit Management Software System. Soporta todo tipo de auditorías, incluidas las auditorías internas, auditorías operativas, auditorías de TI, auditorías a proveedores y auditorías de calidad. El sistema de gestión y auditoría dispone de extremo a extremo de la funcionalidad de la gestión del ciclo completo de vida de la auditoría. Incluye la planificación de la auditoría y la programación, desarrollo

de planes de auditoría estándar y listas de control, la recogida de datos de campo, elaboración de informes y recomendaciones de auditoría, la revisión de las recomendaciones de auditoría por las entidades fiscalizadas y de gestión y la aplicación de las recomendaciones de auditoría y la remediación [42].

Este módulo posibilita la creación de un programa de auditoría con un objetivo bien definido y el alcance ligada a los procesos de gestión de calidad, cumplimiento y riesgo. Los auditores pueden organizar una auditoría en una estructura lógica y la jerarquía con las plantillas de auditoría detallada y órdenes de trabajo. La evaluación, las listas de control y las tareas que deben realizarse para la ejecución de la auditoría, también se pueden definir [42].

Las soluciones MetricStream están 100% basadas en la Web para aumentar la colaboración entre los propietarios de procesos, auditores y demás partes interesadas dentro de un mismo entorno de aplicación lo que refuerza la importancia de construir un sistema basado en la web.

1.8.5. MKinsight

Es una aplicación privativa en la cual los usuarios pueden desarrollar cualquier número de planes de auditoría a través de cualquier horizonte de tiempo, ya sea de 12 meses, 3 años, o simplemente el próximo trimestre [43].

Todos los planes de auditoría se pueden utilizar para generar informes de rendimiento que comparan cualquier plan de auditoría elegido con lo que ha sucedido realmente durante ese período. La planificación de auditoría comienza con la creación de un universo de auditoría que puede tener un número ilimitado de niveles.

Junto con el registro de las evaluaciones de riesgos, otra información, como datos de contacto e información permanente de archivos también pueden ser almacenados, esto puede incluir todos los documentos electrónicos [43]. La licencia de este producto informático es privativa.

1.8.6. AMS9000

Esta solución está diseñado para emplear todos los aspectos de un programa de auditoría interna, desde la planificación de auditorías para el seguimiento de las acciones correctivas frente a las deficiencias encontradas [44].

Funciones de AMS9000, software de gestión de auditoría:

- Mantiene el calendario de la auditoría, la preparación lista y toda la información de auditoría.
- Permite introducir elementos propios de lista de verificación y/o texto directamente de procedimientos.
- Permite tomar acciones de contención, correctivas y preventivas en contra de las deficiencias detectadas en la auditoría.
- Seguimiento de todas las no conformidades, incluyendo las acciones y la verificación.
- Incluye informes sobre análisis de tendencias y resúmenes e informes de auditoría "recordatorio" para realizar un seguimiento de acciones correctivas y las implementaciones.
- Todos los usuarios obtienen la información relevante para sus necesidades por correo electrónico.

Los precios de este programa para una sola persona de 495 hasta 20 000 dólares estadounidense [44]. Es un producto informático con licencia privativa.

1.8.7. 5W2H o SE Audit

Es un software que realiza la gestión de todas las etapas del proceso de planificación de las actividades y planes de acción, desde el registro hasta la aprobación, ya que incorpora herramientas de organización, clasificación e investigación. Estas características dan al producto simplicidad, agilidad, confiabilidad y eficiencia [45].

SE Audit es un sistema 100% WEB, multiusuario y multidepartamental, que incorpora herramientas de: organización, clasificación y búsqueda. Estas características dan al producto simplicidad, agilidad, confiabilidad y eficiencia. Es un software con licencia privativa [45].

1.8.8. QAction

Es un software que lleva un control completo de todas las auditorías, quejas de clientes, reportes de productos o servicios no conformes y de las acciones correctivas y preventivas. QAction permite, además: [46]

- Planificar las auditorías al sistema de calidad.
- Generar de manera automática hojas de verificación.
- Planificar acciones correctivas y preventivas para cada problema.
- Incorporar planes de auditoría escritos con cualquier procesador de textos.
- Verificar y registrar la implantación y efectividad de las acciones correctivas efectuadas.
- Controlar las quejas de clientes.

Este software cumple con los requisitos de las normas ISO 9000 y QS 9000 y tiene como desventaja ser un software privativo. Para su adquisición es necesaria la compra de varias licencias como la principal, que tiene un costo de $900 (USD), la empresarial, cuyo monto asciende a $3 470 (USD) y la corporativa asciende a $9000 (USD) [46].

1.8.9. Valoración de las soluciones informáticas internacionales.

Los sistemas informáticos descritos anteriormente fueron seleccionados para el estudio porque tienen incorporados el ciclo completo del proceso de auditoría. Los mismos no están enfocados a manejar la información de múltiples entidades a excepción de APEX, pero su método de entrada de las estructuras no está sujeto a las condiciones que obliga la ONE a cumplir. La ONE es la única entidad capacitada para registrar las empresas cubanas, por tanto solo se pueden incorporar lo que la oficina publique en una base de datos con formado DBF.

Las aplicaciones estudiadas tienen funcionalidades que necesitan ser utilizada en la CGRC para la planificación de las acciones de control y el seguimiento de los controles de cumplimiento como puede ser el módulo MetricStream Audit Management del sistema Management Software System. Pero existen particularidades del sistema nacional de auditoría cubano que constituirían escollos para las aplicaciones mencionadas: una de ellas es el tratamiento de la doble moneda y la generación del plan exactamente según el Modelo 001 especificado en la Resolución 091/08 de la CGRC (Anexo 1, Tabla T2). Otra particularidad es el nivel de autorización a la información del plan anual; además de ser jerárquica, debe estar dividida por dominios; los jefes de grupos, supervisores y auditores que atienden una provincia y/o la Unidad Central de Auditoría Interna (UCAI), no tienen derecho a ver lo planificado para otra provincia o para otra UCAI

Otra limitante identificada en los sistemas informáticos estudiados es que la planificación es basada en el análisis de riesgos y objetivos, mientras que en el Plan Nacional de Auditoría, se construye anualmente por otros elementos especificados en la resolución 091/08 como pueden ser: los intereses del gobierno y del partido, por quejas y denuncias que provienen de la población y otros. Los sistemas estudiados son de licencia privativa y con precios altos.

Las particularidades del proceso de planificación y control de auditorías en Cuba no son cumplidas por las soluciones informáticas internacionales e impiden la aplicación de las mismas para planificar las auditorías en el entorno cubano.

1.9. Sistemas nacionales de planificación

1.9.1. Versat Sarasola.

Es un sistema integrado de gestión económica diseñado para ser utilizado de acuerdo a las características de cada entidad, pues es configurable por cada una de ellas en el momento de su instalación. Tiene como objetivo fundamental permitirle a los directivos analizar, controlar y evaluar los resultados de su negocio o actividad en tiempo real, al contar con un instrumento seguro, rápido, eficaz y de fácil manejo para la planificación,

control y el análisis de la gestión económica y financiera. Está orientado a todas las entidades del sector empresarial tanto productivas, presupuestadas, de servicios y comercializadoras, que necesiten registrar su gestión económica de forma eficiente. Es una herramienta indispensable para la máxima dirección y para las unidades intermedias de cualquier empresa u organización económica. Este sistema cuenta con un módulo para la planificación (está relacionada con los principios Contables – Financieros en que descansa el sistema, por tanto el procesamiento de la misma siempre tendrá un carácter totalmente Contable) [47].

1.9.2. Presupuesto Maestro.

El Presupuesto Maestro es una aplicación que implementa una técnica internacionalmente utilizada, que le permite a las empresas conjugar integralmente todos los objetivos de trabajo de las distintas subdivisiones estructurales de la misma y a la vez cuantificarlos para mostrar los resultados esperados en el período previsto, todo esto sobre una concepción financiera de las operaciones a realizar. Este programa de computador, puede ser utilizado por cualquier entidad de un organismo, ya que la captura, cálculo y presentación de los diferentes presupuestos, está diseñada de forma general y no específicamente para un organismo [47].

1.9.3. Subsistema de Planificación Presupuestada y Empresarial del sistema integral de gestión Cedrux.

El sistema informático tiene divido el proceso de planificación según la categoría al cual pertenezca la empresa:

- En las entidades empresariales híbridas, productoras o de servicio: se comienza por la preparación del **Presupuesto de ventas y cobros por meses** con el objetivo de planificar las ventas previstas de la entidad. Una vez que se tenga este documento detallado y aprobado por el Director Comercial lo próximo a realizar es el **Plan de producción**.

- Seguido a esto se determina el **Costo de la producción planificada** y se prepara el **Presupuesto de compras y pagos.**
- Posteriormente se elabora el **Presupuesto de gastos de operación, de distribución y ventas, generales y de administración** y una vez obtenidos los documentos anteriores se podrá obtener los estados finales que son un resumen del presupuesto empresarial y están compuesto por el **Presupuesto de efectivo por meses**, el **Estado de resultados presupuestado del año** y el **Balance general presupuestado del año** [47].

Paralelamente a la elaboración de los documentos del presupuesto, se elabora el plan llenando todos los documentos que lo componen y remitiéndolos al grupo empresarial que es el encargado de analizar y evaluar el plan de la empresa. Aquí se obtiene el primer nivel de aprobación del plan, una vez discutido y analizado en este nivel será enviado al OACE (Órgano de la Administración Central del Estado) que lo dirige, nivel donde se aprobará, teniendo en cuenta siempre que el OACE emite al MEP (Ministerio de Economía y Precios) su PIGD (Plan de Ingresos y Gastos en Divisas) y el de algunas empresas seleccionadas. El MEP es el encargado de aprobar los gastos en divisas, que recibe de modelos seleccionados del plan de determinadas empresas. De esta forma se realiza la etapa de anteproyecto en las entidades empresariales [47].

El subsistema informático está dedicado para la realización del plan financiero o contables de la empresa y por tanto recoge solo aquello procesos que están relacionados con la preparación del presupuesto de gastos de operación, de distribución y ventas, generales y de administración y no está dentro de su contenido o misión el proceso de planificación de auditorías.

Los sistemas **Presupuesto Maestro**, **Versat Sarasola** y el **Subsistema de Planificación Presupuestada y Empresarial** del sistema integral de gestión Cedrux, no fueron desarrollados con el objetivo de planificar auditorías. Su misión principal radica en la planificación de los procesos contables o financieros de una empresa. Por lo que no se pueden emplear para el proceso de planificación y control de auditorías.

1.10. Conclusiones parciales

El estudio del estado del arte permitió plantear las bases conceptuales de la investigación para el entendimiento del marco teórico. Se arribaron a las siguientes conclusiones:

- La planificación de las auditorías y su seguimiento es clasificado como normativo por la fuerte relación a las normas gubernamentales por el cual está regido, característico del sistema socialista existente en Cuba. Por lo que otro tipo de planificación como los que proponen los estándares internaciones para el control interno y las auditorías no son aplicables.
- La utilización de un modelo como guía para normar el proceso de planificación, permite que se logre generalizar la solución para todas aquellas entidades que necesitan planificar auditorías. Por eso es necesario desarrollar una aplicación que cumpla con las exigencias de las normas o la Resolución 091/08 e incorpore mecanismos de control de la autorización para la planificación de las auditorías en Cuba.
- Los estándares y modelos para el control interno y las auditorías estudiados están orientados a la confección de la planificación para realizar las auditorías, pero no especifican los mecanismos para lograr la compartimentación de la información en entornos multidominio. Además, parten de la gestión de los riesgos como punto de partida de la planificación, a diferencia de la resolución cubana, en la cual parte de otros elementos para su elaboración mencionados en el epígrafe 1.2. Por estas razones no es posible utilizar ninguno de los modelos existentes en la literatura para la solución informática.
- Los sistemas informáticos descritos anteriormente no están enfocados a manejar la información de múltiples dominios a excepción de APEX, pero él método de entrada de las estructuras no está acorde a las condiciones de Cuba. La ONE es la única entidad capacitada para registrar las empresas cubanas, por tanto solo se pueden incorporar lo que la oficina publique en una base de datos con formado DBF, funcionalidad que no está soportada en

ninguno de los sistemas informáticos estudiados. Los sistemas informáticos estudiados realizan la planificación basada en el análisis de riesgos, mientras que en el Plan Nacional de Auditoría se construye anualmente por otros elementos especificados en la Resolución 091/08. Entre los que se encuentran: los intereses del gobierno y del partido, por quejas y denuncias que provienen de la población entre otros. Otros problemas encontrados con las aplicaciones estudiadas fueron las licencias, las cuales son privativas y los precios altos. A partir del estudio realizado de las herramientas de planificación, se identificó que desarrollar sistemas basados en la Web, aumenta la colaboración entre los propietarios de los procesos, los auditores y demás partes interesadas, dentro de un mismo entorno de aplicación.

- Los modelos de control de autorización estudiados no son capaces de cubrir los requisitos impuestos por el control de la autorización en entornos los multidominios. Es necesario realizar una extensión al modelo RBAC para proponer una solución que brinde un mecanismo de control de acceso en los entornos multidominio.

CAPÍTULO II: PROPUESTA DE MODELO PARA LA PLANIFICACIÓN Y CONTROL DE AUDITORÍAS EN ENTORNOS CUBANOS MULTIDOMINIOS.

En este capítulo se describe el modelo para la planificación y control de auditorías en entornos cubanos multidominios. El mismo extiende el modelo RBAC incorporándole los elementos necesarios para solucionar el problema planteado. El modelo propuesto es aplicado en el desarrollo de un sistema informático que debe ser capaz de cubrir los requisitos establecidos el proceso de planificación y control de las auditorías en entornos cubanos multidominios. Como resultado de la aplicación, se exponen los artefactos más significativos generados en el proceso de desarrollo.

2.1. Modelo para la Planificación y Control de Auditorías en Entornos Cubanos Multidominios (PCAECM).

El modelo PCAECM es una extensión del modelo RBAC dirigido al proceso de planificación y control de auditorías en entornos cubanos multidominios. 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 2.1 ilustra los conceptos y relaciones que conforman el modelo PACEMC.

2.1.1. Elementos del modelo PCAECM

Los conceptos que componen el modelo son los siguientes:

- **Usuario:** Pueden tratarse de personas o sistemas a los que se le asignan privilegios sobre los diferentes recursos de una o varias organizaciones.

- **Rol:** Son funciones de trabajo en el contexto de una organización con una semántica asociada a la autoridad y la responsabilidad conferida a una persona. Ejemplo: un contador, administrador, director, evaluador, entre otros.

- **Permiso:** Es un concepto que agrupa las operaciones que se pueden realizar sobre uno o varios objetos.

- **Operación:** Son acciones que se realizan sobre uno o varios objetos, pueden iniciarse debido a la petición de un usuario o por configuraciones internas del SI (Sistema Informático).

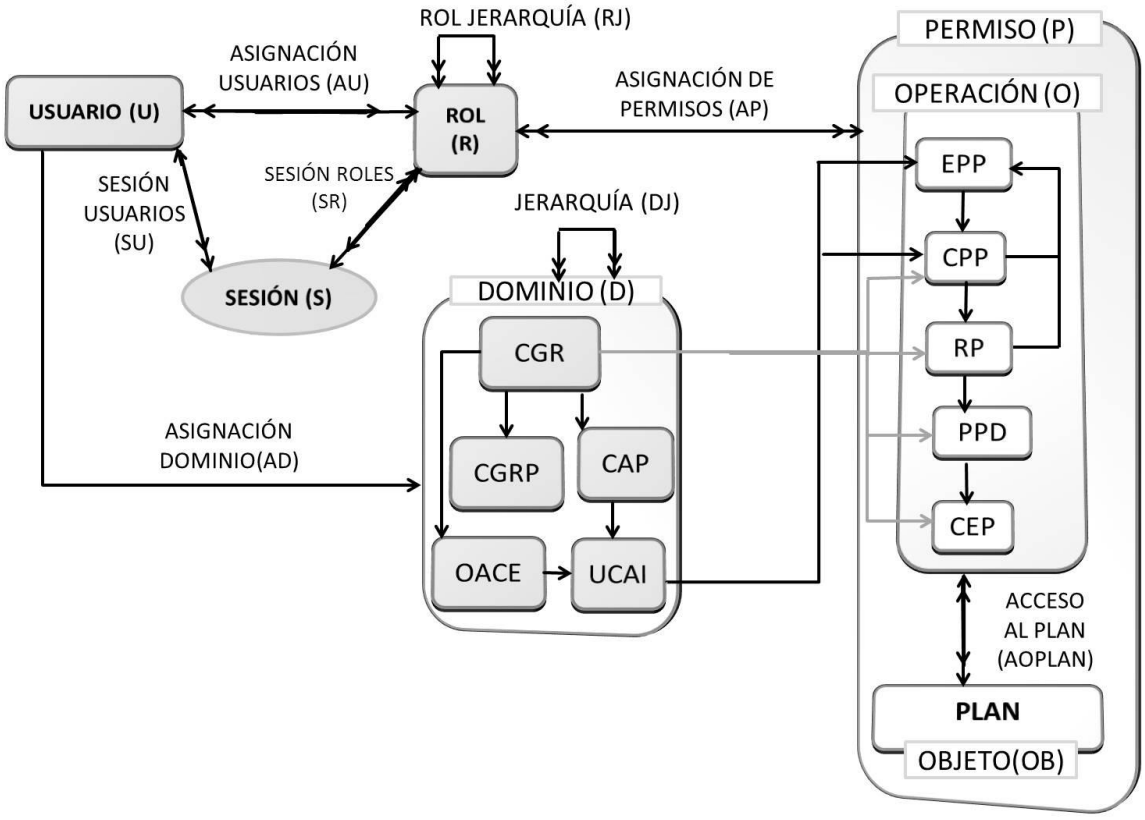


Figura 2.1: Modelo PCAECM.

- **EPP:** Son las iniciales de la operación llamada Elaboración de la Propuesta de Plan Anual. Primer paso en la planificación de auditoría y control de auditorías en Cuba.

- **CPP:** Son las iniciales de la operación llamada Conciliación de la Propuesta de Plan Anual. Segundo paso en la planificación de auditoría y control de auditorías en Cuba.

- **RP:** Son las iniciales de la operación llamada Revisión del Plan Anual. Tercer paso en la planificación de auditoría y control de auditorías en Cuba.

- **PPD:** Son las iniciales de la operación llamada Presentar Propuesta al Directorio. Cuarto paso en la planificación de auditoría y control de auditorías en Cuba.

- **CEP:** Son las iniciales de la operación llamada Controlar y Ejecutar el Plan Anual. Último paso en la planificación de auditoría y control de auditorías en Cuba.

- **Plan:** Constituye el objeto con el cual interactúan las operaciones identificadas en el modelo para la planificación y control de las auditorías.

- **Dominio:** Representa las agrupaciones de entidades que tienen en común algún criterio. Ejemplo: las entidades pueden agruparse por una región o por ministerio, sociedades anónimas, entre otros.

- **CGR:** Es un subdominio el cual se identifica como la Contraloría General de la República el cual tiene subordinada a otras entidades o subdominios como los CAP y CAM.

- **CGRP:** Comprende un subdominio el cual se subordina a la CGR. Se identifica como una delegación de la Contraloría General de la República a nivel provincial.

- **CAP:** Simboliza un subdominio el cual el cual se identifica como Consejo de Administración Provincial y se subordina a la CGR.

- **OACE:** Constituye un subdominio que se subordina a la CGR el cual el cual se identifica como Organismo de Administración Central de Estado.

- **UCAI:** Forma un subdominio perteneciente de la OACE al cual pertenece.

2.1.2. 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. 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.

En la introducción del concepto Dominio, se incluyen tres procesos que deben formar parte de cualquier sistema que necesite incorporar el modelo PCAECM. En los epígrafes 2.1.3.1, 2.1.3.2 y 2.1.3.3 se describen los procesos para la gestión del dominio y la asignación de los permisos a los usuarios sobre un dominio.

Las restricciones por localización, mecanismo aportado por el modelo GEO-RBAC, está de una manera indirecta presente en el concepto dominio. La restricción por localización funciona cuando al usuario se le otorgan permisos sobre un dominio que

está delimitado por una provincia; es decir, que el conjunto de entidades u organizaciones por el cual está conformado cierto dominio, pertenecen todos a una misma provincia en específico. Un ejemplo de ello es cuando se le asigna un CAP. De esta manera, al usuario que se le asigne este tipo de dominio, solo tiene acceso a los datos del plan y de los controles de la auditoría que pertenezca al CAP de una provincia.

2.1.2.1. Formalización del modelo

Las políticas RBAC (PL) consisten en: [48, 49]

- R es un conjunto de roles.
- U es un conjunto de usuarios.
- P es un conjunto de permisos.
- S es un conjunto de sesiones.
- 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 son organizadas 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 un rol puede tener muchos usuarios. Del mismo modo, un rol puede tener muchos permisos y al mismo tiempo los permisos pueden ser asignar a muchos roles.[49]

Definiciones adicionales:

- D es un conjunto de dominios.
- Plan es el objeto contenedor de la información del plan de auditoría.
- O 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.
- US ⊆ U×S es una relación de asignación de sesiones a roles de muchos a muchos.
- DJ ⊆ D×D. La jerarquía de dominio son organizadas 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 pertenece al dominio CGR.
- CAP ∈ CGR. El dominio CAP pertenece al dominio CGR.

- OACE ∈ CGR. El dominio OACE pertenece al dominio CGR.
- UCAI ∈ CAP. El dominio UCAI pertenece al dominio CAP.
- OACE ∈ UCAI. El dominio UCAI pertenece al 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 distribuido 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.

2.1.3. Descripción de los procesos fundamentales para preservar la confidencialidad de la información en el PCAECM

Para incorporar el modelo PCAECM utilizando el concepto dominio en la planificación de auditoría y control en entornos cubanos multidominios, se identificaron dos procesos necesarios. En los epígrafes 2.1.3.1 y 2.1.3.2 están descritos estos procesos.

2.1.3.1. Proceso Gestionar Dominio

Un dominio es un conjunto de estructuras que pueden ser ministerios, asociaciones anónimas o cualquier otro tipo de organización. El acceso de los usuarios a la información del plan se restringe a través de los dominios que se le asigne para desempeñar sus funciones. Para ello se debe permitir crear los dominios de estructuras que serán asignados a los usuarios atendiendo al rol que desempeñan dentro de cada estructura. Para la creación de las estructuras por dominio, se debe importar la base de datos con formado DBF, publicada por la ONE (Oficina Nacional de Estadística), donde se encuentran todas las estructuras registradas del país. Al importar los datos, a través del campo de identificación REUP, se identifican los niveles de subordinación unas de otras, para formar una jerarquía de estructuras. El usuario clasifica las estructuras según su nivel de jerárquico en: UCAI, UAI, CAP (Consejo de

Administración Pública) o CAM (Consejo de Administración Municipal), logrando de esta forma para permitir posteriormente la creación de dominios por niveles. La Figura 2.2 muestra el flujo de actividades contenidas en el proceso.

Con el proceso Gestionar Dominio se logra introducir las estructuras del país de forma oficial, ya que la ONE es la entidad autorizada para el registro o actualización de las mismas en el país. Se logra minimizar los posibles errores humanos en la entrada de las estructuras al sistema.

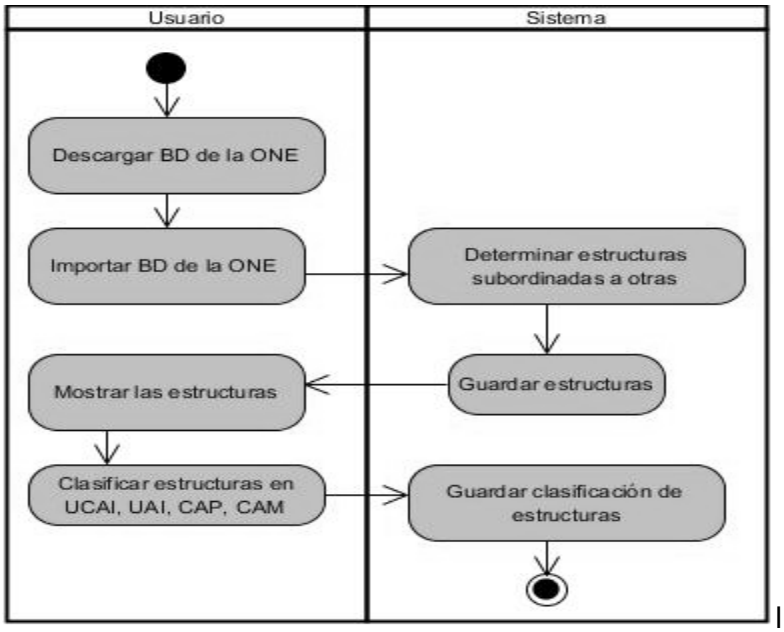


Figura 2.2: Proceso Gestionar Dominio

2.1.3.2. Proceso Configurar Permisos

El proceso Configurar Permisos permite asignar privilegios a usuarios existentes en el sistema informático para que puedan acceder a la información del plan y el control de las auditorías, según el dominio al cual pertenezcan. La Figura 2.3 muestra como se efectúa este proceso. El acceso a la información se filtra o se controla según el nivel de acceso del usuario; de esta forma, se logra la compartimentación de la información en entornos multidominio.

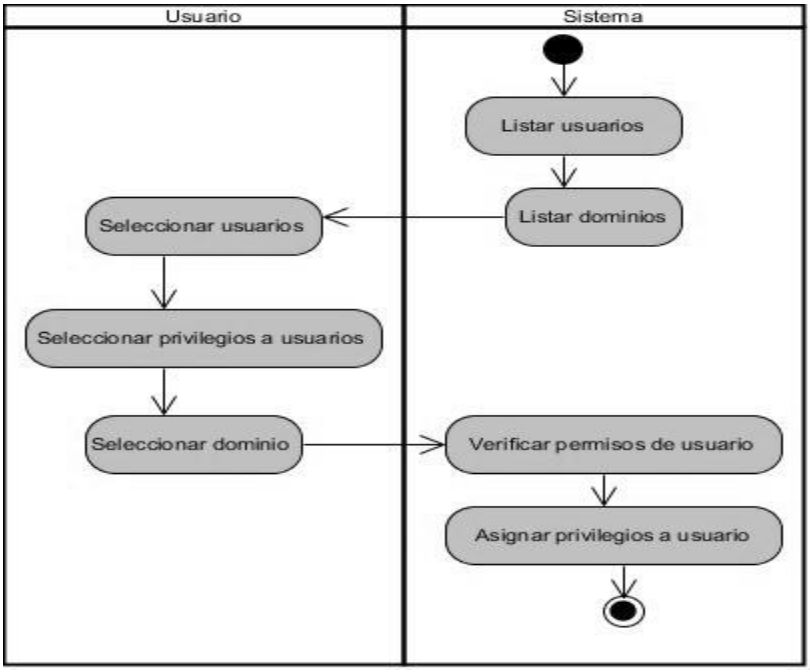


Figura 2.3: Proceso Configurar Permisos.

El resto de los procesos se pueden encontrar en el expediente de proyecto ICON del centro Telemática perteneciente a la facultad 2 de la UCI, en el documento: Modelación del negocio.

2.2. Descripción del sistema.

A partir de las necesidades existentes en la CGRC de informatizar el proceso de planificación y control de las auditorías, el modelo PACEMC fue aplicado en el desarrollo de un sistema informático que permite cubrir las necesidades del cliente y preservar la confidencialidad de la información del plan anual en entornos cubanos multidominios.

En los subepígrafes siguientes se describe el sistema informático que incorpora el modelo propuesto.

2.2.1. Requisitos funcionales del sistema

- **Elaborar propuestas de acciones de control** con posibilidad de elegir entre todos los tipos de acciones de control y los tipos de auditorías existentes. Se puede elegir el trimestre en el que se realiza, el nombre completo de la UCAI sobre la cual se realiza la acción de control, el nombre completo y el tipo de estructura sobre la que se realiza la acción de control, por ejemplo: Ministerio, Grupo Empresarial, Sucursal, Unión y otros tipos. Además, se recoge el código del Registro Estatal de Empresas y Unidades Presupuestadas (REEUP) y las particularidades de la estructura auditada. (Anexo 4, figura A7).

- **Elaborar los controles de cumplimiento de las acciones planificadas**. En esta funcionalidad se gestiona la cantidad de presuntos hechos delictivos (PHD), de corrupción (PHC) y el monto de las afectaciones económicas tanto en moneda libremente convertible (CUC) como nacional (CUP). Además el nombre y tipo de estructura que ejecuta la acción de control, el rango de fecha planificada y la real en la cual se ejecutó el control. La funcionalidad puede realizar modificaciones para rectificar datos de los planes con errores como podría ser el REEUP o las particularidades. (Anexo 4, figura A8).

- **Revisar según el nivel de jerarquía, las acciones de control** que le corresponda a los auditores, supervisores, jefes de grupo, directores y contralora principal. Entre los parámetros a revisar están: el tipo de acción de control planificada, el tipo de auditoría, en que trimestre está planificado su realización, el nombre completo de la UCAI sobre la que se realiza la acción de control y otras especificaciones del plan.

- **Revisar según el nivel de jerarquía, el cumplimiento de las acciones de control** que le corresponda a los auditores, supervisores, jefes de grupo, directores y contralora principal. Los datos más importantes a revisar para el cumplimiento del plan son: la cantidad de PHD y la cantidad de PHC, la

afectación económica en CUP, CUC y el tipo de estructura que ejecuta la acción como las sociedades anónimas, contralorías provinciales, UCAI y otros tipos.

- **Exportar e importar propuesta del plan:** Para establecer un formato entre todos los organismos del país y otros tipos de estructuras estatales que brindan una propuesta de planificación anualmente a la CGRC.
- **Emitir aprobación o rechazo de propuesta del plan anual** de las acciones de control.
- **Generar el Plan Anual**: Emite el Modelo 01 según la Resolución 091/08 de la CGRC para la creación y seguimiento del Plan Anual de Auditoría.
- **Actualizar las entidades estatales** existentes en el país por la base de datos pública de la Oficina Nacional de Estadísticas (ONE).
- **Gestionar Unidades Estatales Básicas (UEB).** Se registran aquellas unidades que no se encuentran en la base de datos de la ONE, pero si están incorporadas como partes de las empresas estatales cubanas y de este modo se logran incluir en el plan anual. Se crean con un código REEUP, otorgándoles una identificación que permite identificar a la empresa que pertenece.
- **Crear entidades auditoras.** Se le otorgan a las entidades seleccionadas el rol de UCAI, de Unidad de Auditoría Interna (UAI), CAP o CAM.
- **Configurar permisos.** Se le otorgan a los usuarios del sistema, permisos de adicionar, modificar, consultar e imprimir el plan de acción perteneciente de las entidades que están en su dominio de alcance de información.

2.2.2. Requisitos no funcionales del sistema

Apariencia o interfaz externa.

- Por el uso que tendrá el software, la interfaz debe ser agradable, que combinen correctamente los colores, tipo de letra y tamaño y que los iconos estén en correspondencia con lo que representan.
- La interfaz debe ser intuitiva al usuario. Deben utilizarse plantillas con un mismo estilo.

Usabilidad

- Debe ser de fácil y rápido manejo para todos los usuarios.
- Podrá ser usado por cualquier persona que posea conocimientos básicos sobre computación o que hayan interactuado anteriormente sobre un ambiente web.

Portabilidad, escalabilidad y reusabilidad.

- El sistema debe ser multiplataforma.
- Debido a los problemas económicos del país, las empresas cubanas toman continuas decisiones que cambian las condiciones en que se desarrollan los procesos, por lo que el sistema debe ser capaz de adaptarse en lo posible ante estas situaciones.

Requisitos	Cliente	Servidor
Hardware	Se requiere tarjeta de red. Se requiere al menos 256 MB de memoria RAM. Se requiere al menos 100MB de disco duro.	Se requiere tarjeta de red. Se requiere que tenga la menos 512MB de RAM. Se requiere al menos 40GB de disco duro.
Software	-Mozilla Firefox 3.X o superior.	Apache 2.x PostgreSQL 8.4 o superior

Tabla 2.1. Requisitos de software y hardware.

El resto de los requisitos no funcionales del sistema se pueden encontrar en el expediente de proyecto ICON del centro Telemática perteneciente a la facultad 2 de la UCI, en el documento: Especificación de requisitos de software.

2.2.3. Diagramas de componentes

Un diagrama de componentes es un diagrama UML que muestra los componentes que integran el sistema y las dependencias entre ellos. [50] El diagrama reflejado en la figura 2.4 contiene una vista general de la solución informática SIGAC. El componente *Planificacion* contiene todos los componentes necesarios para asegurar la planificación y control de las auditorías: *PropuestaPlan*, *PlanAnual*, *ControlesCumplimiento.* Para gestionar la compartimentación de la información en los entornos cubanos multidominios se desarrollaron los componentes: *GestionarEntidades* y *GestionarPermisos*.

El componente *Planificacion,* a través de la interfaz *IntegracionService*, se comunica con el componente *Integracion* para lograr la interacción con el gestor documental Alfresco. Además se puede evidenciar la integración con el sistema Acaxia a través de la interfaz *AuntenticationService*, para asegurar la autenticación y autorización por roles a los usuarios de las funcionalidades del componente *Planificacion*. En la figura 2.4 se muestra el diagrama general de componentes del SIGAC. Los diagramas fueron elaborados con la herramienta Visual Paradigm, el cual soporta UML.

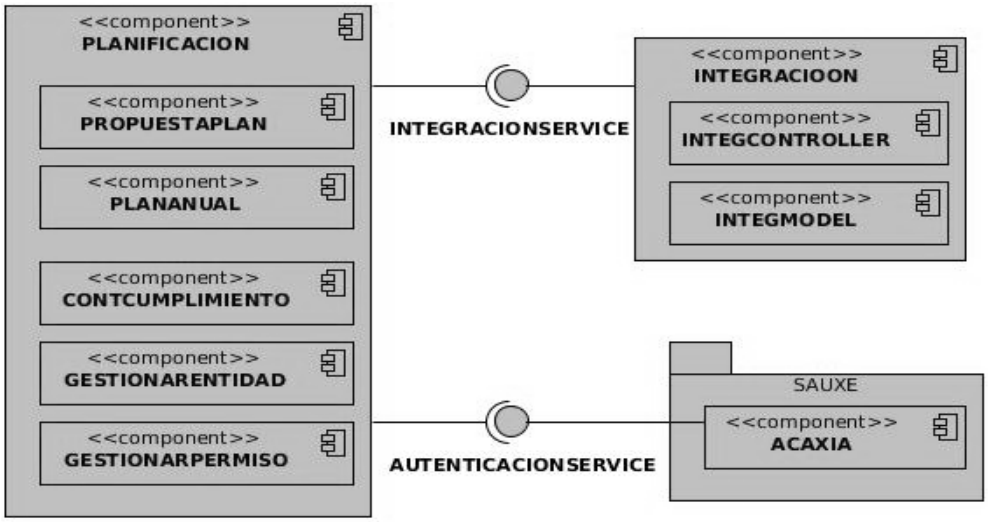


Figura 2.4: Diagrama general de componentes del SIGAC.

Planificacion e *Integracion* son componentes dependientes del Cedrux, significa que la arquitectura está determina por el sistema de gestión empresarial. Los componentes están basados en el marco de trabajo SAUXE e implementa el MVC como se ilustra la figura 1.2. Se utiliza el *framework* ExtJS para las interfaces de usuario, el Doctrine para el Mapeo de Objeto Relacional y el Zend Framework para la capa de negocio. En el epígrafe 1.5 se pueden encontrar más detalle acerca del marco de trabajo.

El diagrama de componente de los procesos Gestionar Dominio y Configurar Permisos refleja como los componentes de ambos procesos se comunican entre sí a través de la interfaz *EntidadService*. Ver figura 2.5.

La utilización del marco de trabajo SAUXE, proporciona la posibilidad de acoplar la solución informática SIGAC, como un subsistema del Cedrux. Los restantes diagramas de componentes del sistema se pueden encontrar en el expediente de proyecto ICON del centro Telemática perteneciente a la facultad 2 de la UCI, en el documento: Modelo del diseño.

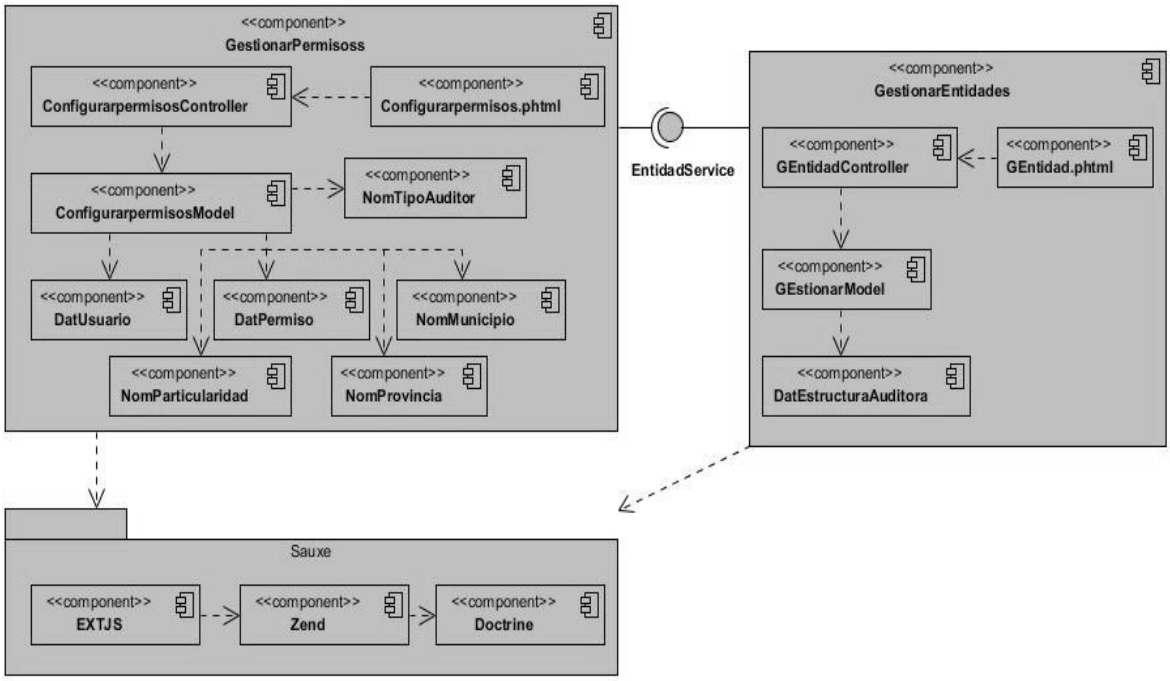


Figura 2.5: Diagrama de componentes de los procesos Gestionar Dominio y Configurar Permiso.

2.2.4. Modelo de datos

Para lograr la compartimentación de la información en los entornos cubanos multidominios se creó una base de datos que contiene los elementos de diseño necesarios para garantizar la clasificación de la información, con el objetivo de almacenar los datos del plan y control de auditoría. En el modelo se encuentran las tablas *dat_plan, dat_cumplimiento* y *dat_accion_control*, que contienen la mayor parte de la información de los planes y los controles. Ellas se relacionan con la tabla *dat_estructura_auditora,* donde se almacenan las entidades auditoras y las estructuras que representan a un dominio. Para representar a la entidad rectora de un dominio, se estableció una relación recursiva con ella misma y se identifica a través del campo *id_estructura_superior*. La relación de las tablas *dat_permiso* con *dat_estructura_auditora,* registran los permisos sobre las estructuras auditoras. En la figura 2.6 se refleja el modelo de la base de datos de la solución. (Anexo 4, figura A6)

2.3. Conclusiones parciales

Con la incorporación del concepto Dominio y su relación con el Usuario se logra introducir el mecanismo para el control de acceso a los recursos por organización que no está presente en el modelo RBAC. Además con la identificación de los dominios más representativos del país que participan en la planificación y control de auditorías en el modelo y la asignación con la operación que le corresponde, se delimitan las operaciones que pueden ostentar cada dominio definido, para el funcionamiento adecuado del proceso de planificación y control en los entornos cubanos multidominios.

La descripción de las principales funcionalidades y requisitos de la aplicación, reflejan los elementos y principios de la planificación que deben ser cumplidos en cualquier proceso de este tipo; así como de los procesos que intervienen como mecanismos de control de acceso a la información. De este modo quedan recogidas las características que debe cumplir una aplicación informática para poder aplicar el modelo PCAECM.

Por medio de los diagramas de componentes se establecieron los elementos encargados y la relación entre estos para implementar los procesos de planificación y control de las auditorías y para gestionar el dominio y la configuración de los permisos.

La integración con el marco de trabajo SAUXE, permite acoplar la solución informática SIGAC, como si fuera un subsistema del sistema de gestión integral Cedrux.

El modelo de datos manifiesta cómo se etiquetó la información para que existan los informes y planes de múltiples entidades en una misma base de datos sin peligro para la confidencialidad de la información.

CAPÍTULO III: VALIDACIÓN DEL MODELO.

En el presente capítulo se describen las pruebas que se aplicaron a la solución informática para comprobar la aplicación del modelo propuesto, a través de la comprobación del cumplimiento de los requisitos funcionales establecidos. Además como paso ulterior, la validación del PCAECM a través de la aplicación informática, para comprobar si con esta propuesta de modelo se logra gestionar la planificación y control de las auditorías en entornos cubanos multidominios preservando la confidencialidad de la información.

3.1. Proceso de validación del modelo

El proceso de validación demuestra que el modelo PCAECM contribuye en mayor medida al fortalecimiento de la confidencialidad de los datos en los SI en entornos cubanos multidominios que los modelos de autorización aceptados según la bibliografía consultada.

La figura 3.1 muestra un esquema general del proceso de validación de la propuesta.

La aplicación del modelo PCAECM en un sistema informático se describió en el capítulo 2 de la presente investigación. Por lo que en los siguientes epígrafes se describen los pasos del 2 al 6 del proceso de validación.

La aplicación del modelo constituye una de las bases fundamentales para el proceso de validación ya que a partir de este primer paso, va a depender el resto de los pasos de dicho proceso.

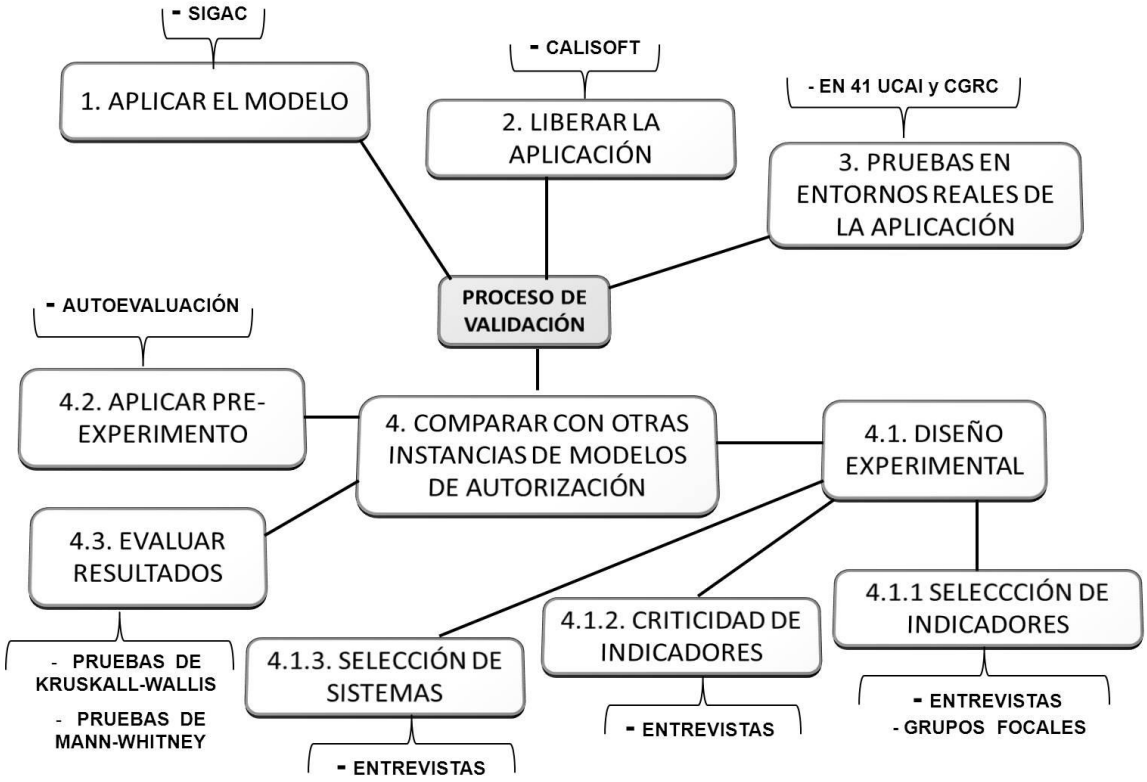


Figura 3.1: Esquema general del proceso de validación.

3.2. Liberación del sistema de planificación y control de auditorías

La validación del software se consigue mediante una serie de pruebas de caja negra que demuestran la conformidad con los requisitos. Un plan de prueba traza la clase de pruebas que se han de llevar a cabo y un procedimiento de prueba define los casos de prueba específicos en un intento por descubrir errores de acuerdo con los requisitos. Tanto el plan como el procedimiento estarán diseñados para asegurar que se satisfacen todos los requisitos funcionales, que se alcanzan todos los requisitos de rendimiento, que la documentación es correcta e inteligible y que se alcanzan otros requisitos (por ejemplo, portabilidad, compatibilidad, recuperación de errores y facilidad de mantenimiento) [51].

Las llamadas pruebas de caja negra se basan en la especificación del programa o componente a ser probado para elaborar los casos de prueba. El componente es visto como una caja negra cuyo comportamiento es desconocido y sólo puede ser evaluado estudiando sus entradas y las salidas obtenidas. También son conocidas como pruebas de comportamiento o pruebas inducidas por los datos.

La realización de los casos de pruebas es un tipo de prueba de caja negra y tiene como objetivo demostrar al cliente la reacción que corresponderá por parte del sistema luego de realizar alguna acción en el mismo [51].

Para asegurar que la planificación y control de auditorías se realizan correctamente, los elementos y principios de la planificación descritos en el epígrafe 1.3 y 1.4 deben estar cumplidos, así como los requisitos funcionales de la aplicación, identificados con el cliente.

Los elementos: o*bjetivos* (¿Qué?), *problema que se resuelve con un objetivo* (¿Para qué?), *los recursos o medios para los ejecutores* (¿Con qué?) *y en qué cantidad, la meta* (¿Cuánto?) no son parte de los elementos de la planificación normativa que se ejecuta en la CGRC y los 41 UCAI de las OACE, aunque el *para qué* está implícito en el plan anual de auditoría. La planificación normativa no es guiada por los objetivos como se explica en el epígrafe 1.2, sino por las normas y parámetros previamente establecidos por el estado. Además la resolución la cual normaliza el proceso de planificación de las auditorías no establece la meta ni la cantidad que se deben realizar, sino que ocurren según la capacidad de la CGRC y las 41 UCAI de las OACE.

Los elementos de la planificación que se pueden cumplir son: c*ronología, secuencia y tiempo* (¿cuándo o en cuanto tiempo?), *responsables y ejecutores* (¿quiénes?) y *en qué lugar* (¿dónde?). Estos elementos están expresados como requisitos del sistema SIGAC.

El principio: la *racionalidad,* no puede ser comprobado porque se relaciona con los objetivos. Pero los principios: *previsión, utilidad, flexibilidad y continuidad* están expresados como requisitos funcionales de la aplicación informática (SIGAC) construida para aplicar el modelo y por tanto son revisados en los casos de uso de prueba creados para constatar el cumplimiento de los requerimientos.

Los elementos y principios están presentes en los requisitos funcionales: **Elaborar propuestas de acciones de control, elaborar los controles de cumplimiento de las acciones planificadas, revisar según el nivel de jerarquía, las acciones de control, revisar según el nivel de jerarquía y el cumplimiento de las acciones de control.** Al realizar las pruebas de caja negra para comprobar el cumplimiento de los requisitos funcionales, se están probando por tanto, el cumplimiento de los elementos y principios de la planificación.

Estas funcionalidades fueron sometidas a pruebas de verificación de su cumplimiento para la liberación del producto informático, por parte del Centro CALISOFT, centro evaluador de calidad de Cuba. Se diseñaron los Casos de Pruebas Funcionales basados en Casos de Uso para verificar que se cumplan los requisitos funcionales del sistema informático. (Anexo 4, figura A5).

En la figura 3.2 se ilustra el análisis del proceso de pruebas ejecutado por el equipo de CALISOFT para verificar la calidad y conformidad de los requisitos implementados. Como se puede apreciar en el inicio se identificaron un gran número de no conformidades que fueron disminuyendo en cada una de las iteraciones hasta erradicarlas totalmente. El éxito de este proceso fue gracias a la disposición y compromiso del equipo de desarrollo con solucionar las no conformidades detectadas en el menor tiempo posible. El resultado final de la aplicación de los casos de prueba a todos los requisitos funcionales se determinó por CALISOFT como satisfactorios.

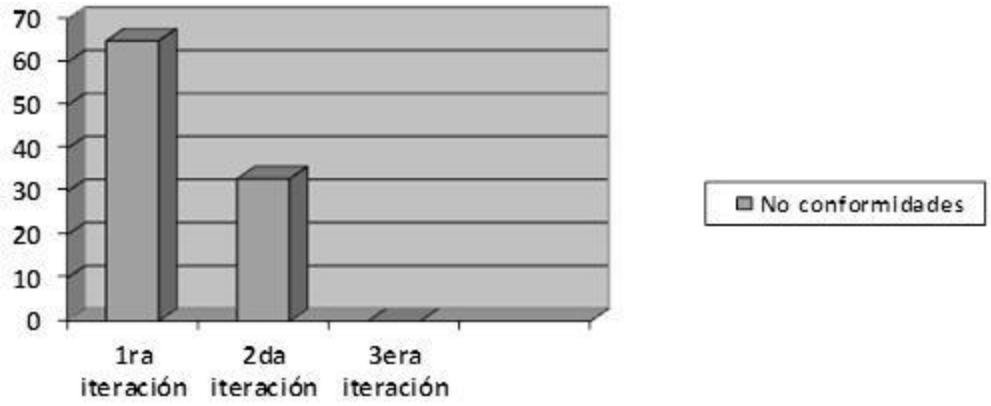


Figura 3.2: Número de conformidades por iteraciones.

3.3. Validación del proceso de planificación de auditoría en entornos reales.

Para garantizar el funcionamiento correcto de la aplicación en entornos reales, se tomó como muestra, las infraestructuras tecnológicas de los 41 UCAI existentes y se les garantizó el soporte por un año para corregir los problemas en la implementación del proceso de planificación y control de las auditorías. La cantidad de UCAI que participaron en la validación del sistema representa el total de las UCAI de país, por lo que significa que el tamaño de la muestra es la población en sí misma. Por la importancia y el nivel de seguridad que lleva la información que se maneja, se decidió llevar el tamaño de la muestra a estas magnitudes, minimizando posibles particularidades qué pudiesen surgir posteriormente en una de las UCAI.

En el despliegue se validó la conformidad de los clientes en aspectos como la completitud de los datos del plan, de los controles y la apariencia de las interfaces visuales de usuario. El aval de la CGRC del año 2010 ubicado en el Anexo 2, figura A1, confirma el despliegue del producto en las diferentes instalaciones tecnológicas.

3.3.1. Pruebas experimentales de la aplicación en entornos reales

Se realizaron diversas pruebas experimentales para cerciorar el funcionamiento adecuado de la solución informático en ambientes reales.

A continuación se detallan dos pruebas experimentales realizadas en la CGRC para demostrar el correcto funcionamiento del mecanismo de control de acceso aportado por el modelo PCAECM para acceder y modificar la información del plan y de esta forma demostrar la confiablidad de la información con el modelo propuesto.

Se les suministró a distintos usuarios acceso a dominios o estructuras auditoras, para evidenciar como se consigue la compartimentación de la información en entornos multidominio y de esta manera como se mantuvo con las funcionalidades, la confidencialidad de los datos. En una primera prueba se otorgó al usuario *yazan* el acceso al plan de la estructura auditora: el Ministerio de Cultura que representa a un dominio, con los permisos de adicionar, modificar, consultar, eliminar e imprimir. Ver figura 3.3. En esta figura se muestra como se asegura que un usuario tenga los permisos pertinentes para que tenga los privilegios necesarios para poder acceder y modificar los valores de los planes pertenecientes a un dominio.

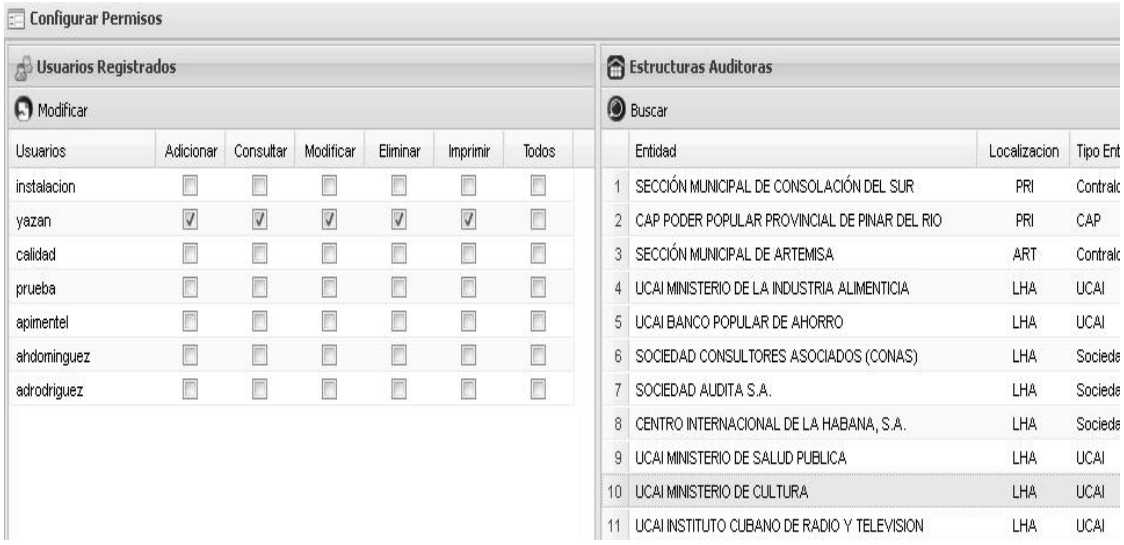


Figura: 3.3: Pantalla para otorgar permisos al usuario para el Ministerio de Cultura.

En la segunda prueba experimental al usuario *prueba*, le fue asignado la estructura auditora: Sociedad Audita SA, que representa a otro dominio, con los permisos de adicionar, modificar, consultar, eliminar e imprimir. Ver figura 3.4.

Para corroborar que los permisos proporcionados a los usuarios en las distintas pruebas experimentales fueron cumplidos, se comprueba en el listar de la funcionalidad: Plan Anual, donde se muestran los planes de auditoría que tienen acceso los usuarios según el permiso concedido en la anterior funcionalidad. En la figura 3.5 se muestra el Plan del Ministerio de Cultura facilitado para el usuario *yazan* en el primer experimento y en la figura 3.6 se muestra el Plan de la Sociedad Audita SA entregado al usuario *prueba* en el segundo experimento.

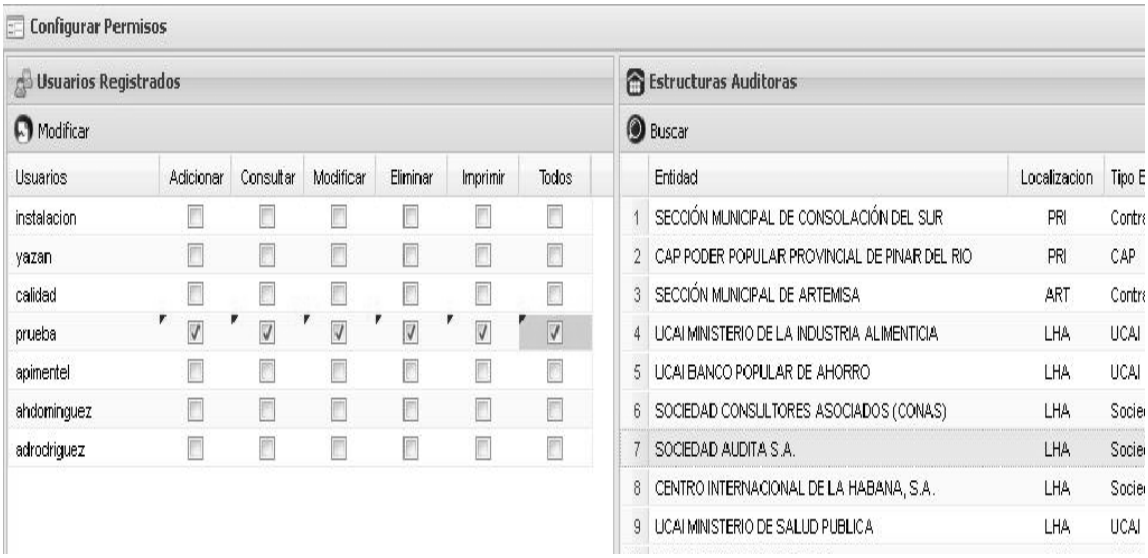


Figura: 3.4: Pantalla para otorgar permisos a un usuario para Sociedad Audita SA.

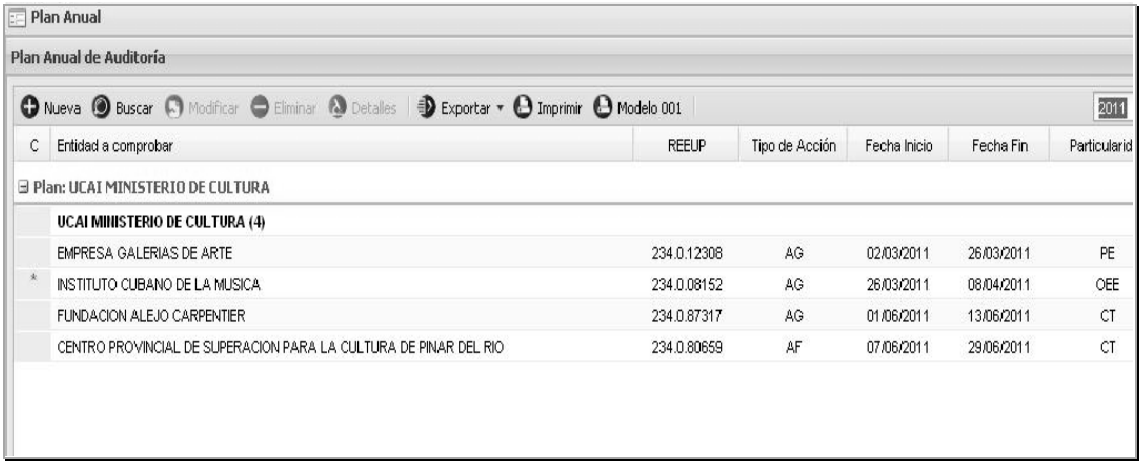


Figura: 3.5: Pantalla del Plan Anual de Ministerio de Cultura.

Con estas pruebas experimentales se confirma que los usuarios solo tienen acceso a la información que les corresponde y solo pueden modificar el plan al cual tienen permitido, por lo cual queda demostrada la confiabilidad de la información en los entornos cubanos multidominios.

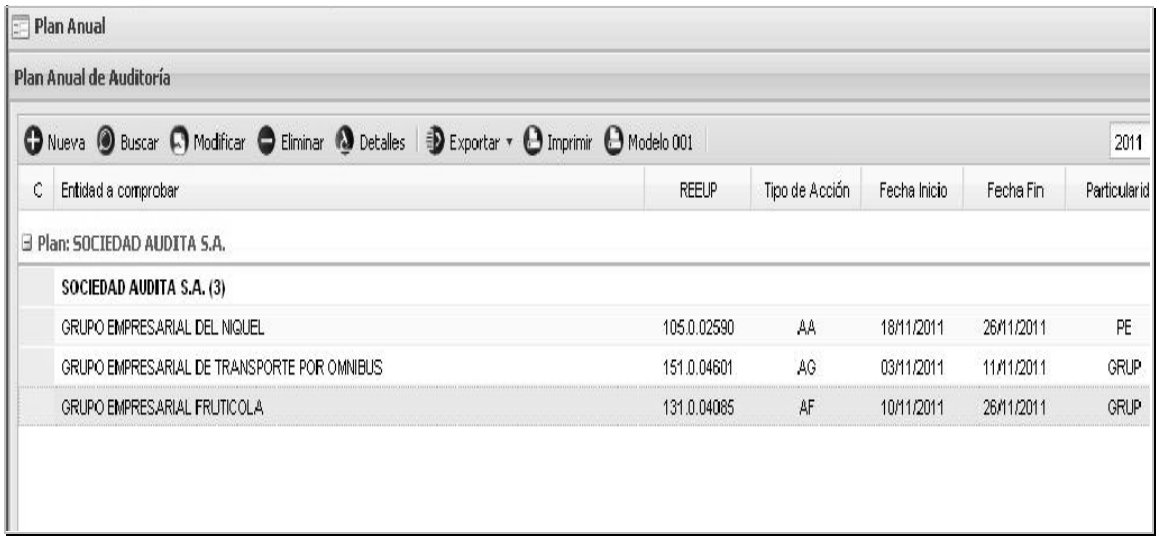


Figura: 3.6: Pantalla del Plan Anual de la Sociedad Audita SA.

Para completar la validación del modelo a través de la aplicación informática en entornos reales, se le suministró soporte a la aplicación durante su primer año de instalación en los 41 UCAI de país y en la CGRC. Salieron durante este periodo

algunos defectos de la aplicación en cuanto a la gestión de la planificación y control de las auditorías que fueron inmediatamente resueltas. Ninguno de los defectos encontrados estuvo relacionado con la compartimentación de la información de la planificación y control de las auditorías de manera que estuviese afectada la confidencialidad de la información.

3.4. Comparación con otras instancias de modelos de autorización

La intención de realizar la comparación con otras instancias de modelos de autorización, es 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.

3.4.1. Selección de indicadores

El análisis de los principales referentes teóricos existentes en la literatura, revela que uno de los dominios más importantes a tener en cuenta para preservar la seguridad de los recursos gestionados por los SI, lo constituye el control de acceso. Las debilidades que presentan los modelos, entre otras soluciones analizadas, influyen de forma negativa en la fortaleza de los sistemas de control de acceso que se desarrollan basados en ellos. Por esta razón es necesario evaluar el nivel de fortaleza de los sistemas de control de acceso para prevenir o detectar violaciones que pongan en riesgo la seguridad de los recursos gestionados por SI en entornos multidominios. Para realizar este tipo de evaluaciones existen dos métodos fundamentales, estos son:

1. Basadas en vulnerabilidades.
2. Basados en objetivos o indicadores.

Las evaluaciones basadas en vulnerabilidades requiere de un conjunto de herramientas y técnicas para realizar hacking ético con el objetivo de evaluar el comportamiento del sistema ante las principales vulnerabilidades publicadas en bases de datos como: la OSVDB (siglas de Base de Datos de Vulnerabilidades de Código Abierto), la NVD (siglas de Base de Datos Nacional de Vulnerabilidad) del NIST, la CVSS (siglas de Registro Común de Vulnerabilidades de Sistemas), entre otras [52-54].

En Cuba, estas pruebas solo se realizan por organizaciones autorizadas como Segurmática, Calisoft, el Misterio del Interior (MINIT), el Ministerio de las Fuerzas Armadas Revolucionarias (MINFAR) y la Oficina de Seguridad para Redes Informáticas (OSRI) que cuentan con los especialistas, las herramientas y técnicas necesarias para llevarlas a cabo. En la presente investigación este tipo de pruebas fueron ejecutadas por las entidades Calisoft y Segurmática.

La evaluación basada en objetivos o indicadores, se apoyan fundamentalmente en los requisitos descritos en las principales normas, guías o recomendaciones publicadas por organizaciones internacionales como la ISO, el NIST, OWASP, entre otras líderes en este tema.

Este método es certificable, a través del Sistema de Gestión de la Seguridad de la Información propuesto en la norma ISO 27001. En la actualidad las empresas que comercializan SI o servicios tecnológicos, utilizan esta certificación como constancia ante sus clientes de la seguridad de sus procesos, productos o servicios. Teniendo en cuenta las características del entorno donde se realiza esta investigación y las entrevistas realizadas a especialistas en el tema, se decidió utilizar también este método con el objetivo de comparar los resultados de ambos métodos.

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 [16, 55-59].

Los indicadores extraídos de estos referentes teóricos fueron evaluados por especialistas en la temática a través de la aplicación de métodos científicos como las entrevistas a profundidad y técnicas de grupos focales. En el proceso de aplicación de estos métodos surgieron nuevos indicadores que a consideración de los especialistas son importantes para evaluar la fortaleza de los sistemas de control de acceso en el entorno cubano. En el proceso de análisis, fundamentación y selección de los indicadores participaron especialistas (Anexo 5) con experiencia práctica en la evaluación o auditoría de seguridad, de las siguientes organizaciones:

- Departamento de Seguridad Tecnológica de la DTS del MININT.
- Centro de Investigaciones de Tecnologías Integradas (CITI).
- Oficina de Seguridad para Redes Informáticas (OSRI).
- Centro Nacional de Calidad de Software (Calisoft).
- Dirección de Comunicaciones del MINFAR.
- Centro para la Compatibilización Integración y Desarrollo para la Defensa (UCID).
- Universidad de las Ciencias Informáticas (UCI).

En estos documentos se avala que los indicadores seleccionados constituyen una herramienta válida para medir el nivel de fortaleza que poseen los sistemas de control de acceso en la actualidad. Estos indicadores se encuentran en el Anexo 6, los cuales se agruparon por procesos para facilitar su comprensión y aplicación. La Figura 3.7 muestra la distribución de indicadores por proceso.

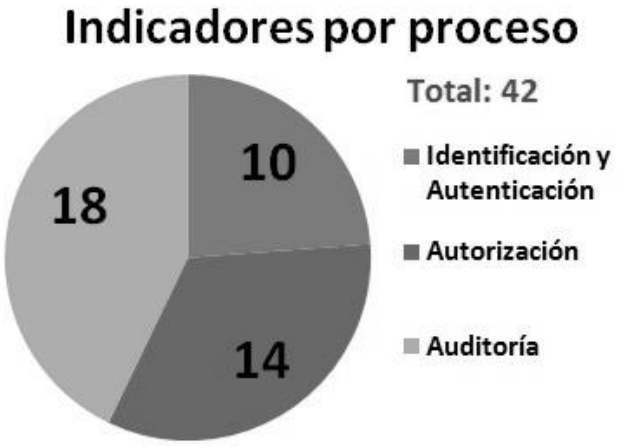


Figura 3.7: Distribución de indicadores por proceso.

Para la presente investigación solo se tomaron en cuenta los indicadores para el proceso de Autorización.

3.4.2. Criticidad de los indicadores

El nivel de criticidad de los indicadores puede variar en función del impacto que tengan en la seguridad de los recursos gestionados por los SI. Atendiendo a esta característica, se aplicó una encuesta a los especialistas de las entidades mencionadas anteriormente, para determinar la criticidad de cada uno de los indicadores. La criticidad se considera importante para evaluar el impacto que tiene la implementación o no de un indicador, con el objetivo de obtener resultados más cercanos a la realidad. Para la selección de los expertos se aplicaron entrevistas a profundidad a varios especialistas de las instituciones que participaron en la definición y aprobación de los indicadores, con el objetivo de detectar los que cumplen con los siguientes requisitos:

- Llevar un tiempo mayor o igual a cinco años trabajando en temas relacionados con la Seguridad Informática.
- Dominar los modelos, estándares, protocolos y metodologías más utilizadas para estandarizar el desarrollo de soluciones de control de acceso y tener experiencia en su aplicación.
- Haber participado en la confección de políticas de Seguridad Informática y en auditorías para controlar su cumplimiento.
- Tener disposición para participar como expertos.

La aplicación de las entrevistas a profundidad arrojaron como resultado que solo diez especialistas cumplían los requisitos establecidos. Estos diez compañeros constituyen los expertos a los cuales se les aplicó la encuesta para definir la criticidad de cada uno de los indicadores. La Figura 3.8 muestra la distribución de los expertos por organizaciones y sus datos se pueden consultar en el Anexo 7.

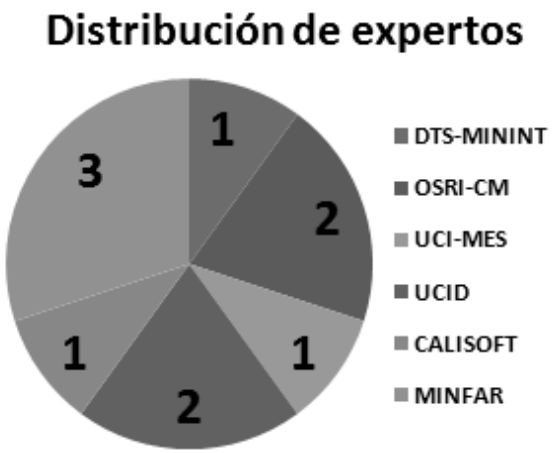


Figura 3.8: Distribución de expertos.

Este método científico evidenció una total coincidencia en que los indicadores tienen un nivel de criticidad entre cuatro y cinco (el rango de valores era entre cero y cinco). Este resultado demuestra la calidad del proceso de selección de los indicadores y la necesidad de cumplir con ellos en el desarrollo de las soluciones de control de acceso para evitar violaciones de seguridad.

3.4.3. 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, según el análisis realizado en el capítulo uno. 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.

Los criterios fueron identificados a partir del estudio documental y las entrevistas a profundidad realizadas a los especialistas de las organizaciones mencionadas anteriormente.

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 3.1 se especifica el nombre de los sistemas, su 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.

Sistemas	**Descripción**	**Nombre del Proceso**	**Soluciones que implementan**	**Entidad evaluadora**
ERP Universitario	Sistema para gestión de los procesos sustantivos del entorno universitario			Calisoft
		Autorización	ABAC	
SIGEP	Sistema para la gestión de información			Cliente en Venezuela
		Autorización	RBAC	

	penitenciaria en Venezuela			
SUIN	Sistema para la gestión de identidades de las personas en Cuba			MININT
		Autorización	RBAC	
SIGEL	Sistema para la gestión del proceso electoral en Cuba			Calisoft y MININT
		Autorización	RBAC y ABAC	
SIIPOL	Sistema para la gestión de los procesos policiales en Venezuela			Cliente en Venezuela
		Autorización	RBAC y ABAC	
SIGAC	Sistema para la planificación y control de Auditorías			
		Autorización	PCAECM	

Tabla 3.1: Descripción de los sistemas seleccionados.

3.4.4. 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.

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

La Tabla 3.2 muestra el diseño del pre-experimento realizado como parte del proceso de validación.

		Sistema 1 (Modelo 1)		**…**	**Sistema n (Modelo n)**	
In	**C**	**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}

Tabla 3.2: Diseño experimental propuesto.

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.

- **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).

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.

3.4.5. 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 In_{11} al In_{24}) 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 la 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 3.9 refleja el porciento de cumplimiento de los indicadores asociados a este proceso por cada uno de los sistemas que forman parte de la muestra.

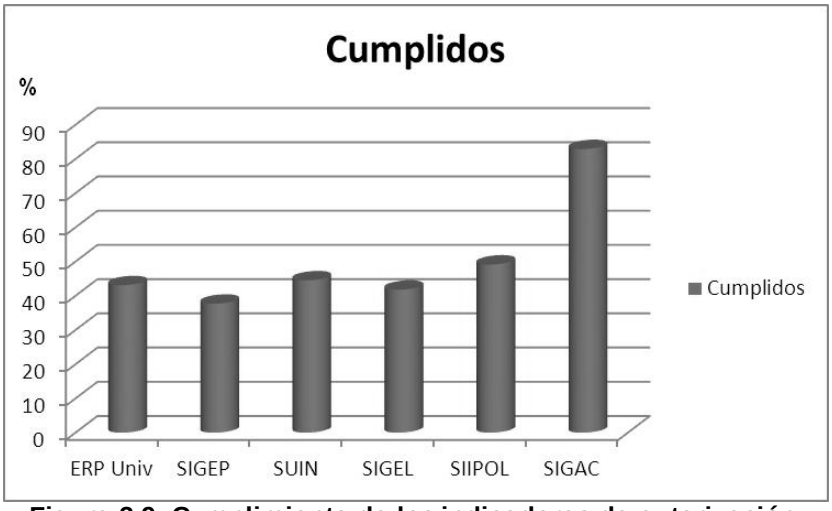


Figura 3.9: Cumplimiento de los indicadores de autorización.

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. 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 el Anexo 8, tabla T6.

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 el Anexo 8, tabla T7. Los sistemas están enumerados del 1 al 6. Con el siguiente orden: ERP Universitario, SIGEP, SUIN, SIGEL, SIIPOL y SIGAC.

Para realizar las comparaciones entre SIGAC y los otros dos sistemas se aplicó el test de Mann-Whitney. 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. (Anexo 9, tabla T8 y T9).

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.

3.5. Conclusiones parciales

En este capítulo se le dio cumplimiento al último objetivo específico de la investigación resaltando que:

- Con el aval obtenido del cliente, de CALISOF y con las pruebas experimentales realizadas en ambientes reales, se confirmó la adecuada aplicación del modelo en los entornos cubanos multidominios. Además el modelo logra obtener el proceso completo de planificación y control de las auditorías con la confidencialidad de los datos del plan anual requeridos en el ambiente convergente de múltiples organizaciones en interoperabilidad.

- Se demuestra que el modelo propuesto (PACECM) permite obtener sistemas de control de acceso con mayor nivel de seguridad que los existentes en la bibliografía.

- El despliegue de la solución informática en los 41 UCAI del país, demostró su valor práctico y económico que tributó, avalados por las cartas de aceptación de los clientes obtenidos.

- Su adaptabilidad a la diversidad de entornos de despliegue existente en cada lugar donde fue instalado. De esta forma manifestó su fortaleza como solución, viable para las políticas migratorias a software libre en la cual está insertado el país.

CONCLUSIONES GENERALES

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

- A partir de la sistematización de los principales referentes teóricos que sustentan la presente investigación se demostró que existen limitaciones en la literatura para gestionar el proceso de planificación y control de las auditorías en entornos cubanos multidominios preservando la confidencialidad de la información.

- El modelo propuesto resuelve el problema planteado con la incorporación de conceptos asociados a los entornos multidominios y el establecimiento de restricciones que aumentan el nivel de granularidad de las políticas de autorización en estos escenarios.

- El modelo propuesto fue aplicado en el desarrollo de un sistema informático que fue desplegado en varios entornos reales del país con resultados satisfactorios.

- Los resultados de experimento realizado permitió 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.

- La calidad e impacto de los resultados de esta investigación fueron avalados por Calisoft y la CGRC.

RECOMENDACIONES

Se recomienda generalizar el modelo propuesto a otros escenarios multidominio.

Se recomienda incluir en las nuevas versiones un módulo para el sistema informático desarrollado, para el análisis de los riesgos para que el sistema sea compatible con los estándares internacionales en cuanto a la planificación.

Incorporar además un módulo para el análisis estadístico y crear informes por diferentes niveles o regiones y ayude a la toma de decisiones.

Crear los servicios necesarios para que se pueda lograr la integración del sistema con el módulo de Auditoría del Cedrux y que permita la colaboración entre los propietarios de procesos, los auditores y demás partes interesadas dentro de un mismo entorno de gestión de las auditorías.

Añadir el módulo de Gestión de Nomencladores del Cedrux para dar la posibilidad a los supervisores y auditores la posibilidad que antes nuevos nomencladores para la planificación de auditorías, puedan ser capaces de introducirlos en el sistema.

REFERENCIA BIBLIOGRÁFICA

1. Examiners, A.o.C.F., *2010 Report to the Nations*. 2010. p. 84.
2. PAGNUTTI, M. *Crece el fraude corporativo en el país: el 41% de las empresas aseguran ser víctimas de estafas*. 2009 [cited 2011; Available from: http://www.elargentino.com/Content.aspx?Id=71653.
3. Cubadebate (2011) *Detectan irregularidades en la contabilidad de las empresas estatales cubana, según Contraloría General*. Cubadebate.
4. Téllez, B.R., *Auditoría: Un enfoque práctico*. 2004.
5. CONTROL, M.D.A.Y., *Síntesis de la Estrategia Comunicación Institucional*. 2009. p. 6.
6. Shafiq, B., *ACCESS CONTROL MANAGEMENT AND SECURITY IN MULTI-DOMAIN COLLABORATIVE ENVIRONMENTS*. 2006, Purdue University: Indiana.
7. Ederlys Hernández Meléndrez, A.R.S.G. (200) *Planeamiento de las auditorías*.
8. Sejong Oh, S.P., *Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment*, in *Dept. of Computer Science*. 2007, Sogang University: Seoul.
9. Elisa Bertino, B.C., Maria Luisa Damiani, Paolo Perlasca (2000) *GEO-RBAC: A Spatially Aware RBAC*. ACM Transactions on Information Systems and Security **00** 1-34.
10. Salvador, M., *Administración aplicada. Teoría y Práctica*. 1995, Editorial Limusa.
11. International, C., *ISO 9000:2000*. 2000. p. 41.
12. Bertolín, J.A., *SEGURIDAD DE LA INFORMACION REDES, INFORMATICA Y: SISTEMAS DE INFORMACION*, PARANINFO. CENGAGE learning: Madrid.
13. *Network Management and Control*, M.M. Ivan.T. Frisch, Shivendra S. Panwar, Editor. 1994: Nueva York.
14. Shafiq, B., *Access Control Management and Security in Multi-Domain Collaborative Environments*, in *Center for Education and Research in Information Assurance and Security*. 2006, Purdue University.: Indiana.
15. Zeinab Iranmanesh, M.A., Rasool Jalili (2008) *A Logic for Multi-Domain Authorization Considering Administrators*. Workshop on Policies for Distributed Systems and Networks, 189 - 196.
16. MIC, *Resolución No. 127 /2007*, in *Oficina de Seguridad para las Redes Informáticas*, M.d.l.I.y.l.C.d.l.r.d. Cuba, Editor. 2007: La Habana, Cuba. p. 1-24. Disponible en: <http://ftur.uh.cu/intra/ftp/Resoluciones%20y%20Reglamentos/Resoluciones/R%20127-07%20Reglamento%20de%20Seguridad%20Informatica.pdf> [Consultado 28/09/2011].
17. María Bonilla, J.M., Frank Morales, *PLANIFICACIÓN: TIPOS Y HERRAMIENTAS*. . 2006, UNIVERSIDAD FERMIN TORO: BARINAS – ESTADO BARINAS.
18. BONILLA, M.M., JOSÉ Y MORALES, FRANK, *Planificación: Concepto e importancia* 2006, UNIVERSIDAD FERMIN TORO: BARINAS
19. Portela, G.B., *RESOLUCION No. 091/08*. 2008, Gaceta Oficial de la República de Cuba: La Habana. p. 11.
20. Melini, R., *Enfoquez en la Aduditoria de Estados Contables*.
21. Samuel Alberto Mantilla Blanco, S.Y.C.S., *Auditoría del control interno*, E. Ediciones, Editor. 2005: Bogotá.
22. Institute, I.G., *COBIT Mapping: Mapping PMBOK to COBIT 4. 0*. 2006.
23. Publishing, V.H., *Gestion de Servicios TI basado en ITIL: Guia De Bolsillo Spanish Version*. 2008.
24. WWW.ISO27000.ES, *ISO 27000*. 2008.
25. Yuan, E.a.J.T. (2005) *Attributed Based Access Control (ABAC) for Web Services*. International Conference on Web Services, 1-9.
26. Shu, C.C., E. Y. Yang, (2009) *Detecting Conflicts in ABAC Policies with Rule-reduction and Binary-search Techniques*. International Symposium on Policy for Distributed Systems and Networks, 182-185.
27. KE, K., O. LI (2010) *Towards Semantic Matching of Attributes in Multi-domain Access Control*. International Symposium on Intelligence Information Processing and Trusted Computing, 349-352.
28. Kuhn, D.R., E. J. Coyne (2010) *Adding Attributes to Role-Based Access Control*. IEEE Computer Society, 79-81.
29. O'Connor, A.C.a.R.J.L. (2010) *Economic Analysis of Role-Based Access Control Final Report*. 1-132.
30. Tao, W., L. Wei-hua, and L. Zun. *RBAC Permission Consistency Static Analysis Framework*. in *International Conference on Multimedia Information Networking and Security*. 2010. Nanjing, Jiangsu: IEEE Computer Society.

31. Abdallah, A.E. and H. Takabi. *Integrating Delegation with the Formal Core RBAC Model*. in *The Fourth International Conference on Information Assurance and Security*. 2008. Naples: IEEE Computer Society.
32. Crampton, J. and H. Khambhammettu. *A Framework for Enforcing Constrained RBAC Policies*. in *International Conference on Computational Science and Engineering*. 2009. Vancouver, BC: IEEE Computer Society.
33. Ferraiolo, D.F., et al., *Proposed NIST Standard for Role-Based Access Control*, U. National Institute of Standards and Technology (NIST), Editor. 2001, ACM Transactions on Information and System Security. p. 224-274.
34. Cheng, D. and H. Wen. *The application of role based access control in the third party logistics information system*. in *International Conference on Information Management, Innovation Management and Industrial Engineering*. 2011. Shenzhen, China: ACM Digital Library.
35. Ma, L., S. Ma, et al (2009) *A Dynamic Description Logic-based Formalism for RBAC*. IEEE Computer Society.
36. Xuexiong, Y., W. Qinxian (2010) *A Multiple Hierarchies RBAC Model*. International Conference on Communications and Mobile Computing, 56-60.
37. *Geospatial Semantics and the Semantic Web: Foundations, Algorithms, and Applications*, A.P.S. Naveen Ashish, Editor. 2011: Nueva York.
38. ELISA BERTINO, P.A.B. (2005) *TRBAC: A Temporal Role-Based Access*

Control Model. IEEE Computer Society **17**, 4-23.
39. Solutions, C.S. *Audit Management* 2011 [cited 2011; Available from: http://www.curasoftware.com/pages/content.asp?SectionID=8&SubSectionID=108.
40. Corporation, E. *Audit Management.* 2010 [cited 2011; Available from: http://www.archer.com/solutions/audit_management.html.
41. System, A.A. *APEX FEATURES*. 2009 [cited 2011; Available from: http://www.apexauditsystem.com/apex_features_overview_en.html.
42. Inc, M. *Audit Management Software System*. 2011 [cited 2011; Available from: http://www.metricstream.com/products/auditmangmt.htm.
43. Limited, M.K. *Key Functionality: Audit Planning*. 2011 [cited 2011; Available from: http://www.mkinsight.com/functionality.aspx?id=3.
44. Ltd, N.C.C. *AMS9000 Quality Management Software:Audit Management System*. 2009; Available from: http://www.noweco.com/ams9000e.htm.
45. Software, S. *SE Audit: Gestión de Auditorías*. 2011 [cited 2011; Available from: http://www.softexpert.es/planificacion-control-auditorias.php.
46. Wilsoft. *QAction Software para el control de Auditorias, Acciones correctivas y Preventivas*. 2011; Available from: http://www.wilsoft-la.com/QAction.htm.
47. Alianet Puentes Hernández, M.P.R., Raúl Rodríguez Proenza, *Módulo para la elaboración del Anteproyecto de Planificación del Sistema Cedrux*. 2009, Universidad de las Ciencias Informáticas: La habana. p. 133.
48. Yue Zhang, J.B.D.J. *A Request-Driven Secure Interoperation Framework in Loosely-Coupled Multi-domain Environments Employing RBAC Policies*. in *Collaborative Computing: Networking, Applications and Worksharing, 2007. CollaborateCom 2007. International Conference on*. 2007. New York, NY.
49. Gail-Joon Ahn, R.S., Myong Kangkand Joon Park (2000) *Injecting RBAC to Secure a Web-based Work ow System*. 1 - 10 DOI: 10.1145/344287.344295.
50. Wendy Boggs, M.B., *UML con Rational Rose 2002*, D. Crossman, Editor. 2002.
51. Pressman, R.S., *Ingeniería del Software. Un enfoque práctico.* 2006, Mc Graw Hill.
52. Wang, J.A., et al. *Measuring Similarity for Security Vulnerabilities*. in *43rd Hawaii International Conference on System Sciences*. 2010. Hawaii, USA: IEEE Computer Society.
53. Aussibal, J. and L. Gallon. *A new distributed IDS based on CVSS framework*. in *International Conference on Signal Image Technology and Internet Based Systems*. 2008: IEEE Computer Society.
54. Gallon, L. *On de Impact of Invironmental Metrics CVSS Scores*. in *International Conference on Privacy, Security, Risk and Trust*. 2010: IEEE Computer Society.
55. IEC, I., *International Standard ISO/IEC 27002*, ISO/IEC, Editor. 2007, Switzerland.
56. ITGI, et al., *Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa*, I. ITGI, OGC, TSO, Editor. 2008. p. 1 - 130. Disponible en: <http://www.isaca.org/Knowledge-

Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf> [Consultado 06/10/2011].

57. Gallagher, P.D. and G. Locke, *Recommended Security Controls for Federal Information Systems and Organizations*, U. National Institute of Standards and Technology (NIST), Editor. 2009. p. 1 - 237. Disponible en: <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf> [Consultado 21/03/2012].
58. Wiesmann, A., et al., *Una Guía para Construir Aplicaciones y Servicios Web Seguros*, T.O.W.A.S.P. (OWASP), Editor. 2005. p. 1 - 311. Disponible en: <https://www.owasp.org/images/b/b2/OWASP_Development_Guide_2.0.1_Spanish.pdf> [Consultado 24/02/2012].
59. ITGI, *Control Objectives for Information and related Technology (COBIT)*, I.G. Institute, Editor. 2007. p. 1 - 211. Disponible en: <http://www.isaca.org/COBIT/Pages/default.aspx> [Consultado 27/03/2011].

ANEXOS

Anexo 1. Descripción del Proceso Nacional de Auditoría.

Ficha de Proceso		
Proceso	Plan Nacional de Auditorías.	
Notación:	[Codificación ICOM]	
Entradas:	[Codificación ICOM]	Directivas trazadas por el Gobierno y la Contraloría para guiar al Sistema Nacional de Auditorías.
		Quejas y denuncias realizadas.
		Intereses del Gobierno y el PCC.
		Otros.
		Propuesta de Plan Anual.
		Plan Anual conciliado y aprobado por los Especialistas de la DASNAC.
		Plan Anual conciliado y aprobado por la directora de la DASNAC.
		Plan Anual presentado al Directorio.
Controles:	[Codificación ICOM]	Representantes de las UCAI de los CAP, OACE, contralorías provinciales, Direcciones y Sociedades.
		Especialistas de la DASNAC.
		Director de la DASNAC.
		Directorio.

Salidas:	[Codificación ICOM]	Propuesta de Plan Anual.
		Plan Anual conciliado y aprobado por los Especialistas de la DASNAC.
		Plan Anual conciliado y aprobado por la directora de la DASNAC.
		Plan Anual presentado al Directorio.
		Control de la ejecución del Plan; controles de cumplimiento.
Mecanismos:	[Codificación ICOM]	Calendario de conciliación.
Reglas del Negocio:		
Descripción del Proceso		

1.1 A1– Presentar Propuestas de Plan.

1.2 Entradas

Directivas. Quejas y denuncias. Intereses del gobierno y el partido. Otros.

Salidas

Propuestas de Plan Anual.

Mecanismos

UCAI de los CAP y OACE, Delegaciones, Direcciones y Sociedades.

Control

Calendario de conciliación.

Descripción

Las contralorías provinciales y Direcciones de la Contraloría, las UCAI de los CAP y OACE realizan la presentación de las propuestas del plan de Acciones de Control según el Calendario de conciliación y las Directivas trazadas por el estado cubano.

1.3 A2– Conciliar y Analizar Propuestas de Plan Anual.

Entradas

Propuestas de Plan Anual.

Salidas

Plan Anual conciliado y aprobado por los especialistas de la DASNAC.

Mecanismos

UCAI de los CAP y OACE, contralorías provinciales, Direcciones de la CGRC, Sociedades y Especialistas de la DASNAC.

Control

Calendario de conciliación.

Descripción

Las contralorías provinciales y Direcciones de la CGRC, las UCAI de los CAP y OACE concilian y analizan con los Especialistas de la Dirección de Planificación, Análisis y Control, las Propuestas de Plan existentes.

1.4 A3– Revisar Plan Anual.

Entradas

Plan conciliado y aprobado por los Especialistas de la DASNAC.

Salidas

Plan Anual revisado y aprobado por la directora de la DASNAC.

Mecanismos

Contralorías provinciales. Direcciones CGRC. Unidad Central de Auditoría de los CAP y OACE. Directora de la DASNAC.

Descripción

Los Especialistas presentan el Plan Anual a la directora de la DASNAC para su aprobación.

1.5 A4– Presentar al Directorio el Plan

Entradas

Plan Anual revisado y aprobado por la directora de la DASNAC.

Salidas

Plan Anual presentado al Directorio.

Mecanismos

Directora de la DASNAC y Directorio.

Descripción

La directora de la DASNAC presenta al Directorio el Plan Anual de Auditorías del año.

1.6 A5– Controlar Ejecución del Plan.

Entradas

Plan Anual presentado al Directorio.

Salidas

Controles de cumplimiento.

Mecanismos

Representantes de las UCAI de los CAP y OACE, direcciones, contralorías provinciales y sociedades

Descripción

Los representantes de las UCAI de los CAP y OACE, direcciones, contralorías provinciales y sociedades verifican el cumplimiento del Plan Anual a través de los controles de cumplimiento.

Tabla T1: Descripción del Proceso Nacional de Auditoría.

Sistema de Información Nacional de las Acciones de Control
Modelo 001

PLAN ANUAL DE LAS ACCIONES DE CONTROL

DE LA _____ **PARA EL AÑO 200__**
(Denominación de la unidad de auditoría)

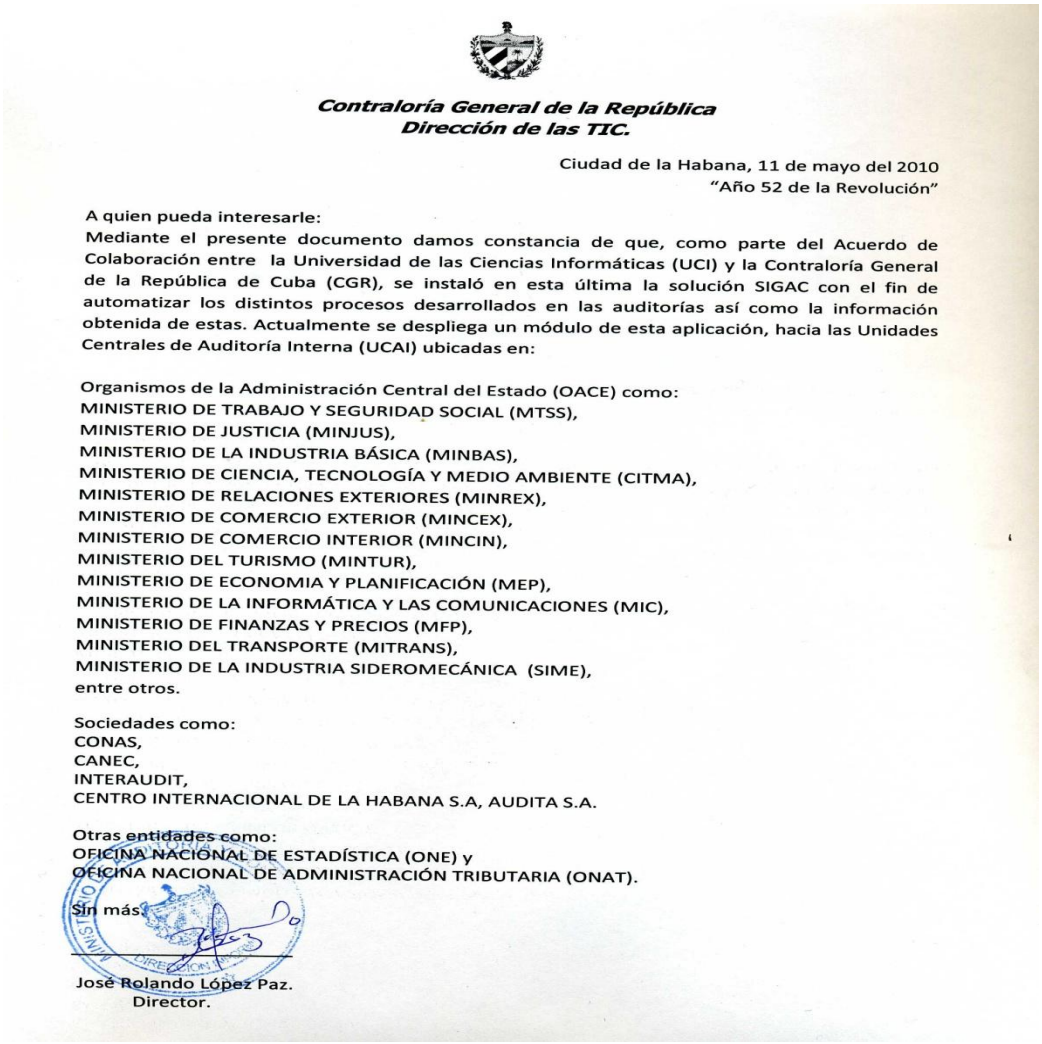
No	Denominación de las Entidades a comprobar	Código REEUP	Tipo de acción	Particularidades				Planificado		Control del cumplimiento						
				Perfeccionamiento empresarial	Presupuestada	Inversión Extranjera	En el exterior	Fecha Inicio	Fecha Terminación	Fecha Inicio	Fecha Terminación	Calificación	PHD	PHC	Afectación económica	
															CUP	CUC
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)	(16)	(17)
	Provincia de:															
	Sub. total provincia															
	Provincia de:															
	Sub. total provincia															
	Total General															

Elaborado por:
Nombres y Apellidos:
Cargo:
Fecha:

Aprobado por:
Nombres y Apellidos:
Cargo:
Fecha:

Tabla T2: Modelo 001 para realizar el Plan Anual de Acciones de Control.

Anexo 2. Aval del cliente.



Contraloría General de la República
Dirección de las TIC.

Ciudad de la Habana, 11 de mayo del 2010
"Año 52 de la Revolución"

A quien pueda interesarle:
Mediante el presente documento damos constancia de que, como parte del Acuerdo de Colaboración entre la Universidad de las Ciencias Informáticas (UCI) y la Contraloría General de la República de Cuba (CGR), se instaló en esta última la solución SIGAC con el fin de automatizar los distintos procesos desarrollados en las auditorías así como la información obtenida de estas. Actualmente se despliega un módulo de esta aplicación, hacia las Unidades Centrales de Auditoría Interna (UCAI) ubicadas en:

Organismos de la Administración Central del Estado (OACE) como:
MINISTERIO DE TRABAJO Y SEGURIDAD SOCIAL (MTSS),
MINISTERIO DE JUSTICIA (MINJUS),
MINISTERIO DE LA INDUSTRIA BÁSICA (MINBAS),
MINISTERIO DE CIENCIA, TECNOLOGÍA Y MEDIO AMBIENTE (CITMA),
MINISTERIO DE RELACIONES EXTERIORES (MINREX),
MINISTERIO DE COMERCIO EXTERIOR (MINCEX),
MINISTERIO DE COMERCIO INTERIOR (MINCIN),
MINISTERIO DEL TURISMO (MINTUR),
MINISTERIO DE ECONOMIA Y PLANIFICACIÓN (MEP),
MINISTERIO DE LA INFORMÁTICA Y LAS COMUNICACIONES (MIC),
MINISTERIO DE FINANZAS Y PRECIOS (MFP),
MINISTERIO DEL TRANSPORTE (MITRANS),
MINISTERIO DE LA INDUSTRIA SIDEROMECÁNICA (SIME),
entre otros.

Sociedades como:
CONAS,
CANEC,
INTERAUDIT,
CENTRO INTERNACIONAL DE LA HABANA S.A, AUDITA S.A.

Otras entidades como:
OFICINA NACIONAL DE ESTADÍSTICA (ONE) y
OFICINA NACIONAL DE ADMINISTRACIÓN TRIBUTARIA (ONAT).

Sin más,

José Rolando López Paz.
Director.

Figura A1. Aval del producto firmado por el cliente.

Anexo 3. Acta de Liberación de Productos Software

Validez desconocida
Digitally signed by Tayché Capote García
Date: 2011.06.28 16:42:29 CDT
Reason: Documento oficial
Location: Cuba

Universidad de las Ciencias Informáticas

Acta de Liberación de Productos Software

Fecha de liberación: 23 de junio de 2011.

Emitida a favor de: Informatización de la Contraloría General de la República de Cuba (ICON).

1. Datos del Producto.

Artefacto	Versión	Estado final	Cantidad Iteraciones	Tipos de pruebas realizadas
Subsistema de Planificación	1.0	0	3	Pruebas Funcionales
Manual de Usuario del subsistema Planificación (Directores de Estructuras)	1.0	0	3	Evaluación Estática
Manual de Usuario del subsistema Planificación (Gestionar UEB)	1.0	0	3	Evaluación Estática
Manual de Usuario del subsistema Planificación (Especialistas de las DPAC)	1.0	0	3	Evaluación Estática
Manual de Instalación del subsistema Planificación	1.0	0	3	Evaluación Estática

Ing. Yudisbel Pérez Moreno
Especialista de CALISOFT

Ing. Antonio Hernández Domínguez
Responsable Proyecto

Figura A2. Acta de productos de software emitido por CALISOFT.

Anexo 4. Descripción del sistema SIGAC

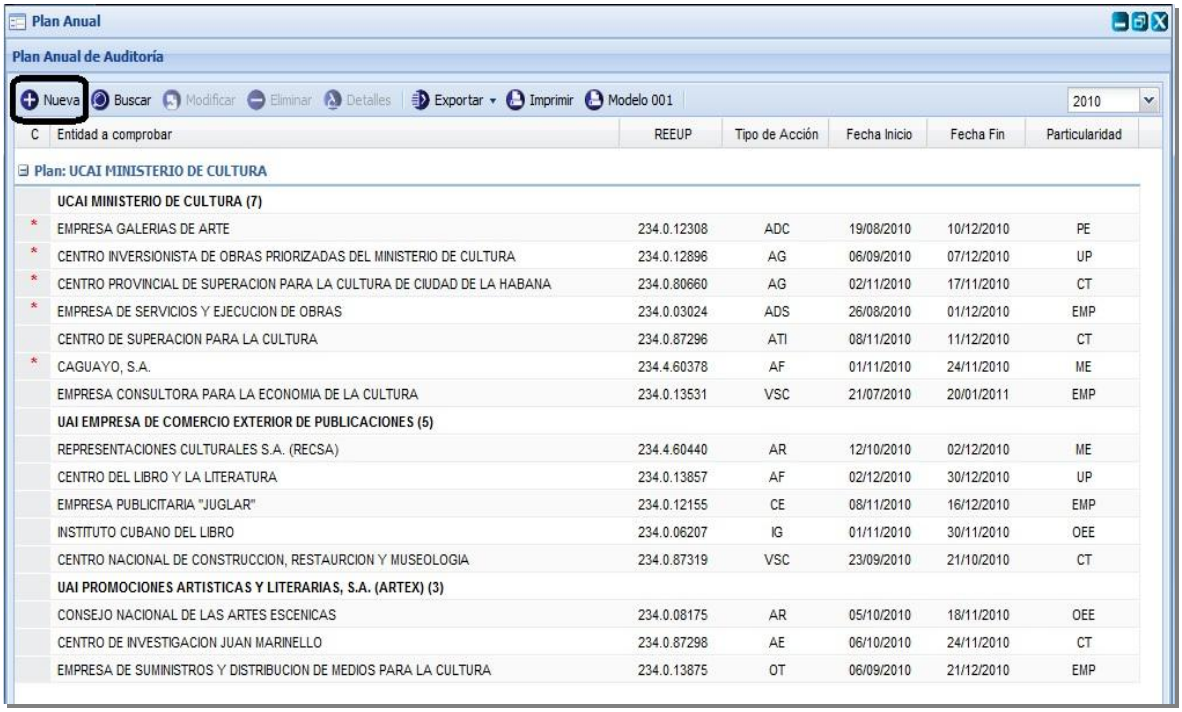


Figura A3. Funcionalidad Gestión del Plan Anual de las Acciones de Control del sistema SIGAC.

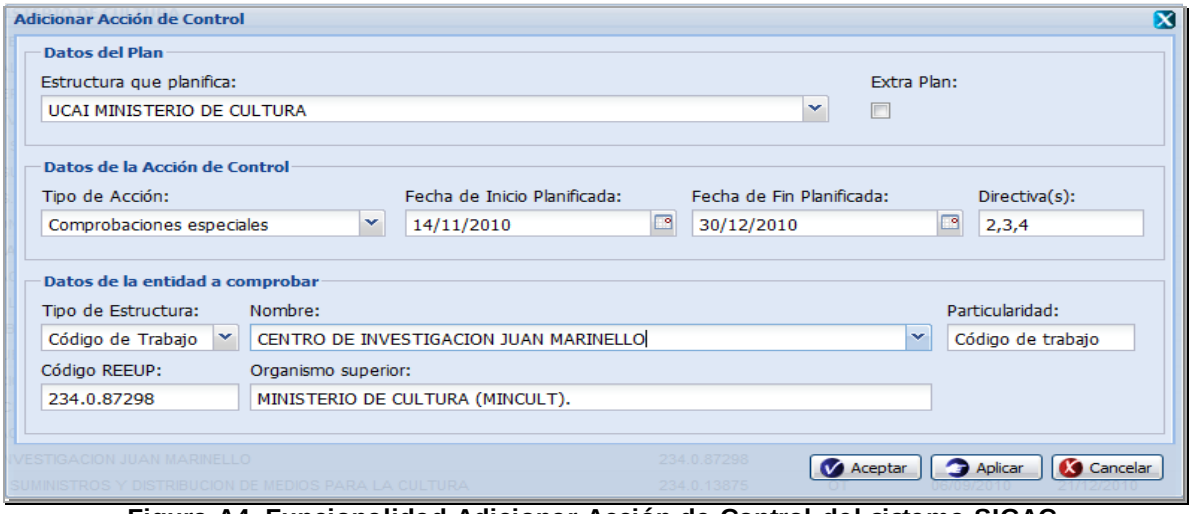


Figura A4. Funcionalidad Adicionar Acción de Control del sistema SIGAC.

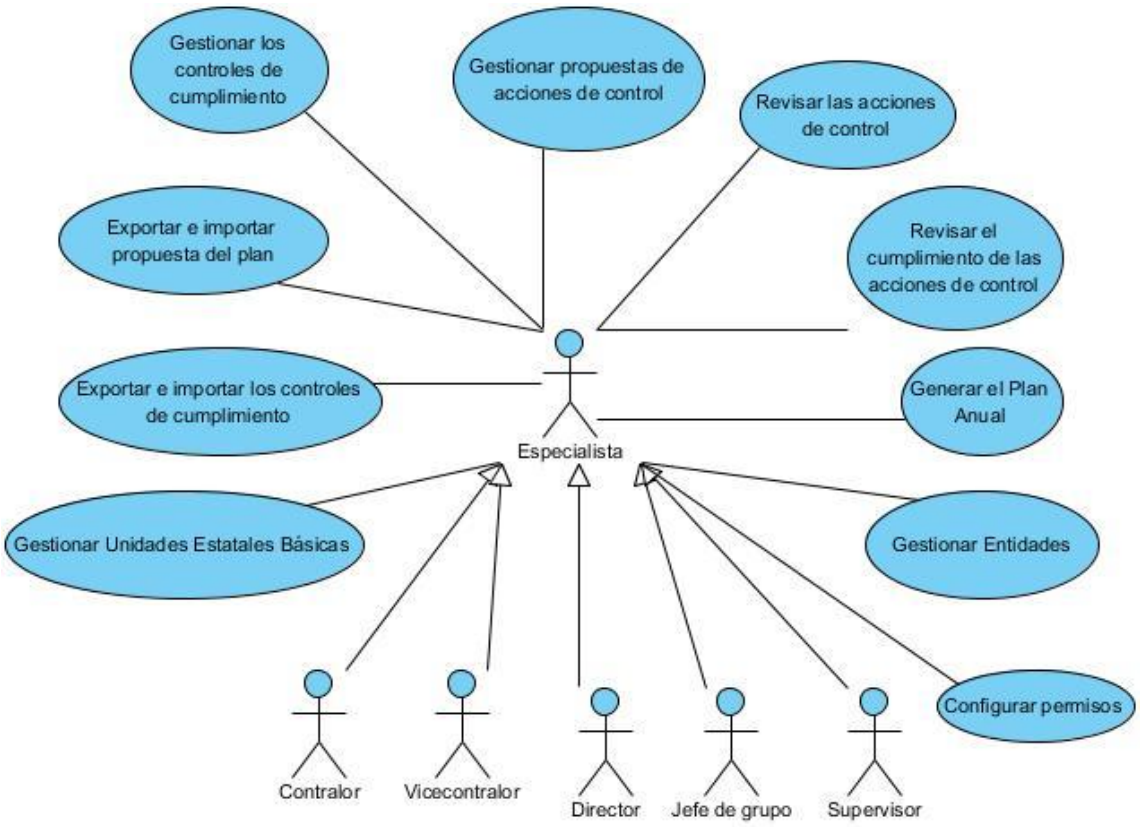


Figura A5: Diagrama de casos de uso del sistema SIGAC.

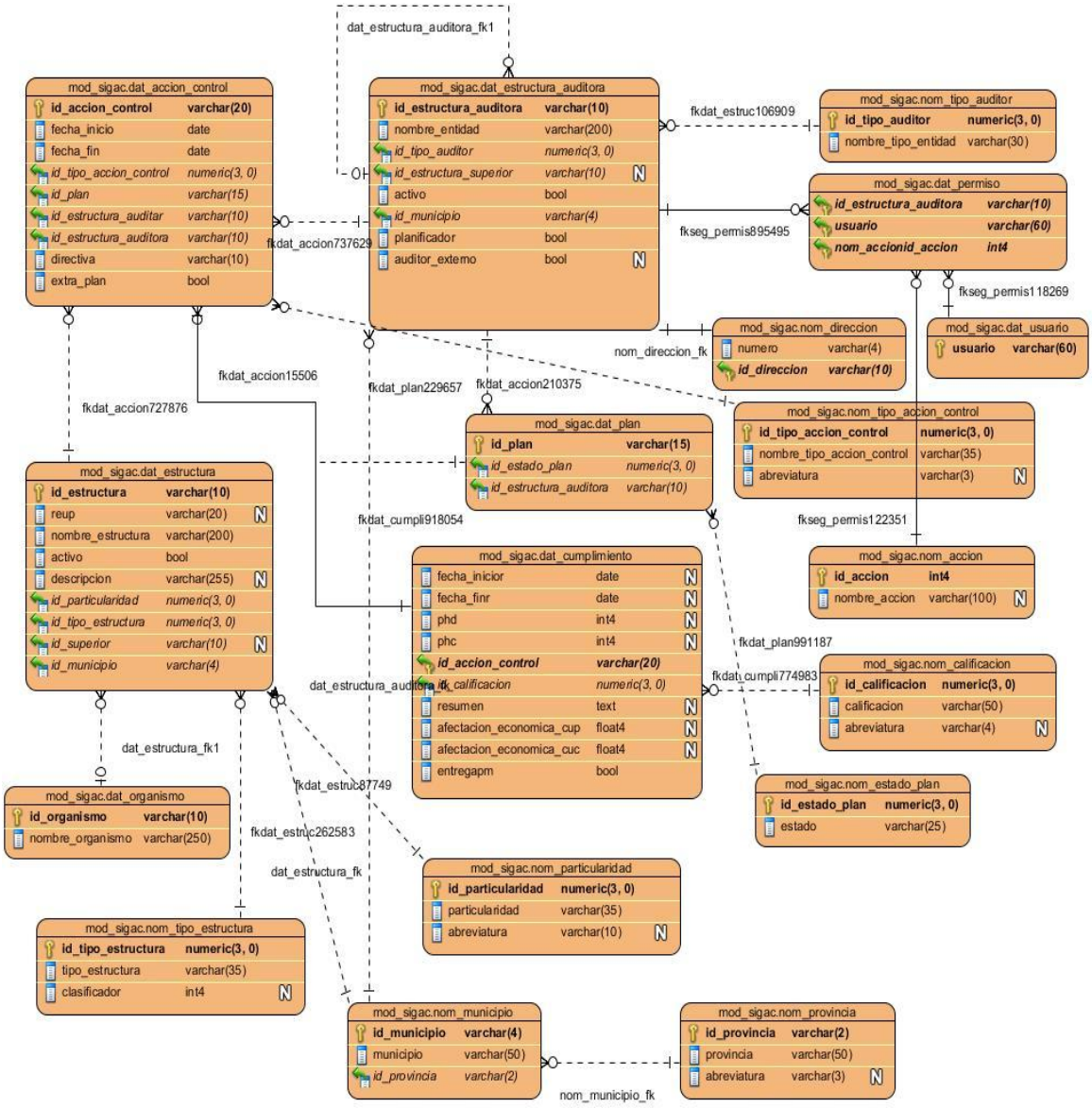


Figura A6. Modelo de datos del SIGAC.

Anexo 5. Especialistas que participaron en el análisis y definición de los indicadores.

Expertos	**Entidad**	**Cargo**	**Experiencia**
Guberto Pérez Torres	Dirección de Tecnologías y Sistemas del Ministerio del Interior	Jefe del Departamento de Seguridad Tecnológica	5 años
Humberto Muñoz Dussac	Oficina de Seguridad para las Redes Informáticas (OSRI)	Director Redes y Transmisión de Datos	12 años
Norqui Ortiz Machado	Oficina de Seguridad para las Redes Informáticas (OSRI)	Especialista Superior del Departamento de Organización y Control	7 años
Yoandrys Morejón Borbon	Unidad de Compatibilización, Integración y Desarrollo de Software para la Defensa(UCID)	Jefe del Centro de Desarrollo y Asimilación de Tecnologías	6 años
Darien García Tejo	Unidad de Compatibilización, Integración y Desarrollo de Software para la Defensa(UCID)	Jefe de la Línea de Seguridad	5 años

Asnier E. Góngora Rodríguez	Centro Nacional de Calidad de Software (Calisoft)	Especialista en Pruebas de Seguridad	5 años
Lázaro Acosta Sigler	Dirección de Comunicaciones del MINFAR	Jefe del Centro de Vigilancia Tecnológica y Certificación	16 años
Yuney López Lugo	Dirección de Comunicaciones del MINFAR	1ra Oficial del Centro de Vigilancia Tecnológica y Certificación	8 años
Teresa Álvarez Rico	Dirección de Comunicaciones del MINFAR	1ra Oficial del Departamento de Informática	29 años
Humberto Díaz Pando	Centro de Investigaciones de Tecnologías Integradas (CITI)	Jefe del Centro de Seguridad Tecnológica	7 años
Renier Tejera Trujillo	Centro de Investigaciones de Tecnologías Integradas (CITI)	Jefe de Proyecto del Centro de Seguridad Tecnológica	7 años

Anissa Gramatges Ortiz	Centro de Investigaciones de Tecnologías Integradas (CITI)	Líder de Gestión del Centro de Seguridad Tecnológica	6 años
Yanelis Formoso Valdez	Centro de Investigaciones de Tecnologías Integradas (CITI)	Especialista de Seguridad del Centro de ST	5 años
Guillermo E. Zandetti García	Centro de Investigaciones de Tecnologías Integradas (CITI)	Especialista de Seguridad del Centro de ST	5 años
Claudia M. Poo Enciso	Centro de Investigaciones de Tecnologías Integradas (CITI)	Especialista de Seguridad del Centro de ST	3 años
Jormari Llanes Rojas	Centro de Investigaciones de Tecnologías Integradas (CITI)	Especialista de Seguridad del Centro de ST	4 años
Jorge L. Martín Correa	Universidad de las Ciencias Informáticas (UCI)	Arquitecto de Seguridad del proyecto Quarxo	6 años
Michael González Jorrín	Universidad de las Ciencias Informáticas (UCI)	Especialista de la Dirección General de	7 años

		Producción	
Liset Feria González	Universidad de las Ciencias Informáticas (UCI)	Especialista de la Dirección General de Producción	2 años
Yadier Perdomo Cuevas	Universidad de las Ciencias Informáticas (UCI)	Subdirector del Centro Identificación y Seguridad Digital	5 años
Orlando Cruz Rojas	Universidad de las Ciencias Informáticas (UCI)	Especialista Superior del Departamento de Gestión Universitaria	6 años
Yosbany Tejas de la Cruz	Universidad de las Ciencias Informáticas (UCI)	Especialista del Centro Informatización Seguridad Ciudadana	2 años
Yaksel Durán Rivas	Universidad de las Ciencias Informáticas (UCI)	Especialista del Centro Informatización Seguridad	2 años

		Ciudadana	
Yosvany Márquez Ruiz	Universidad de las Ciencias Informáticas (UCI)	Director del Centro Gobierno Electrónico	5 años
Carlos Acosta Montejo	Universidad de las Ciencias Informáticas (UCI)	Departamento de Implantación y Soporte Técnico	4 años

Tabla T3. Especialistas que participaron en el análisis y definición de indicadores.

Anexo 6. Indicadores seleccionados para medir la fortaleza de los sistemas de control de acceso.

Procesos	No.	Indicadores	Criterios de evaluación
Identificación y Autenticación	In_1	Solución de identificación y autenticación de los usuarios (personas y sistemas)	• Provee alguna solución para la identificación de los usuarios. • Provee alguna solución para la autenticación de los usuarios. • Provee alguna solución alternativa para garantizar la disponibilidad ante fallos o posibles ataques. • Nivel de seguridad, robustez y escalabilidad que se provee en los demás indicadores que integran este proceso.
	In_2	Implementación de estándares para el intercambio de mensajes de identificación y autenticación	• Implementa algún estándar existente (SAML, WS-Federation, OpenID, Perfil ECP, entre otros). • Seguridad, robustez y escalabilidad que proveen los estándares implementados. • Tipos de esquemas que soportan (Clave, Kerberos, Llave pública–X.509, Llave pública–PGP, Llave pública–SPKI, tarjetas inteligentes, Teléfono, entre otros).
	In_3	Soporte para nuevas técnicas de identificación y autenticación de los usuarios	• Cuenta con la escalabilidad necesaria para incorporar nuevos mecanismos. • No requiere de un gran esfuerzo incluir nuevos mecanismos a nivel de servicios o Plugin, teniendo en cuenta la relación costo beneficio.

Identificación y Autenticación			
	In $_4$	Gestión de identidades de los usuarios	• Provee alguna solución para la gestión de identidades de los usuarios. • Garantiza un identificador único para cada usuario. • Implementa alguna solución para evitar la duplicidad de usuarios a partir de atributos que identifican únicamente a una persona. • Soporta la definición de nuevos atributos y valores que fortalecen la identidad de los usuarios de forma dinámica.
	In $_5$	Implementación de métodos criptográficos y mecanismos seguros de comunicación (envío, recepción y almacenamiento de información sensible)	• Utiliza alguna solución criptográfica para almacenar información sensible (claves, tarjetas de créditos, entre otras). • Escalabilidad para soportar varios métodos criptográficos. • Esfuerzo necesario para incorporar nuevos métodos, teniendo en cuenta la relación costo beneficio. • Provee alguna solución para generar números pseudo-aleatorios. • Las soluciones criptográficas implementan algoritmos o estándares reconocidos por la seguridad que proveen (DES, TDES, RIJNDAEL, RC6, SERPENT, TWOFISH, MARS, entre otros). • Las soluciones criptográficas cumplen con estándares y protocolos reconocidos por la

			seguridad que proveen (X.509, SSL, DNSSEC, GSSAPI, SHTTP, PKCS, IEEE P1363, entre otros). • Nivel de seguridad que proveen las soluciones empleadas a partir de los algoritmos que implementan.
	In 6	Implementación del patrón Single Sign-On	• Implementa el patrón Single Sign-On y Single Sign-Out. • Implementa el patrón basado en algún estándar.
	In 7	Solución para la federación de identidades entre dominios	• Provee alguna solución para la federación de identidades. • Implementa algún estándar (Passport, Liberty, Shibboleth, SAML, WS-Federation, PAPI, entre otros). • Permite la identificación y autenticación de usuarios externos que pertenecen a otro dominio.
	In 8	Solución para gestionar la fortaleza y seguridad de las claves de acceso	• Provee alguna solución para gestionar la fortaleza de las claves en función del nivel de seguridad que se requiera (combinación de letras, signos, números, longitud y que no contengan palabras triviales (nombres, número de identidad, entre otros) o en blanco). • Implementa alguna solución que sirve de guía para que los usuarios establezcan claves seguras a través de evaluaciones y recomendaciones. • Provee alguna solución para

			gestionar el histórico de las claves y el tiempo de expiración. • Brinda la posibilidad de configurar los parámetros mencionados anteriormente teniendo en cuenta el escenario de aplicación. • Provee alguna solución para el cambio de claves que valida que las nuevas claves cumplan con la fortaleza establecida. • Mantiene actualizadas todas las fuentes de autenticación.
	In 9	Empleo de pruebas desafío-respuesta en los eventos donde se necesite determinar cuando el usuario es una persona o no	• Implementa algún tipo de pruebas desafío-respuesta para determinar si los eventos son ejecutados por personas o no (CAPTCHA, reCAPTCHA, Captcha BotCheck, voz, selección, entre otras). • Flexibilidad para ser utilizadas en cualquier parte del sistema.
Identificación y Autenticación	In 10	Restricciones de identificación y autenticación basadas en los atributos que identifican a los host en la red	• Provee alguna solución que permite establecer políticas de control de acceso basadas en los atributos que identifican a los host en la red (IP, MAC, entre otros). • Versiones del protocolo IP que soporta. • Provee alguna solución para garantizar las restricciones en escenarios donde se utilice el direccionado dinámico.
Autorización	In	Solución de autorización	• Provee alguna solución para gestionar la autorización de los

Autorización	11		usuarios. • Capacidad para validar los privilegios de acceso por cada acción en los diferentes niveles de la aplicación. • Seguridad, robustez y escalabilidad que se provee en los demás indicadores que integran este proceso.
	In 12	Implementa algún estándar para la asignación de privilegios y el intercambio de mensajes de autorización	• Reutiliza o implementa alguna solución que basada en estándares para la asignación de privilegios (ACL, MAC, DAC, RBAC, ABAC, entre otros). • Implementa algún estándar para el intercambio de mensajes de autorización (XACML, SPML, WS-Security, P3P, entre otros). • Tipos de mensajes que soporta (Peticiones de decisión de acceso, Decisión de acceso, Políticas, entre otros).
	In 13	Gestión de privilegios basado en roles	• Provee alguna solución para la gestión de privilegios basado en roles. • Implementa herencia de roles. • Asigna privilegios a los roles sobre los recursos del nivel de sistema. • Gestiona roles con privilegios sobre los recursos del nivel de datos. • Establece relaciones entre los privilegios de los roles del nivel de sistema y los roles del nivel de base de datos. • Asigna usuarios a múltiples roles.

			• Provee alguna solución que al eliminar un rol determinado se desactiven las cuentas de usuarios asociados, siempre que estos no tengan privilegios asignados directamente o posibilidad de acceder a recursos públicos.
	In 14	Gestión de privilegios a nivel de usuario	• Provee alguna solución para la asignación de privilegios basado en los usuarios. • Permite establecer privilegios diferentes entre usuarios que desempeñan un mismo rol.
	In 15	Gestión de las estructuras del nivel de base de datos y su relación con los sistemas	• Provee alguna solución para la gestión de las estructuras del nivel de datos de múltiples sistemas (servidor, gestor, base de datos, entre otros conceptos). • Establece una relación entre las estructuras del nivel de base de datos y los sistemas. • Gestiona los parámetros de conexión por sistemas.
	In 16	Gestión de privilegios a nivel de base de datos	• Gestiona los privilegios sobre las estructuras de base de datos. • Establece una relación entre las acciones que se ejecutan a nivel de sistema y las que se realizan a nivel de base de datos. • Soporte para varios gestores 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	• Provee alguna solución para definir criterios que identifiquen a los objetos. • Define y establece reglas sobre los criterios. • Restringe los privilegios

		reglas sobre ellos	(mostrar, insertar, modificar, eliminar, entre otros) sobre los recursos atendiendo a las reglas establecidas. • Garantiza la compartimentación de la información.
	In 18	Gestión de privilegios a nivel de funcionalidades	• Provee alguna solución para la gestión de privilegios sobre los procesos y actividades. • Establece una relación entre las actividades y las acciones o servicios que se deben ejecutar. • Permite definir los privilegios de los roles o usuarios sobre las actividades. • Provee alguna solución para la gestión de privilegios sobre las acciones en los diferentes niveles o capas del sistema. • Provee alguna solución para la validación de los privilegios sobre las acciones ejecutadas en entornos multisistemas.
	In 19	Gestión de privilegios teniendo en cuenta las estructuras y los dominios organizacionales (entornos multidominios)	• Provee alguna solución para la gestión de las estructuras y dominios organizacionales. • Provee alguna solución para la gestión de privilegios teniendo en cuenta las estructuras y dominios organizacionales. • Permite que los administradores de seguridad puedan crear administradores de niveles inferiores y definirles los recursos sobre los que pueden asignar privilegios. • Gestiona la compartimentación de la información teniendo en cuenta las estructuras y los

Autorización			dominios organizacionales.
	In 20	Gestión centralizada de privilegios en entornos multisistemas	• Provee alguna solución que permite gestionar los privilegios de acceso de múltiples sistemas simultáneamente. • Provee alguna solución para garantizar la interoperabilidad de información de autorización con otros sistemas. • Implementa algún estándar para la interoperabilidad de información de autorización con otros sistemas.
	In 21	Mínimo privilegio	• Implementa los procedimientos que establece la política de mínimo privilegio.
	In 22	Administración de cuentas	• Provee alguna solución para activar, desactivar o bloquear cuentas de usuario ante requisitos del negocio o posibles ataques. • Define y establece reglas para tomar acciones con respecto al estado de las cuentas de usuarios.
	In 23	Federación de privilegios entre dominios	• Provee una solución para la federación de privilegios de autorización. • Implementa algún estándar (ADL-R, XACML, FeDCOR, WS-Federation, entre otros). • Seguridad, robustez y escalabilidad que provee el estándar.
	In 24	Administración de sesiones de usuarios	• Provee una solución para la gestión de sesiones concurrentes.

			• Se gestiona el tiempo de expiración de la sesión en función de la criticidad de los recursos gestionados. • Permite visualizar y deshabilitar las sesiones activas. • Los usuarios pueden tener varias sesiones de forma concurrente. • En el Proveedor de Identidades se garantiza una única sesión por usuario.
Auditoría	In 25	Solución de auditoría	• Provee alguna solución para el registro y auditoría de los eventos ejecutados en los sistemas. • La solución adopta un formato o tipo de visualización en función del tipo de los análisis realizados. • La solución permite establecer filtros para el análisis y visualización de información. • La solución garantiza que los registros de eventos no contengan información sensible de los usuarios (clave, tarjetas de créditos, entre otras). • Seguridad, robustez y escalabilidad que se provee en los demás indicadores que integran este proceso.
	In 26	Implementa estándares para el registro y auditoría de los eventos que se ejecutan en los sistemas	• Los estándares permiten realizar auditorías centradas en la seguridad y funcionamiento de los sistemas. • Los estándares permiten realizar auditorías centradas en los

			procesos de negocio que informatizan los sistemas. • Beneficios que reportan los estándares implementados.
	In 27	Sistema de notificación de uso y funcionamiento de los sistemas	• Provee alguna solución para el envío de notificaciones relacionadas con el uso y funcionamiento del sistema. • Soporte para el envío de mensajes por varias vías (servicios web, Beeper, SMS, Jabber, entre otros). • Define y utiliza reglas de decisión para el envío de mensajes.
	In 28	Auditoría de eventos de ejecución de funcionalidades	• Provee alguna solución para el registro y visualización de la información asociada a las funcionalidades ejecutadas en los sistemas. • La solución permite gestionar los parámetros siguientes: usuario, rol, fecha, hora, dirección IP, organización, sistema, clase, método, si inició correctamente y si concluyó correctamente. • Si el sistema está orientado a procesos incluye los siguientes parámetros: proceso, instancia, actividad y objetos involucrados.
	In 29	Auditoría de eventos de ocurrencia de errores	• Provee alguna solución para el registro y visualización de la información asociada a los errores, noticias y advertencias que se producen en los sistemas. • La solución permite determinar los parámetros fundamentales

			por cada error producido en los sistemas. Ejemplo: usuario, rol, fecha, hora, dirección IP, organización, sistema, clase, método, tipo de evento y descripción.
	In 30	Auditoría de eventos de inicio y cierre de sesión	• Provee alguna solución para el registro y visualización de la información asociada al inicio y cierre de sesión de los usuarios en los sistemas. • La solución permite determinar los parámetros fundamentales por cada inicio o cierre de sesión. Ejemplo: usuario, dirección IP, fecha y hora de inicio y cierre de sesión.
Auditoría	In 31	Auditoría de eventos de integración	• Provee alguna solución para el registro y visualización de la información asociada a la integración entre componentes o sistemas. • La solución permite determinar los parámetros fundamentales por cada evento de integración entre componentes o sistemas. Ejemplo: usuario, rol, fecha, hora, dirección IP, organización, sistema y acción de origen, WSDL o sistema, clase y método de destino.
	In 32	Auditoría de eventos de operaciones a nivel de base de datos	• Provee alguna solución para el registro y visualización de la información asociada a las operaciones ejecutadas en las bases de datos. • La solución permite determinar los parámetros fundamentales

			por cada operación ejecutada. Ejemplo: usuario, rol, fecha, hora, dirección IP, organización, sistema, clase, método, tabla, objeto y operación.
	In 33	Auditoría de eventos de rendimiento	• Provee alguna solución para el registro y visualización de la información asociada al rendimiento por cada acción ejecutada. • La solución permite determinar los parámetros de rendimiento fundamentales por cada acción ejecutada. Ejemplo: usuario, rol, fecha, hora, dirección IP, organización, sistema, clase, método, tiempo de ejecución y uso de memoria.
	In 34	Nivel de respuesta ante fallos, vulnerabilidades o posibles ataques	• Provee alguna solución que permite definir acciones a ejecutar en caso que ocurran fallos, se detecten vulnerabilidades o posibles ataques. • Capacidad para identificar e informar en caso que se modifiquen o eliminen los registros de eventos.
	In 35	Protección de los registros de eventos	• Provee alguna solución que permite preservar la seguridad de los registros de eventos de acciones no autorizadas como: visualizar, modificar, eliminar, exportar, entre otras. • Se garantiza la compartimentación de la información contenida en los registros de eventos por

			organización, dominio, entre otros criterios. • Provee alguna solución para realizar salvas de seguridad.
	In 36	Mecanismo para incluir la auditoría de nuevos atributos y eventos	• Provee alguna solución que permite incluir la auditoría de nuevos eventos. • Complejidad para incluir la auditoría de nuevos eventos, teniendo en cuenta la relación costo beneficio. • Uso de patrones o elementos arquitectónicos que disminuye la complejidad para incluir la auditoría de nuevos eventos (Programación Orientada a Aspectos, uso de contenedores). • Están delimitadas las responsabilidades del sistema y de la solución de auditoría. El sistema captura los datos que necesita auditar y se los envía a la solución de auditoría por la vía establecida. El componente de auditoría provee las vías que pueden utilizar los sistemas para enviar los datos, los recibe, los almacena y los analiza en función de los objetivos que se persigan.
	In 37	Definición de incidente de seguridad	• Provee alguna solución para definir los eventos que se consideren incidentes de seguridad. • Los incidentes pueden relacionar varios atributos simultáneamente como la fecha y hora del evento, el usuario involucrado, recursos afectados, origen de la petición,

			entre otros. • Define y utiliza reglas para decidir las acciones a seguir ante los incidentes de seguridad.
Auditoría	In 38	Completitud de los registros de eventos para aplicar técnicas de descubrimiento o minería de proceso	• Los datos contenidos en los registros de eventos permiten aplicar técnicas de descubrimiento de procesos. • Los datos contenidos en los registros de eventos contienen los atributos que necesitan estándares como MXML y XES para aplicar técnicas de minería de procesos. • Completitud de los datos contenidos en los registros de eventos para predecir, evaluar y recomendar acciones que mejoren los resultados de la organización.
	In 39	Completitud de los registros de eventos para realizar análisis enfocados en las violaciones o ataques que afecten la seguridad	• La información contenida en los registros de eventos permite realizar análisis enfocados en las violaciones o ataques que afecten la seguridad. • En los análisis es posible determinar los usuarios involucrados, el origen, las causas y los recursos afectados por las violaciones o ataques.
	In 40	Completitud de los registros de eventos para realizar análisis enfocados en el desempeño de los sistemas	• La información contenida en los registros de eventos permite realizar análisis enfocados en el desempeño de los sistemas en los diferentes niveles o dominios organizacionales. • Permite evaluar el comportamiento de la

			integración entre los sistemas. • Permite evaluar el comportamiento del rendimiento por sistemas, clases o métodos. • Permite evaluar el comportamiento de los errores por sistemas, clases o métodos.
Auditoría	In 41	Completitud de los registros de eventos para realizar análisis enfocados en el recorrido histórico de los recurso y usuarios	• La información contenida en los registros de eventos permite realizar análisis enfocados en el recorrido histórico de los recursos. • La información contenida en los registros de eventos permite realizar análisis enfocados en el recorrido histórico de los usuarios. • Calidad de los análisis realizados.
	In 42	Capacidad para gestionar los registros de eventos de forma centralizada en entornos multisistema	• Provee una solución que soporta la gestión de eventos de varios sistemas simultáneamente. • Implementa soluciones arquitectónicas para proveer los mecanismos de integración necesarios. • Soporte para almacenar o exportar los registros de eventos a múltiples formatos. • Complejidad para incluir la gestión de eventos de nuevos sistemas.

Tabla T4: Indicadores seleccionados para medir la fortaleza de los sistemas de control de acceso.

Anexo 7. Expertos que participaron en la encuesta aplicada para determinar la criticidad de los indicadores.

Expertos	**Entidad**	**Cargo**	**Experiencia**
Guberto Pérez Torres	Dirección de Tecnologías y Sistemas del Ministerio del Interior	Jefe del Departamento de Seguridad Tecnológica	5 años
Humberto Muñoz Dussac	Oficina de Seguridad para las Redes Informáticas (OSRI)	Director Redes y Transmisión de Datos	12 años
Norqui Ortiz Machado	Oficina de Seguridad para las Redes Informáticas (OSRI)	Especialista Superior del Departamento de Organización y Control	7 años
Jorge L. Martín Correa	UCI-MIC	Arquitecto de Seguridad del proyecto Quarxo	6 años
Yoandrys Morejón Borbon	Unidad de Compatibilización, Integración y Desarrollo de Software para la Defensa(UCID)	Jefe del Centro de Desarrollo y Asimilación de Tecnologías	6 años
Darien García Tejo	Unidad de Compatibilización, Integración y Desarrollo de Software para la Defensa(UCID)	Jefe de la Línea de Seguridad	5 años
Asnier E. Góngora Rodríguez	Centro Nacional de Calidad de Software (Calisoft)	Especialista en Pruebas de Seguridad	5 años
Lázaro Acosta Sigler	Dirección de Comunicaciones del MINFAR	Jefe del Centro de Vigilancia Tecnológica y Certificación	16 años
Yuney López Lugo	Dirección de Comunicaciones del MINFAR	1ra Oficial del Centro de Vigilancia Tecnológica y Certificación	8 años

Teresa Álvarez Rico	Dirección de Comunicaciones del MINFAR	1ra Oficial del Departamento de Informática	29 años

Tabla T5: Expertos que participaron en la encuesta aplicada para determinar la criticidad de los indicadores.

Anexo 8. Prueba estadística de Kruskall-Wallis.

			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

Tabla T6: Significación obtenida entre todas las muestras en el proceso de autorización.

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	

Tabla T7: Rango medio de las evaluaciones de cada uno de los sistemas en el proceso de autorización por el test de Kruskall-Wallis.

Anexo 9. Prueba estadística de Mann-Whitney U.

			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 T8: Significación obtenida en la comparación por pares de las evaluaciones de SIGAC y el sistema SIGEL

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

Tabla T9: Significación obtenida en la comparación por pares de las evaluaciones de SIGAC y el sistema SIIPOL.