UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

TESIS DE GRADO

"MODELO DE SISTEMA EXPERTO PARA LA AUDITORÍA DE SISTEMAS INFORMÁTICOS"

PARA OPTAR AL TÍTULO DE LICENCIATURA EN INFORMATICA

MENCION: INGENIERIA DE SISTEMAS INFORMATICOS

POSTULANTE: VLADIMIR ALBERTO GUERRA GUERRA
TUTOR METODOLOGICO: LIC. GROVER ALEX RODRIGUEZ RAMIREZ
ASESOR: LIC. MARCELO ARUQUIPA CHAMBI

LA PAZ – BOLIVIA

2014

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS PURAS Y NATURALES
CARRERA DE INFORMÁTICA

LA CARRERA DE INFORMÁTICA DE LA FACULTAD DE CIENCIAS PURAS Y NATURALES PERTENECIENTE A LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AUTORIZA EL USO DE LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO SI LOS PROPÓSITOS SON ESTRICTAMENTE ACADÉMICOS.

LICENCIA DE USO

El usuario está autorizado a:

a) visualizar el documento mediante el uso de un ordenador o dispositivo móvil.
b) copiar, almacenar o imprimir si ha de ser de uso exclusivamente personal y privado.
c) copiar textualmente parte(s) de su contenido mencionando la fuente y/o haciendo la referencia correspondiente respetando normas de redacción e investigación.

El usuario no puede publicar, distribuir o realizar emisión o exhibición alguna de este material, sin la autorización correspondiente.

DEDICATORIA

Con Todo mi amor a mi mamá, Lidia…….

A mi esposa María y a mí querido hijo Santiago.

AGRADECIMIENTOS

A Dios, por haberme guiado en todos los pasos que di durante todos los años de mi vida.

Al Lic. Grover Rodríguez Ramírez y Lic. Marcelo Aruquipa Chambi, Tutor Metodológico y Asesor correspondiente, del presente trabajo, quienes con sus observaciones y sugerencias contribuyeron a perfeccionar y culminar el presente trabajo.

A mis padres, Alberto y Lidia (†), a quien debo lo que soy. A mi esposa María y mi hijo Santiago por el apoyo incondicional.

Finalmente, a los docentes y compañeros estudiantes de la Carrera de Informática y a La Universidad Mayor de San Andrés por permitir mi formación como profesional

Vladimir Alberto Guerra Guerra

INDICE DE CONTENIDO GENERAL

INDICE DE FIGURAS

INDICE DE CUADROS

RESUMEN

La Auditoria Informática es una actividad que ha cobrado fuerza en el campo de la Auditoria (tradicionalmente en el área financiera), con el incremento de las tecnologías de información; la auditoria informática se expande a todas las áreas donde intervienen las tecnologías, la seguridad es un aspecto en la evaluación, por lo que es necesario la auditoria a la información de la seguridad.

A menudo se presentan riesgos, amenazas y vulnerabilidades en la seguridad de la información de los sistemas informáticos, por esta razón, la presente investigación está dirigida a fortalecer las evaluaciones de Auditoria Informática de forma completa, para que a través de la evaluación exista una adecuada toma de decisiones.

Un sistema basado en conocimiento se define como “un sistema software capaz de soportar la representación explicita del conocimiento de un dominio especifico y de explotarlo a través de los mecanismos apropiados de razonamiento para proporcionar un comportamiento de alto nivel en la resolución de problemas”.

La investigación plantea un Modelo de sistema experto para la auditoria de sistemas informáticos, desarrollado mediante la metodología de sistemas expertos IDEAL, y el empleo del método Grover para la adquisición de conocimiento. El sistema experto se desarrolló en JAVA y CLIPS.

La investigación es un aporte para auditores o instituciones interesadas en realizar y aplicar una auditoria a la seguridad de la información.

Palabras Clave: Sistema experto Basado en reglas, Seguridad de la Información, Metodología IDEAL

CAPÍTULO I: MARCO REFERENCIAL

En este capítulo se presenta una descripción detallada del problema, hipótesis y objetivos que llevaron a desarrollar este trabajo.

1.1. INTRODUCCION

La proliferación de la Tecnología de la Información ha incrementado la demanda de control de los sistemas de información. La Seguridad de la Información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo para el negocio y maximizar el retorno de las inversiones.

La seguridad de la información es necesaria, debido a que la información y los procesos, sistemas y redes que lo soportan son activos importantes. La definición, el logro, el mantenimiento y la mejora de la seguridad de la información pueden ser esenciales para los procesos de la empresa [ISO 27002, 2007].

La actividad de evaluar y verificar el funcionamiento correcto, eficaz, eficiente de los sistemas de información y el entorno informático; es conocida como Auditoria Informática. El propósito de este proceso metodológico, es asesorar a los diferentes niveles de la administración de la empresa en el cumplimiento efectivo de sus responsabilidades, facilitándoles análisis, apreciaciones, comentarios y recomendaciones relacionados con las actividades del procesamiento de la información [Echenique, 2001].

La Auditoría Informática, abarca diferentes áreas y se establece divisiones para definir el alcance; como la Auditoría Informática de Explotación, Sistemas, Comunicaciones, Desarrollo de Proyectos y Seguridad.

Todos los tipos de auditorías y auditores pueden tomar ventaja mediante las técnicas y herramientas de software para ser más eficientes y efectivos, estas son las herramientas de

auditoría asistida por computadoras (CAATs). El software de auditoría consiste en programas de computadora usados por el auditor, como parte de sus procedimientos de auditoría, para procesar datos de importancia. Puede consistir en programas de paquete, programas escritos para un propósito, programas de utilería o programas de administración del sistema. Independientemente de la fuente de los programas, el auditor debe verificar su validez para fines de auditoría antes de su uso. Entre los tipos de software de auditoría tenemos: software de auditoría generalizado, específico, software de utilidad, especializado y sistemas expertos.

Los sistemas expertos, capturan el conocimiento de un experto e imitan sus procesos de razonamiento al resolver problemas en un determinado dominio, razón por lo cual en el presente trabajo de investigación, se aplican los sistemas expertos en el área de la Auditoria Informática, más propiamente en la Auditoria Informática a la Seguridad de la Información; las medidas de protección están en base a la serie de normas ISO 27000.

1.2. ANTECEDENTES

La auditoría ha cambiado notablemente en los últimos años, con el enorme impacto que han venido obrando las técnicas informáticas, en la forma de procesar la información para la gerencia. La necesidad de adquirir y mantener conocimientos actualizados de los sistemas informáticos, se vuelve cada vez más acuciante si bien los aspectos básicos de la profesión no han variado. Los Auditores Informáticos aportan conocimientos especializados, así como su familiaridad con la tecnología informática. Se siguen tratando las mismas cuestiones de control en la auditoría, pero los especialistas en auditoría informática de sistemas basados en computadores prestan una ayuda valiosa a la organización y a los otros auditores en todo lo relativo a los controles sobre dichos sistemas [Piattini, 2001].

De la misma manera, ha hecho necesaria la utilización de herramientas prácticas y confiables para llevar a cabo auditorías en los diferentes procesos informáticos dentro de

las organizaciones. Esta necesidad ha generado varias metodologías y herramientas que cuenten con estándares comunes. Detallados a continuación:

ISACA (Information System Audit and Control Association), es una organización conformada por auditores de sistemas de información, consultores, educadores, profesionales en seguridad de sistemas de información, operativos, directores ejecutivos de información, auditores internos y otros, de diversos países; estos están vinculados a la comunidad de auditoría y control de sistemas de información. ISACA ofrece la posibilidad de obtener certificaciones como (CISA) "Certifed Information System Auditor" y (CISM) "Certifed Information Security Manager".

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commision), que proporciona un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización [ISO 27002, 2007].

ISO 27001: "Sistemas de Gestión de la Seguridad de la Información (SGSI), Requisitos". Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. Los Sistemas de Gestión de Seguridad deberán ser certificados por auditores externos a las organizaciones [ISO 27001, 2007].

ISO 27002: (anteriormente denominada ISO17799). Guía de buenas prácticas que describe objetivos de control y controles recomendables en cuanto a la seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles [ISO 27002, 2007].

ISO 27005: Consiste en una guía para la gestión del riesgo de la seguridad de la información y sirve, por tanto, de apoyo a la ISO 27001 y a la implantación de un SGSI. Incluye partes de la ISO 13335.

ISO 27006: Publicada en febrero de 2007. Especifica los requisitos para acreditación de entidades de auditoria y certificación de sistemas de gestión de seguridad de la información.

En la carrera de Informática de la Universidad Mayor de San Andrés existen trabajos relacionados con el área de Auditoria Informática, de los cuales se puede Citar:

Modelo de Auditoría Informática para la Seguridad Física. En el cual plantea un modelo de auditoría informática para la seguridad, la información y activos físicos de unidades de sistemas, aplicable a toda institución independiente del tipo, tamaño y naturaleza a la que pertenezca. El modelo propuesto está basado en normas, técnicas de seguridad y requisitos (NB–ISO–IEC 27002) y la metodología de Objetivos y Control para la Información y las Tecnologías Relacionadas (COBIT). [Flores, 2008].

Herramienta Metodológica para la realización de Auditorías Informáticas en Organizaciones. En el cual se seleccionan normas, se especifica objetivos de control para la planificación, el desarrollo, implementación y monitoreo basados en la metodología COBIT, COSO, ITIL, y además plantea la construcción de herramientas de evaluación de acuerdo a los objetivos de control especificados.

Diseño de Auditoría Informática para la Seguridad Lógica. En el cual se presenta el material para realizar una auditoría a cualquier sistema de gestión de información, el mismo está basado en la NB ISO 17799 Seguridad de la Información el cual establece diez dominios de control que cubren por completo la gestión de la seguridad de información. También aplica la metodología de objetivos de control para la información y Tecnología relacionadas COBIT. [Cuela, 2007].

1.3. PLANTEAMIENTO DEL PROBLEMA

El proceso de conducción de una auditoria al departamento de informática de una determinada organización presenta una serie de complejidades en las fases de su desarrollo. El auditor informático debe tener la experiencia necesaria en el campo, el conocimiento de las normas y metodologías, como también el uso de las diferentes herramientas y técnicas para el desarrollo de una auditoria informática.

El auditor informático en la actualidad realiza el proceso de auditoría de manera manual, con base en las metodologías existentes, adoptando los papeles de trabajo y las hojas de Excel, como medio informático para el desarrollo de una Auditoría Informática, ocasionando en algunos casos el incumplimiento de resultados o informes periódicos en los plazos establecidos. Por lo que provoca un incremento en los costos de operación de procesos.

1.3.1. Formulación del Problema

Las ambigüedades existentes en el conocimiento de las normas y estándares de la rama, provocan dificultades en la recolección de evidencias.

El problema principal es definido de la siguiente manera: La ausencia de auditoría informática en los sistemas de información de las instituciones, lo que provoca vulnerabilidades y exponiendo a riesgos y amenazas al activo más importante que tiene una organización: su información.

1.4. OBJETIVOS

1.4.1. Objetivo General

Desarrollar un sistema experto para la Auditoría Informática a la seguridad de la información de aplicaciones software, que permita evaluar e identificar las amenazas y riesgos existentes. Además proporcione recomendaciones.

1.4.2. Objetivos Específicos

- Adquirir conocimiento heurístico del experto, relacionado a la seguridad de la información
- Representación del conocimiento del sistema experto.
- Implementar normativas y técnicas de seguridad de la información.
- Desarrollo de un sistema experto de acuerdo al dominio planteado, para la implementación del mismo.
- Evaluar el sistema experto construido.

1.5. HIPÓTESIS

La implementación de un sistema experto en auditoria informática evalúa la seguridad de un sistema de información, lo que permitirá la identificación de vulnerabilidades, riesgos y amenazas.

1.5.1. Identificación de variables

Variable Independiente X: La auditoría informática de un sistema de Información por un sistema experto.

Variable dependiente Y: Identificar vulnerabilidades, riesgos y amenazas en la seguridad de un Sistema Informático.

1.6. ALCANCES Y LÍMITES

1.6.1. Alcance

El presente trabajo plantea el desarrollo de un de sistema experto, para una adecuada toma de decisión en el desarrollo de una auditoria informática de Sistemas de información en la

seguridad del Repositorio de Datos y Programas ejecutables, de tal modo que una persona no experta pueda aprovechar esta información.

1.6.2. Límites

La investigación se realiza en el campo de la Auditoria Informática, específicamente en el área de seguridad de la información y activos físicos. De acuerdo la clasificación la Norma ISO-IEC-27002, los activos son: información, recursos de software, recursos físicos, servicios, personas e intangibles; de los cuales se toma en cuenta: Información. Del mismo modo se establece los subdominios: Los Programas ejecutables y el Repositorio de Datos.

1.7. JUSTIFICACION

1.7.1. Técnica

El presente trabajo se justifica técnicamente por que proporciona una herramienta automatizada que permite identificar amenazas, riesgo y vulnerabilidades de los sistemas de información. Proporciona bastante información sobre metodología de desarrollo de sistemas expertos y métodos de adquisición del conocimiento en el conocimiento en el campo de la inteligencia artificial de una manera práctica.

1.7.2. Social

El presente trabajo beneficia especialmente a los auditores informáticos dotando a ellos de una herramienta para el desempeño de sus funciones. De la misma manera la organizaciones o instituciones en el resguardo de sus activos y en especial de la información que poseen.

1.7.3. Económica

La presente investigación es de suma importancia para una organización, ya que lo más importante que esta posee es su información, recuperarse de un desastre informático le resultaría más difícil y costoso.

1.8. METODOLOGIAS Y HERRAMIENTAS

Se utiliza la metodología de investigación científica deductiva:

a) **Observación.** Se realiza un relevamiento y teorización del diagnóstico de la seguridad de la información en los Sistemas Informáticos. Incluyendo el análisis del sistema experto.

b) **Planteo de la hipótesis.** Se plantea dar con un diagnóstico de la seguridad de la información mediante el sistema experto para su mantenimiento.

c) **Diseño de la aplicación.** Se procede al diseño de la solución al problema de toma de decisiones para el diagnóstico de la seguridad de la información.

d) **Casos de prueba.** Con el prototipo terminado se evalúa la calidad con un conjunto de casos de uso.

e) **Conclusiones.** Un informe relacionado con el desarrollo del prototipo para la toma de decisiones en el diagnóstico de la seguridad de la información de un Sistema Informático.

La ingeniería del conocimiento aborda el desarrollo de sistemas expertos como una actividad de modelado que conlleva la utilización de una metodología de desarrollo que asegure modelos bien formados en el nivel de conocimiento, para así poder manejar la complejidad de la construcción del nivel simbólico. Para el desarrollo del sistema experto se utiliza la metodología IDEAL, esta metodología pretende ajustarse a las tendencias con el software del futuro en lo concerniente a reutilización, integración, requisitos abiertos y diversidad de modelos computacionales teniendo en cuenta la ingeniería del software [Blum, B.I.; 1996]. Según Salvador (2006), la metodología IDEAL fue desarrollada tomando en cuenta metodologías anteriores incorporando los puntos fuertes de estas e intenta suplir los puntos débiles de las otras metodologías.

1.9. APORTES

Los aportes del presente trabajo son:

- Desarrollo de un Sistema Experto para realización de auditorías informáticas a la seguridad de la información de los sistemas de información.
- El uso de la metodología IDEAL para el modelado y desarrollo de sistemas expertos basados en conocimientos

CAPITULO II: MARCO TEORICO

En este capítulo se plantea la teoría relacionada con La Auditoria Informática, Seguridad de la Información y Sistemas Expertos, y la metodología a seguir.

2.1. AUDITORIA

2.1.1. Concepto

Con Frecuencia la palabra auditoría se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas. Por eso se ha llegado a usar la frase "tiene auditoría" como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoría. El concepto de auditoría es más amplio; no solo detecta errores: es un examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar cursos alternativos de acción para mejorar la organización y lograr objetivos propuestos [Echenique, 2001].

Proceso sistemático por el cual una persona competente e independiente, obtiene y evalúa objetivamente evidencia relativa a aseveraciones sobre una entidad o evento económico, con el propósito de formarse una opinión y reportar el grado en que la aseveración está acorde con un conjunto de estándares identificados [ISACA, 2009].

Conceptualmente la auditoría, toda y cualquier auditoría, es la actividad consistente en la emisión de una opinión profesional sobre si el sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas [Piattini, 2001]

2.1.2. Clases de Auditoria

La Auditoria se clasifica desde diversos puntos de vista: (a) por su amplitud, (b) por su frecuencia, (c) según el sujeto, (d) según el contenido y fines [Piattini, 2001].

a) Por amplitud:

- Auditoría total: Afecta a todos los elementos de la empresa.
- Auditoría parcial: Se concentra en determinados elementos de la empresa.

b) Por su frecuencia:

- Auditoría permanente: Se realiza periódicamente a lo largo del ejercicio económico.
- Auditoría ocasional: Se realiza de forma esporádica.

c) Según el sujeto que la efectúa:

- Auditoría interna: Está a cargo de empleados de la propia empresa, encuadrados en un departamento directamente dependiente de la dirección general.
- Auditoría externa: Está a cargo de auditores profesionales, ajenos a la empresa y totalmente independientes.

d) Por su contenido y fines:

- Auditoría de gestión: Afecta a la situación global de la empresa.
- Auditoría financiera: Examen y verificación de los estados financieros de la empresa, para emitir una opinión fundada sobre el grado de fiabilidad de dichos estados.

- Auditoría contable: Analiza la adecuación de los criterios empleados para recoger los hechos derivados de la actividad de la empresa y su representación, mediante apuntes contables, en los estados financieros.

- Auditoría operacional: determina hasta qué punto una organización, una unida o función dentro de una organización, cumple con lo objetivos establecidos por la gerencia; así como identificar la condiciones que necesiten mejora.

Se extiende a todas las áreas o campos de trabajo como ser:

- Auditoría organizativa: Analiza si la estructura organizativa de la empresa es la adecuada, según las necesidades y problemas de la misma.

- Auditoría informática: Examen y verificación del correcto funcionamiento y control del sistema informático de la empresa.

En otras palabras se acepta el término de Auditoría para cualquier actividad que implique revisión, evaluación, análisis, estudio, exposición de deficiencias y propuestas de medidas para solucionar o eliminar las mismas. En muchos casos, las fronteras éntrelos tipos de auditoría no están bien definidos.

2.2. AUDITORIA INFORMATICA

Según Ron Weber en Auditing Conceptual Foundations and Practice, la auditoria informática "es la revisión y evaluación de los controles, sistemas y procedimientos de los equipos de cómputo, su utilización, eficiencia y seguridad; de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente, confiable y segura de la información que sirva para una adecuada toma de decisiones" [Echenique, 2001].

Al hablar de sistemas informatizados se considera la siguiente definición de auditoría de sistemas informáticos. Proceso de recolección y evaluación de evidencia para determinar si los sistemas de información y los recursos relacionados:

- salvaguardan adecuadamente los activos,
- mantienen la integridad del sistema,
- proveen información relevante y confiable,
- alcanzan efectivamente los objetivos organizacionales,
- consumen los recursos eficientemente, y
- cuentan con controles internos que provean una seguridad de que los objetivos operacionales y de control serán satisfechos y de que los eventos no deseados serán prevenidos o detectados y corregidos de manera oportuna [ISACA, 2013].

2.3. SEGURIDAD INFORMATICA

Debido a que el uso de internet se encuentra en aumento, cada vez más compañías permiten a sus socios y proveedores acceder a sus sistemas de información.

Por lo tanto, es fundamental saber qué recursos de la compañía necesitan protección para así controlar el acceso al sistema y los derechos de los usuarios del sistema de información. Los mismos procedimientos se aplican cuando se permiten el acceso a la compañía a través.

La amenaza representa el tipo de acción que tiende a ser dañina, mientras que la vulnerabilidad representa el grado de exposición a las amenazas en un contexto particular. Finalmente, la contramedida representa todas las acciones que se implementan para prevenir la amenaza.

Para que un sistema sea seguro deben identificarse las posibles amenazas y por lo tanto, conocer y prever el curso de acción del enemigo

2.4. CONTROL INTERNO

El Control Interno informático controla diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijados por la Dirección de la Organización y/o la Dirección de Informática, así como los requerimientos legales [Piattini, 2001].

Como principales objetivos podemos indicar los siguientes:

- Controlar que todas las actividades se realizan cumpliendo los procedimientos y normas fijados, evaluar su bondad y asegurarse del cumplimiento de las normas legales.
- Asesorar sobre el cumplimiento de las normas.
- Colaborar y apoyar el trabajo de Auditoría Informática, así como de las auditorías externas al grupo.
- Definir, implantar y ejecutar mecanismos y controles para comprobar el logro de los grados adecuados del servicio de informática, lo cual no debe considerarse como que la implantación de los mecanismos de medida y la responsabilidad del logro de esos niveles se ubique exclusivamente en la función de Control Interno, sino que cada responsable de objetivos y recursos es responsable de esos niveles, así como de la implantación de los medios de medida adecuados.

2.5. SEGURIDAD DE LOS PROGRAMAS EJECUTABLES

Son tres puntos medulares para mencionar relacionados con la seguridad de los programas ejecutables, ellos son auditoría de código fuente, log de aplicaciones y validaciones.

2.5.1. Auditoría de código.

La auditoría consiste en registrar determinadas acciones vitales para la seguridad de la información en un dominio dado. El proceso de auditar operaciones es útil para controlar la secuencia de eventos que involucró un acto de ataque o para identificar a un usuario malicioso. La auditoría se puede llevar a cabo durante la autenticación, los cierres de sesión y los accesos a determinados recursos.

Existen varios mecanismos, entre ellos la inyección de fallas a un sistema y la auditoría de código fuente propiamente dicha. El primer mecanismo denominado *fuzzing* es un proceso automático por el cual se ingresan datos a la aplicación y a través de los resultados devueltos se evalúan las vulnerabilidades.

La auditoría de programas fuente, se utiliza mayormente para detectar vulnerabilidades muy complejas. Esta tarea puede insumir mucho tiempo y requiere un gran conocimiento del lenguaje auditado así como del proceso de negocio que involucra el programa.

"Las mejores prácticas indican que una revisión de código puede generar reportes indicando qué es necesario hacer para mejorar la seguridad de las aplicaciones.

2.5.2. Log de Aplicaciones

Se debe llevar a cabo una adecuada gestión y análisis de log de las aplicaciones. La información que se registra en el proceso de auditoría puede variar de acuerdo a las políticas de seguridad de la información que se adopte en la organización. Los especialistas en seguridad de la información deben ajustar varias fases del ciclo de desarrollo de software que garanticen que la aplicación registrará los datos correctos a fin de cumplir con los requerimientos normativos y operativos. Entre los datos a registrar se pueden mencionar:

- Clase de evento
- Identidad del usuario
- Identificación del recurso al que se intentó acceder

- Identificación de la acción que intentó llevar a cabo
- Permiso requerido para tener acceso al recurso
- Ubicación desde donde se intentó acceder al recurso
- Fecha y hora de acceso
- Datos del proceso que se actualizaron en caso de tener un acceso exitoso. En ese punto es importante remarcar que la información a ser registrada deberá ser estipulada, por el propietario de la misma, en función de su criticidad.

Los registros de auditoría se utilizan para dar evidencia relacionadas con las acciones que pueden ser vitales para la seguridad, por lo tanto el resguardo de los registros también debe ser vital. Por esta razón los registros se deben proteger adecuadamente para que sólo puedan ser accedidos por quienes deban verificar las pistas de auditoría y se debe evitar que usuarios maliciosos puedan corromperlos o cambiar la información que contienen.

Cabe destacar que para poder efectuar una adecuada trazabilidad de la seguridad de una aplicación no solo es importante contar con una buena administración de registros de auditoría sino con carpetas operativas estandarizadas que se alineen con los requerimientos que exigen los especialistas en seguridad de la información. Las carpetas operativas deben respetar los formatos establecidos y vigentes en la organización, y estar disponibles para todos los involucrados en el proceso de desarrollo de software en el momento requerido.

2.5.3. Validaciones

No sólo es importante validar datos entrantes contra patrones de aceptación y rechazo, también deben validarse los datos de salida, se debe controlar que no se exhiba información sobre la estructura interna de los programas. A su vez, es recomendable evaluar todas las interfaces, no sólo las expuestas al usuario sino también aquellas que relacionan programas. En relación a los patrones mencionados anteriormente se pueden mencionar dos tipos:

- Patrones de aceptación: los datos ingresados se examinan contra patrones de aceptación, haciéndolos más selectivos si se manifiestan nuevas vulnerabilidades. En caso de que ninguno de los patrones sea satisfecho, los datos se rechazan.
- Patrones de rechazo: los datos ingresados se prueban contra patrones de rechazo, sumando patrones a medida que se descubren nuevas vulnerabilidades. En caso de que ninguno de los patrones sea satisfecho los datos se aceptan.

Cada uno de estos métodos tiene ventajas y desventajas. Si bien el patrón de rechazo resulta más fácil al momento de agregar nuevos modelos, requiere pruebas adicionales para cada patrón. El patrón de aceptación se considera más claro y genérico. Por este motivo es el modelo recomendable dado que trabaja reduciendo los patrones de aceptación, siendo así un esquema más proactivo y factible de mantener, así como menos propenso a generar errores.

2.6. SEGURIDAD DE DATOS

La seguridad de la información se define como la preservación de:

- Confidencialidad. Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.
- Integridad. Garantía de la exactitud y completitud de la información y de los métodos de su procesamiento.
- Disponibilidad. Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados. [ISO 27002, 2007]

En relación a la protección de datos, es significativo subrayar que se pretende proteger un "intangible", y normalmente lo más valioso de una empresa: la información. El objetivo es restringir las fugas incontroladas y permitir la detección de las mismas en caso de que se originen, a través de procedimientos estandarizados. El acceso indisciplinado a la información es la raíz de conflictos imprevistos, dado que valorar el efecto que produciría en un tercero una determinada información, es casi imposible; toda la información debería

ser objeto de protección frente a fugas incontroladas, incluso aquella información considerada inútil o no productiva.

Para permitir que los datos permanezcan seguros y sean accedidos sólo por aquellos usuarios autorizados, garantizando los principios básicos de seguridad de la información: integridad, confidencialidad y disponibilidad deben existir procedimientos claramente establecidos relacionados con el resguardo y recupero de la información, la clasificación de datos y seguridad en las Bases de Datos, así como tecnologías de soporte entre las que se pueden mencionar hash y encripción de datos.

2.6.1. Procedimientos relacionados con la seguridad de los datos

a) **Resguardo y recupero**, en relación a la seguridad de los datos, no se debería pasar por alto dónde residen los mismos. El entorno de almacenamiento podrá ser centralizado o distribuido, al momento de mantener los datos seguros se deberán evaluar las particularidades de las distintas arquitecturas.

   Se debe garantizar que los datos se encuentren en el lugar indicado, en el momento requerido por los usuarios autorizados, para ello se deberá planificar una adecuada estrategia de resguardo y recupero. Los elementos básicos en un correcto plan de disponibilidad de datos son:

   - Planificar el futuro.
   - Comprender los riesgos que involucran las transacciones y saber cómo utilizarlos para restaurar los datos.
   - Tener una política de resguardo estandarizada.
   - Realizar copias de resguardo, administrarlas y almacenarlas debidamente.
   - Mantener copias de seguridad completas en un lugar seguro.
   - Efectuar periódicamente comprobaciones de consistencia de acuerdo a un plan de contingencia estandarizado a fin de restaurar los datos en caso de posibles fallas.

Se debe incluir en este contexto el resguardo de archivos de configuración que no contiene información directamente vinculada con los datos de negocios. Dado que muchas aplicaciones utilizan archivos personalizados para incluir aspectos de configuración tales como nombres de usuarios impersonados y sus contraseñas y cadenas de conexión a Bases de Datos entre otros, estos archivos deben ser rigurosamente almacenados y resguardados a fin de evitar que accedan usuarios malintencionados.

b) Clasificación de datos, los datos que conforman la estructura de las aplicaciones así como la información brindada por las mismas, deben ser clasificados según distintos niveles de criticidad y sensibilidad y administrados cuidadosamente indicando grados de protección. En una organización con un alto nivel de madurez en términos de seguridad de la información se debe contar con usuarios responsables, también denominados propietarios de datos, que establezcan y avalen lineamientos claros relacionados con la clasificación de los datos y la información.

Un esquema de clasificación básico para datos e información puede ser el siguiente:

- Público. Abarca aquellos datos e información cuya divulgación al público en general se considera apropiada.
- Confidencial. Comprende todo dato o información distribuido a determinadas personas, dentro o fuera de la organización, cuya exposición debe ser implementada, controlada y administrada por todo el personal responsable de la seguridad de la información.

2.7. METODOLOGIA COBIT

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de plan, construir, ejecutar y Monitorear. Dentro del marco COBIT estos dominios, como es muestra en la figura

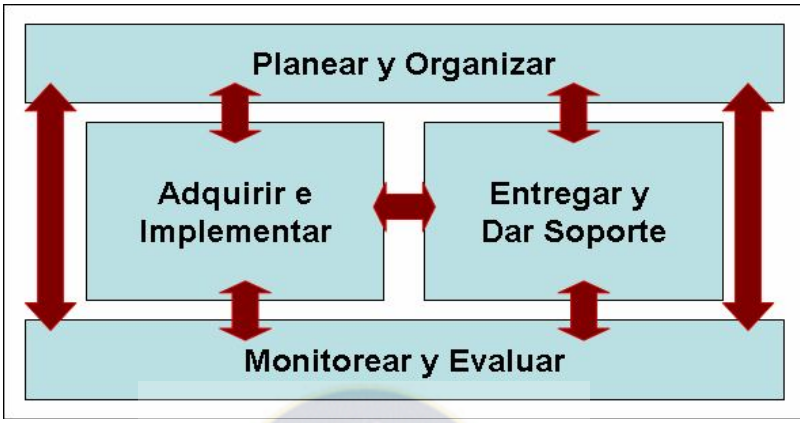


FIG. 1 LOS CUATRO DOMINIOS INTERRELACIONADOS DE COBIT
FUENTE: [COBIT 4.1, 2005]

- **Planear y Organizar (PO).** Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.

- **Adquirir e Implementar (AI).** Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

- **Entregar y Dar Soporte (DS).** Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluya la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.

- **Monitorear y Evaluar (ME).**Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de

control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.

A lo largo de estos cuatro dominios, COBIT ha identificado 34 procesos de TI generalmente usados. Mientras la mayoría de las empresas ha definido las responsabilidades de planear, construir, ejecutar y monitorear para TI, y la mayoría tiene los mismos procesos claves, pocas tienen la misma estructura de procesos o le aplicaran los 34 procesos de COBIT.

Para cada uno de estos 34 procesos, tienen un enlace a las metas del negocio y TI que soporta. Información de cómo se pueden medir las metas, también se proporcionan cuáles son sus actividades claves y entregables principales, y quién es el responsable de ellas.

2.8. INTELIGENCIA ARTIFICIAL

La Figura presenta definiciones de inteligencia artificial extraídas. A lo largo de la historia se han seguido los cuatro enfoques mencionados. Como es de esperar, existe un enfrentamiento entre los enfoques centrados en los humanos y los centrados en torno a la racionalidad. El enfoque centrado en el comportamiento humano debe ser una ciencia empírica, que incluya hipótesis y confirmaciones mediante experimentos. El enfoque racional implica una combinación de matemáticas e ingeniería. Cada grupo al mismo tiempo ha ignorado y ha ayudado al otro. A continuación revisaremos cada uno de los cuatro enfoques con más detalle.

Sistemas que piensan como humanos	Sistemas que piensan racionalmente
"El nuevo y excitante esfuerzo de hacer que los computadores piensen….maquinas con mentes, en el más alto sentido literal"	"El estudio de las facultades mentales mediante el uso de modelos computacionales"
Sistemas que actúan como humanos	**Sistemas que actúan racionalmente**
"El arte de desarrollar maquinas con capacidad para realizar funciones que cuando son realizadas por personas requieren inteligencia"	"La inteligencia computacional es el estudio del diseño de agentes inteligentes"

FIG. 2 DEFINICIONES DE INTELIGENCIA ARTIFICIAL
Fuente: [Russell y Norvig, 2004]

2.8.1. Sistemas Expertos

En la literatura existente se pueden encontrar muchas definiciones de sistema experto. Por ejemplo, Stevens, da la siguiente definición: "Los sistemas expertos son máquinas que piensan y razonan como un experto lo haría en cierta especialidad o en cierto campo. Un Sistema Experto de verdad, no solo realiza las funciones tradicionales de manejar grandes cantidades de datos, sino que también manipula esos datos de forma tal que el resultado sea inteligible y tenga significado para responder a preguntas incluso no completamente especificadas.

Aunque la anterior es toda una definición razonable de un sistema experto, han surgido desde entonces otras definiciones, debido al rápido desarrollo de la tecnología. "Un Sistema experto puede definirse como un sistema informático (hardware y software) que simula a los expertos humanos en un área de especialización dada".

Como tal, un sistema experto debería ser capaz de procesar y memorizar información, aprender y razonar en situaciones deterministas e inciertas, comunicar con los hombres y/u otros sistemas expertos, tomar decisiones apropiadas, y explicar por qué se han tomado tales decisiones. Se puede pensar también en un sistema experto como un consultor que

puede suministrar ayuda a (o en algunos casos sustituir completamente) los expertos humanos con un grado razonable de fiabilidad [Castillo, 2000].

2.8.2. Tipos de Sistemas Expertos

Los problemas con los que pueden tratar los sistemas expertos pueden clasificarse en dos tipos: problemas esencialmente deterministas y problemas esencialmente estocásticos.

Consecuentemente, los sistemas expertos pueden clasificarse en dos tipos principales según la naturaleza de los problemas para los que están diseñados: deterministas y estocásticos. Los problemas de tipo determinista pueden ser formulados usando un conjunto de reglas que relacionen varios objetos bien definidos. Los sistemas expertos que tratan problemas deterministas son conocidos como sistemas basados en reglas, por que sacan sus conclusiones sus conclusiones basándose en un conjunto de reglas utilizando un mecanismo de razonamiento lógico.

- **Sistemas Expertos basado en reglas**, la construcción de la base de conocimiento es en base a reglas, lo cual, en algunos casos se elabora sencillamente, la explicación de las conclusiones es simple. El motor de inferencia se realiza con algoritmos complejos, lo cual es relativamente lento, además que el aprendizaje estructural es complejo.
- **Sistemas Expertos basado en probabilidades,** la construcción de la base de conocimiento es en base a frecuencias lo cual requiere de mucha información, la explicación de las conclusiones resulta más compleja. El motor de inferencia se realiza con algoritmos simples, el aprendizaje paramétrico es sencillo

2.8.3. Componentes de un Sistema Experto

Los componentes se muestran esquemáticamente en la figura y se explican seguidamente:

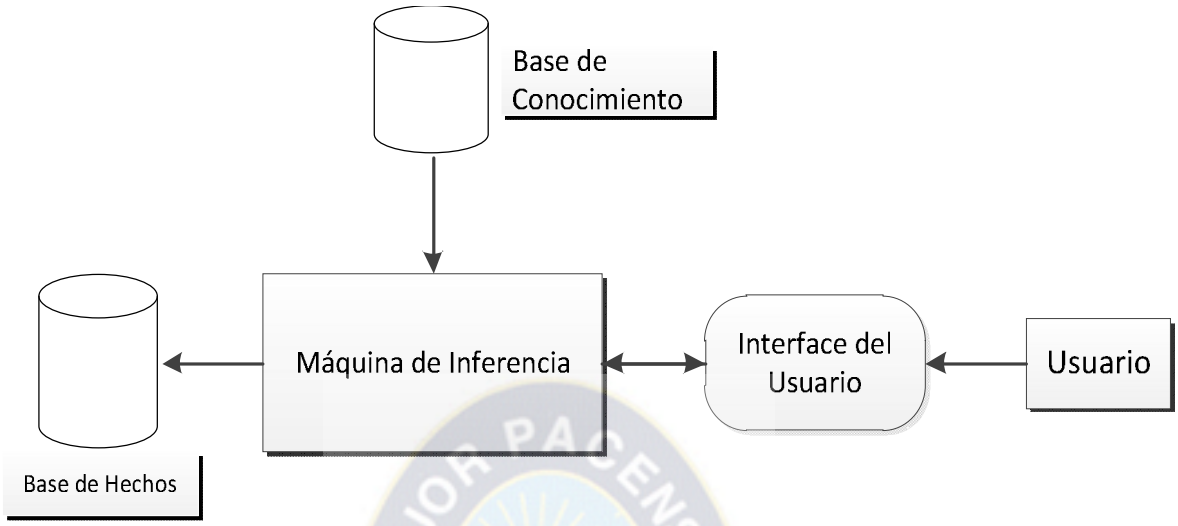


FIG. 3 COMPONENTES DE UN SISTEMA EXPERTO
Fuente: [Lahoz, 2004]

A continuación se explica de forma individual cada uno de los componentes:

- **Base de Conocimiento,** la base de conocimiento contiene el conocimiento especializado extraído del experto en el dominio. Es decir, contiene conocimiento general sobre el dominio en el que se trabaja. El método más común para representar el conocimiento es mediante reglas de producción. El dominio de conocimiento representado se divide en pequeñas partes de conocimiento (reglas). Cada regla consta de una parte denominada condición y de una parte denominada acción. Cuando el conocimiento almacenado queda obsoleto o se dispone de conocimiento nuevo, es relativamente fácil añadir reglas nuevas, eliminar las antiguas o corregir errores en las existentes. Según Samper (2005), las reglas suelen almacenarse en alguna secuencia jerárquica lógica pero esto no es estrictamente necesario. Se pueden tener en cualquier secuencia y la máquina de inferencia las usará en el orden adecuado que necesite para resolver un problema.

  Según Samper (2005), existen reglas de producción que no pertenecen al dominio del problema. Estas reglas se llaman meta reglas y su función es indicar bajo que condición deben considerarse unas reglas en lugar de otras

- **Base de Datos o Base de Hechos,** es una parte de la memoria de la computadora que se utiliza para almacenar los datos recibidos inicialmente para la resolución de un problema. Contiene conocimiento sobre el caso concreto en el que se trabaja. También se registra en ella las conclusiones intermedias y los datos generados en el proceso de inferencia. Al memorizar todos los resultados intermedios, conserva el vestigio de los razonamientos efectuados; por lo tanto, se puede utilizar para explicar las deducciones y el comportamiento del sistema [Samper, 2005].

- **Máquina de Inferencia,** según Samper (2005), es un programa que controla el proceso de razonamiento que seguirá el sistema experto. Utilizando los datos que se le suministran, recorre la base de conocimiento para alcanzar una solución. La estrategia de control puede ser de encadenamiento hacia adelante o encadenamiento regresivo.

  La Técnica de encadenamiento hacia adelante extrae conclusiones a partir del cumplimiento de las condiciones de ciertas reglas. Esta estrategia se denomina "encadenamiento hacia adelante" o "razonamiento de datos dirigidos", comienza con los datos conocidos y aplica el modus ponens sucesivamente hasta obtener los resultados que se requieren. La base de conocimiento y el sistema no dependen del orden en el que las reglas son establecidas, almacenadas o procesadas. Esta técnica suele utilizarse cuando la cantidad de datos es potencialmente grande, y resulta de interés algún conocimiento específico que se toma en consideración.

  El modus ponens es la regla de inferencia comúnmente utilizada, se utiliza para obtener conclusiones simples. Se examina la premisa de la regla y si es cierta, la conclusión pasa a formar parte del conocimiento. Como ilustración, supóngase que se tiene la regla "SI A es cierto, entonces B es cierto" y se sabe además que " A es cierto". Entonces tal como muestra la figura, la regla modus ponens concluye que "B es cierto". Esta regla de inferencia que parece trivial debido a su familiaridad, es la base de un gran número de sistemas expertos, es decir que necesita información de los objetos de la premisa para concluir [Castillo, 2005].

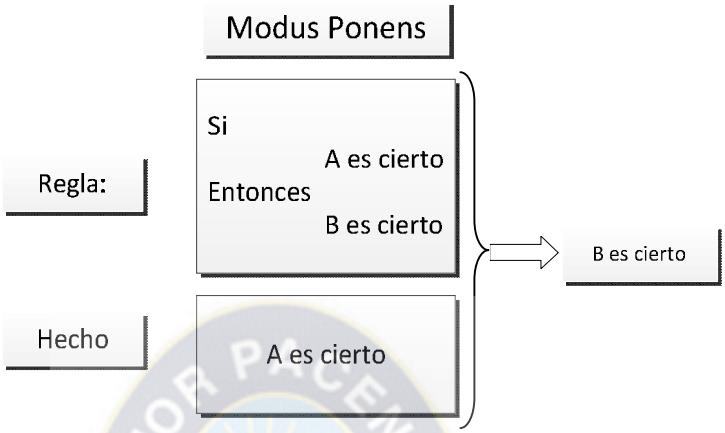


FIG. 4 REGLA DE INFERENCIA MODUS PONENS.
Fuente: [Castillo, 2005]

- **Interfaz Hombre – Máquina,** la interfaz de usuario es el enlace entre el sistema experto y el usuario. Por ello, para que un sistema experto sea una herramienta efectiva, debe incorporar mecanismos eficientes para mostrar y obtener información de forma fácil y agradable. Un ejemplo de la información que tiene que ser mostrada tras el trabajo de la máquina de inferencia, es el de las conclusiones, las razones que expliquen tales conclusiones y una explicación de las acciones iniciadas por el sistema experto. Por otra parte, cuando la máquina de inferencia no puede concluir debido, por ejemplo, a la ausencia de información, la interfaz de usuario debe obtener la información necesario del usuario [Castillo, 2005].

2.8.4. Control de la coherencia

En situaciones complejas, incluso verdaderos expertos pueden dar información inconsistente (por ejemplo, reglas inconsistentes, combinaciones de hechos no factibles). Por ello es muy importante controlar la coherencia del conocimiento en la construcción de la base de conocimiento y en los procesos de adquisición de datos y razonamiento. Si la información de hechos y reglas contiene información inconsistente, es muy probable que el

sistema experto se comporte forma poco satisfactoria y obtenga conclusiones absurdas. El objetivo del control de la coherencia consiste en:

a) Ayudar al usuario a no proporcionar hechos inconsistentes, por ejemplo, indicando al usuario las restricciones que debe satisfacer la información demandada.

b) Evitar que ingrese en la base de conocimiento cualquier tipo de conocimiento inconsistente o contradictorio.

El control de la coherencia debe hacerse controlando la coherencia de las reglas y delos hechos [Gutiérrez, 2006].

2.8.4.1. Coherencia de reglas

Un conjunto de reglas se denomina coherente si existe, al menos, un conjunto de valores de todos los objetos que producen conclusiones no contradictorias. En consecuencia, un conjunto coherente de reglas no tiene por qué producir conclusiones no contradictorias para todos los posibles conjuntos de valores de los objetos.

2.8.4.2. Coherencia de hechos

Los datos o evidencias suministrados por los usuarios deben ser consistentes. Por ello, el sistema no debe aceptar hechos que contradigan el conjunto de reglas y el conjunto de hechos existente en cada instante del proceso. El sistema debe también comprobar si existe o no, una solución factible e informar al usuario en consecuencia, la inconsistencia surge de que los hechos y la reglas sean inconsistentes [Gutiérrez, 2006].

2.8.5. Equipo de Desarrollo

Según Criado (2005), las personas que componen un grupo o un equipo, como en todos los ámbitos deben cumplir unas características y cada uno de ellos dentro del equipo desarrolla un papel distinto. A continuación se detalla cada componente del equipo dentro del desarrollo y cuál es la función de cada uno:

a) Experto.- La función del experto es la de poner su conocimiento especializado a disposición del sistema experto.

b) Ingeniero del Conocimiento.- Plantea las preguntas al experto, formaliza el conocimiento y los implementa en la base de conocimiento.

c) Usuario.- El usuario aporta sus deseos y sus ideas, determinando especialmente el escenario en el que debe aplicarse el sistema experto.

En el desarrollo del sistema experto, el ingeniero del conocimiento y el experto trabajan muy unidos. El primer paso consiste en elaborar los problemas que deben ser resueltos por el sistema. Precisamente en la primera fase de un proyecto es de vital importancia determinar correctamente el ámbito estrechamente delimitado de trabajo. Aquí se incluye ya el usuario posterior, o un representante del grupo de usuarios. Una vez delimitado el dominio, se ampliara el sistema con el conocimiento del experto. El experto debe comprobar constantemente si su conocimiento ha sido transmitido de la forma más conveniente. El ingeniero del conocimiento es el responsable de una implementación correcta, pero no de la exactitud del conocimiento. La responsabilidad de esta exactitud recae en el experto. De ser posible, el experto debe tener comprensión para los problemas que depara el procesamiento de datos. Ello facilita mucho el trabajo. Además, no debe ignorarse nunca al usuario durante el desarrollo, para que al final se disponga de un sistema que le sea de máxima utilidad. La estricta separación entre usuario, experto e ingeniero del conocimiento no deberá estar siempre presente. Pueden surgir situaciones en las que el experto puede ser también el usurario [Criado, 2005].

2.8.6. Ingeniería del conocimiento

La ingeniería del conocimiento es aquella disciplina moderna que forma parte de la inteligencia artificial y cuyo fin es el diseño y desarrollo de sistemas expertos o sistemas basados en conocimiento. El ingeniero del conocimiento debe cerciorarse que la computadora disponga del conocimiento necesario para la solución de problemas. El ingeniero de conocimiento debe elegir una o más formas en las cuales representar el

conocimiento requerido como patrones de símbolos en la memoria de la computadora (representación del conocimiento), también debe asegurarse de que la computadora pueda utilizar el conocimiento de manera eficiente mediante métodos de razonamiento [Castillo, 2005].

La ingeniería del conocimiento es una parte aplicada de la inteligencia artificial que, a su vez, es pate de la informática. Teóricamente, entonces, un ingeniero del conocimiento es un informático que sabe diseñar y poner programas en ejecución que incorporan técnicas de inteligencia artificial. Un Ingeniero del conocimiento se entrevista y observa a una persona experta o a un grupo de expertos y aprende lo que ellos saben y como razón con su conocimiento. El ingeniero entonces traduce el conocimiento a un lenguaje útil para la computadora y diseña una máquina de inferencia, una estructura del razonamiento que utilice apropiadamente el conocimiento. El también determina como integrar el uso del conocimiento incierto en el proceso del razonamiento y que clase de explicación será útil para el usuario final. El conocimiento del dominio consiste en conocimiento formal, los libros de textos, el conocimiento experimental y el talento de los expertos [Pignani, 2006]

2.8.7. Desarrollo de un Sistema Experto

Se sugieren las siguientes etapas para el diseño e implementación de un sistema experto:

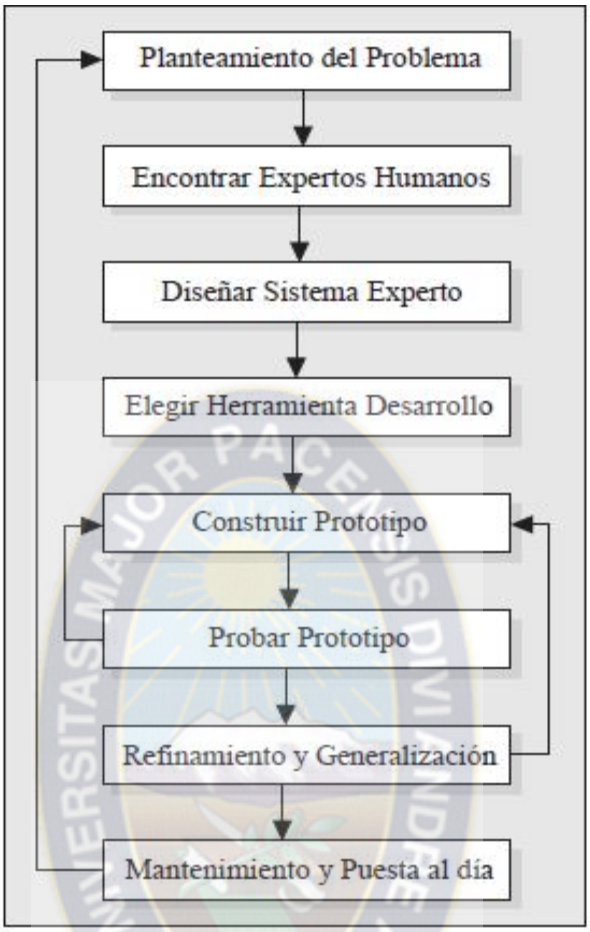


FIG. 5 ETAPAS DEL DESARROLLO DE UN SISTEMA EXPERTO
Fuente: [Castillo, 2005]

- **Planeamiento del problema.** La primera etapa en cualquier proyecto es normalmente la definición del problema a resolver. Puesto que el objetivo principal de un sistema experto es responder a preguntas y resolver problemas, esta etapa es quizás la más importante en el desarrollo de un sistema experto. Si el sistema está mal definido, se espera que el sistema suministre respuestas erróneas.

- **Encontrar expertos humanos que puedan resolver el problema.** En algunos casos, sin embargo, las bases de datos pueden jugar el papel del experto humano.

- **Diseño de un sistema experto.** Esta etapa incluye el diseño de estructuras para almacenar el conocimiento, el motor de inferencia, el subsistema de explicación, la interfase de usuario, etc.

- **Elección de la herramienta de desarrollo, concha, o lenguaje programación.** Debe decidirse si realizar un sistema experto a medida, o utilizar una concha, una herramienta, o un leguaje de programación.

- **Desarrollo y prueba de un prototipo.** Si el prototipo no pasa las pruebas requeridas, las etapas anteriores (con las modificaciones apropiadas) deben ser repetidas hasta que se obtenga un prototipo satisfactorio.

- **Refinamiento y generalización.** En esta etapa se corrigen los fallos y se incluyen nuevas posibilidades no incorporadas en el diseño inicial.

- **Mantenimiento y puesta al día.** En esta etapa el usuario plantea problemas o defectos del prototipo, corrige errores, actualiza el producto con nuevos avances, etc.

2.8. DISEÑO METODOLÓGICO

Para la elaboración del presente trabajo se empleara el Método Científico, que tiene los siguientes pasos:

- Observación.- Consiste en el estudio de un fenómeno que se produce en sus condiciones naturales. La observación de be ser cuidadosa, exhaustiva y exacta.

- Identificación del problema.- A partir de la observación surge la identificación del problema que se va a estudiar, lo que lleva a emitir alguna hipótesis.

- Hipótesis.- O suposición provisional de la que se intenta extraer una consecuencia. Una hipótesis confirmada se puede transformar en una ley científica que establezca una relación entre dos o más variables, y al estudiar un conjunto de leyes se puede

hallar algunas regularidades entre ellas que den lugar a unos principios generales con los cuales se constituya una teoría.

- Experimentación.- Consiste en el estudio de un fenómeno, en las condiciones particulares de estudio que interesan, eliminando o introduciendo aquellas variables que puedan influir en él. Se entiende por variable todo aquello que pueda causar cambios en los resultados de un experimento y se distingue entre variable independiente, dependiente y controlada.

- Resultados.- Los resultados de un experimento pueden describirse mediante tablas, gráficos y ecuaciones de manera que puedan ser analizados con facilidad y permitan encontrar relaciones entre ellos que confirmen o no las hipótesis emitidas.

2.9. METODOLOGIA DE DESARROLLO DE SISTEMAS EXPERTOS

Para el diseño del sistema experto se utilizará la metodología IDEAL pretende ajustarse a las tendencias relacionadas con el software del futuro en lo que concierne a la reutilización, integración, requisitos abiertos y diversidad de modelos computacionales [Salvador, 2006].

La Metodología IDEAL, incorpora un ciclo de vida en espiral cónico en tres dimensiones (espiral troncocónico), el modelo está basado por una parte en la idea de Spengler retomada por Barthlomew, empleada para mostrar los ciclos históricos de la geología terrestre y la base en un modelo en espiral en la que cada fase del ciclo de vida finaliza con un prototipo, la tercera dimensión representa el mantenimiento perfectivo que se produce por la incorporación de conocimiento una vez implantado el conocimiento [Boehm, B.W.;1987].

Al inicio del funcionamiento del sistema se obtienen grandes cantidades de conocimiento de distinta calidad pero a medida que el sistema se usa, el conocimiento se refina, se obtiene menos conocimiento, pero de mayor calidad como se muestra en la figura. Los ejes de la base del cono representan el costo y el tiempo, el eje de la calidad se representa de abajo hacia arriba, va de mayor diámetro, o sea conocimiento menos específicos y de menor calidad, conocimientos más exactos y de mayor calidad.

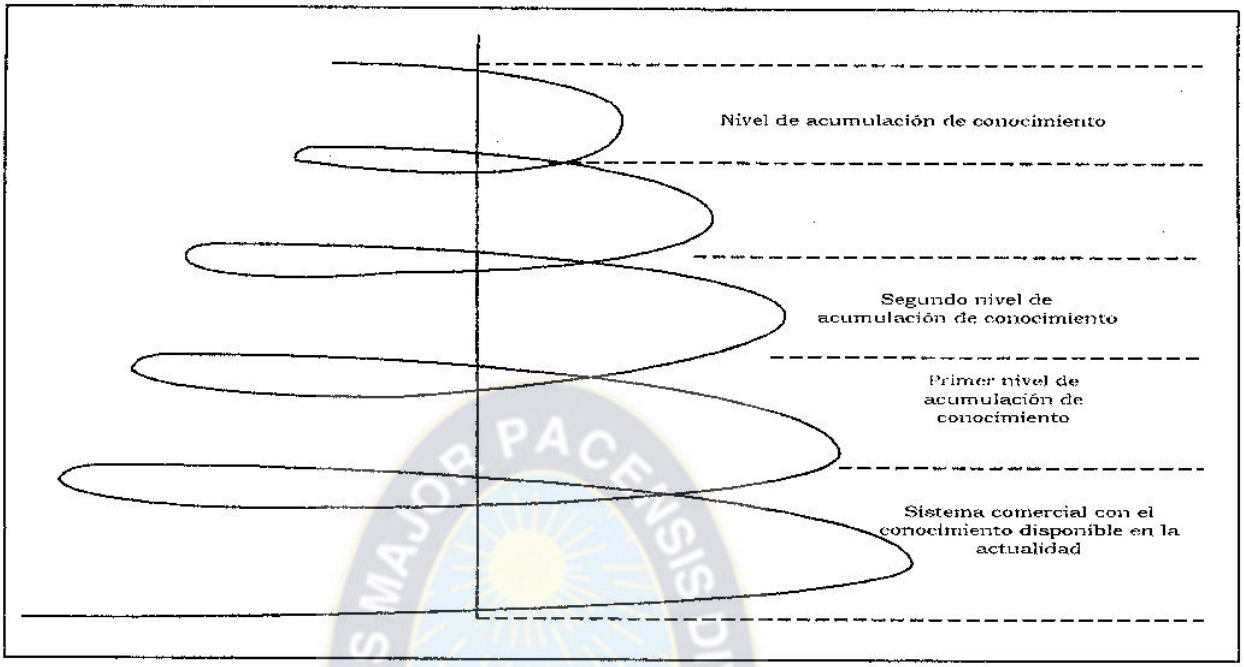


FIG. 6 MODELO TRONCOCÓNICO – EJE DE CALIDAD
Fuente: [Salvador, 2006]

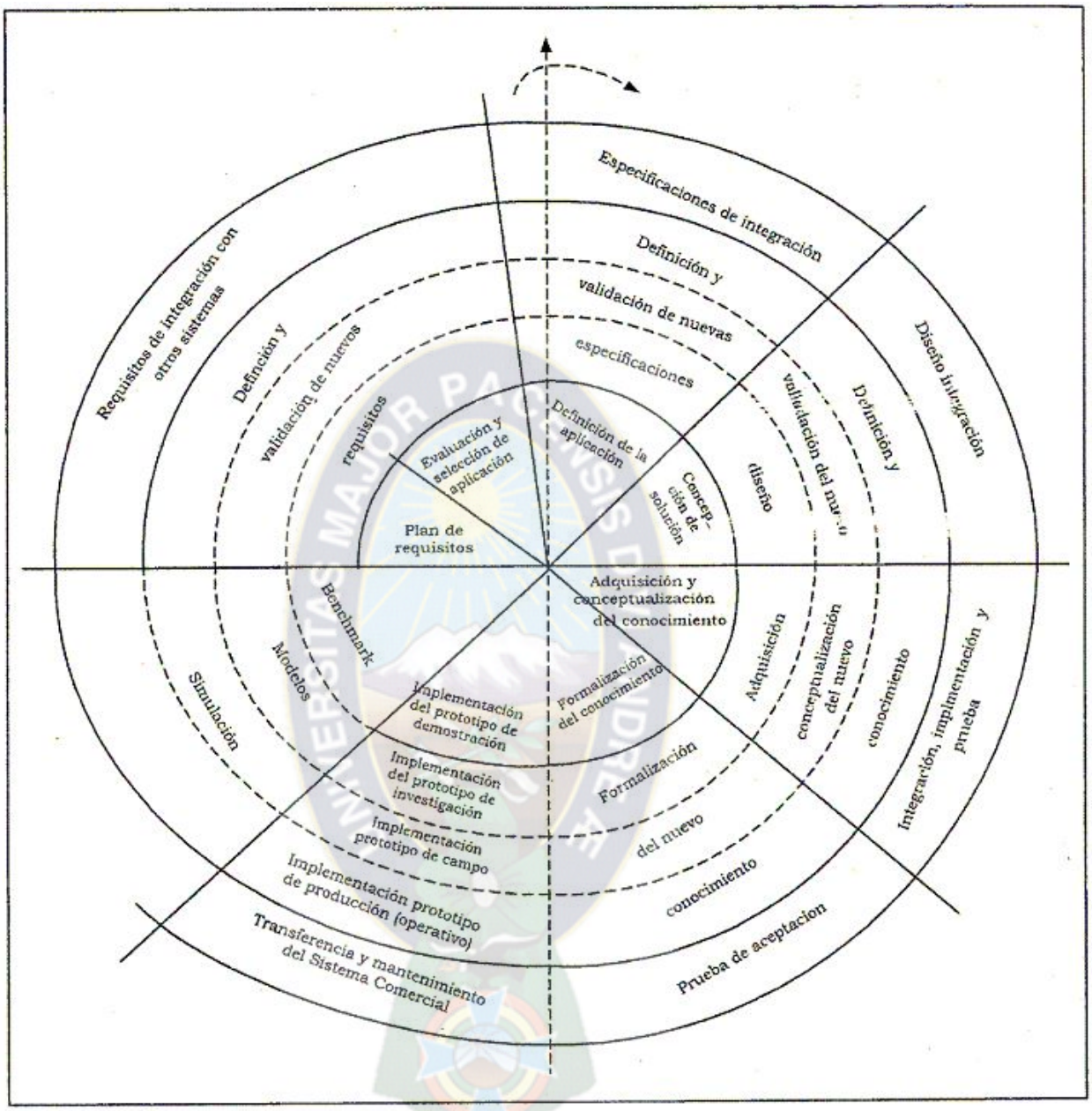


FIG. 7 MODELO TRONCOCÓNICO BASE
Fuente: [Salvador, 2006]

Las fases que componen las Metodología IDEAL se describen a continuación [Gómez, A. et al ;1997]:

- **Fase I**: Identificación de la tarea. Esta etapa considera los objetivos del proyecto del sistema experto (SE). Involucra el proceso de adquisición de conocimiento. Aplicado al problema a resolver, significará adquirir el conocimiento necesario en lo referente al marco regulatorio para seguridad informática, así como hacer educción de expertos en esta materia.
- **Fase II**: Desarrollo del prototipo. Es la etapa principal de la metodología. Continuará con la adquisición de conocimientos, la viabilidad del sistema y llegará a la conceptualización y formalización de los conocimientos e implementación del prototipo que permitirá validar con el experto el modelo de SBC.
- **Fase III**: Ejecución de la construcción del sistema integrado. Esto significa integrar un sistema experto (SE) dentro de un sistema general.
- **Fase IV**: Actuación para conseguir el mantenimiento perfectivo sobre el conocimiento. Se basará en la incorporación de nuevos conocimientos. Habrá una equiparación entre la participación del usuario y la devolución a través de las respuestas del sistema, lo que servirá para el mantenimiento actualizado del conocimiento.
- **Fase V**: Lograr una adecuada transferencia tecnológica. Comprenderá la actualización continua del conocimiento y su explicitación.

El desarrollo del presente trabajo abarca las fases I y II de la metodología IDEAL (para el desarrollo del sistema experto), teniendo en cuenta que la propuesta es de construcción de un prototipo de sistema experto para la auditoria informática a la seguridad de la información.

a) Fase I. Identificación de la tarea

La fase I considera la definición de los objetivos del proyecto del sistema experto y determinar si la tarea asociada es susceptible de ser tratada con la tecnología de Ingeniería del Conocimiento. En caso afirmativo se definen las características del problema, se especifican los requisitos que enmarcan la solución del problema. Esta fase se subdivide en las siguientes etapas:

i. **Etapa I.1. Plan de requisitos y adquisición de conocimiento**.- lo primero que debe hacer el ingeniero de conocimiento es tratar de identificar las necesidades del cliente describiendo para ello, los objetivos del sistema.

Estos objetivos pueden ser:

- Finalidades de carácter filosófico.
- Fines, de carácter cualitativo.
- Metas u objetivos a plazo fijo, de carácter cuantitativo.

Además se debe determinar qué información se va a obtener y suministrar, funcionalidades a exigir y requisitos necesarios para todo ello. Los parámetros fundamentales de este plan de requisitos son:

- Fines específicos y generales del sistema.
- Funcionamiento y rendimiento requeridos.
- Fiabilidad y calidad.
- Limitaciones de costo/tiempo.
- Requisitos de fabricación.
- Tecnología disponible.
- Competencia
- Ampliaciones futuras.

Para confeccionar el plan de requisitos es necesario comenzar con la adquisición de conocimiento, entrevistándose con directivos, expertos y usuarios.

ii. **Etapa I.2. Evaluación y selección de la tarea**.- Esta etapa que conforma el estudio de viabilidad, se lleva a cabo realizando la evaluación de la tarea,

cuantificando dicha evaluación para ver qué grado de dificultad presenta la tarea. Existen varias formas de llevar a cabo dicha evaluación.

iii. **Etapa I.3. Definiciones de las características de la tarea.-** Aquí se establecen y, eventualmente, definen las características más relevantes asociadas con el desarrollo de la aplicación. En este particular, se dan:

- Una definición, lo más formal posible, de la aplicación desde el punto de vista del sistema. Se pasa de una descripción informal de los requisitos del usuario a una especificación técnica completa emitida por el ingeniero del conocimiento. Para esto hay que llevar a cabo una especificación inicial de los siguientes tipos de requisitos:
  - Funcionales: tipos de información: (datos, noticia y conocimiento) que se van a tratar, operaciones a realizar sobre ellos, salidas deseada.
  - Operativos o de funcionamiento: estáticos que no varían con el tiempo, y dinámicos, que varían con el tiempo.
  - De interfaz: de usuarios, con otros productos y sistemas.
  - De soporte: plataforma de base requerida tanto hardware como software.
- Criterios de éxito, que básicamente consisten en identificar las necesidades reales de los usuarios finales y decisores del sistema propuesto y definir el grado de satisfacción de dichas necesidades que debe cumplir el sistema.
- Casos de prueba o juegos de ensayo, que permita validar tanto el grado y la calidad del experto humano como las prestaciones del sistema experto obtenido.

- Recursos para desarrollar el sistema experto. Dentro de estos recursos, hay que especificar tanto los materiales (económicos, hardware y software) como los humanos (expertos, ingenieros del conocimiento, ingenieros del software, programadores convencionales e inteligencia artificial).

- Análisis de costo/beneficio y evaluación de riesgos desglosando por conceptos de gastos (personal, material y varios) tipos de beneficios (tangibles, intangibles, concomitantes) y clases de riesgo (institucionales, económicos, estratégicos, tácticos, a corto, medio y largo plazo).

- Puntos de control y calendario, que estable el plan de desarrollo del sistema, así como el programa para llevarlo a cabo.

Esta etapa configura la especificación del sistema. Mientras que la etapa I.1., plan de requisitos, se describen mini especificaciones que sirven de base para la evaluación de la tarea que se lleva a cabo en la etapa I.2., en la etapa I.3, se complementa la especificación como el conocimiento inicial del sistema.

Con la definición de esta fase, los ingenieros del conocimiento, los expertos, usuarios y directivos, consiguen perfilar satisfactoriamente el ámbito del problema; definir coherentemente sus funcionalidades, rendimiento e interfaces; analizar el entorno de la tarea el riesgo del desarrollo del sistema experto. Todo ello hace que el proyecto se justifique y asegura que los ingenieros del conocimiento y los clientes tengan la misma percepción de los objetivos del sistema. En cualquier caso, siempre hay que tener presente que las especificaciones iniciales de los sistemas basados en conocimiento suelen ser inciertas por: incompletas, imprecisas, inconsistentes o contradictorias por lo que su obtención real y completa exigirá el desarrollo de distintos prototipos.

b) **Fase II. Desarrollo de prototipos**

La fase II concierne al desarrollo de los distintos prototipos que permiten ir definiendo y refinando más rigurosamente las especificaciones del sistema, de una forma gradual hasta conseguir las especificaciones exactas de lo que se puede hacer y cómo realizarlo. Pero aún más, pues en el desarrollo de los distintos prototipos suceden muchos problemas a los que el ingeniero del conocimiento se enfrenta por primera vez y a los que debe dar solución.

La construcción relativamente rápida de un prototipo de demostración permitirá al ingeniero del conocimiento, al experto y directivos comprobar la viabilidad de la aplicación y comprender mejor los requisitos de los usuarios y las especificaciones del sistema. Es decir, conocer mejor la problemática de la aplicación.

A continuación de establecen paulatinamente los prototipos de: investigación, campo y operación, que son sucesivos refinamiento cada uno del anterior.

Para llevar a cabo estos prototipos, hay que realizar distintas etapas. Existiendo ligeras diferencias entre las etapas del prototipo de demostración y los otros. Dicho esto, para el desarrollo del prototipo de demostración hay que llevar a cabo las etapas siguientes;

i. **Etapa II.1. Concepción de la solución.-** Esta etapa tiene como objetivo producir un diseño general del sistema prototipo. Inicialmente el ingeniero del conocimiento y el experto estudian las especificaciones parciales del sistema y el plan del proyecto obtenidas en la fase anterior y en base a ellos producen un diseño general. Esta etapa engloba dos actividades principales: el desarrollo del diagrama de flujo de datos (DFD) y el diseño arquitectónico del sistema. Para los subsiguientes prototipos esta etapa se convierte en refinamientos de la concepción de la solución o, si se quiere, en sucesivas reconceptualizaciones.

ii. **Etapa II.2. Adquisición de conocimiento y conceptualización del conocimiento.-** Aunque la adquisición de conocimiento es una actividad que impregna toda la ingeniería de conocimiento, desde que se inicia el estudio de viabilidad hasta que finaliza el uso del sistema experto desarrollado, es en esta etapa donde adquiere su mayor uso. La adquisición, en sus dos facetas de extracción del conocimiento público de fuentes (libro, documentos, manuales de procedimientos) y la deducción del conocimiento privado de los expertos, se alterna cíclicamente con la etapa de conceptualización para modelar el comportamiento del experto.

iii. **Etapa II.3. Formalización del conocimiento.-** Esta etapa presenta dos actividades fundamentales:

- La selección de los formalismos para representar el conocimiento que conforman la conceptualización obtenido en la etapa anterior.
- La realización del diseño detallado del sistema experto.

La formalización o representación del conocimiento, se encuentra ligada con los tipos de conocimiento más apropiados para su representación y las herramientas disponibles en su desarrollo.

En lo que concierne a la actividad de diseño detallado del sistema, consiste en una estructura modular del sistema que incorpora todos los conceptos que participan en el prototipo. Esta actividad debe desarrollar la arquitectura general del prototipo, Especificada en la etapa II.1. Concepción de la solución. En esta actividad hay que establecer los módulos que definen el motor de inferencias, base de conocimiento, interfaces (de usuario y a otros sistemas).

iv. **Etapa II.4. Implementación.-** SI en la etapa anterior fue seleccionada una herramienta de desarrollo adecuada y el problema se ajusta y viceversa, la implementación es inmediata y automática. En otro caso, es necesario

programar, al menos, parte del sistema basado en conocimiento, con las dificultades y problemas que implica cualquier implementación.

En todo caso, hay que dejar constancia aquí de que el uso de herramientas de desarrollo, a pesar de las facilidades que aportan, presenta algunos inconvenientes en absoluto despreciables, como son:

- Dependencia. El prototipo construido queda ligado a la herramienta, sin que se genere un ejecutable independiente, limitado con ello su portabilidad.
- Eficiencia. AL quedar incorporada la herramienta al sistema, este ocupa mucho espacio con una herramienta de la que solo se utiliza una parte muy pequeña.
- Gran tamaño, complejidad y costo. Por ser la buenas herramientas: grandes complejas y caras.

v. **Etapa II.5. Validación y Evaluación.-** La fiabilidad de los resultados es el punto más sensible de todo sistema experto y por tanto su punto crítico. Es una de las tareas más difíciles dado que estos sistemas están construidos para contextos en los que las decisiones son, en cierta mediad discutibles. Sin embargo, existen técnicas que permiten realizar esta validación de una forma satisfactoria. Para ello se deben realizar las siguientes acciones, independientes entre sí pero complementarias:

- Casos de prueba o juego de ensayo que, a modo de Test de Turing, permiten comparar las respuestas de los expertos frente a las del sistema y ver si hay discrepancias. Si las hay habrá que refinar el sistema, si no, se da por válido.
- Ensayo en paralelo que es una consecuencia del anterior y consiste en que los expertos usen rutinariamente el sistema experto desarrollado

para ver las discrepancias entre ambos. Aquí se examina detalladamente la interfaz de usuario para ver si se ajusta a los deseos de expertos y usuarios finales tanto en su ergonomía como en las explicaciones que proporciona.

vi. **Etapa II.6. Definición de nuevos requisitos, especificaciones y diseño.-** Como se ha mencionado, los sistemas basados en conocimiento se construyen de forma incremental, primero un prototipo de investigación, que se convierte en un prototipo de campo para, finalmente, resultar un prototipo de operación. Esta etapa se corresponde con la definición de los requisitos, especificaciones y diseño del siguiente prototipo, que para ser construido deberá pasarse, de nuevo, por la II.1 hasta la etapa II.5. Esta fase acaba con la obtención del sistema experto completo.

2.9.1. Método de adquisición de conocimiento

En esta sección se presenta el método de adquisición del conocimiento desarrollado por Grover, se utiliza para las fases de adquisición de conocimiento correspondientes a la metodología IDEAL [Garcia, Rossi y Britos, 2006].

El método de Grover se concentra en la definición del dominio (conocimiento, referencias, situaciones y procedimientos) en la formulación del conocimiento fundamental (reglas elementales, creencias y expectativas) y en la consolidación del conocimiento de base (revisión y ciclos de corrección). Tradicionalmente, la fase de adquisición del conocimiento en el desarrollo de un sistema experto considera dos enfoques, en el primero, un modelo existente provisto para el nuevo dominio es usado para desarrollar una base de conocimiento, en el segundo método se forma un equipo donde el experto del dominio y el ingeniero del conocimiento intercambian opiniones hasta construir un modelo del cuerpo del conocimiento y un sistema comparable en rendimiento al especialista humano. El ingeniero del conocimiento debe resolver el problema de la limitada disponibilidad de expertos en disciplinas donde el experto es único e indispensable y no puede ser separado

de las tareas diarias. Estos expertos no pueden dedicar meses a desarrollar un sistema experto que podría ser utilizado para ayudar en el proceso de toma de decisiones. Cuanto más eficientemente aprovecha el tiempo disponible un ingeniero del conocimiento, mas valido es el modelo producido. Esta técnica puede ser aplicada al caso más general de especificar soluciones de tareas de la ingeniería del software de gran escala las cuales utilizan acercamientos heurísticos y algorítmicos. [García, Rossi y Britos, 2006].

2.9.1.1. Ciclo de adquisición de conocimiento

Muchas técnicas de adquisición de conocimiento son intuitivas y de práctica ordinaria. Una innovación significativa es la producción de serie de documentos de adquisición de conocimiento. La formulación de esta documentación es un sustituto parcial del experto y provee a los diseñadores de sistemas y usuarios, un medio de comunicación y referencia. La metodología de adquisición de conocimiento para el dominio del problema según García y su equipo (2006), presenta tres fases:

a) Definición del dominio

b) Formulación fundamental del conocimiento.

c) Consolidación del conocimiento basal.

El contenido de los documentos de las tres fases permitirá a los usuarios expertos y diseñadores de sistemas a poseer un conjunto de experiencia humana documentada consistente, organizada y actualizada sobre la cual se basa el sistema experto.

a) Definición del dominio.- Después que el problema es definido por el usuario, según García y sus colegas (2006), la primera fase de adquisición de conocimiento consiste en un cuidadoso entendimiento del dominio. El objetivo es la producción de un Manual de Definición de Dominios Contenidos:

i. Descripción general del problema.

ii. Bibliografía de los documentos referenciados.

iii. Glosario de términos, acrónimos y símbolos.

iv. Identificación de expertos autorizados.

v. Definición de métricas de rendimiento apropiadas y realistas.

vi. Descripción de escenarios de ejemplos razonables.

b) Formulación fundamental del conocimiento.- En la segunda fase de adquisición de conocimiento, se revisan los escenarios seleccionados por el experto que satisfacen los siguientes cinco criterios de conocimiento "fundamental": el más nominal, el más esperado, el más importante, el más arquetípico y el mejor entendido. Esta revisión forma una base para determinar el rendimiento mínimo, realizar la prueba efectuar la corrección y determinar las capacidades del sistema experto que pueden ser expandidas y sujetas a experimentación. Esta base de conocimiento fundamental, según García y su colegas (2006), debe incluir:

i. Una filosofía de entidades del dominio, relaciones entre objetos (clases) y descripciones objetivas.

ii. Un léxico seleccionado (vernáculo).

iii. Una definición de fuentes de entrada y formatos.

iv. Una descripción del estado inicial incluyendo un conocimiento estático.

v. Un conjunto básico de razones y reglas de análisis.

vi. Una lista de estrategias humanas (meta-reglas) las cuales pueden ser consideradas por los diseñadores del sistema experto como reglas a incluir en la base del conocimiento.

Este cuerpo debe estar escrito, parte de él habrá sido adquirido previamente durante la definición del dominio. La validez de este cuerpo de conocimiento puede ser probada implementándola en una base de conocimiento que se contraste con los escenarios desde los cuales fue adquirida y verificando que se produzca un comportamiento similar al del experto en el mismo escenario.

c) **Consolidación del conocimiento basal.** El último paso en este proceso es el ciclo de "revisión y mejoramiento" del conocimiento deducido. La actividad basal puede ser definida en el mismo sentido que la medicina: el menor nivel de actividad (comportamiento del sistema) esencial para el mantenimiento de funciones vitales. En un sistema experto, esto se refiere a que todos los componentes del sistema experto operacional están desarrollados, pero sin la amplitud ni profundidad que la versión final necesitara. El conocimiento basal, es el conjunto de reglas y definiciones adecuadas para producir actividad basal. El cuerpo fundamental del conocimiento es revisado e integrado a través de la apropiada reconstrucción de reglas. La corroboración con expertos adicionales puede colaborar con el cumplimiento de este objetivo. En esta etapa pueden trabajarse los niveles de confianza de las distintas piezas de conocimiento.

CAPITULO III: MARCO APLICATIVO

Este capítulo muestra los pasos para la elaboración del modelo siguiendo la metodología IDEAL, mencionando identificación de la tarea, la adquisición del conocimiento, definición del dominio, base de conocimientos, reglas y base de hechos.

3.1. MODELADO DEL SISTEMA EXPERTO

La construcción de un sistema experto involucra determinar que metodología utilizar, es decir, determinar la guía del desarrollo del mismo, como se implementara la base de conocimiento y el motor de inferencia, principalmente, y como complemento se debe elegir el lenguaje que se utilizará para el proyecto.

Como se mencionó en el Capítulo dos se empleará como metodología de desarrollo del sistema experto, las dos primeras fases y sus etapas de la metodología IDEAL: Identificación de la Tarea y Desarrollo del prototipo.

Un tipo de sistema experto es el basado en reglas, el cual es el apropiado para resolver problemas de tipo determinístico. Un sistema experto basado en reglas tiene dos elementos constitutivos importantes, uno, los datos que son los valores que toman las variables en una situación particular, estos datos pueden variar entre las distintas aplicaciones, no son permanentes y se almacenan en la memoria de trabajo. El otro elemento, es la base de conocimiento que representa el conocimiento de los expertos humanos y consiste en un conjunto de reglas que gobiernan las relaciones entre las variables. La información contenida en la base de conocimiento es permanente y estática [Sampallo, 2007].

La base del conocimiento se construyó a partir de la información suministrada por expertos humanos y la disponible en la bibliografía especializada, que permitió establecer reglas que vinculan las variables y encadenar sus conclusiones, para extraer finalmente una posible

causa y una sugerencia para el usuario. En la Etapa de Adquisición de conocimiento, se utilizará el método de Adquisición de Conocimiento Grover, descrito en el Capítulo dos.

El sistema se puede constituir en una ayuda interesante para aquellos usuarios que no tienen conocimiento sobre el tema y también, como instrumento de objetivo de control para las instituciones.

El Sistema Experto es el resultado de la contribución del experto y el ingeniero del conocimiento, además se considera al usuario que proporcionó el conocimiento necesario para el contenido.

Los componentes del sistema experto son los que se ven en la figura:

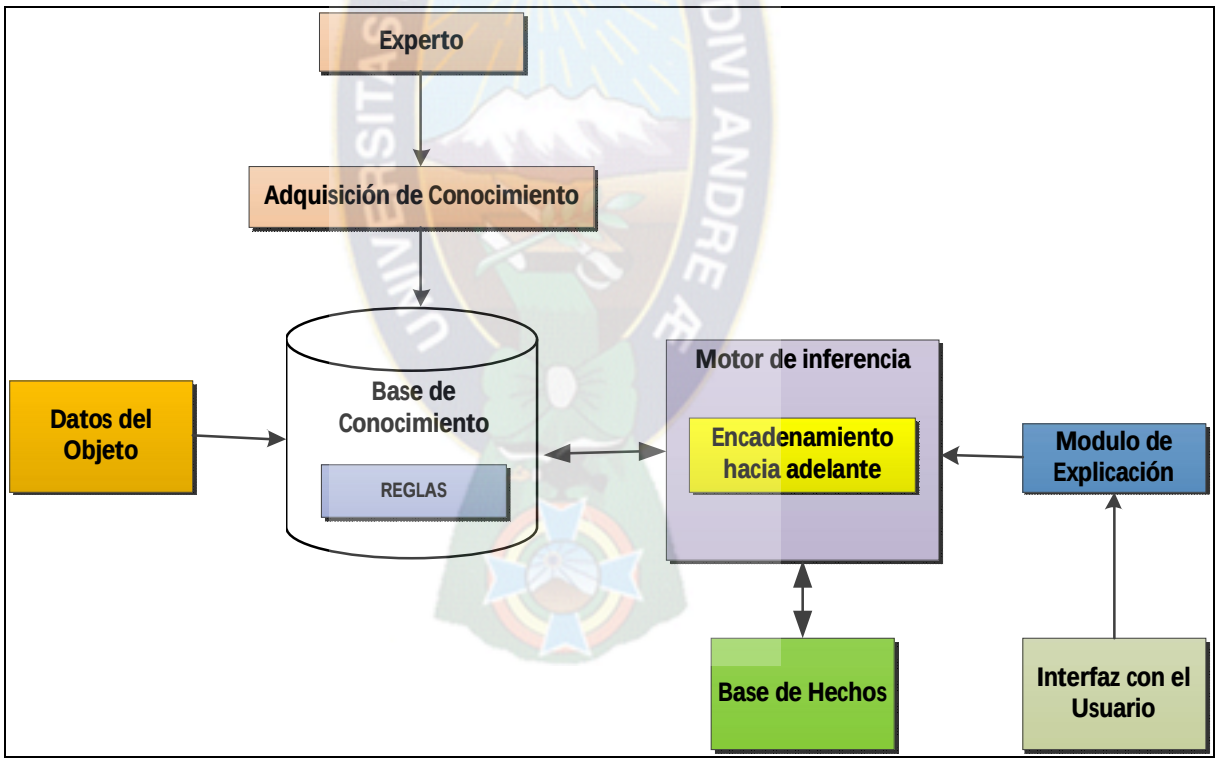


FIG. 8 ESTRUCTURA DEL SISTEMA EXPERTO
Fuente: Basado [Castillo, 2005]

3.2. METODOLOGIA DE DESARROLLO DEL SISTEMA EXPERTO

3.2.1. IDENTIFICACIÓN DE LA TAREA

En el capítulo I se describen los objetivos de la investigación, a continuación se mencionan las actividades a realizar:

a) Investigar Información sobre la seguridad de información de aplicaciones de software.
b) Análisis y abstracción del problema de la seguridad de información de aplicaciones de software.
c) Entrevista con el experto en auditoria informática a la seguridad de la información
d) Investigar información sobre sistemas expertos.
e) Desarrollar el sistema experto.
f) Evaluación del prototipo de sistema experto.

3.2.2. Adquisición del conocimiento

Debido a que la adquisición de conocimientos no es una fase o etapa de la metodología de desarrollo de sistemas expertos y se extiende durante todo el ciclo de vida del sistema experto, en la etapa de conceptualización se debe asegurar una adecuada adquisición del conocimiento. De este modo se presentan las etapas que describe el método de Grover.

3.2.3. Definición del dominio

Glosario de Términos

TÉRMINO	DESRIPCION
Integridad	La información se mantiene completa, exacta y no corrupta
Confidencialidad	La información es accedida sólo para aquellas personas autorizadas

Disponibilidad	La información se encuentra disponible en el lugar indicado y en el momento requerido
Clasificación de Información	La información debería ser clasificada, por quien corresponda, según su nivel de criticidad y sensibilidad
Algoritmos de cifrado	Proceso que convierte texto “en claro” en texto ilegible llamado “texto cifrado” o “criptograma”.
Activos de la empresa	Todo aquello tangible o intangible que tenga valor para la empresa
Credencial de usuario	Conjunto de datos que identifican a un usuario en un sistema determinado, asignándole permisos específicos
Recurso	Todo aquello tangible o intangible al que se quiere tener acceso
Proceso de Autenticación	Proceso que valida la identidad de un usuario que quiere acceder a un recurso
Autorización	Proceso que verifica si un recurso puede tener acceso a otro recurso de acuerdo al Rol
Perfiles de acceso (Roles)	Conjunto de permisos a recursos que adquiere una persona en función a las actividades que desempeña en la empresa
Programa ejecutable	Archivo binario que contiene información que sólo puede ser interpretada por el sistema operativo
Programa fuente	Archivo de texto que contiene un conjunto de instrucciones escritas por el programador, en un determinado lenguaje de programación, y que describe el propósito y el funcionamiento del mismo
Repositorio de Datos	Espacio físico y/o lógico donde se almacenan datos
Estándar	Especificación que regula la realización de procesos en un determinado contexto de seguridad
Vulnerabilidad	Agujero o debilidad de una aplicación
Validación	Proceso que garantiza que el ingreso, el proceso y la salida de los datos cumple con las restricciones de seguridad de la información

Lista de verificación	Repositorio de vulnerabilidades conocidas y actualizadas para filtrar el ingreso de datos de acuerdo a determinados patrones
Patrón de aceptación	Método por el cual los datos son rechazados si no cumplen con lo establecido en listas de verificación de aceptación.
Patrón de rechazo	Método por el cual los datos son aceptados si no cumplen con lo establecido en listas de verificación de rechazo.
Resguardo y recupero de información	Implementación de políticas de backup de la organización
Versionado	Gestión de los cambios que puede sufrir un programa, archivo, documento, etc.
Transacción	Conjunto de instrucciones que se ejecutan como una unidad indivisible o atómica
Riesgo informático	Evento fortuito que en caso de producirse puede tener un efecto negativo sobre algún recurso
Requerimientos Funcionales	Aspectos que una aplicación deberá cumplir exhaustivamente fin de no poner en riesgo la seguridad de la información
Requerimientos No Funcionales	Aspectos relacionados con la configuración, la administración y el mantenimiento de un entorno seguro donde se ejecuten las aplicaciones
Auditoría de código	Revisión exhaustiva de cada línea de programa fuente

CUADRO 1 GLOSARIO DE TERMINOS
Fuente: Ingeniero del Conocimiento

El dominio considerado es la seguridad de los sistemas de información, para el presente trabajo se considera los siguientes subdominios:

- Programas Ejecutables
- Base de Datos

3.2.4. Formulación del conocimiento fundamental

Se realizó el estudio de la documentación disponible sugerida por el experto, dentro el dominio planteado de la seguridad de la información se dedujo los siguientes grupos que se establece como conocimiento fundamental.

a) Dominio
b) Control
c) Objetivo de control
d) Valor
e) Definición

Se estable la siguiente tabla:

DOMINIO	**PROGRAMAS EJECUTABLES**		
CONTROL	**OBJETIVO DE CONTROL**	**VALOR**	**CONCEPTO**
Control de programas ejecutables	Log de Aplicaciones	ADECUADO-INADECUADO	Archivo que contiene registro de las actividades de usuarios del sistema.
	Detección de errores	ADECUADO-INADECUADO	Administración errores o eventos no esperados generados cuando se envían mensajes entre aplicaciones.
Control de programas fuente	Política	ADECUADO-INADECUADO	Conjunto de procedimientos estandarizados para efectuar el control de programas fuente en relación a los datos de entrada, el procesamiento y los datos de salida.
	Auditoria de Código	ADECUADO-INADECUADO	Análisis exhaustivo de las líneas de programas fuente

	Criticidad	ALTA - BAJA	Grado de importancia que tienen los programas fuente en relación a la continuidad de las operaciones.
	Validaciones de Datos de Entrada	ADECUADO-INADECUADO	Análisis de la tipificación de datos que ingresan a un programa para su procesamiento.
	Validaciones de Datos de Salida	ADECUADO-INADECUADO	Análisis del tipo de salida que genera un programa tanto para datos que deben ser exhibidos al usuario o para datos que deben ser enviados a otros programas.
	Validaciones de procesamiento de datos	ADECUADO-INADECUADO	Comprobación del adecuado procesamiento de los datos de entrada.
Resguardo de programas fuente	Política	ADECUADO-INADECUADO	Conjunto de procedimientos estandarizados para efectuar el control de Resguardo de Programas Fuente.
	Control de gestión de repositorio	ADECUADO-INADECUADO	Revisión de la administración del repositorio de Programas fuentes.
	Ejecución	CUMPLE -NO CUMPLE	Almacenar copias de resguardo de programas fuente.
	Monitoreo	ADECUADO-INADECUADO	Revisión y control de las bibliotecas de resguardo de programas fuente

Recupero de programas fuente	Política	ADECUADO-INADECUADO	Conjunto de procedimientos estandarizados para efectuar el control de Recupero de Programas Fuente.
	Ejecución	CUMPLE -NO CUMPLE	Recuperar copias de resguardo de los programas fuente.

CUADRO 2 PROGRAMAS EJECUTABLES
Fuente: Ingeniero del Conocimiento y Cuadro 1

DOMINIO	**REPOSITORIO DE DATOS**		
CONTROL	**OBJETIVO DE CONTROL**	**VALOR**	**CONCEPTO**
Resguardo de datos	Política	ADECUADO-INADECUADO	Conjunto de procedimientos estandarizados para efectuar el control de resguardo de los Datos
	Planificación	ADECUADO-INADECUADO	Organización y programación del resguardo de Datos
	Ejecución	CUMPLE -NO CUMPLE	Almacenar copias de resguardo de los Datos
	Monitoreo	ADECUADO-INADECUADO	Revisión y control de las bibliotecas de resguardo de Datos
Recupero de datos	Política	ADECUADO-INADECUADO	Conjunto de procedimientos estandarizados para efectuar el control de Recupero de Datos
	Simulación	CUMPLE -NO CUMPLE	Recuperar copias de resguardo de los datos
	Ejecución	CUMPLE -NO CUMPLE	Recuperar copias de resguardo de los datos
Acceso a Datos	Política	ADECUADO-INADECUADO	Conjunto de procedimientos estandarizados para efectuar el control del Acceso a Datos
	Comunicación	ADECUADO-INADECUADO	Procedimiento de notificaciones de la política de Acceso a Datos

	Ejecución	CUMPLE -NO CUMPLE	Efectuar el acceso a Datos
	Monitoreo	ADECUADO-INADECUADO	Revisión y control de los permisos de acceso a los datos
	Ubicación de la lógica del negocio	SQL Estático – SQL Dinámico	Localización de rutinas, algoritmos, reglas de negocio, etc. vinculadas estrechamente con datos.
	Cifrado	CUMPLE -NO CUMPLE	Algoritmo que convierte texto plano legible en un texto cifrado ilegible o criptograma

CUADRO 3 REPOSITORIO DE DATOS
Fuente: Ingeniero del Conocimiento y Cuadro 1

3.2.5. Consolidación del conocimiento

La consolidación del conocimiento está reflejada en:

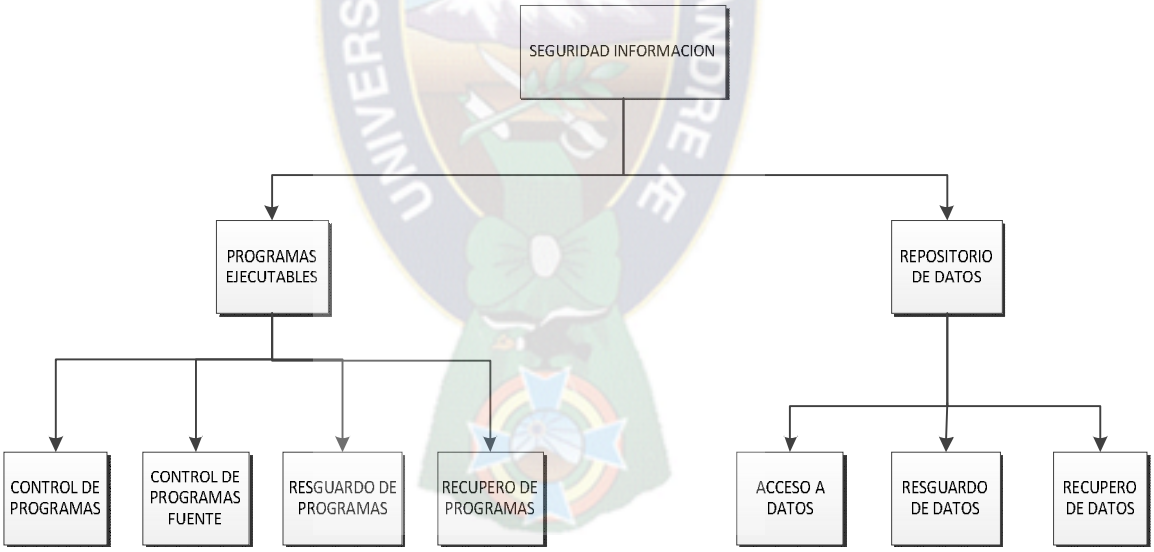


FIG. 9 CONSOLIDACIÓN DEL CONOCIMIENTO
Fuente: Elaboración Propia

3.2.6. Base de conocimiento

La base del conocimiento que almacena y representa el conocimiento del dominio del Sistema Experto, facilita su acceso, manipulación y actualización. El conocimiento del experto está representado por todos los dominios, objetivos de control, controles causas y recomendaciones; que convierten en hechos y reglas que son importantes para la solución del problema, de forma sencilla, independiente, fácil de modificar, transparente y relacional como se muestra.

3.2.7. Reglas

Es la forma más extendida de representación del conocimiento. Representan la forma de razonar. Tienen la forma:

SI "A_1, A_2, A_3, ..A_n"

Y **"**B_1, B_2, B_3, ..B_n"

ENTONCES "C_1, C_2, C_3, ..C_n".

ESTADO DE LA REGLA	**TEXTO DE LA REGLA**
Formulación de la Regla	**SI** Control de programas fuente. Validación de datos de entrada = Adecuado **Y** Control de programas fuente. Política = Adecuado **ENTONCES** Es factible validar datos de entrada en las aplicaciones.
Descripción de la Regla	Si el control de datos ingresados para su procesamiento se adecúa a los estándares de Seguridad de la Información, y las políticas de control de programas fuente en relación a la entrada de datos es la adecuada. Entonces es factible validar datos de entrada en las aplicaciones.
Nombre de la Regla	**Regla 1**

CUADRO 4 ENTRADA DE DATOS
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Control de programas fuente. Criticidad = Baja **Y** Control de programas fuente. Validaciones de procesamientos de Datos = Adecuado **ENTONCES** No es factible realizar control de código fuente.
Descripción de la Regla	Si el grado de importancia que tienen los programas fuente en relación a la continuidad de las operaciones es bajo y la comprobación del adecuado procesamiento de los datos de entrada cumple, entonces no es factible realizar control de código fuente.
Nombre de la Regla	**Regla 2**

CUADRO 5 VERIFICACIÓN Y CONTROL DE CÓDIGO FUENTE
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Resguardo de Datos. Planificación = Adecuado **Y** Resguardo de Datos. Ejecución = Adecuado **Y** Control de Programas ejecutables. Log de Aplicaciones = Adecuado **ENTONCES** No es factible efectuar auditoria de las actividades de los usuarios.
Descripción de la Regla	En caso que las copias almacenadas de resguardo de los datos son adecuadas, de la misma manera el log de aplicaciones que es el archivo que contiene registro de las actividades de usuarios del sistema es el adecuado. Y la organización y programación del resguardo de datos cumple. Entonces no es factible efectuar una auditoria a las actividades de los usuarios.
Nombre de la Regla	**Regla 3.**

CUADRO 6 LOG DE APLICACIONES
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Control de programas fuente. Validaciones de procesamientos de Datos = Adecuado **Y** Control de Programas Fuente. Auditoria de Código = Adecuado **ENTONCES** Es factible mantener el correcto procesamiento de la información.
Descripción de la Regla	En caso que las validaciones de procesamiento de los datos son adecuadas y de la misma manera la auditoria de Código fuente. Entonces es factible mantener el correcto procesamiento de la información.
Nombre de la Regla	**Regla 4.**

CUADRO 7 RESGUARDO DE DATOS
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Capa de seguridad. Seguridad Externa = Cumple **Y** Capa de seguridad. Autenticidad = Adecuada **ENTONCES** Es factible garantizar la adecuada gestión de accesos a las aplicaciones.
Descripción de la Regla	Si los mecanismos de gestión de perfiles de acceso se cumplen, y por otro lado el mecanismo de autenticación es el adecuado. Entonces es factible garantizar la adecuada gestión de accesos a las aplicaciones.
Nombre de la Regla	**Regla 5.**

CUADRO 8 ACCESO A APLICACIONES
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Resguardo de Programas fuente. Política = Adecuada **Y** Resguardo de Programas fuente. Ejecución= Cumple **Y** Recupero de Programas fuente. Política = Adecuada **Y** Recupero de Programas fuente. Ejecución = Cumple **ENTONCES** Es factible administrar las copias de resguardo de programas fuente adecuadamente.
Descripción de la Regla	Si existe una política de resguardo y recupero, del mismo modo se cumple, se considera factible administrar las copias de resguardo de programas fuente adecuadamente.
Nombre de la Regla	**Regla 6.**

CUADRO 9 ADMINISTRACIÓN DE COPIAS DE RESGUARDO
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Resguardo de Programas fuente. Política = Adecuada **Y** Resguardo de Programas fuente. Monitoreo = Adecuado **ENTONCES** Es factible garantizar la integridad, confidencialidad y disponibilidad de los programas fuente resguardados.
Descripción de la Regla	Si existe una política de resguardo adecuada, del mismo modo la revisión y control de las bibliotecas de resguardo de programas fuente de manera adecuada, por lo tanto se considera factible garantizar la integridad, confidencialidad y disponibilidad de los programas fuentes resguardadas.
Nombre de la Regla	**Regla 7**

CUADRO 10 INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD
Fuente: Conocimiento del Experto y Cuadro 2

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Acceso a Datos. Política = Adecuada **Y** Acceso a Datos. Comunicación = Adecuado **ENTONCES** Es factible garantizar el correcto acceso a la Base de Datos.
Descripción de la Regla	En el caso que el conjunto de procedimientos estandarizados para efectuar el control del acceso a Datos es el adecuado y el procedimiento de notificación de las políticas es correcto, entonces es factible garantizar el correcto acceso a la Base de Datos.
Nombre de la Regla	**Regla 8**

CUADRO 11 ACCESO A LA BASE DE DATOS
Fuente: Conocimiento del Experto y Cuadro 3

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Acceso a Datos. Ejecución = Cumple **Y** Acceso a Datos. Monitoreo = Adecuado **ENTONCES** Es factible garantizar la integridad de los datos almacenados.
Descripción de la Regla	En el caso que al efectuar el acceso a Datos es el adecuado y del mismo modo la revisión y control de los permisos de acceso a los datos es el correcto, esto implica que es factible garantizar la integridad de los datos almacenados.
Nombre de la Regla	**Regla 9**

CUADRO 12 INTEGRIDAD DE DATOS
Fuente: Conocimiento del Experto y Cuadro 3

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Acceso a Datos. Cifrado = Cumple **Y** Resguardo de Datos. Ejecución = Cumple **Y** Acceso a Datos. Política = Adecuada **ENTONCES** Es factible almacenar datos sensibles a través de un mecanismo cifrado.
Descripción de la Regla	En el caso que el algoritmo que convierte texto plano legible en un texto cifrado o ilegible o criptograma es el adecuado, del mismo modo almacenar copias de resguardo de Datos y el conjunto de procedimientos estandarizados para efectuar el control del acceso a datos es el correcto, esto implica que es factible almacenar datos sensibles a través de mecanismos cifrados.
Nombre de la Regla	**Regla 10**

CUADRO 13 MECANISMO CIFRADO
Fuente: Conocimiento del Experto y Cuadro 3

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Resguardo de Datos. Política = Adecuada **Y** Resguardo de Datos. Ejecución= Cumple **Y** Recupero de Datos. Política = Adecuada **Y** Recupero de Datos. Ejecución = Cumple **ENTONCES** Es factible administrar las copias de resguardo de Datos adecuadamente.
Descripción de la Regla	Si existe una política de resguardo y recupero de Datos, y están cumplen adecuadamente, se considera factible administrar las copias de resguardo de datos adecuadamente.
Nombre de la Regla	**Regla 11**

CUADRO 14 ADMINISTRACIÓN DE COPIAS DE DATOS
Fuente: Conocimiento del Experto y Cuadro 3

ESTADO DE LA REGLA	TEXTO DE LA REGLA
Formulación de la Regla	**SI** Resguardo de Datos. Política = Adecuado **Y** Resguardo de Datos. Monitoreo = Adecuado **Y** Recupero de Datos. Simulación = Cumple **ENTONCES** Es factible garantizar la integridad, confidencialidad y disponibilidad de los datos resguardados.
Descripción de la Regla	Si existe una política de resguardo de datos adecuada, del mismo modo la revisión y control de las bibliotecas de resguardo de datos de manera adecuada y se recupera de manera correcta los datos, por lo tanto se considera factible garantizar la integridad, confidencialidad y disponibilidad de los datos resguardados.
Nombre de la Regla	**Regla 12**

CUADRO 15 ADMINISTRACIÓN DE COPIAS DE DATOS
Fuente: Conocimiento del Experto y Cuadro 3

3.2.8. Base de hechos

Representan el conocimiento del sistema experto en un cierto instante, está representada en una base de datos, y su información está directamente enlazada con la base de conocimiento.

3.2.9. Arquitectura

En la arquitectura de la propuesta, el conocimiento estará representado en XML, es decir la base de conocimiento, los procedimientos capaces de razonar se implementaran en CLIPS. Es necesario la presencia de interfaces que permitan el acceso al sistema ya sea por parte del ingeniero del conocimiento que es el encargado de alimentar la base de conocimiento como el usuario del sistema que proporciona los hechos que determinan una utilización concreta del sistema experto que al igual que la máquina de inferencia, estas se encontraran en JAVA.

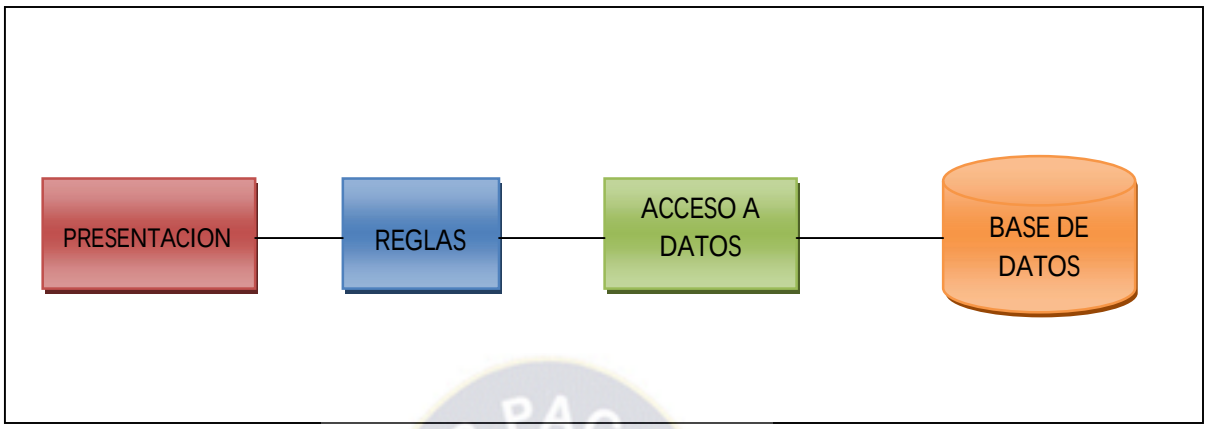


FIG. 10 ARQUITECTURA DEL PROTOTIPO
Fuente: Basado en [Vergara, 2004]

3.3. DISEÑO Y DESARROLLO DEL PROTOTIPO

Para el Desarrollo de la propuesta se utiliza la metodología del proceso unificado racional, con el objetivo de producir software de alta calidad que cumpla con los requerimientos de los usuarios, dentro de una planificación que cubra el ciclo de vida del desarrollo del software.

3.3.1. Fase de Inicio y Elaboración

3.3.1.1. Funciones principales

Los procesos que se realizan en el Sistema, se agrupan de la siguiente manera:

a) Registro

- Hechos
- Reglas
- Meta reglas
- Usuarios

- Tipo

b) Actualización

- Hechos
- Reglas
- Meta reglas
- Usuarios
- Tipo

c) Consulta

- Selección de hechos
- Aplicación de reglas

d) Reporte de resultados

- Diagnostico

3.3.1.2. Descripción de Actores

Un actor es un usuario del sistema, estos tipos de usuarios tendrán diferentes privilegios y permisos, de acuerdo a estos permisos los usuarios podrán realizar determinadas tareas en el sistema. Los tipos de usuarios que se lograron identificar son:

- **Ingeniero del conocimiento**, es el encargado de administrar el sistema, este usuario podrá registrar y modificar (hechos, reglas, meta reglas, usuarios), procesos de consulta e imprimirlos.

- **Auditor,** entre sus atribuciones está el de consultar e imprimir la mencionada consulta.

3.3.1.3. Diagrama de Casos de Uso

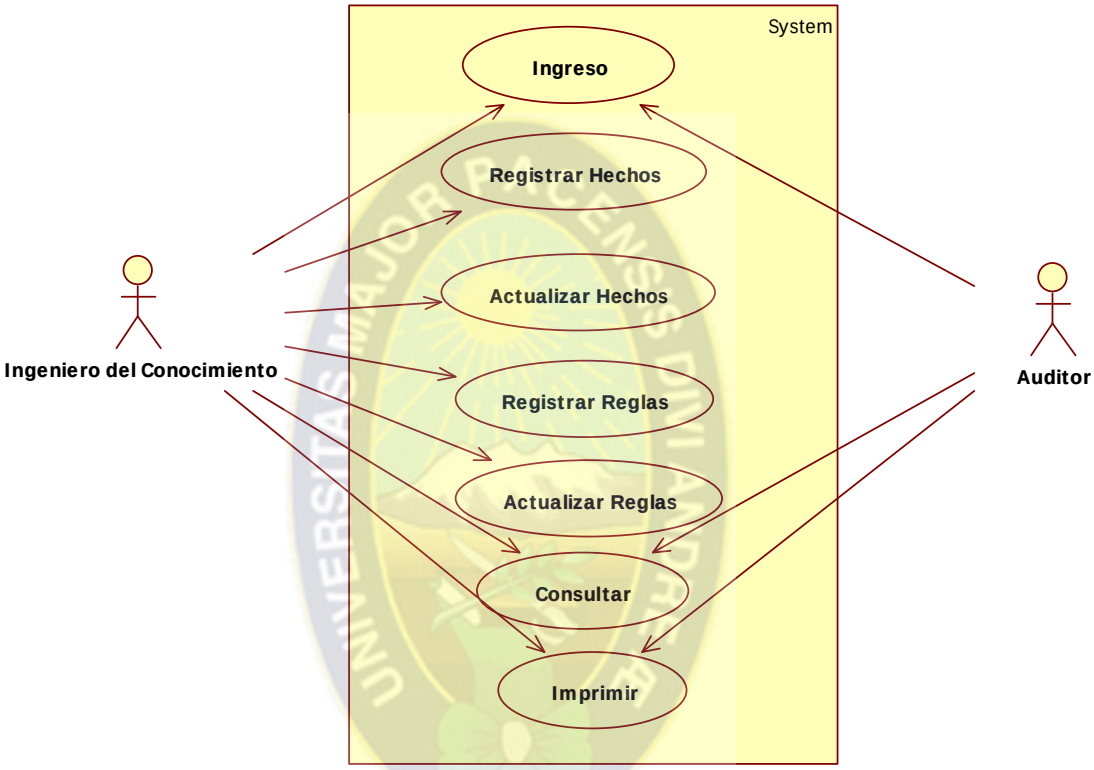


FIG. 11 DIAGRAMA DE CASOS DE USO
Fuente: Basado en [Larman, 2004]

3.3.1.4. Descripción de Casos de Uso

Caso de Uso	**Ingreso al Sistema**
Actores:	Ingeniero del Conocimiento y Auditor
Propósito:	Ingresar al Sistema
Resumen:	Los usuarios deben introducir su nombre para consultar, solo el ingeniero del conocimiento tiene una contraseña para la administración del Sistema.
Tipo:	Esencial
Curso Normal de los eventos	**Respuesta del Sistema**
1. Los usuarios inician el Sistema	
2. El usuario introduce su nombre	3. Registrar el nombre del Usuario
	4. Habilita nueva consulta
Cursos alternos:	
• Línea 2: Si el usuario es el ingeniero del conocimiento deberá introducir su nombre y su contraseña.	
• Línea 4: El sistema habilita las opciones	

Caso de Uso	**Registrar Hechos**
Actores:	Ingeniero del Conocimiento.
Propósito:	Almacenar Hechos en la Base de Conocimiento.
Resumen:	Registrar Hechos en la Base de Conocimiento.
Tipo:	Primario.
Curso Normal de los eventos	**Respuesta del Sistema**
1. El Ingeniero del Conocimiento Ingresa al Sistema.	
	2. Verifica al Usuario.
3. El Ingeniero del Conocimiento selecciona el menú de Hechos/Registro.	
4. El Ingeniero del Conocimiento registra nuevos hechos.	
5. Ingeniero del Conocimiento guarda los Hechos.	6. Almacena en la Base de Conocimiento
Cursos alternos:	
• Línea 4: El ingeniero del Conocimiento cancela el Proceso.	

Caso de Uso	**Actualiza Hechos**
Actores:	Ingeniero del Conocimiento.
Propósito:	Actualiza la Base de Conocimiento.
Resumen:	Modificar o eliminar Hechos en la Base de Conocimiento.
Tipo:	Primario.
Curso Normal de los eventos	**Respuesta del Sistema**
1. El Ingeniero del Conocimiento Ingresa al Sistema.	2. Verifica al Usuario.
3. El Ingeniero del Conocimiento selecciona el menú de Hechos/Edición.	
4. El Ingeniero del Conocimiento edita los hechos.	5. Actualiza la Base de Conocimiento.
Cursos alternos:	
• Línea 4: El ingeniero del Conocimiento cancela el Proceso.	

Caso de Uso	**Registrar Reglas**
Actores:	Ingeniero del Conocimiento.
Propósito:	Almacenar Reglas en la Base de Conocimiento.
Resumen:	Registrar Reglas en la Base de Conocimiento.
Tipo:	Primario.
Curso Normal de los eventos	**Respuesta del Sistema**
1. El Ingeniero del Conocimiento Ingresa al Sistema.	2. Verifica al Usuario.
3. El Ingeniero del Conocimiento selecciona el menú de Reglas/Registro.	
4. El Ingeniero del Conocimiento registra nuevas Reglas a partir de los hechos registrados.	
5. Ingeniero del Conocimiento guarda las Reglas.	6. Almacena en la Base de Conocimiento
Cursos alternos:	
• Línea 4: El ingeniero del Conocimiento cancela el Proceso.	
•	

Caso de Uso	Actualiza Reglas
Actores:	Ingeniero del Conocimiento.
Propósito:	Actualiza la Base de Conocimiento.
Resumen:	Modificar o eliminar Reglas en la Base de Conocimiento.
Tipo:	Primario.

Curso Normal de los eventos	Respuesta del Sistema
1. El Ingeniero del Conocimiento Ingresa al Sistema.	
	2. Verifica al Usuario.
3. El Ingeniero del Conocimiento selecciona el menú de Reglas/Edición.	
4. El Ingeniero del Conocimiento edita las Reglas.	5. Actualiza la Base de Conocimiento.

Cursos alternos:

- Línea 4: El ingeniero del Conocimiento cancela el Proceso.

Caso de Uso	Consulta
Actores:	Ingeniero del Conocimiento y Auditor.
Propósito:	Consultar al Sistema.
Resumen:	Consultar al Sistema para la evaluación del objeto a auditar
Tipo:	Esencial.

Curso Normal de los eventos	Respuesta del Sistema
1. El Usuario Ingresa al Sistema.	2. Verifica al Usuario.
3. El Usuario selecciona los hechos.	4. Filtra los hechos.
5. El Usuario finaliza la consulta.	6. Proporciona la respuesta a la consulta.
7. Guarda en formato digital o imprime la consulta.	8. Guarda la consulta en la memoria de trabajo.
	9. Se prepara para la siguiente consulta

Cursos alternos:

- Línea 4: El ingeniero del Conocimiento cancela el Proceso.

Caso de Uso	Imprimir
Actores:	Ingeniero del Conocimiento y Auditor.
Propósito:	Imprimir la consulta.
Resumen:	Documenta la consulta del Usuario.
Tipo:	Esencial.
Curso Normal de los eventos	**Respuesta del Sistema**
1. El Usuario Imprime la consulta.	2. Filtra la consulta del Usuario
Cursos alternos:	

3.3.1.5. Diagrama de secuencias

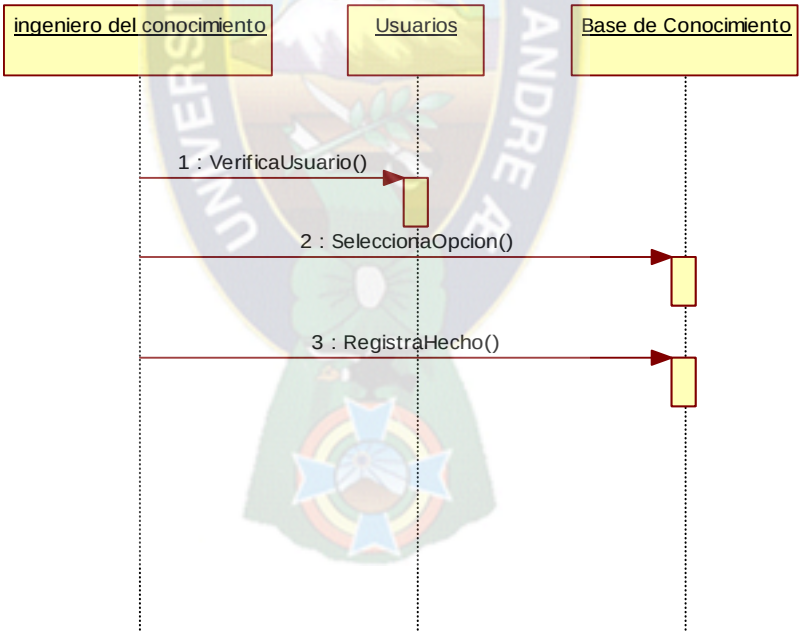


FIG. 12 DIAGRAMA DE SECUENCIA REGISTRO DE HECHOS

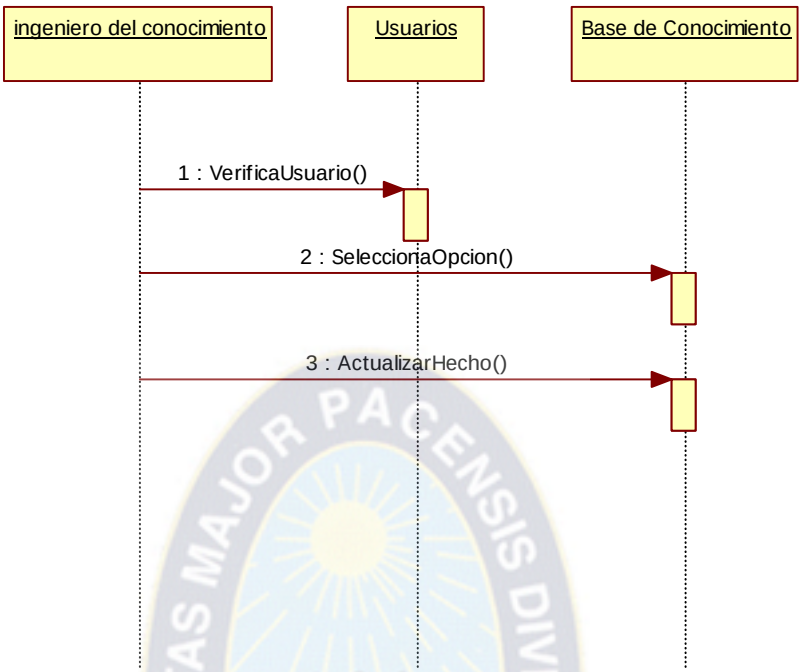


FIG. 13 DIAGRAMA DE SECUENCIA ACTUALIZAR HECHOS

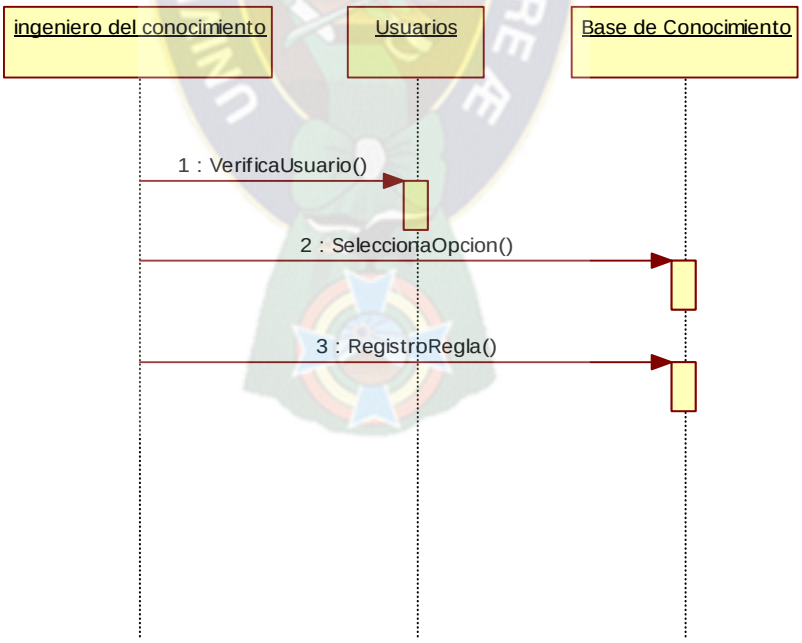


FIG. 14 DIAGRAMA DE SECUENCIA REGISTRO DE REGLA

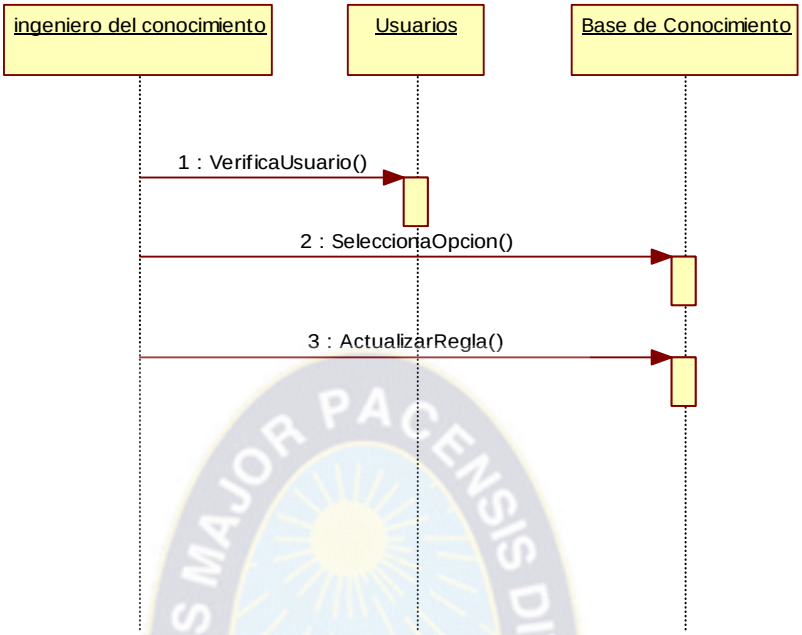


FIG. 15 DIAGRAMA DE SECUENCIA ACTUALIZAR REGLA

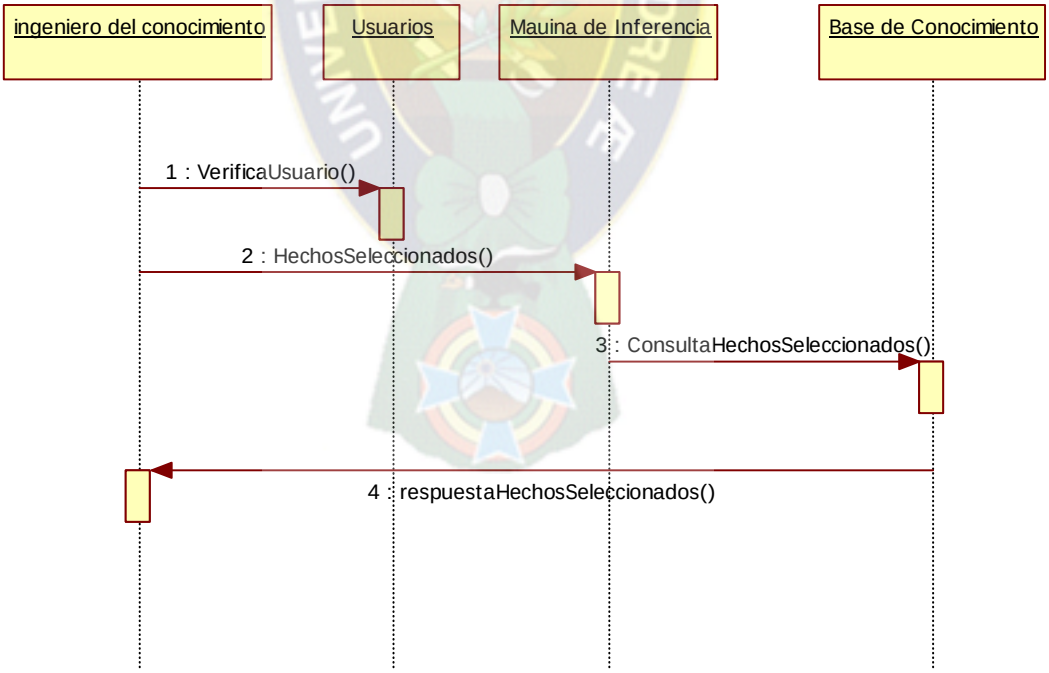


FIG. 16 DIAGRAMA DE SECUENCIA DE CONSULTA

3.3.1.6. Diagrama de Transición de estados

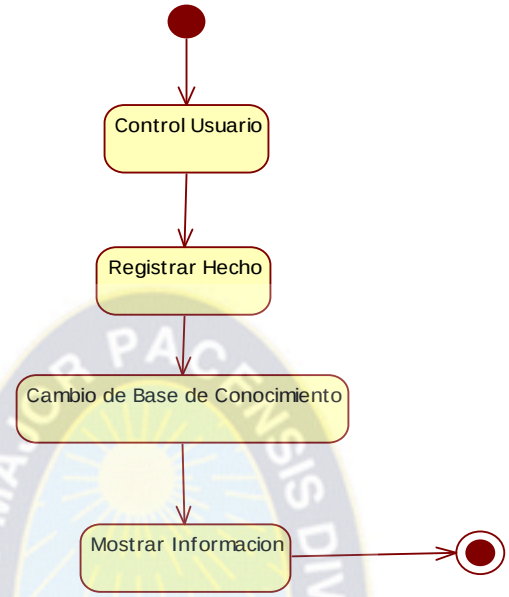


FIG. 17 DIAGRAMA DE ESTADO CASO DE USO REGISTRAR HECHO

FIG. 18 DIAGRAMA DE ESTADO CASO DE USO ACTUALIZAR HECHO

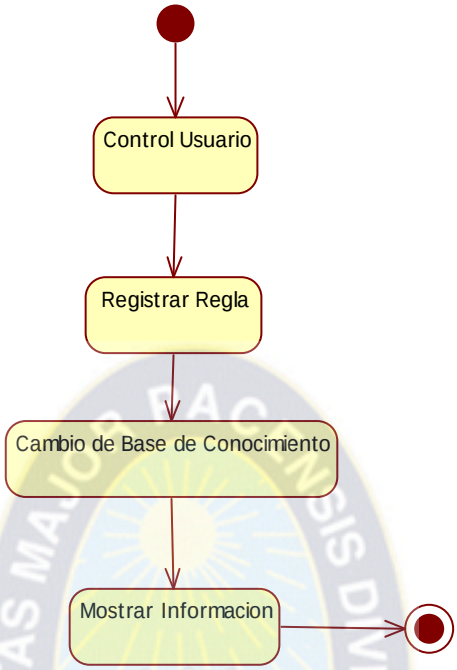


FIG. 19 DIAGRAMA DE ESTADO CASO DE USO REGISTRAR REGLA

FIG. 20 DIAGRAMA DE ESTADO CASO DE USO ACTUALIZAR REGLA

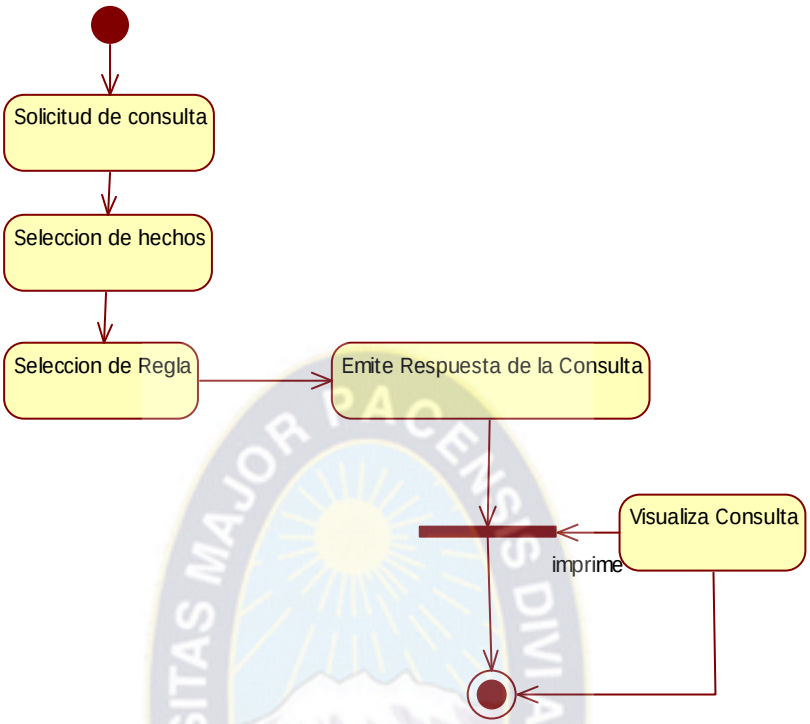


FIG. 21 DIAGRAMA DE ESTADO CASO DE USO CONSULTAR

3.3.1.7. Diagrama de clases

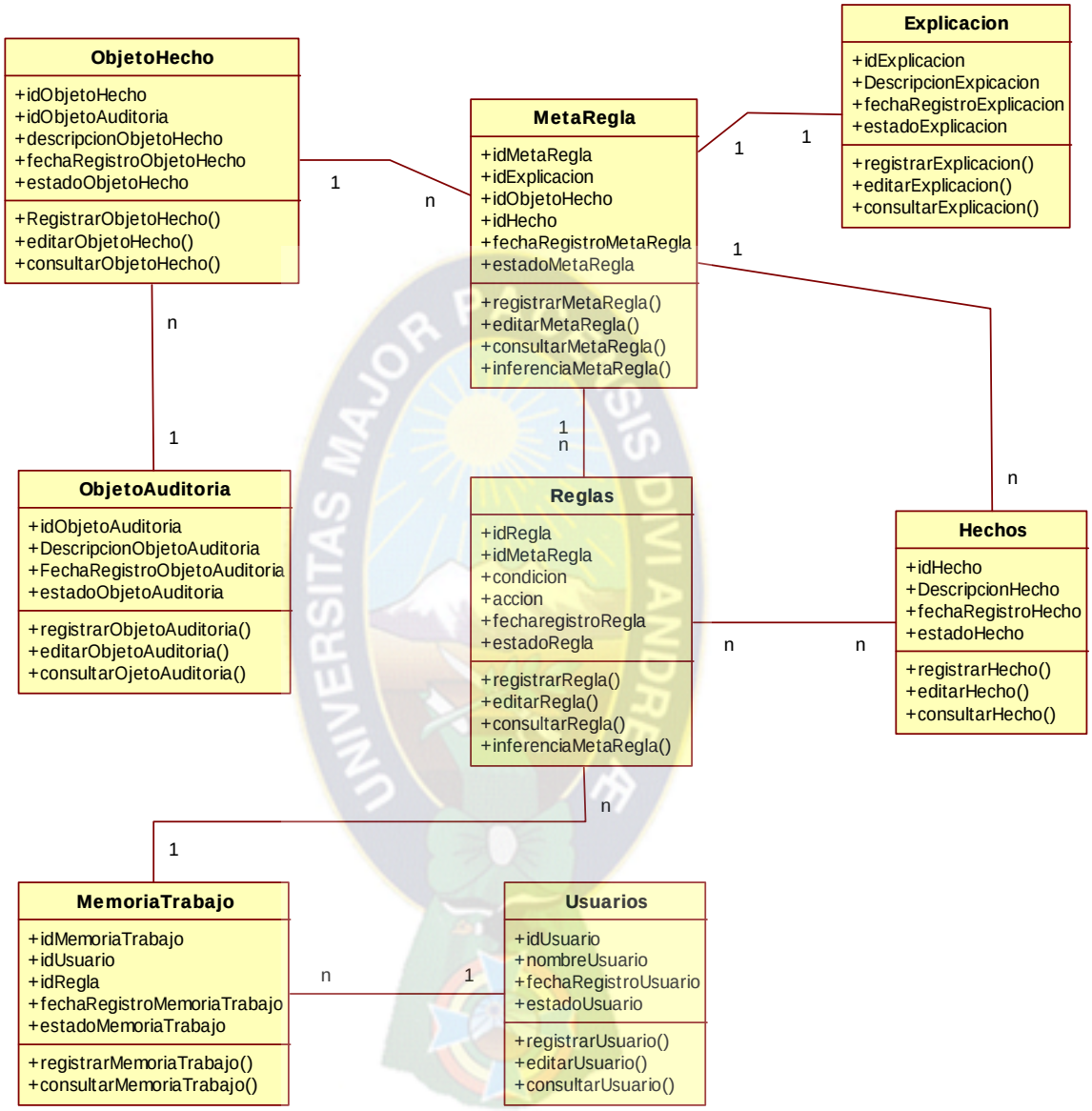


FIG. 22 DIAGRAMA DE CLASES
Fuente: Basado en [Booch, Rumbaugh, 1999]

3.3.2. FASE DE CONSTRUCCION

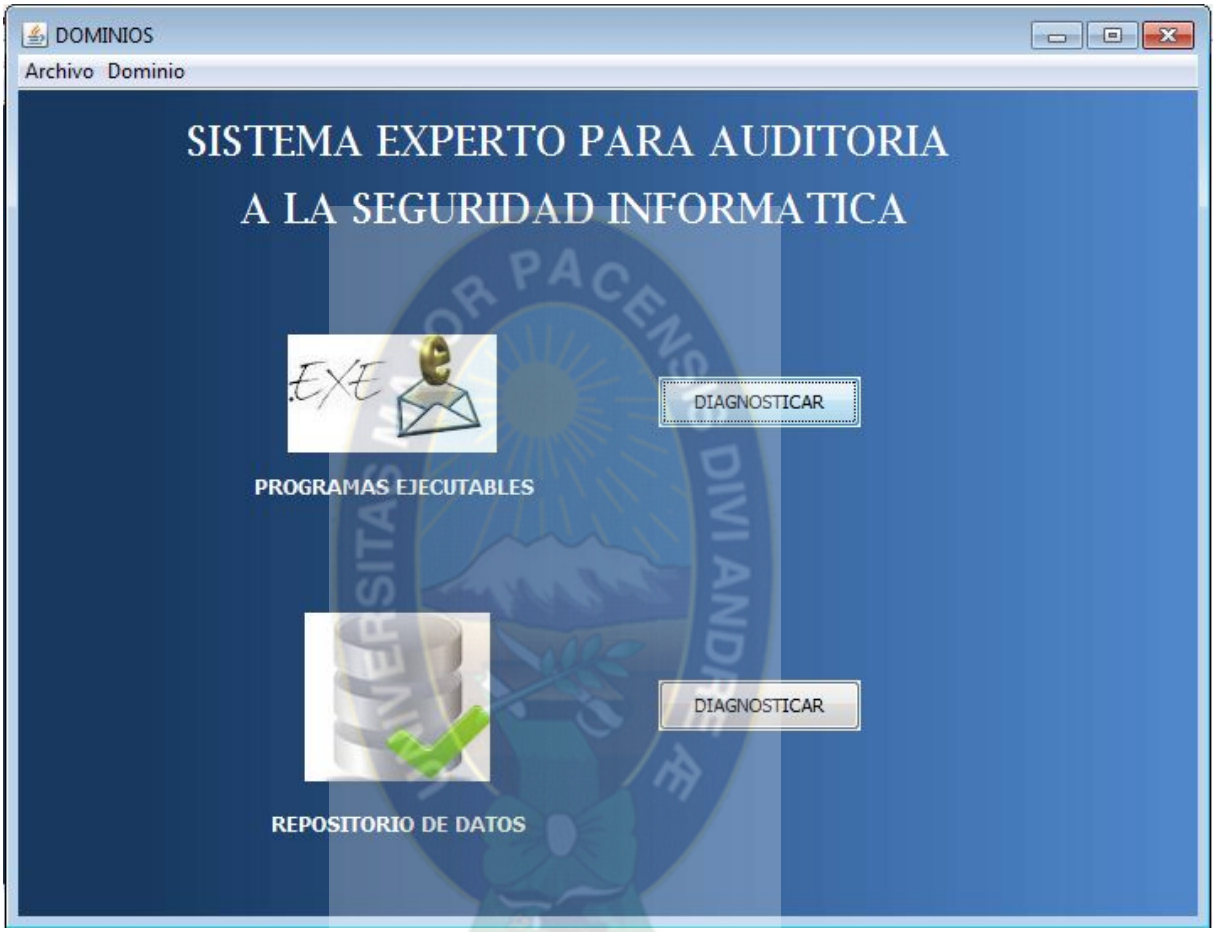
Según Gómez (2007), el diseño de interfaces de usuario es una tarea que ha adquirido relevancia en el desarrollo de un sistema. La calidad de interfaz de usuario puede ser uno de los motivos que conduzca a un sistema al éxito o al fracaso. El diseño de interfaces realizado para el prototipo, fue realizado con base al modelado del prototipo.

a) Interfaz inicio de sesión

En esta interfaz se escribe el nombre de usuario y la contraseña para iniciar sesión en el sistema.

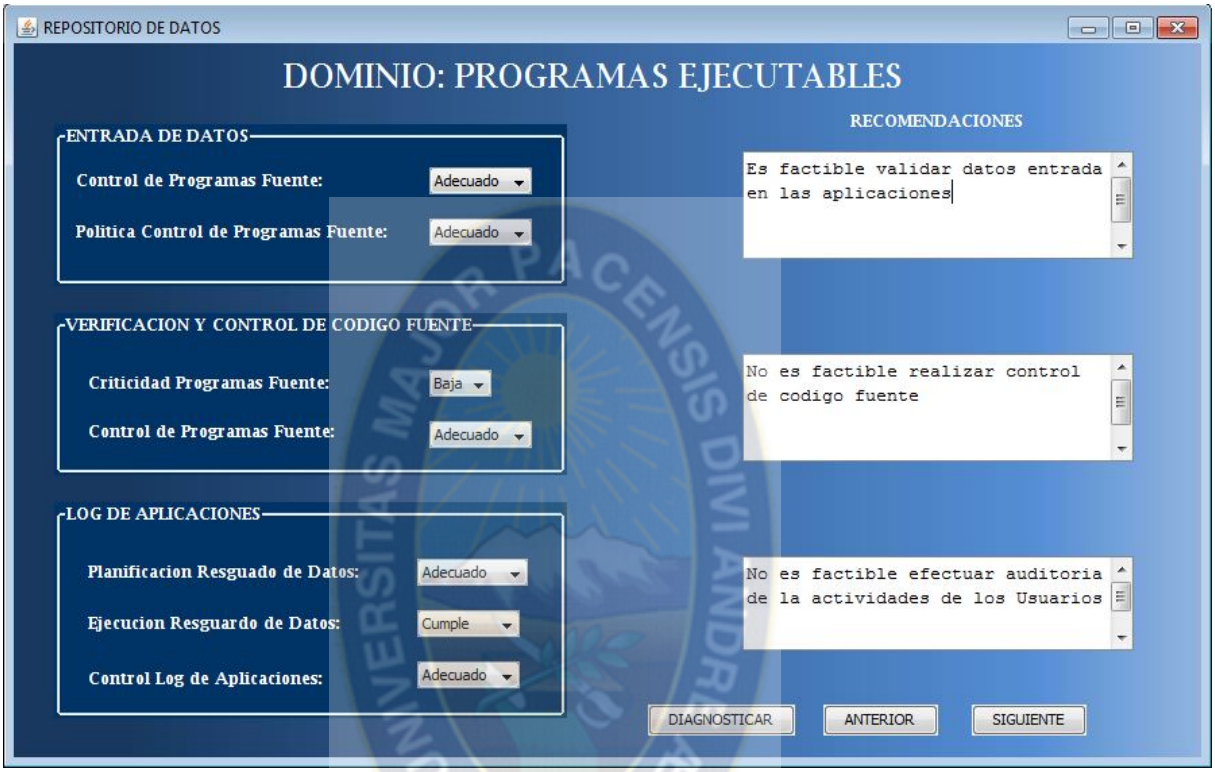
b) Interfaz de consulta

Muestra los dominios correspondientes:



c) Interfaz, Dominio de Programas ejecutables

Muestra la ventana de diagnóstico del Dominio de Programas Ejecutables:



CAPITULO IV: EVALUACION DE RESULTADOS

En este capítulo muestra el análisis de datos para posteriormente demostrar la hipótesis planteada en el Capítulo I.

4.1. ANÁLISIS DE DATOS

Diagnóstico capa Programas Ejecutables, El usuario selecciona/ ingresa los valores conforme a lo detallado en la siguiente tabla:

CASO 1.-

Identificación	Sentencia	Valor
Entrada de Datos	Validación de Datos	Adecuado
	Política de Control de Programas	Adecuado
Verificación Control de Código Fuente	Criticidad Programas Fuente	Alta
	Validación de Procesamiento de Datos	Adecuado
Log de Aplicaciones	Planificación de Resguardo de Datos	Inadecuado
	Ejecución de Resguardo de Datos	Adecuado
	Control de Log de Aplicaciones	Adecuado
Resguardo de Datos	Ejecución de Resguardo de Datos	Adecuado
	Auditoria de Código Fuente	Adecuado
Acceso a Aplicaciones	Seguridad Externa	Cumple
	Autenticidad	Adecuada
Administración de Copias de Resguardo	Política de Resguardo de Programas	Adecuada

	Ejecución de Reguardo de Programas	Cumple
	Política de Recupero de Programas	Adecuada
	Ejecución de Recupero de Programas	Cumple
Integridad, Confidencialidad y Disponibilidad	Política de Resguardo de Programas	Adecuada
	Monitoreo de Resguardo de Programas	Adecuado

CUADRO 16 PROGRAMAS EJECUTABLES, VALORES

Resultados esperados de la capa de Repositorio de Datos:

Identificación	**Experto**	**Sistema Experto**	**Similitud Valor 1 = SI Valor 0 =NO**
Entrada de Datos	Se ajusta a una política y se valida la entrada de datos.	Es factible validar datos de entrada en las aplicaciones.	1
Verificación Control de Código Fuente	La información es altamente critica, se debe realizar control de código fuente	No es factible realizar control de código fuente	0
Log de Aplicaciones	Se recomienda realizar una auditoría a las actividades de los usuarios	Es factible efectuar auditoria de las actividades de los usuarios.	1
Resguardo de Datos	Se mantiene el concepto de integridad en los datos almacenados	Es factible mantener integridad en los datos almacenados.	1
Acceso a Aplicaciones	Se debe efectuar controles de autenticidad	Es factible garantizar la adecuada gestión de accesos a las aplicaciones.	0

Administración de Copias de Resguardo	Gestión de resguardo correcto	Es factible administrar las copias de resguardo de programas fuente adecuadamente.	1
Integridad, Confidencialidad y Disponibilidad	Se garantiza I – D – C en los programas fuente	Es factible garantizar la integridad, confidencialidad y disponibilidad de los programas fuente resguardados.	1
SUBTOTAL (SIMILITUDES DE 7 SUBDOMINIOS)			5

CUADRO 17 SIMILITUD ENTRE EXPERTO Y SISTEMA

Diagnóstico capa Repositorio de Datos, El usuario selecciona/ ingresa los valores conforme a lo detallado en la siguiente tabla:

Identificación	**Sentencia**	**Valor**
Acceso a la Base de Datos	Política de Acceso a Datos	Adecuado
	Comunicación de Acceso a Datos	Adecuado
Integridad de Datos	Ejecución de Acceso a Datos	Cumple
	Monitoreo de Acceso a Datos	Adecuado
Mecanismo Cifrado	Cifrado	Cumple
	Ejecución de Resguardo de Datos	Adecuado
	Política de Acceso a Datos	Adecuado
Administración de Copias de Datos	Política de Resguardo de Datos	Adecuada
	Ejecución de Reguardo de Datos	Cumple
	Política de Recupero de Datos	Adecuada
	Ejecución de Recupero de Datos	Cumple

Integridad, Confidencialidad y Disponibilidad de Datos	Política de Resguardo de Datos	Adecuada
	Monitoreo de Resguardo de Datos	Adecuado
	Simulación de Recupero de Datos	Cumple

CUADRO 18 REPOSITORIO DE DATOS, VALORES

Resultados esperados de la capa de Repositorio de Datos:

Identificación	**Experto**	**Sistema Experto**	**Similitud** **Valor 1 = SI** **Valor 0 =NO**
Acceso a la Base de Datos	Correcto acceso a Base de Datos	Es factible garantizar el correcto acceso a la Base de Datos.	1
Integridad de Datos	Con los atributos seleccionados se garantiza la integridad de datos	Es factible garantizar la integridad de los datos almacenados.	1
Mecanismo Cifrado	Es factible la encriptación de datos	Es factible almacenar datos sensibles a través de un mecanismo cifrado.	1
Administración de Copias de Datos	Existe una política formal para el resguardo y recupero y se cumple adecuadamente	Es factible administrar las copias de resguardo de Datos adecuadamente.	1
Integridad, Confidencialidad y Disponibilidad de Datos	Se garantiza I – D – C para los atributos	Es factible garantizar la integridad, confidencialidad y disponibilidad de los datos resguardados.	1
SUBTOTAL (SIMILITUDES DE 5 SUBDOMINIOS)			5

CUADRO 19 SIMILITUD ENTRE EXPERTO Y SISTEMA

Subdominio Programas ejecutables:

SUBTOTAL (SIMILITUDES DE 7 SUBDOMINIOS) = 5

Subdominio de Repositorio de Datos:

SUBTOTAL (SIMILITUDES DE 5 SUBDOMINIOS) = 5

CASO 1: TOTAL (SIMILITUDES DE 12 SUBDOMINIOS) = 10

Del mismo se realizaron 4 casos y se obtuvieron los siguientes resultados:

CASO 2: TOTAL (SIMILITUDES DE 12 SUBDOMINIOS) = 9

CASO 3: TOTAL (SIMILITUDES DE 12 SUBDOMINIOS) = 11

CASO 4: TOTAL (SIMILITUDES DE 12 SUBDOMINIOS) = 10

CASO 5: TOTAL (SIMILITUDES DE 12 SUBDOMINIOS) = 9

CASO	SIMILITUDES	SUBDOMINIOS	PORCENTAJES
1	10	12	83%
2	9	12	75%
3	11	12	92%
4	11	12	92%
5	10	12	83%
Medias	10,2	12	85%

CUADRO 20 CASOS DE ESTUDIO
Fuente Elaboración Propia

4.2. Prueba de Hipótesis

La presente investigación, plantea la hipótesis: “La implementación de un sistema experto en auditoria informática evalúa la seguridad de un sistema de información, lo que permitirá la identificación de vulnerabilidades, riesgos y amenazas”.

Para fines de prueba de hipótesis, se propone la hipótesis Nula: “La implementación de un sistema experto en auditoria informática **no** evalúa la seguridad de un sistema de información, lo que permitirá la identificación de vulnerabilidades, riesgos y amenazas”

Se realizó 5 casos de estudio, cada uno con 12 subdominios de los cuales se obtuvieron un promedio de similitud entre los resultados del Sistema Experto y el Experto del 85 %, para confirmar o no este supuesto se considera el nivel de significancia 0.05.

1. Formulamos las siguientes hipótesis H_0 y H_1:

   $H_0 : \mu = 8.5$ y $H_1: \mu \neq 8.5$

2. Nivel de significancia $\alpha = 0.05$

3. Puesto que n = 5 es pequeño y suponiendo que población tiene distribución normal, se usa la variable aleatoria que tiene una distribución t con n-1 = 4 grados de libertad.

$$T = \frac{\bar{X} - \mu_0}{S/\sqrt{n}}$$

4. La Región Critica: $T < t_{\alpha/2} = -2.776$ ó $T > t_{\alpha/2} = 2.776$, Con $\alpha/2=0.025$, en tablas $1 - \alpha/2=0.975$ luego la región de aceptación es <-2.776, 2.776>

5. Con los Datos $\bar{X} = 10.2$; $S = 0.8366$ y para n = 5, entonces:

$$T = \frac{10,2 - 8,5}{0,8366/\sqrt{5}}$$

$$T = 1.3258$$

6. Conclusión: ya que t = 1.3258 € a la Región de Aceptación se acepta $H_{0:}$ Se acepta el sistema experto con un grado de confianza de al menos un 85%

7. En la prueba realizada se acepta que al Sistema experto desarrollado con un grado de confianza de al menos un 85%; por lo cual el sistema experto evalúa la seguridad de un sistema de información, por tanto se rechaza la hipótesis Nula y se acepta la hipótesis de investigación.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

En este capítulo se realiza las conclusiones generales que se obtienen del trabajo de investigación, recomendaciones y propuestas de trabajo futuro

5.1. CONCLUSIONES GENERALES

El desarrollo del prototipo de Sistema experto para la Auditoria de Sistemas de Información, permitió la identificación de amenazas, riesgos y vulnerabilidades, a manera de recomendaciones correctivas.

Con base en los casos de estudio realizados, que se puede observar en la tabla se constata que el sistema tiene un grado de similitud del 85% entre los resultados obtenidos del sistema experto en la relación ala criterio del experto.

La herramienta brinda al auditor un marco teórico practico para un relevamiento en tareas de auditoria, basados en aspectos fundamentales que involucra al desarrollo de aplicaciones, abarcando no solo las tareas de una unidad de desarrollo, si no también haciendo parte de esta al nivel gerencial de una organización para que forme parte integral en el desarrollo de aplicaciones y tengan conocimiento sobre las tareas que se desarrollan en una unidad de sistemas.

Aplica, para el área de Ingeniería en Conocimiento, un marco metodológico a través de la metodología IDEAL, asegurando el desarrollo y posterior crecimiento del Sistema Experto, en los aspectos relativos al mantenimiento del conocimiento.

Sistematización y documentación, con metodología de Sistemas Expertos, el conocimiento requerido para el área de la seguridad de la información de aplicaciones. Del mismo modo se documenta y modela la educción y extracción de conocimiento. Se apoya en técnicas de adquisición de conocimiento, la elaboración de una taxonomía de los requisitos funcionales

y no funcionales, la conceptualización de los conocimientos estratégicos, facticos y tácticos para el domino de seguridad de las aplicaciones, la formalización y la posterior implementación de un prototipo, validado a través de casos de pruebas determinados.

5.2. CUMPLIMIENTO DE LOS OBJETIVOS

El objetivo general: "Desarrollar un sistema experto para la Auditoría Informática a la seguridad de la información de aplicaciones software, que permita evaluar e identificar las amenazas y riesgos existentes. Además proporcione recomendaciones", se cumple con el modelado y desarrollo de un sistema experto siguiendo las fases de la metodología de sistemas experto IDEAL explicado en Capítulo 3.

El objetivo específico: "Adquirir conocimiento heurístico del experto, relacionado a la seguridad de la información", se cumple con la adquisición del conocimiento mediante el método Grover explicado en Capítulo 3.

El objetivo específico: "Desarrollo de un sistema experto de acuerdo al dominio planteado, para la implementación del mismo", se cumple al identificar dos dominios: Programas ejecutables y repositorio de datos, y desarrollar el sistema en el marcos de los dominios explicado en Capítulo 3.

El objetivo específico: "Evaluar el sistema experto construido", se cumple con las pruebas de estudio realizadas, contrastando los resultados del sistema con el criterio del experto explicado en Capítulo 4.

5.3. ESTADO DE LA HIPOTESIS

Se realizó estudios de caso con el promedio de similitud entre los resultados del Sistema Experto y el Experto del 85 %, por lo cual se verificó con la prueba de T Student con nivel significación de 0.05, que el sistema experto tiene un grado de confianza de al menos un 85%.

Al aceptar que el Sistema experto tiene un grado de similitud del 85% con el criterio del Experto se verifica que el sistema experto en auditoria informática evalúa la seguridad de

un sistema de información, lo que permitirá la identificación de vulnerabilidades, riesgos y amenazas, por lo cual se acepta la hipótesis planteada.

5.4. RECOMENDACIONES

Incrementar los dominios de estudios, con el propósito de aumentar la confiabilidad de las auditorias de los sistemas de información.

Debido al constante cambio de las tecnologías de la información y en consecuencia a la actualización de las normas y metodologías de seguridad de la información, se recomienda la investigación de otras normas e instrumentos de evaluación que puedan contribuir en el mejoramiento de las organizaciones.

Las Auditorias Informáticas se deben realizar de forma periódica al igual que las auditorias financieras, ya que de estas evaluaciones dependen el control, mejoramiento y prevención de riesgos en las instituciones.

Se recomienda realizar otras investigaciones en el campo de la auditoria informática y seguridad de la información ampliando los dominios de conocimiento, ya que estos lograran un óptimo funcionamiento de las unidades sistemas.

5.5. TRABAJOS FUTUROS

A continuación se lista las sugerencias de trabajos futuros:

- Desarrollo de sistema experto para computadoras de bolsillo.
- Realizar un estudio de JESS y JAVA, para el desarrollo de Sistemas Expertos
- Desarrollo de un sistema experto para la Auditoria informática, con un motor de inferencia basado en COBIT.

REFERENCIAS BIBLIOGRAFICAS

[Piattini, 2001] Mario G. Piattini, Emilio del Peso (2001).”AUDITORIA INFORMATICA” Un Enfoque Práctico, Segunda edición

[Echenique, 2001] José Antonio Echenique García (2001).”Auditoría en Informática”, segunda edición.

[ISO 27002, 2007] Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información, Instituto boliviano de Normalización y Calidad (IBNORCA), Primera Edición, Noviembre 2007.

[ISO 27001, 2007] Tecnología de la información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la información - Requisitos, Instituto boliviano de Normalización y Calidad (IBNORCA), Primera Edición, Noviembre 2007.

[COBIT 4.1, 2005] Objetivos de Control para la Información y las Tecnologías, IT Governance Institute (ITGI).

[Castillo, 2000] Enrique Castillo, José Manuel Gutiérrez y Ali S. Hadi (2000), Sistemas Expertos Y Modelos de Redes Probabilísticos, Universidad de Cantabria Santander España.

[Martínez, 2009] Martínez Díaz María del Carmen (2009). "Aprendizaje Artificial y sistemas expertos" llevado a cabo en la División de Sistemas del Departamento de Ciencias Básicas de la Universidad Nacional de Luján. Disponible en: http://www.unl.edu.mx.

[Russell y Norvig, 2004] Stuart J. *Russell* y Peter Norvig, INTELIGENCIA ARTIFICIAL. UN ENFOQUE MODERNO. Segunda edición, 2004.

[Lahoz, 2004] Rafael Lahoz, 2004: Bioinformática simulación, vida artificial e inteligencia artificial 455, Edición Díaz de Santo. S. A. Madrid.

[Flores, 2008] Flores Yujra Alejandra Yumar. "MODELO DE AUDITORIA INFORMATICA PARA LA SEGURIDAD FISICA". La Paz-Bolivia 2008.

[Cuela, 2009] José Luis Cuela Mamani. "HERRAMIENTA METODOLOGICA PARA LA REALIZACION DE AUDITORIAS INFORMATICAS EN ORGANIZACIONES", La Paz-Bolivia 2009.

[Surco, 2009] David Juan Surco Limachi. "Diseño de Auditoría Informática", La Paz-Bolivia 2009.

[ISACA, 2013] Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), publicado en la pagina http://www.isaca.org/Spanish/Pages/default.aspx [Fecha de acceso, 2013]

[Gutierrez, 2006] José Manuel Gutierrez, 2006: Sistemas Expertos Basados en Reglas, publicado en internet http://personales.unican.es/gutierjm/cursos/expertos/Reglas.pdf .

[Criado, 2005] Criado J., 2005: Sistemas Expertos, publicado en internet http://homeworldonline.es/jmariocr/

[Pignani, 2006] Pigani Juan Manuel, 2006: Sistemas Expertos, publicado en internet http://www.unlu.edu.ar/ogarcia/

[Salavador, 2006] Jorge Salvador Ierache, 2006, Sistema experto para el entrenamiento y asistencia en la toma de decisiones en un Centro de Información y Control Aéreo

[García, Rossi y Britos, 2006] Ramón García Martínez, Bibiana Rossi y Paola Britos, 2006 Metodologías de Educación de Conocimiento para la construcción de sistemas informáticos expertos.

[Vergara, 2004] David Esteban Vergara Zapata, Introduccion a la programación multicapas, publicado en internet http://www.elguille.info/colabora/puntoNET/jevergara_Multitier.htm