UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACION

ESCUELA DE INGENIERIA EN SISTEMAS

"Software de Auditoría para la Gestión de Recursos de TI basado en Cobit"

Monografía previo a la obtención del Título de
Ingeniero de Sistemas.

Autores:

Daniel Vintimilla A.
David Zamora R.

Director:
Ing. Lenín Erazo Garzón

Cuenca, Ecuador
2012

DEDICATORIA

Dedico este trabajo de Graduación a mí Familia, a mi novia Cristina y a Dios por el apoyo incondicional que me han dado siempre para alcanzar las metas que me he planteado.

Daniel.

Deseo dedicar este trabajo de Graduación a Dios por que guía mi vida, a mis padres y a mi esposa Anne, que con amor y apoyo me acompañan cada día.

David.

AGRADECIMIENTOS

Agradezco a Dios por las bendiciones y oportunidades que ha puesto en mi camino.

A mis Abuelos, a mi Ma, a mi Tío Rafa y mi familia quienes siempre me apoyaron, educaron e inculcaron los valores que han guiado mi vida.

Daniel.

Agradezco a Dios por su amor y generosidad ya que ha sido mi fortaleza para vivir.

A mis padres, que me han inculcado con su amor y ejemplo, las buenas costumbres y principios para llevar una vida digna.

A mi esposa Anne que alegra cada uno de mis días.

David.

Agradecemos a la Universidad del Azuay por el nivel de educación impartido a lo largo de nuestros estudios, de igual forma al Ing. Lenín Erazo por sus conocimientos trasmitidos y por haber dirigido este trabajo de Grado.

Índice de Contenidos

Índice de Ilustraciones

Resumen

El presente trabajo de graduación en el aspecto teórico, da a conocer los conceptos básicos de Cobit, sus prácticas y su utilización en la auditoría de sistemas. En cuanto a la parte práctica comprende la implementación de una solución informática que permita al personal de auditoría realizar un análisis claro y conciso mediante formularios e informes en lo que comprende al manejo de recursos según la metodología Cobit en una empresa. La aplicación es desarrollada en un ambiente web, facilitando de esta manera al auditor la utilización de la misma, de igual manera al cliente y administradores de la empresa auditora para visualizar los resultados obtenidos por la aplicación.

ABSTRACT

The present graduation project presents the theoretical concepts of the COBIT methodology, its practice and use in the audit system. As for the practical aspect, the project presents the implementation of an informatics solution that will allow performing a clear and concise analysis through resource management forms and reports employed by the COBIT methodology. The application is developed in a web environment, which makes it easy to use by the auditor, the client, and the administrators of the audit company, helping them visualize the results obtained through this application.

Translated by,

Diana Lee Rodas

Introducción

En la actualidad la utilización de un sistema informático dentro de un negocio es considerado primordial ya que sin él no podrá competir con los que sí lo poseen. Las aplicaciones informáticas permiten ahorrar recursos, optimizar procesos, organizar y garantizar el manejo de la información, todo ello con el fin de aportar a la consecución de los objetivos y estrategias de la empresa.

El realce de Cobit para poder gestionar un Gobierno de TI se produce en búsqueda de buenas prácticas internacionales en el mercado de desarrollo y el uso de software, hardware y telecomunicaciones, para implementar soluciones tecnológicas que faciliten las tareas y procesos presentes en las diversas actividades de negocio.

He aquí donde se requiere la implementación de una aplicación web basada en Cobit, con un enfoque en la gestión de recursos para la realización de una Auditoría de calidad. En la misma se consideran procesos de Adquisición e implementación, entrega y soporte, monitorización y evaluación para el manejo de recursos, todo esto contribuirá para cumplir los objetivos de la empresa.

La utilización de este software no garantizara el éxito de la empresa, sin embargo de hecho proveerá una importante ventaja competitiva a la misma.

La aplicación implementa una solución que permita al auditor contar con una herramienta sencilla y confiable para registrar los datos requeridos por el procedimiento de auditoría en la gestión de recursos de la empresa, que inmediatamente serán tabulados y resueltos por la aplicación.

En lo que corresponde al cliente y a la empresa auditora contarán con una herramienta de consulta en línea de los resultados obtenidos por la aplicación sobre la auditoría realizada, todo esto según los privilegios de usuario correspondientes a cada uno de ellos, los mismos que serán configurados previamente en la aplicación según se halla estipulado en el contrato de servicios.

Definiciones, abreviaturas y acrónimos

Auditoría: Es el proceso de recolección y evaluación de evidencias utilizadas para determinar cuándo un sistema mantiene la integridad de sus datos, salvaguarda sus activos, ejecuta eficazmente con efectividad los objetivos marcados por la Organización y consume los recursos eficientemente.

Auditoría Informática: Es la revisión técnica, especializada y exhaustiva, que se realiza a los sistemas computacionales, software e información utilizados en una empresa sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes.

Enlace: Un enlace (también llamado hipervínculo, vínculo, o hiperenlace) es un elemento de un documento electrónico que hace referencia a otro recurso, por ejemplo una página web, a otro recurso, o a una posición determinada en una página web.

ISACA: Asociación para la Auditoría y Control de Sistemas de Información.

ITGI: Instituto de Administración de las Tecnologías de la Información.

CISA: CertifiedInformationSystems Auditor – Certificación para auditores respaldada por la Asociación ISACA.

CISM: CertifiedInformation Security Manager – Gerente certificado en Seguridad de la Información.

CISSP: CertifiedInformationSystems Security Professional. – Certificación para profesionales con formación en el área de seguridad de la información.

CGEIT: Certified in theGovernance of Enterprise IT – Es un Certificado en Gobierno de Tecnologías de la Información Empresarial.

CRISC: CertifiedRisk and InformationSystems Control – Es un Certificado en Riesgo y Control de Sistemas de Información.

COSO: Committee of SponsoringOrganizations of theTreadwayCommission- El Comité de Organizaciones Patrocinadoras de la Comisión Treadway.A través del desarrollo de los marcos y directrices sobre la gestión del riesgo, provee liderazgo, control interno y la disuasión del fraude.

COBIT: Objetivos de Control para Tecnologías de información y relacionadas.

CAPITULO 1

Gobierno de las Tecnologías de la Información (TI)

1.1 Introducción.

Las tecnologías de la información y la comunicación son un conjunto de servicios, redes, software, aparatos que tienen como fin la mejora de la calidad de vida de las personas dentro de un entorno, y que se integran a un sistema de información interconectado y complementario.

ILUSTRACION # 1

El gobierno de TI es una estructura de relaciones y procesos para dirigir y controlar la empresa con el objeto de alcanzar los objetivos de la misma y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos.

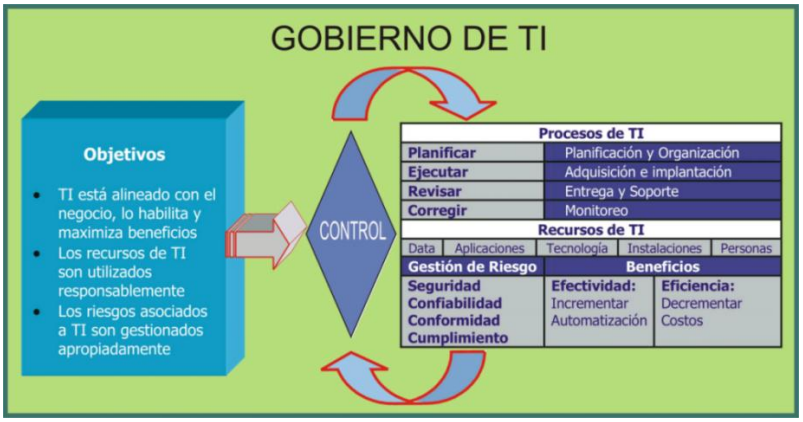
Las empresas exitosas reconocen los beneficios de la tecnología de información y la utilizan para impulsar el valor de sus interesados. Los más valiosos activos que poseen muchas empresas son la información y la tecnología que las soportan, aunque con frecuencia son poco entendidos.

El Gobierno Empresarial es parte integral de las TI, el mismo consiste en el Liderazgo, los Procesos y las Estructuras Organizacionales que aseguran que las estrategias y los objetivos de la organización, se sustentan y extienden adecuadamente en el ámbito de las tecnologías de la información.

El valor, el riesgo y el control constituyen la esencia del gobierno de TI, en resumen un Gobierno de TI debe administrarse con “Certidumbre y Control”.

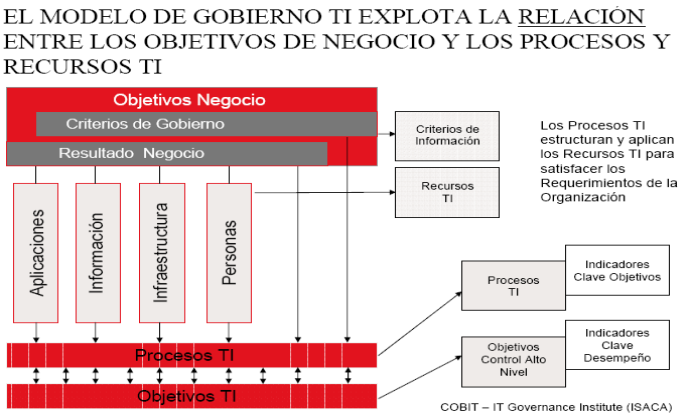
1.2 Objetivos.

Un Objetivo de Control en TI es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de TI.



ILUSTRACION # 2

El Gobierno TI es una metodología, no una solución. Las empresas deben satisfacer la calidad, optimizar los requerimientos monetarios a partir del presupuesto y garantizar la seguridad de su información, así como de todos sus activos. La dirección también debe optimizar el uso de los recursos disponibles de TI, incluyendo aplicaciones, información, infraestructura y personas. Para descargar estas responsabilidades, así como para lograr sus objetivos, la dirección debe entender el estatus de su arquitectura empresarial para TI y decidir qué tipo de gobierno y de control debe aplicar.



ILUSTRACION # 3

1.3 Principales Responsabilidades.

1. Evaluar la efectividad de la estructura de gobierno de TI para asegurar el control adecuado de la Junta sobre las decisiones, las instrucciones y el desempeño de TI, para que soporte las estrategias y objetivos de la organización.
2. Evaluar la estructura organizativa de Tl y la administración de los recursos humanos (personal) para asegurar que éstos soporten las estrategias y objetivos de la organización.
3. Evaluar la estrategia de TI y el proceso para su desarrollo, aprobación, implementación y mantenimiento para asegurar que soporta las estrategias y objetivos de la organización.
4. Evaluar las políticas, los estándares, los procedimientos y los procesos de TI de la organización para desarrollarlos, aprobarlos, implementarlos y mantenerlos, para asegurar que éstos soporten la estrategia de TI y cumplan con los requerimientos regulatorios y legales.
5. Evaluar las prácticas gerenciales para asegurar el cumplimiento con la estrategia, las políticas, los estándares y los procedimientos de TI de la organización.
6. Evaluar la inversión de recursos de TI, el uso y las prácticas de asignación para asegurar que están en conformidad con las estrategias y objetivos de la organización.
7. Evaluar las estrategias y políticas de contratación de TI y las prácticas de administración de contratos para asegurar que soporten las estrategias y los objetivos de la organización.
8. Evaluar las prácticas de administración de riesgos, para asegurar que los riesgos relacionados con TI de la organización sean debidamente administrados.
9. Evaluar las prácticas de monitoreo y aseguramiento, para asegurar que la Junta y la Alta Dirección reciban información suficiente y oportuna sobre el desempeño de TI.

1.4 Ciclo de vida del Servicio TI.

Para las empresas la creciente importancia de la información hace que estas sometan la calidad de sus servicios de información a requisitos internos y externos más estrictos. Los estándares desempeñan un rol cada vez más importante, mientras que los marcos de

trabajo de “Mejores Prácticas” contribuyen al desarrollo de un sistema de gestión que satisfaga los requisitos exigidos. Es por ello que las organizaciones, públicas o privadas, que no controlen sus procesos de información no podrán conseguir buenos resultados en el nivel del Ciclo de Vida del Servicio de (TI), ni en la gestión de punta a punta de dichos servicios para obtener la mejor alineación entre el negocio y las TI.

ILUSTRACION # 4

El concepto de Gerencia Estratégica de TI se fundamenta en las mejores prácticas de Gestión de Servicio y Gobierno de TI, ITIL y COBIT respectivamente.

1.5 Enfoque de la Gestión de TI.

La gestión de TI se enfoca en atender:

- Objetivos Alineados con negocio.
- Patrimonio Debidamente cuidado.
- Intereses Máximo valor.

La Gestión de TI se encarga de:

- Recursos.
- Políticas, procesos, organización y métricas.

La Gestión de TI tiene que tomar en cuenta:

- Restricciones.
- Riesgos: (conocidos y administrados).
- Responsabilidad: máxima eficiencia, máximo valor.

1.5.1 TI Orientadas a Optimizar la Gestión de Recursos.

Se enfoca en inversiones óptimas y la gestión correcta de los recursos críticos de TI: aplicaciones, información, infraestructura y gente.

Una adecuada gestión de recursos por parte de TI abarca las siguientes áreas.

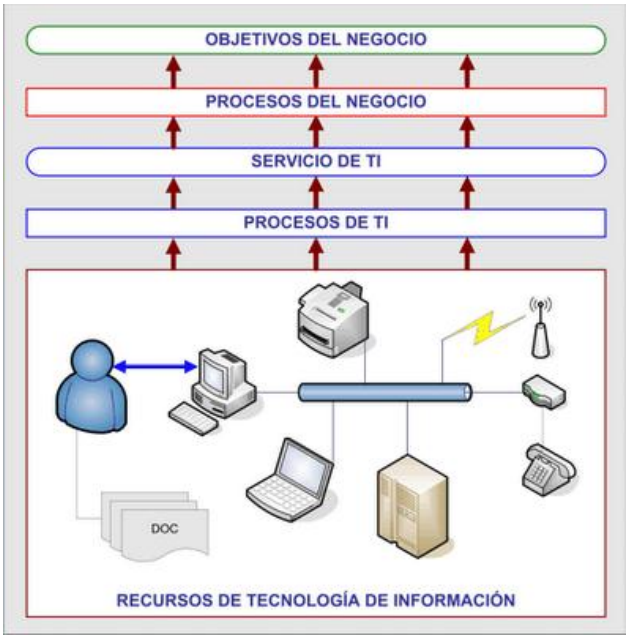
– Maximizar el uso de los recursos en la tarea y lugares apropiados.

– Calidad de servicios de TI, acuerdos de nivel de servicio con el negocio.

– Gestión del talento humano.

– Entrenamiento y desarrollo de habilidades.

– Instalaciones.



ILUSTRACION # 5

Una estrategia de mediano y largo plazo ayuda a gestionar la situación actual y a desarrollar competencias y capacidades para el futuro.

CAPITULO 2

COBIT (Control Objetives for Information and RelatedTechnology) Basado en ISACA

2.1 ISACA

Es un líder mundialmente reconocido, proveedor de conocimiento, certificaciones, comunidad, apoyo y educación en seguridad y aseguramiento de sistemas de información, gobierno empresarial, administración de TI así como riesgos y cumplimiento relacionados con TI. Tiene más de 95.000 miembros en 160 países, fue fundada en 1969, es independiente y no lucrativa. Su principal objetivo es organizar conferencias internacionales, las mismas que publica en un diario de su sitio web. ISACA se encarga de desarrollar estándares internacionales de auditoría y control de sistemas de información que ayudan a sus miembros a garantizar la confianza y el valor de los sistemas de información, de igual manera se encarga de certificar los avances y habilidades de los conocimientos de TI a través CISA, CISM, CGEIT y CRISC.

ISACA actualiza continuamente a COBIT, que ayuda a los profesionales y líderes empresariales de TI a cumplir con sus responsabilidades de administración y gestión, particularmente en las áreas de aseguramiento, seguridad, riesgo y control, para agregar valor al negocio.

2.2 Introducción a COBIT

Cobit es un marco de referencia y un paquete de herramientas de soporte que permiten a la gerencia estrechar la brecha con respecto a los requerimientos de control, temas técnicos y riesgos de negocio, y comunicar ese nivel de control a los participantes. El enfoque de Cobit es desarrollar políticas claras y de buenas prácticas para control de TI en las empresas, constantemente se actualiza y armoniza con otros estándares, se ha convertido en el integrador de las mejores prácticas de TI y el marco de referencia general para el gobierno de TI que ayuda a comprender y administrar los riesgos y beneficios ligados a TI. La estructura de procesos de Cobit y su enfoque de alto nivel orientado al negocio

brindan una visión completa de TI y de las decisiones a tomar acerca de las mismas.

2.3 Beneficios de implementar COBIT sobre TI.

COBIT se basa en proporcionar la información que la empresa requiere para lograr sus objetivos, la empresa necesita administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información.

ILUSTRACION # 6

• Mejor alineación, con base al enfoque del negocio.

• Una visión, entendible para la gerencia, sobre que hace TI.

• Propiedad y responsabilidades claras, con base a la orientación a procesos de la empresa.

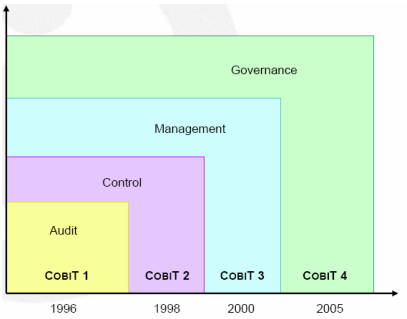
• Aceptación general de terceros y reguladores de la metodología de Cobit.

• Entendimiento compartido entre todos los participantes, con base en un lenguaje común.

• Cumplimiento de los requerimientos COSO para el ambiente de control de TI.

2.4 Historia y evolución de COBIT

El modelo fue creado por ISACA e ITGI. La primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000; la cuarta edición en diciembre de 2005, la versión 4.1 está disponible desde mayo de 2007, y el lanzamiento de la quinta edición está previsto para el primer trimestre del año 2012.



ILUSTRACION # 7

En su cuarta edición, COBIT tiene 34 objetivos de alto nivel que cubren 318 objetivos de control específicos clasificados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte; y, Supervisión y Evaluación.

2.5 Enfoque sobre las áreas de gobierno de TI

2.5.1 Enfocado al Negocio

La orientación a negocios es el tema principal de COBIT, está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI, sino también y principalmente, como guía integral para la gerencia y para los propietarios de los procesos de negocio.

El marco de trabajo COBIT ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

Para que los objetivos del negocio se cumplan, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en COBIT como requerimientos de información del negocio.

2.5.1.1Criterios de Información de Cobit.

• La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

• La eficiencia consiste en que la información sea generada optimizando los recursos (más productivo y económico).

• La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.

• La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.

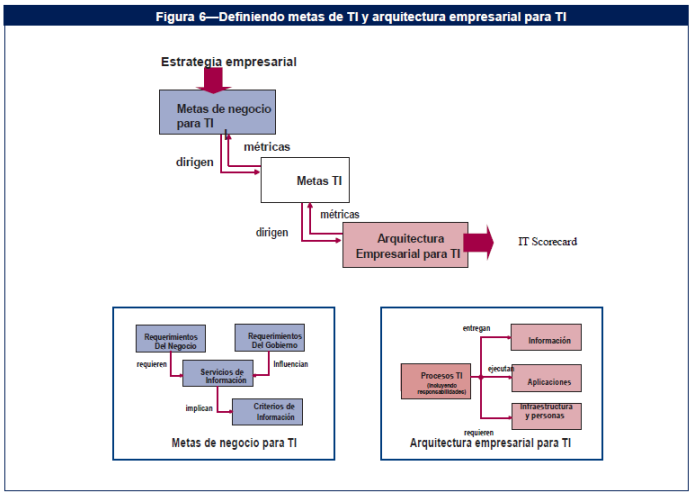
• La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento, así como con la protección de los recursos y las capacidades necesarias asociadas.

• El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios, es decir, criterios de negocios impuestos externamente, así como políticas internas.

• La confiabilidad significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades fiduciarias y de gobierno.

2.5.1.2 Metas de Negocios y de TI.

La definición de un conjunto de metas genéricas de negocio y de TI ofrece una base más refinada y relacionada con el negocio para el establecimiento de requerimientos de negocio y para el desarrollo de métricas que permitan la medición con respecto a estas metas. Cada empresa usuaria de TI, habilita las iniciativas del negocio y estas pueden ser representadas como metas del negocio para TI.



ILUSTRACION #8

Estos ejemplos genéricos se pueden utilizar como guía para determinar los requerimientos, metas y métricas específicas del negocio para la empresa.

Si se pretende que la TI proporcione servicios de forma exitosa para dar soporte a la estrategia de la empresa, debe existir una propiedad y una dirección clara de los requerimientos por parte del negocio (el cliente) y un claro entendimiento para TI, de cómo y qué debe entregar (el proveedor). La Figura 6 ilustra como la estrategia de la empresa se debe traducir por parte del negocio en objetivos para su uso de iniciativas facilitadas por TI (Las metas de negocio para TI). Estos objetivos a su vez, deben conducir a una clara definición de los propios objetivos de la TI (las metas de TI), y luego éstas a su vez definir los recursos y capacidades de TI (la arquitectura empresarial para TI) requeridos para ejecutar de forma exitosa la parte que le corresponde a TI de la estrategia empresarial. Todos estos objetivos se deben expresar en términos de negocios significativos para el cliente, y esto, combinado con una alineación efectiva de la jerarquía de objetivos, asegurará que el negocio pueda confirmar que TI puede, con alta probabilidad, dar soporte a las metas del negocio.

2.5.1.3 Recursos de TI.

La organización de TI se desempeña con respecto a estas metas como un conjunto de procesos definidos con claridad que utiliza las habilidades de las personas, y la infraestructura de tecnología para ejecutar aplicaciones automatizadas de negocio, mientras que al mismo tiempo toma ventaja de la información del negocio. Estos recursos, junto con los procesos, constituyen una arquitectura empresarial para TI, como se muestra en la figura 6. Para responder a los requerimientos que el negocio tiene hacia TI, la empresa debe invertir en los recursos requeridos para crear una capacidad técnica adecuada (ej., un sistema de planeación de recursos empresariales) para dar soporte a la capacidad del negocio (ej., implementando una cadena de suministro) que genere el resultado

deseado (ej., mayores ventas y beneficios financieros). Los recursos de TI identificados en COBIT se pueden definir como sigue:

• Las aplicaciones incluyen tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.

• La información son los datos en todas sus formas de entrada, procesados y generados por los sistemas de información, en cualquier forma en que son utilizados por el negocio.

• La infraestructura es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

• Las personas son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por outsourcing o contratadas, de acuerdo a como se requieran.

2.5.2 Orientado a Procesos

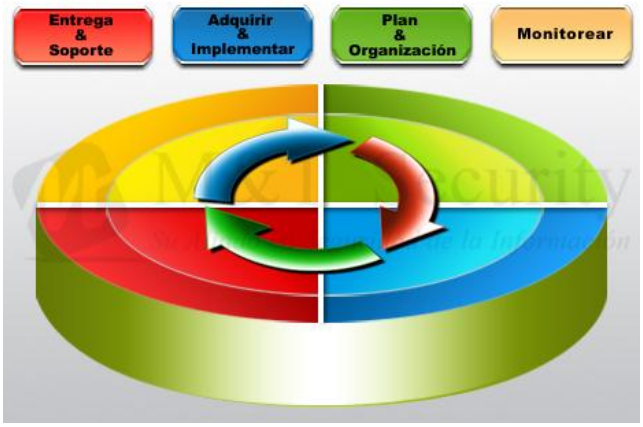
Cobit define las actividades de TI en un modelo genérico de procesos en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar.

Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Cobit ha identificado 34 procesos generalmente utilizados dentro de estos dominios.

Para cada uno de los procesos se tiene una relación con los objetivos de TI y los objetivos del negocio.

En el presente trabajo de graduación realizamos una selección de procesos según el área en la que nos enfocamos “La Gestión de Recursos de TI”, la misma que esta en el Anexo 1.



ILUSTRACION #9

PLANEAR Y ORGANIZAR (PO)

Este dominio es el que cubre las estrategias y las tácticas, está relacionado con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio, 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.

Este dominio cubre los siguientes cuestionamientos típicos de la gerencia:

• ¿Están alineadas las estrategias de TI y del negocio?

• ¿La empresa está alcanzando un uso óptimo de sus recursos?

• ¿Entienden todas las personas dentro de la organización los objetivos de TI?

• ¿Se entienden y administran los riesgos de TI?

• ¿Es apropiada la calidad de los sistemas de TI para las necesidades del negocio?

ADQUIRIR E IMPLEMENTAR (AI)

Para que la estrategia de TI pueda ser llevada a cabo, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. De igual manera, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

Este dominio, por lo general es el que cubre los siguientes cuestionamientos de la gerencia:

• ¿Los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?

• ¿Los nuevos proyectos son entregados a tiempo y dentro del presupuesto?

• ¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?

• ¿Los cambios afectarán las operaciones actuales del negocio?

ENTREGAR Y DAR SOPORTE (DS)

Este dominio es quien cubre la entrega en sí de los servicios requeridos, lo que incluye 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 operacionales.

Aclara las siguientes preguntas de la gerencia:

•¿Se están entregando los servicios de TI de acuerdo con las prioridades del negocio? •¿Están optimizados los costos de TI?

•¿Es capaz la fuerza de trabajo de utilizar los sistemas de TI de manera productiva y segura?

•¿Están implantadas de forma adecuada la confidencialidad, la integridad y la disponibilidad?

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

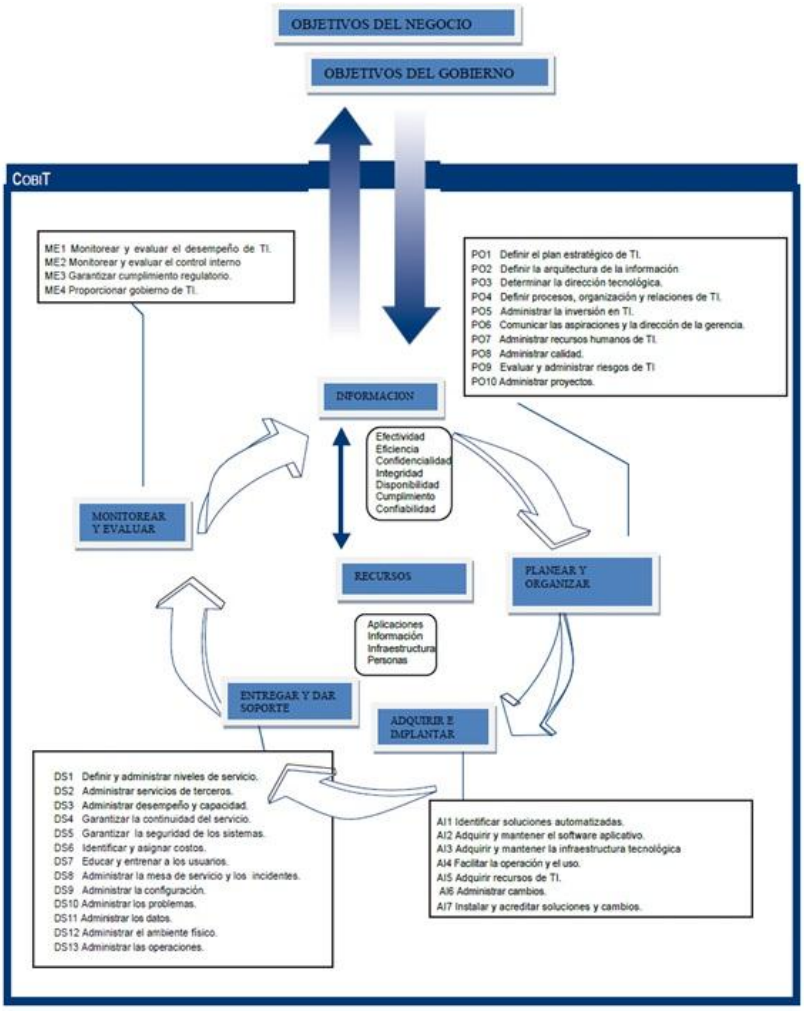
Responde a las siguientes preguntas de la gerencia:

•¿Se mide el desempeño de TI para detectar los problemas antes de que sea demasiado tarde?

•¿La Gerencia garantiza que los controles internos son efectivos y eficientes?

•¿Puede vincularse el desempeño de lo que TI ha realizado con las metas del negocio?

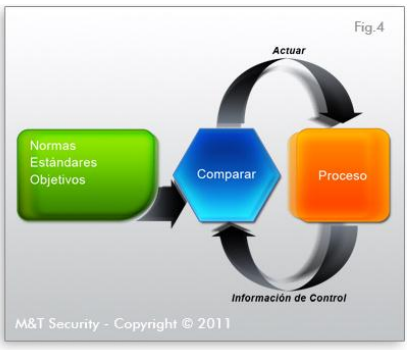
•¿Se miden y reportan los riesgos, el control, el cumplimiento y el desempeño?



ILUSTRACION #10

2.5.3 Basado en Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales que proveen aseguramiento razonable de que los objetivos del negocio serán alcanzados y los eventos no deseados serán prevenidos, detectados y corregidos.



ILUSTRACION #11

2.5.4Administrado por Medidas

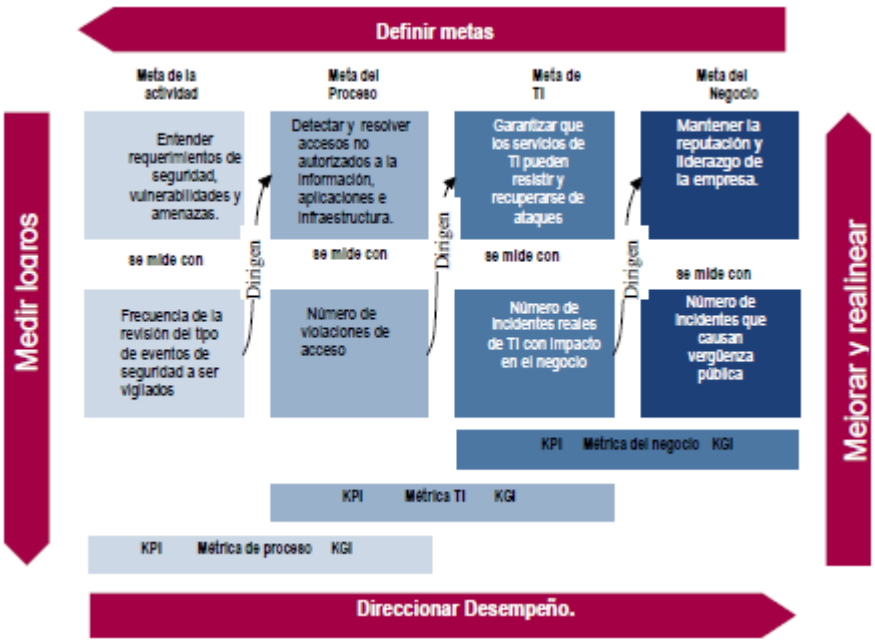
Para una empresa es clave entender el estado de sus propios sistemas de TI y decidir qué nivel de administración y control debe proporcionar a la misma. La obtención de una visión objetiva del nivel de desempeño propio de una empresa no es sencilla. Las empresas deben medir dónde se encuentran y dónde se requieren mejoras, e implementar un juego de herramientas gerenciales para monitorear esta mejora. Para decidir cuál es el nivel correcto, la gerencia debe preguntarse a sí misma:

¿Qué tan lejos debemos ir, y si está o no justificado el costo por el beneficio?

Para ello se requieren:

1. Modelos de Madurez que faciliten la evaluación mediante el benchmarking e identificación de mejoras en la capacidad.
2. Metas y mediciones de desempeño para los procesos de TI, que demuestran cómo los procesos satisfacen las necesidades de negocio y de TI, y cómo se usan para medir el desempeño de los procesos internos basados en los principios del Balanced Scorecard.
3. Metas de actividades para facilitar el desempeño efectivo de los procesos.

Existe una relación entre proceso, metas y métricas que está ilustrado en el siguiente gráfico.



ILUSTRACION #12

2.6 Grafico RACI (Matriz de Asignación de Responsabilidades)

Matriz RACI

Actividades	CEO	CFO	Ejecutivo del Negocio	CIO	Dueño de Proceso del Negocio	Jefe de Operaciones	Arquitecto en Jefe	Jefe de Desarrollo	Jefe de Administración de TI	PMO	Cumplimiento, Auditoría, Riesgo y Seguridad
	Funciones										
Crear y mantener modelo de información corporativo / empresarial		C	I	A	C		R	C	C		C
Crear y mantener diccionario de datos corporativo				I	C		A/R	R			C
Establecer y mantener esquema de clasificación de datos	I	C	A	C	C	I	C	C			R
Brindar a los dueños procedimientos y herramientas para clasificar los sistemas de información	I	C	A	C	C	I	C	C			R
Usar el modelo de información, el diccionario de datos y el esquema de clasificación para planear los sistemas optimizados de negocio	C	C	I	A	C		R	C			I

Una matriz **RACI** identifica quien es **R**esponsable, quien debe rendir cuentas (**A**), quien debe ser **C**onsultado y/o **I**nformado

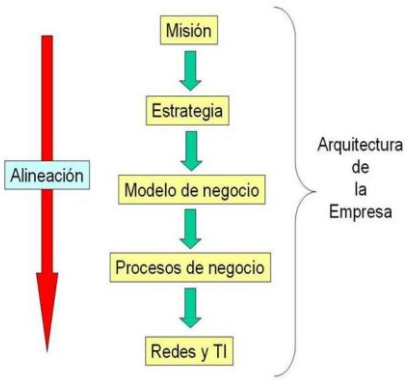
CAPITULO 3

Requisitos Previos a la Auditoría

3.1 Análisis Previo

3.1.1 Tamaño de Empresa

Para hacer una adecuada planeación de la auditoría en informática, hay que seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo; con ello podremos determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato deservicios.



ILUSTRACION #13

La naturaleza y alcance del planteamiento puede variar según el tamaño del ente, el volumen de sus operaciones, la experiencia del auditor y el conocimiento de las operaciones.

3.1.2 Tipo de Empresa

La Auditoría Informática se aplica en especial a empresas que poseen tecnologías de comunicaciones y/o sistemas de información que están conectados ya sea mediante intranet o internet, los recursos informáticos en la mayoría de los casos están ligados al tamaño de la empresa o a la actividad económica de la misma, siendo esta la que determine la cantidad de infraestructura informática presente.

Empresas según su tamaño

Grande: Su constitución se soporta en grandes cantidades de capital, un gran número de trabajadores y el volumen de ingresos al año, su número de trabajadores excede a 100 personas, cuenta con una infraestructura informática grande, una intranet estructurada, un departamento de informática encargado del manejo de los recursos de hardware y software de la empresa.

Mediana: Su capital, el número de trabajadores y el volumen de ingresos son limitados y muy regulares, número de trabajadores superior a 20 personas e inferior a 100, su infraestructura informática es media, cuando sus trabajadores superan los treinta cuentan con uno o varios responsables del área informática.

Pequeñas: No cuentan con un departamento o un responsable encargado del área informática, poseen recursos de hardware y software limitados. Se dividen a su vez en.

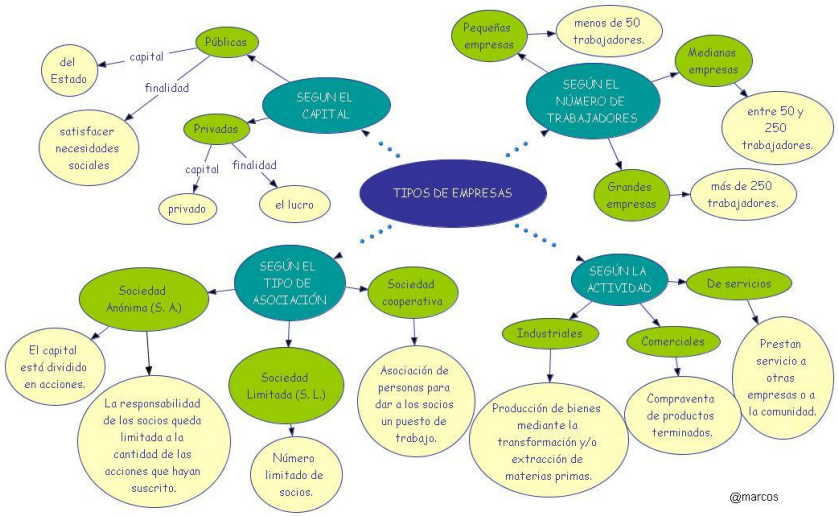
Pequeña: Su capital, número de trabajadores y sus ingresos son muy reducidos, el número de trabajadores no excede de 20 personas.

Micro: Su capital, número de trabajadores y sus ingresos solo se establecen en cuantías muy personales, el número de trabajadores no excede a 10 trabajadores.

Empresas Familiares: Es un nuevo tipo de explotación en donde la familia es el motor del negocio convirtiéndose en una unidad productiva.

La aplicación de auditoría desarrollada en el presente trabajo de graduación está enfocada para empresas de tamaño pequeño o mediano, debido a su diseño y alcance.

Tipos de Empresa:



ILUSTRACION #14

3.1.3 Recursos Necesarios para el análisis

3.1.3.1 Mesa de Ayuda

Conocida como HelpDesk, es un servicio dedicado a recibir y registrar todos los incidentes de tecnología de la información y brinda asistencia telefónica directa, desempeñando el rol del primer nivel de soporte para consultas de uso de software base, software de escritorio y computadoras personales con sus dispositivos.

En el caso de incidentes que requieran un nivel mayor de especialización, estos serán escalados al soporte apropiado. Los tipos de incidentes que tengan un proveedor externo como responsable del servicio serán canalizados y monitoreados por la mesa de ayuda.

Los incidentes pueden involucrar recursos de TI como software base (sistemas operativos) y software de escritorio (automatización de oficina, control de virus,

etc), software de red (correo electrónico, base de datos, servicios de internet, etc), software aplicativo, computadoras personales, sus dispositivos (impresoras, escaners, etc) y accesorios; además de componentes asociados con la infraestructura informática.

Los tipos de incidentes que pueden reportarse en la mesa de ayuda son:

- Incidentes de Red
- Incidentes de Hardware
- Incidentes de Software
- Incidentes de Procesos
- Incidentes de Seguridad
- Incidentes de Capacitación

Además se encargara de realizar las tareas siguientes:

- Definición de tipos de incidentes y sus niveles de servicio
- Administración de las garantías técnicas y contratos de mantenimiento y soporte
- Mantenimiento de software aplicativo

La mesa de ayuda aun no ha sido implementada en la mayor parte de empresas, es una gran alternativa para canalizar los problemas en el área de TI dentro de una empresa, y generalmente en los informes finales de las auditorías se sugiere la implementación de la misma.

3.1.4 Tiempo de Implementación

El propósito de la auditoría informática es establecer las acciones que se deben desarrollar para instrumentar la auditoría en forma secuencial y ordenada, tomando en cuenta las condiciones que

tienen que prevalecer para lograr en tiempo y forma los objetivos establecidos.

El tiempo de implementación varía dependiendo de factores como:

- El grado de alineación actual de los procesos de la empresa
- El número de personas que laboran en la empresa
- El número de sucursales de la empresa
- El grado de involucramiento y compromiso de la dirección
- La existencia actual de un sistema de información del negocio compuesta de un software ERP y una metodología de medición ejecutivo gerencial u operacional Balaced Score Card o similar.

El promedio de implementación es de 45 a 60 días para una empresa mediana y de 15 a 30 días en una empresa pequeña, todo ello contando con el total compromiso de nuestro personal y el de la empresa auditada, este tiempo varía dependiendo de la complejidad de la infraestructura informática de la misma.

3.1.5 Resultados de Auditorías Anteriores, autoevaluaciones y certificaciones del departamento de TI

Son necesarios para identificar si los procesos de TI estuvieron al alcance del trabajo realizado en auditorías anteriores. De haber existido anteriormente, se podrán revisar las conclusiones a las que se han llegado y para darle un seguimiento a las mismas.

3.1.6 Situación Actual de la Gestión de T. I. en la Empresa

3.1.6.1.1.1 Recolección de documentación correspondiente al Área de T. I

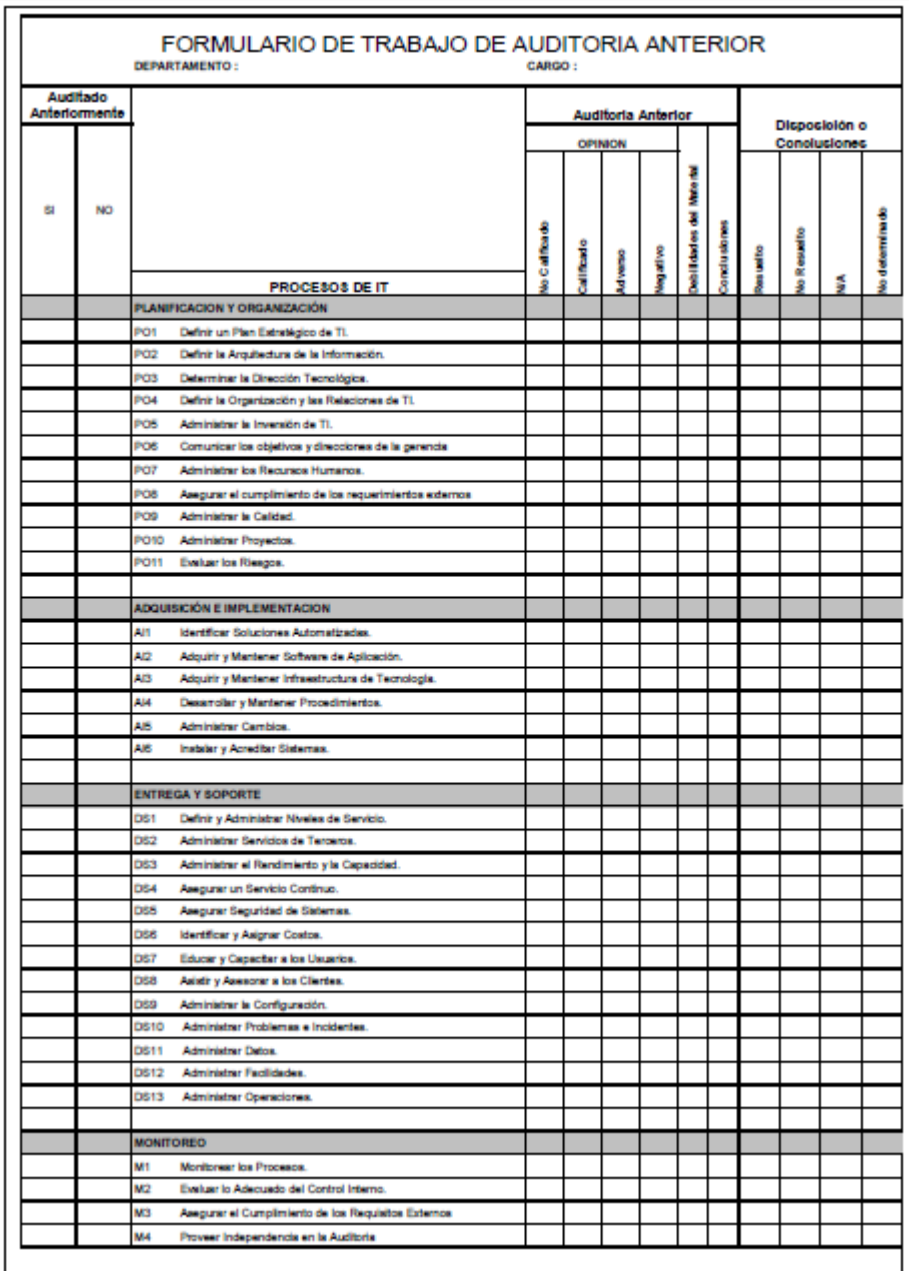
Para tener un criterio del medio de trabajo se sigue una metodología de auditoría general, y los criterios del modelo de

COBIT que nos da un marco de referencia y de trabajo estandarizado, que involucran documentos con temas clasificados a través de dominios, procesos y actividades.

Para identificar las áreas que serán auditadas, se usara un grupo de matrices o encuestas para trabajar con ellas durante todo el proceso de pre auditoría y que sirven para hacer el análisis de prioridades que dará información de fuentes directas como la Gerencia, Administración de TI y usuarios finales, para hacer la priorización y la auditoría. Todo esto estará presente en la aplicación y se almacenara en la base de datos para cálculos y obtención de informes, como para consultas posteriores.

3.1.6.1.2 Informe de Estado Actual

Para tener una noción del estado actual de la empresa en el área de TI llenaremos los principales criterios de evaluación según Cobit con el siguiente formulario, de esta manera tendremos una documentación física del estado actual, la cual será nuestro punto de partida, finalmente esta información será ingresada en nuestro aplicación, para posteriormente iniciar la nueva Auditoría.



FORMULARIO DE TRABAJO DE AUDITORIA ANTERIOR

DEPARTAMENTO : CARGO :

Auditado Anteriormente			Auditoria Anterior						Disposición o Conclusiones			
			OPINION									
SI	NO	PROCESOS DE IT	No Calificado	Calificado	Adverso	Negativo	Debilidades del Material	Conclusiones	Resuelto	No Resuelto	N/A	No determinado
		PLANIFICACION Y ORGANIZACIÓN										
		PO1 Definir un Plan Estratégico de TI.										
		PO2 Definir la Arquitectura de la Información.										
		PO3 Determinar la Dirección Tecnológica.										
		PO4 Definir la Organización y las Relaciones de TI.										
		PO5 Administrar la Inversión de TI.										
		PO6 Comunicar los objetivos y direcciones de la gerencia										
		PO7 Administrar los Recursos Humanos.										
		PO8 Asegurar el cumplimiento de los requerimientos externos										
		PO9 Administrar la Calidad.										
		PO10 Administrar Proyectos.										
		PO11 Evaluar los Riesgos.										
		ADQUISICIÓN E IMPLEMENTACION										
		AI1 Identificar Soluciones Automatizadas.										
		AI2 Adquirir y Mantener Software de Aplicación.										
		AI3 Adquirir y Mantener Infraestructura de Tecnología.										
		AI4 Desarrollar y Mantener Procedimientos.										
		AI5 Administrar Cambios.										
		AI6 Instalar y Acreditar Sistemas.										
		ENTREGA Y SOPORTE										
		DS1 Definir y Administrar Niveles de Servicio.										
		DS2 Administrar Servicios de Terceros.										
		DS3 Administrar el Rendimiento y la Capacidad.										
		DS4 Asegurar un Servicio Continuo.										
		DS5 Asegurar Seguridad de Sistemas.										
		DS6 Identificar y Asignar Costos.										
		DS7 Educar y Capacitar a los Usuarios.										
		DS8 Asistir y Asesorar a los Clientes.										
		DS9 Administrar la Configuración.										
		DS10 Administrar Problemas e Incidentes.										
		DS11 Administrar Datos.										
		DS12 Administrar Facilidades.										
		DS13 Administrar Operaciones.										
		MONITOREO										
		M1 Monitorear los Procesos.										
		M2 Evaluar lo Adecuado del Control Interno.										
		M3 Asegurar el Cumplimiento de los Requisitos Externos										
		M4 Proveer Independencia en la Auditoria										

3.1.6.1.3 Inventario de Recursos de T. I. de la empresa.

Los recursos Informáticos de TI deben administrarse de manera adecuada, desempeñan una función crucial para garantizar el éxito o contribuir al fracaso de las iniciativas estratégicas de negocio de una empresa.

Las empresas necesitan saber dónde están todos sus activos de TI, quién los utiliza y qué software se ejecuta en ellos. El hecho de no disponer de esta información incrementa los costos de soporte y mantenimiento, para ello es importante contar con un detalle de cada uno de estos recursos.

El inventario de hardware y software se lo puede llevar en las siguientes matrices:

INVENTARIO HARDWARE

Oficina		Departamento	

Código	Serial	Nombre	Marca	Capacidad	Tipo	Velocidad	Status

INVENTARIO SOFTWARE

Oficina		Departamento	

Nombre	Tipo de Licencia	Plataforma	Serial	Nro. Maquinas	Tipo de Software	Status

CAPITULO 4

Capacitación y Recursos para la Auditoría.

La auditoría informática o también conocida como auditoría a la tecnología de la información involucra diferentes áreas por lo que el auditor deberá conocer sobre estas, aunque no se le pueda pedir ser un experto en todas ellas.

4.1.1 Recursos Humanos

Los recursos humanos son la mezcla equilibrada entre personas con formación en auditoría y organización, con personas con un perfil informático.

4.1.1.1 Perfil del Auditor

El auditor debe tener una formación básica con una mezcla de conocimientos de auditoría financiera y de informática en general (Desarrollo de aplicaciones, Gestión de proyectos, BD, S.O., redes, etc.), debe poseer una especialización en función del entorno empresarial, gestión del cambio y calidad total, que hará que su trabajo sea reconocido como un elemento valioso dentro de la empresa y que los resultados sean aceptados en su totalidad. El auditor debe poseer un amplio conocimiento sobre la metodología de Cobit, las normativas ISO y de seguridad de la información.
El Auditor debe contar con las siguientes titulaciones:

- CISA
- CISM
- CISSP

El auditor debe cumplir, con una serie de preceptos, normas y obligaciones, tanto en los ámbitos ético y moral como en el social, jurídico, laboral y profesional que le obligan a sujetarse a las normas establecidas por la sociedad.

4.1.1.2 Funciones del Auditor Informático.

ILUSTRACION # 15

Revisar

- Controles generales en los sistemas informáticos, para determinar que se ha diseñado de acuerdo con las normas internas en vigor y los requerimientos legales aplicables
- Controles de las aplicaciones informáticas instaladas para evaluar su fiabilidad procesando datos a tiempo, de forma exacta y completa
- El diseño y desarrollo de nuevas aplicaciones informáticas
- Los costos en que se incurra en las diferentes etapas de sistematización y hacer recomendaciones que permitan su reducción.
- La organización existente para determinar si responde a los criterios fijados por la Dirección y a las necesidades actuales, y asegurar la salvaguarda física de la información de la empresa (Funciones Básicas de Gestión, Administración, Organización, Normativa General)

Verificar

- Controles globales del Sistema Informático y las medidas de Seguridad del equipo, los programas y los datos (Seguridad Lógica y Física de Instalaciones y Datos)

- La planeación del departamento de sistemas obedezca y responda a la planeación global de la empresa
- Las definiciones de sistematización se desarrollen en base a un estudio formal y serio de las necesidades de la empresa y como respuestas a ellas
- Que se cuente con personal idóneo para trabajar en sistemas y que su administración sea eficaz
- Si existe y es adecuada la metodología de diseño, desarrollo y mantenimiento de aplicaciones
- Que haya facilidad de ajuste, cambio y mantenimiento en los programas.

Evaluar

- La justificación económica y de negocios de la adquisición de equipos y programas de computador
- El uso que se le dará a los recursos de computación de acuerdo con sus capacidades, para evitar obsolescencia prematura o la ocurrencia de un lucro cesante.
- Los procedimientos operacionales y administrativos seguidos en la adquisición, adaptación e instalación de recursos
- Situaciones de fraude en los sistemas automatizados
- La seguridad de las instalaciones, equipos y programas, contra acceso indebido, actos mal intencionados y desastres físicos
- Los planes de respaldo para las instalaciones, equipos y programas
- El mantenimiento que se le da a los equipos e instalaciones
- Los controles que garanticen un procesamiento de datos oportuno, exacto y completo
- El software adquirido para microcomputadores, con el fin de evitar el uso no autorizado de programas que puedan implicar litigios y sanciones, así como contaminación por virus de computadores.
- Si hay una clara definición de objetivos, políticas, planes y metas para el área de sistemas

- La calidad de la ejecución de las políticas administrativas del área de sistemas

Velar

- Porque se cumplan las normas y políticas administrativas establecidas para el diseño y desarrollo de aplicaciones
- Porque se establezcan controles y se den dentro del sistema las pistas de auditoría necesarias
- Porque el diseño de sistemas se haga dentro de un marco de eficiencia, economía y efectividad
- Porque haya una adecuada integración de los sistemas y aplicaciones dentro de la compañía

4.1.1.3Perfiles Profesionales de los auditores informáticos

Profesión	**Actividades y conocimientos deseables**
Informático Generalista	Experiencia amplia en ramas distintas. Importante que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.
Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación

Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costos	Economista con conocimiento de Informática. Gestión de costos.

4.1.1.4Definición del Responsable del Proyecto

El responsable del proyecto es una persona capacitada y experimentada que se designa por una autoridad competente, para revisar, examinar y evaluar profesionalmente los resultados de la gestión administrativa y financiera de una dependencia o entidad, con el propósito de informar o dictaminar acerca de ellas, realizando las observaciones y recomendaciones pertinentes para mejorar su eficacia y eficiencia en su desempeño.

4.1.1.5 Auditores

4.1.1.5.1 Tiempo de Capacitación

El tiempo de capacitación no está claramente delimitado, como la pegunta ¿cuánto tiempo de entrenamiento requiere el auditor al año? Es difícil de responder, probablemente si decimos que tres semanas durante el año pueden resultar insuficientes debido a los cambios tecnológico que se dan en un año. El nivel de tecnología que se utiliza en la instalación es un factor determinante del tiempo de capacitación para el auditor, en una empresa en donde recientemente se ha instalado hardware, software o dispositivos tecnológicos nuevo

o se planea su instalación a corto plazo es probable que se requiera más tiempo de capacitación para el auditor en comparación que el año anterior. Por el contrario si la empresa auditada posee tecnología para el manejo de su información con varios años ya de instalada y un software que ha ido evolucionando, probablemente el tiempo de capacitación al año sea menor o la capacitación se torne permanente paralela a los cambios en la aplicación.

4.1.1.5.2 Entrenamiento

En lo que concierne al entrenamiento de un auditor, es necesario balancear los costos y los beneficios de la educación continua del mismo, por lo que se tendría que hacer un análisis detallado de los cursos de capacitación que el auditor está tomando y los que deberá tomar. La calidad que tenga la auditoría dependerá de una adecuada planeación en el entrenamiento anual del auditor esto permitirá asegurar en buena medida el nivel de calidad con el que se desempeñe y los resultados a los que se llegue.

4.1.2 Recursos Materiales

4.1.2.1 Equipos

Para la elaboración de la aplicación y el documento se requerirá.

Hardware

- ComputadorPortatil Sony Vaio VPCEG 61ª12L
  - Procesador Intel Core I5
  - Memoria 4GB RAM
  - Disco 640 Gb
  - BLURAY Drive
- ComputadorPortatil ToshibaSatellite L515-SP3014L
  - Procesador Pentium Dual Core 2,2 Ghz
  - Memoria 4GB RAM
  - Disco 320 Gb
  - DVD Drive
- Impresora Samsung Laser ML2010

Software

- Procesador de Textos Microsoft Word 2010
- Hoja de Cálculo Microsoft Excel 2010
- Microsoft Visio 2003
- Rational Rose Enterprise Edition
- Lenguaje de Programacion Visual.Net 2010
- Gestor de Base de Datos MySql
- Internet Explorer 6.0 o superior.

4.1.2.2 Suministros

Gasto	Cantidad	Valor Unitario	Valor Total
Resma de papel bond	2	5.50	11.00
DVD	5	1.00	5.00
Toner MLT2010	1	65.00	65.00
Carpetas	5	1.00	5.00
Imprevistos			30.00

Capítulo 5

Especificación de Requisitos de Software (ERS)

5.1 Introducción

El presente documento es una especificación de requisitos de software para la Interfaz Web a desarrollar en Visual Basic .Net para la Gestión de Recursos de TI basados en Cobit 4.1, la misma que será elaborada con la colaboración de usuarios, directivos y desarrolladores, de una muestra de empresas que requieran una auditoría de carácter informático, así también con la colaboración de auditores, diseñadores y desarrolladores de software de la empresa auditora.

5.2 Propósito

El objetivo de la especificación de requisitos de software es definir de manera clara y precisa las funcionalidades y condicionantes técnicas de la aplicación web a desarrollar.

5.3 Ámbito del Sistema

La aplicación web contempla lo siguiente:

- Registro de los procesos de Auditoría.
- Reportes gerenciales sobre los hallazgos y estado de las auditorías.

El objetivo de la aplicación es contar con una solución que permita realizar el proceso de auditoría para la Gestión de Recursos de TI basados en Cobit 4.1, con el fin de orientar a las empresas auditadas para que obtengan una normativa de manejo óptimo de los recursos de TI según los parámetros de esta metodología.

5.4 Definición de Términos

Usuarios	Enlace para el manejo y clasificación de los Usuarios del Sistema según su rol.
Empresas	Enlace de registro, actualización y consulta para las empresas ha ser auditadas.
Auditorías	Enlace para realizar todo lo que comprende al proceso de auditoría.
Reporte Grafico	Enlace que muestra los resultados de las auditorías de forma grafica.

5.5 Funciones del Sistema

El objetivo de implementar esta aplicación web es facilitar y optimizar el tiempo de evaluación de una auditoría, así como, tener una interfaz clara y concreta de los procesos de auditoría realizados, tanto para el cliente como para la Empresa Auditora.

Esta aplicación permitirá al usuario, ya sean Auditores, Administradores, realizar modificaciones, consultas y tabulaciones de resultados según el rol de los mismos establecido para cada uno. Se podrá hacer consultas sobre auditorías anteriores realizadas con el mismo software.

La aplicación permitirá analizar y consultar los criterios evaluados en la auditoría según la metodología internacional Cobit.

5.6 Perfiles de Usuario

Auditores: Personal de la Firma Auditora previamente capacitado en el manejo e interpretación de la interfaz del software, los mismos que realizarán la evaluación y el proceso correspondiente a la auditoría.

Administrador, Gerente y Responsable: Son los directivos de la Empresa, quienes según su rol estarán capacitados para la evaluación y revisión de los resultados obtenidos en las auditorías realizadas en cada empresa.

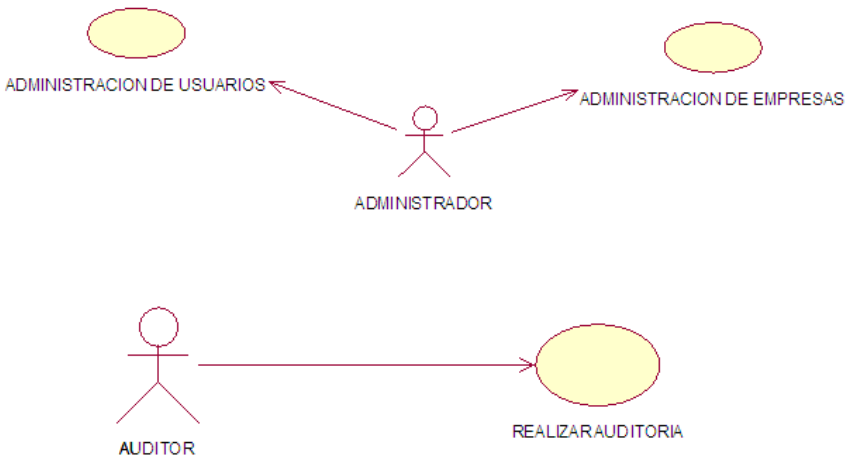
Cliente/Usuario: Dueño/Dirigente de la Empresa auditada que según su rol tendrá únicamente acceso a los resultados obtenidos de la auditoría de su institución.

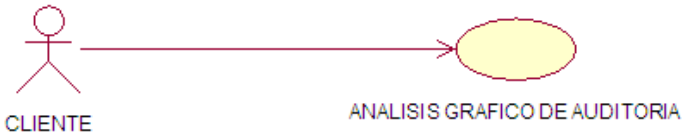
5.7 Requisitos Específicos

Los requisitos son generados en base a la experiencia del usuario en sus diferentes roles. Ellos son quienes determinaran el funcionamiento óptimo de la aplicación según las necesidades y criterios de ellos. Es clave determinar los elementos básicos de la aplicación tal como la percibe el usuario, y en base a ello implementar mejoras y soluciones en el diseño de la interfaz de la misma. Es importante determinar el flujo y la estructura de la información presente en la aplicación, de tal manera que se pueda optimizar todas las funciones de la misma. Se deben establecer las características que estarán presentes en la interfaz para determinar las necesidades en el diseño de la misma, todo ello con el fin de cumplir con todos los criterios de un diseño adecuado para la interfaz de una aplicación de este tipo.

5.8 Requisitos Funcionales

5.8.1.1 Casos de Uso





5.8.1.1.1 Descripción de actores

Auditor: Personal de la empresa auditora, encargado de realizar el proceso de auditoría.

Administrador: Personal de la empresa auditora responsable de la administración de usuarios y de empresas, las mismas que serán registradas con sus respectivos parámetros una vez firmado el contrato por los servicios de auditoría entre la empresa auditora y la empresa auditada

Cliente: Representante de la empresa auditada que tiene acceso a los reportes de resultados obtenidos en la auditoría, puede ser más de una persona, por lo general aparte del representante legal, se puede registrar al presidente y gerente de la empresa con este rol.

5.8.1.2 Descripción de casos de uso

- **Caso de Uso #1**

Caso de uso 1	Administración de Usuarios
Actor:	Administrador
Descripción:	Módulo donde se Administran los Usuarios, se asigna sus roles, permisos, se ingresan, actualizan y eliminan sus datos.

Prioridad:	Obligatorio
REQUISITOS ASOCIADOS	
R.1.1 La aplicación permitirá registrar nuevos usuarios que se almacenarán en la base de datos, los campos registrados para cada usuario serán los siguientes: Cédula, Nombre, Cargo, Login, Clave y Perfil. R.1.2 La administración de usuarios permitirá consultar, actualizar y eliminar los registros almacenados. R.1.3 Los usuarios para acceder a los módulos según sus privilegios lo harán a través de un login. R.1.4 La administración de usuarios permite clasificar por roles a los actores que utilizarán la aplicación. Los roles son los siguientes: Administrador, Responsable de Proyecto, Auditor y Cliente.	

- **Caso de Uso #2**

Caso de uso 2	Administración de Empresas.
Actor:	Administrador
Descripción:	Módulo donde se Administran las empresas, se registran, actualizan consultan y eliminan sus datos, con el registro de una empresa obligatoriamente se asigna un usuario como representante legal con el rol de cliente.
Prioridad:	Obligatorio
REQUISITOS ASOCIADOS	
R.2.1 La aplicación permitirá registrar nuevas empresas que se almacenarán en la base de datos, los campos que se registrarán por cada empresa son: RUC, Razón social, Dirección. Teléfono y Observaciones. R.2.2 La administración de empresas permitirá consultar, actualizar y eliminar los registros almacenados. R.2.3 Las empresas se registrarán con un código único que será el cual se maneje en todo el proceso de auditoría. R.2.4 Cada empresa contará con un representante legal el cual se creara obligatoriamente el momento en que se registre la misma.	

- **Caso de Uso #3**

Caso de uso 3	Realizar Auditoría
Actor:	Auditor
Descripción:	Modulo principal que engloba todo el proceso de auditoría.
Prioridad:	Obligatorio
REQUISITOS ASOCIADOS	
R.3.1 La aplicación permite evaluar el proceso de Tide Planear y Organizar. R.3.2 La aplicación permite evaluar el proceso de TI de Adquirir e Implementar R.3.3 La aplicación permite evaluar el proceso de TI de Entrega y Soporte R.3.4 La aplicación permite evaluar el proceso de TI de Monitorear y Evaluar R.3.5 La aplicación permite visualizar los resultados de la Auditoría de forma grafica. R.3.6 La aplicación permite comparar una auditoría previa con una actual de forma grafica. R.3.7 La aplicación permitirá seleccionar entre grabar los cambios o salir sin grabar.	

- **Caso de Uso #4**

Caso de uso 4	Análisis Grafico de Auditoría
Actor:	Cliente
Descripción:	Módulo donde el cliente visualiza de forma grafica los resultados obtenidos en el proceso de Auditoría realizado en su empresa(s).
Prioridad:	Obligatorio

REQUISITOS ASOCIADOS
R.4.1 La aplicación permitirá visualizar el resultado de los procesos de la auditoría en un grafico radial. R.4.2 El grafico de tipo radial abarca los 4 procesos de Cobit con sus respectivos subprocesos. R.4.3 El usuario puede visualizar e imprimir el grafico, pero no modificarlo.

5.8.2 Requisitos No Funcionales

5.8.2.1 Rendimiento

La infraestructura de red, así como los terminales de la empresa auditada deben cumplir con normas según la IEEE en la forma de conexión de sus equipos, para poder garantizar tiempos de respuesta mínimos y conexiones estables.

- Número de Servidores de Base de Datos a manejar:

Se contará con un servidor de base de datos en la matriz de la empresa auditora.

- Número de usuarios simultáneos:

El número de usuarios que interactuaran simultáneamente con nuestra aplicación será hasta de 5 usuarios.

- Número de transacciones a manejar dentro de ciertos periodos de Tiempo:

Se estima que se manejaran alrededor de 5 auditorías por día, es decir unas 30 transacciones o procesos por día. El servidor de base de datos, deberá tener un respaldo apropiado, así como personal técnico listo para cualquier eventualidad.

5.8.2.2 Seguridad

La seguridad del sistema es por:

- Uso de contraseñas para cada usuario (administrador, gerente, responsable de proyecto, auditor) en el caso de la empresa Auditora, en caso de la Empresa Auditada tendrá un rol general para consulta de resultados, llamado cliente (Dueño de la empresa, Presidente, Gerente), de esta forma la aplicación garantizara que se tenga acceso al sistema solo las personas que tienen autorización.
- Registro de ingreso al sistema por usuario, punto de acceso, fecha y hora.
- Roles previamente definidos para administrar los privilegios de usuario.

5.8.2.3 Fiabilidad

Es uno de los factores que dará confianza al cliente, para lo cual el sistema está controlando todo tipo de transacción o proceso, estando apto a responder todo tipo de incidente.

5.8.2.4 Disponibilidad

La aplicación ha sido desarrollado tomando en cuenta las necesidades, requerimientos, reglas, política, misión, objetivos globales de una empresa del sigo 21, por lo tanto se encuentra disponible el 80% del tiempo del día tomando en cuenta que el día tiene 24 horas; mientras que el 20% del tiempo es para tareas administrativas sobre el sistema.

5.8.2.5 Mantenibilidad

La aplicación deberá ser diseñada para que su mantenimiento sea fácil y su escalabilidad sea alta.

5.8.2.6 Portabilidad

La aplicación debe ser portable, al ser una aplicación de tipo web tendrá que funcionar en los principales navegadores de internet como Internet Explorer, Mozilla Firefox, Google Chrome y Safari, esto para que pueda ser utilizado en diferentes plataformas de Sistemas Operativos y equipos.

Capítulo 6

Diseño e Implementación de la Aplicación

6.1 Diseño de la Base de Datos.

La Base de datos desarrollada en MySql Server 5.5 está estructurada por las siguientes tablas y atributos.

TABLA	**Auditorías**

CAMPOS			
Name	Type	Null	Comment
Ad_id	INT(11)	N	Identificación de la Auditoría
Ad_ep_ruc	VARCHAR(13)	N	RUC de la Empresa Auditada
Ad_ci_responsable	VARCHAR(10)	N	Cedula de Identidad del Responsable
Ad_ci_auditor	VARCHAR(10)	N	Cedula de Identidad del Auditor
Ad_estado	VARCHAR(30)	N	Estado de la Auditoría
Ad_fecha_inicio	DATE	N	Fecha de Inicio de la Auditoría
Ad_fecha_fin	DATE	N	Fecha Final de la Auditoría

La tabla Auditorías contiene los datos básicos sobre la auditoría y las llaves foráneas que la relacionan con las otras tablas.

TABLA	**Empresas**

CAMPOS			
Name	Type	Null	Comment
Ep_ruc	VARCHAR(13)	N	RUC de la empresa auditada.
Ep_razon_social	VARCHAR(50)	N	Razón Social de la Empresa Auditada
Ep_direccion	VARCHAR(45)	N	Dirección de la Empresa
Ep_telefono	VARCHAR(9)	N	Teléfono de la Empresa
Ep_observaciones	VARCHAR(50)	N	Observaciones sobre la Auditoría

La tabla Empresas contiene toda la información de las empresas y las observaciones sobre el proceso de auditoría de las mismas.

TABLA	**Niveles de Madurez**

CAMPOS			
Name	Type	Null	Comment
Nm_id	INT(11)	N	Identificación de los Niveles de Madurez
Pc_id	VARCHAR(5)	N	Identificación del proceso
Nm_titulo	VARCHAR(5)	N	Titulo del Nivel de Madurez
Nm_descripcion	VARCHAR(1500)	N	Descripción del Nivel de Madurez

La tabla Niveles de Madurez contiene los datos que corresponden a los niveles de madurez analizados en el proceso de auditoría.

TABLA	**Perfiles**

CAMPOS			
Name	Type	Null	Comment
Pf_codigo	TINYINT(4)	N	Código del Perfil
Pf_descripcion	VARCHAR(45)	N	Descripcion del Perfil

La tabla Perfiles contiene El código y la descripción del perfil de usuarios de la aplicación.

TABLA	**Procesos Auditados**

CAMPOS			
Name	Type	Null	Comment
ad_id	INT(11)	N	Identificación de la Auditoría
Nm_id	INT(11)	N	Identificación de los Niveles de Madurez
Pc_id	VARCHAR(5)	N	Identificación del proceso
Nm_descripcion	VARCHAR(1500)	N	Descripción del Nivel de Madurez
Pa_observaciones	VARCHAR(500)		Observaciones sobre el proceso auditado.

La tabla Procesos Auditados contiene la información de cada uno de los procesos a considerar para la evaluación de la auditoría con su respectiva información y observaciones.

TABLA	**Procesos_Cobit**

CAMPOS			
Name	Type	Null	Comment
Pc_id	VARCHAR(5)	N	Identificación del proceso
Pc_descripcion	VARCHAR(100)	N	Descripción del Proceso de Auditoría
Pc_orden	INT(11)	N	Ordena la Secuencia de los Procesos

La tabla Procesos Cobit contiene la descripción y la secuencia de los procesos según su clasificación.

TABLA	**Usuarios**

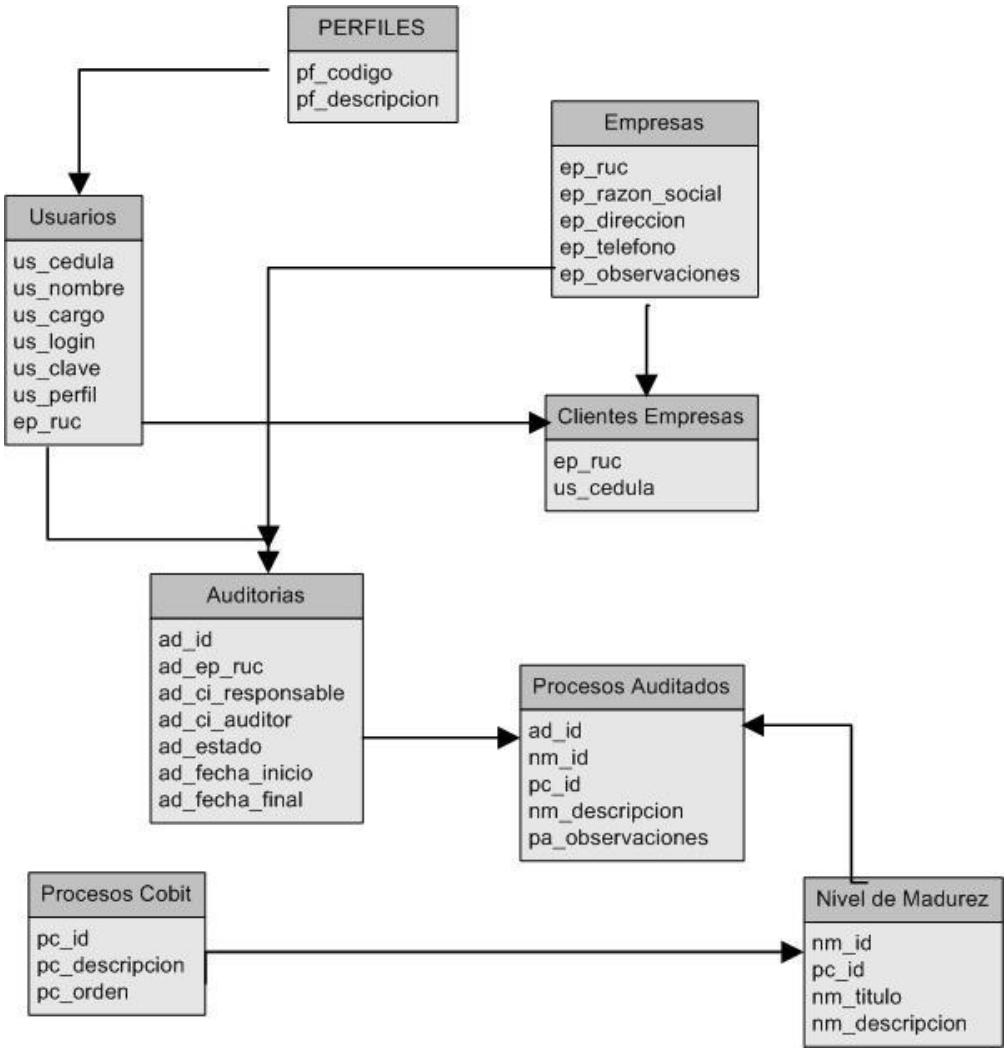
CAMPOS			
Name	Type	Null	Comment
Us_cedula	VARCHAR(10)	N	Cedula del Usuario
Us_nombre	VARCHAR(45)	N	Nombre del Usuario
Us_cargo	VARCHAR(45)	N	Cargo del Usuario
Us_login	VARCHAR(10)	N	Login del Usuario
Us_clave	VARCHAR(10)	N	Clave del Usuario
Us_perfil	TINYINT(4)	N	Identificación del Perfil del Usuario
Ep_ruc	VARCHAR(13)	N	Ruc de la Empresa

La tabla Usuarios contiene toda la información relacionada a los usuarios y sus relaciones con las otras tablas.

TABLA	**Clientes_Empresas**

CAMPOS			
Name	Type	Null	Comment
Ep_ruc	VARCHAR(13)	N	Ruc de la Empresa
Us_cedula	VARCHAR(10)	N	Cedula del Usuario

6.2 Modelo Entidad Relación



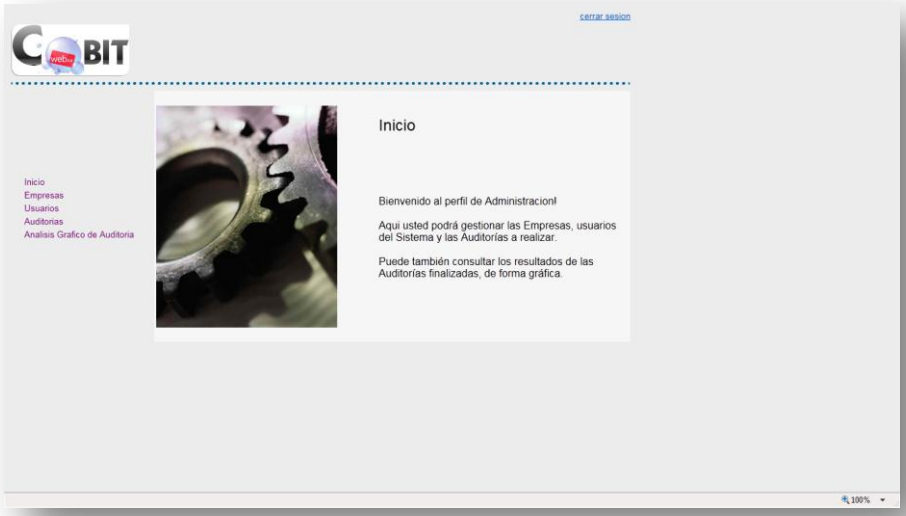
6.3 Diseño de Interfaces de la aplicación

La aplicación esta desarrollada en entorno web, con una interfaz amigable, de tipo grafico, con colores e interfaces afines entre cada una de las páginas que forma parte de la misma.

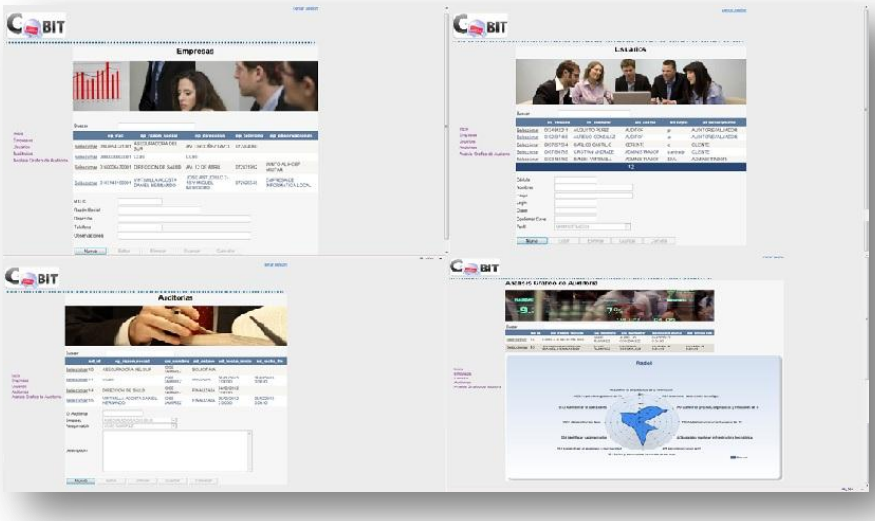
6.3.1 Interfaz Principal (Home Page)

Esta pantalla contiene el menú principal de la aplicación. Una vez realizado el login el usuario según su perfil tiene acceso a siguientes opciones: Empresas, Usuarios, Auditoría, Análisis Grafico de Auditoría.

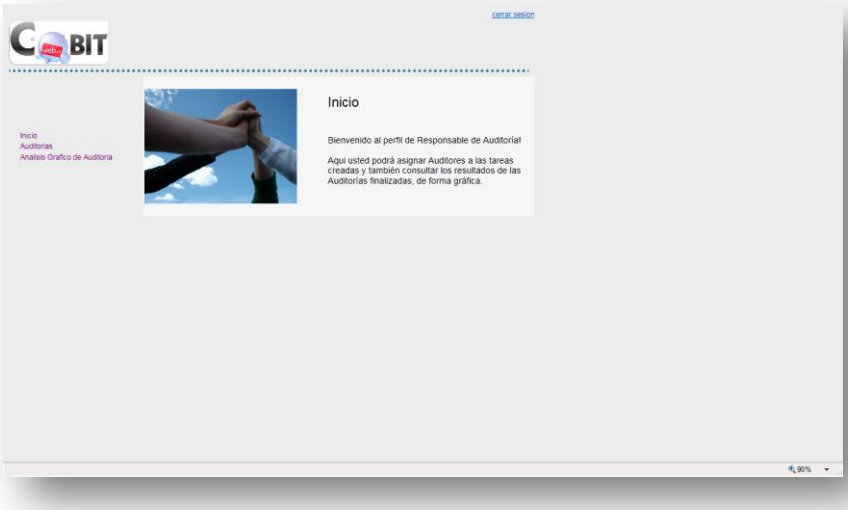
6.3.2 Interfaz Administrador



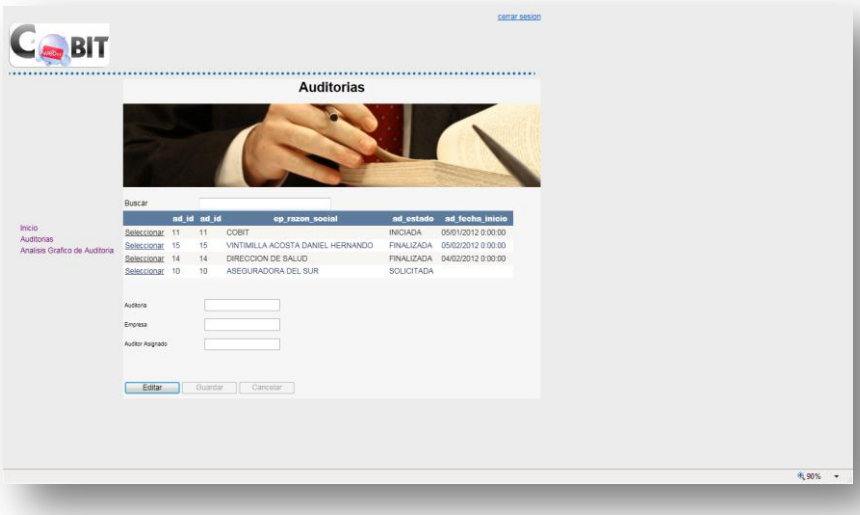
Esta pantalla permite la creación, modificación, actualización y eliminación y consulta de empresas, auditorías y usuarios. El usuario administrador es empleado de la empresa auditora.



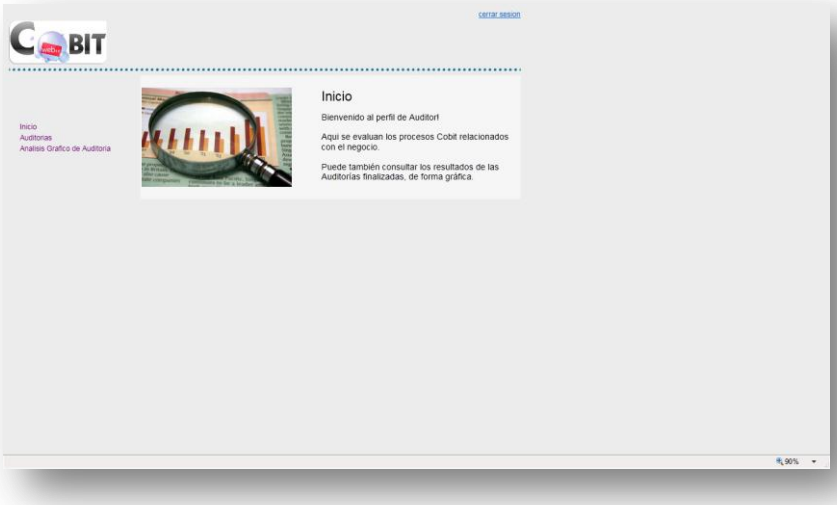
6.3.3 Interfaz Responsable



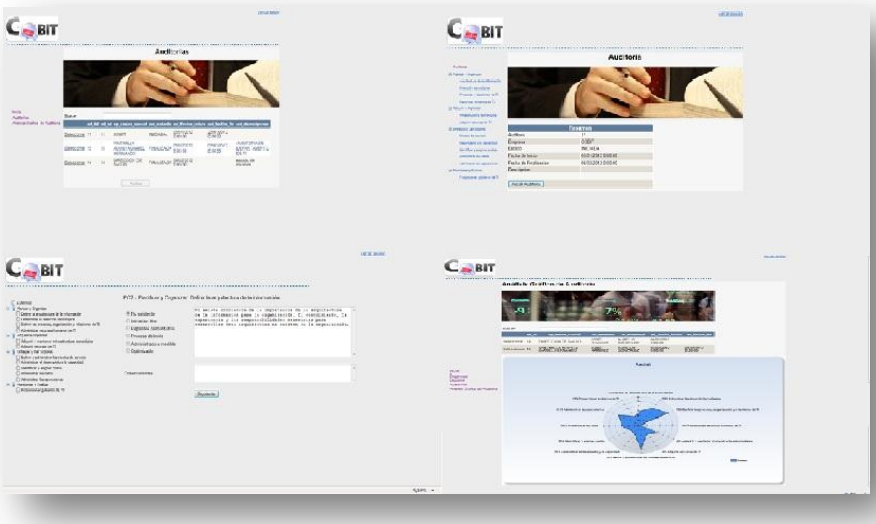
Esta pantalla permite la asignación de Auditores para un proceso de auditoría determinado de una empresa, permite la consulta de Auditorías y reportes gráficos de las auditorías que ha realizado o esta llevando a cavo la empresa auditora.



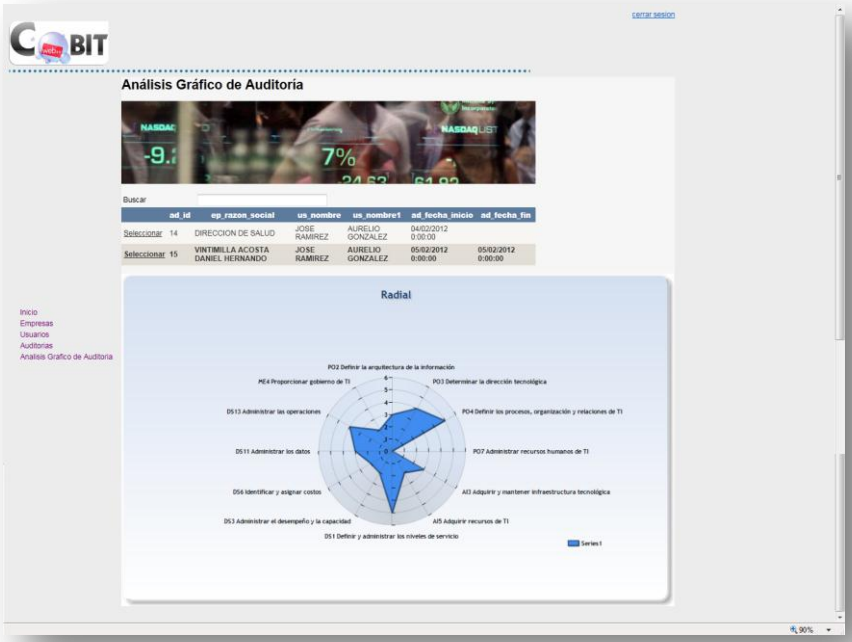
6.3.4 Interfaz Auditor



Esta pantalla permite la ejecución del proceso de auditoría como tal, el auditor es el único perfil que tiene acceso a esta función, así como la visualización de los resultados de la auditoría a la cual esta asignado.



6.3.5 Interfaz Cliente



Esta pantalla permite la consulta del resultado de la auditoría realizada. A esta interfaz tienen acceso únicamente los Presidentes, Gerentes o el personal de la empresa auditada designado para este fin.

6.4 Codificación y Pruebas del Software

La aplicación esta desarrollada en Aspx Microsoft .Net Framework 4, la codificación es en la plataforma Visual Basic 2010, la conexión con la BD se realiza por controlador ODBC a una base de datos relacional de MySql.

Pruebas de Software

La utilización de la aplicación esta determinada por perfiles de usuario, por ello las pruebas a realizar sobre la misma se realizan a cada usuario según su respectivo perfil de la siguiente manera.

Administrador

- Ingreso de Usuario y Contraseña
- Navegación sobre el menú.
- Creación de Empresas
- Creación de Usuarios
- Creación de Auditorías
- Asociación de Clientes a Empresas.
- Visualización de Resultados

Responsable

- Ingreso de Usuario y Contraseña
- Navegación sobre el menú.
- Asignación de un Auditor a una Auditoria.
- Visualización de Resultados

Auditor

- Ingreso de Usuario y Contraseña
- Navegación sobre el menú.
- Realización del Proceso de Auditoría
- Visualización de Resultados

Cliente

- Ingreso de Usuario y Contraseña
- Navegación sobre el menú.
- Visualización de Resultados

En Resumen:

- Las pruebas que se realizaron fueron unitarias, es decir según los perfiles antes detallados se accedió a cada una de las opciones del menú.
- Se realizaron pruebas de integración para verificar el correcto funcionamiento del sistema en su conjunto.

- Se cumplió con las pruebas de aceptación verificando que se cumplan con los requisitos establecidos.

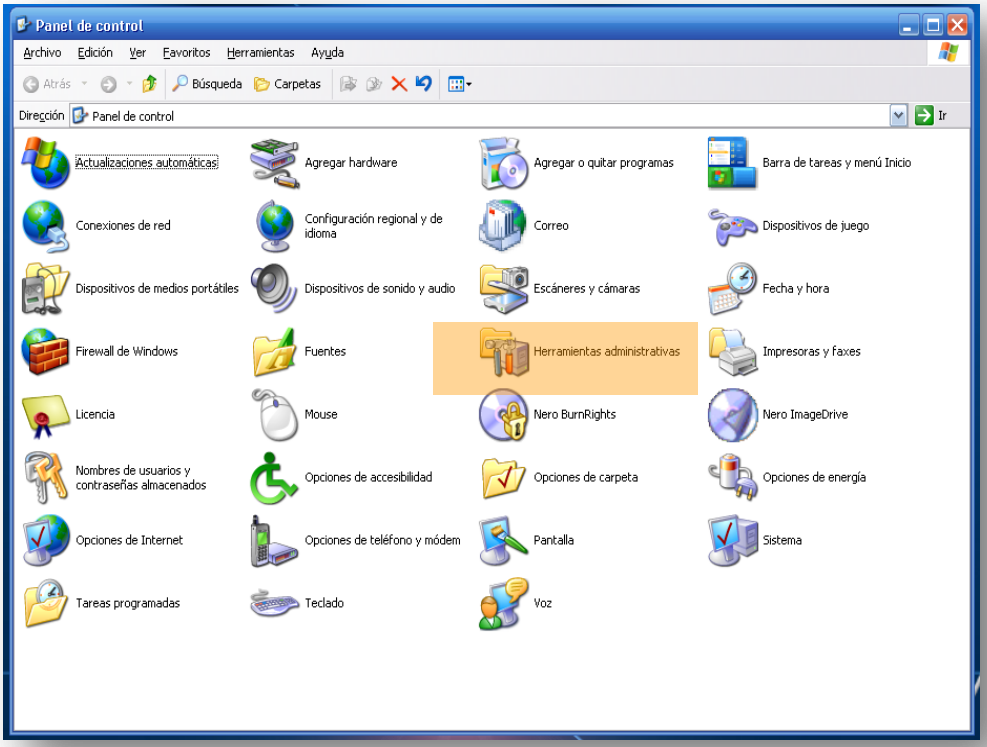
6.5 Instalación y puesta en operación del software

Es necesario instalar Internet Information Server, IIS, es una serie de servicios para los ordenadores que funcionan con Windows. Originalmente era parte del Option Pack para Windows NT, posteriormente fue integrado en otros sistemas operativos de Microsoft destinados a ofrecer servicios, como Windows 2000 o Windows Server 2003. Windows XP, Vista, 7 Pro incluyen una versión limitada de IIS. Los servicios que ofrece son: FTP, SMTP, NNTP y HTTP/HTTPS.

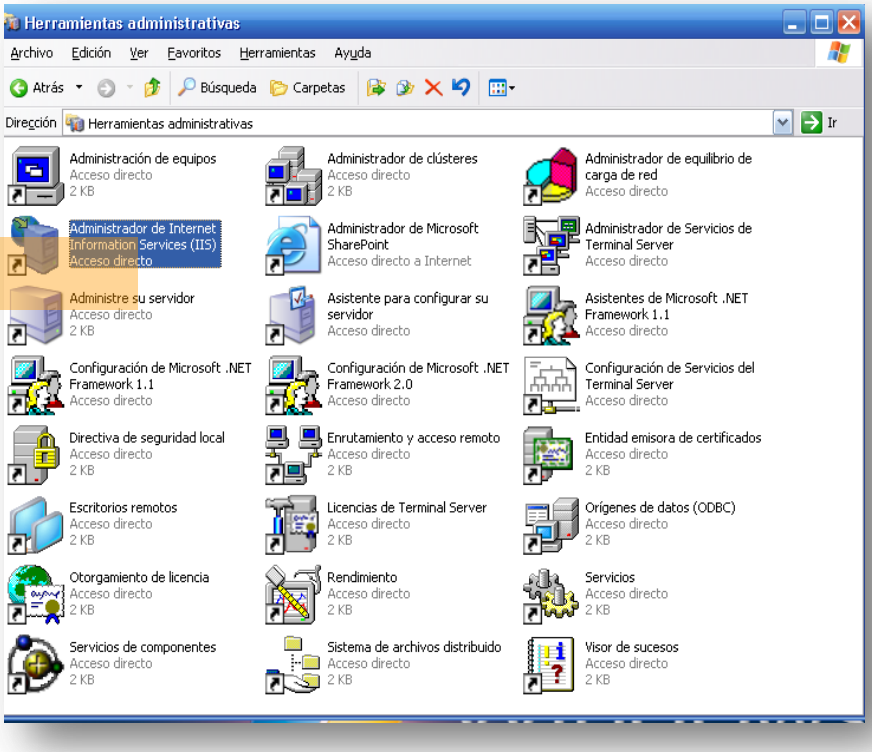
Este servicio convierte a un ordenador en un servidor de Internet o Intranet es decir que en las computadoras que tienen este servicio instalado se pueden publicar páginas web tanto local como remotamente (Servidor Web).

El Servidor Web se basa en varios módulos que le dan capacidad para procesar distintos tipos de páginas, por ejemplo Microsoft incluye los de Active Server Pages (ASP) y ASP.NET. También pueden ser incluidos los de otros fabricantes, como PHP o Perl.

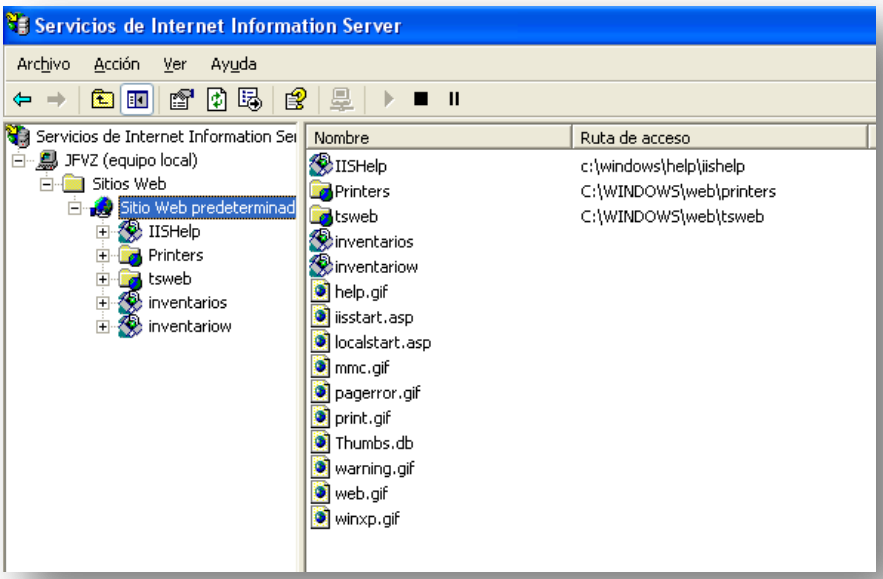
Como primer paso tenemos que entrar al panel de control y damos doble Click en Herramientas Administrativas para abrir la siguiente ventana.



Una vez que estamos en la ventana de Herramientas Administrativas seleccionamos y damos doble click en el Icono de Administrador de Internet Information Server (IIS)



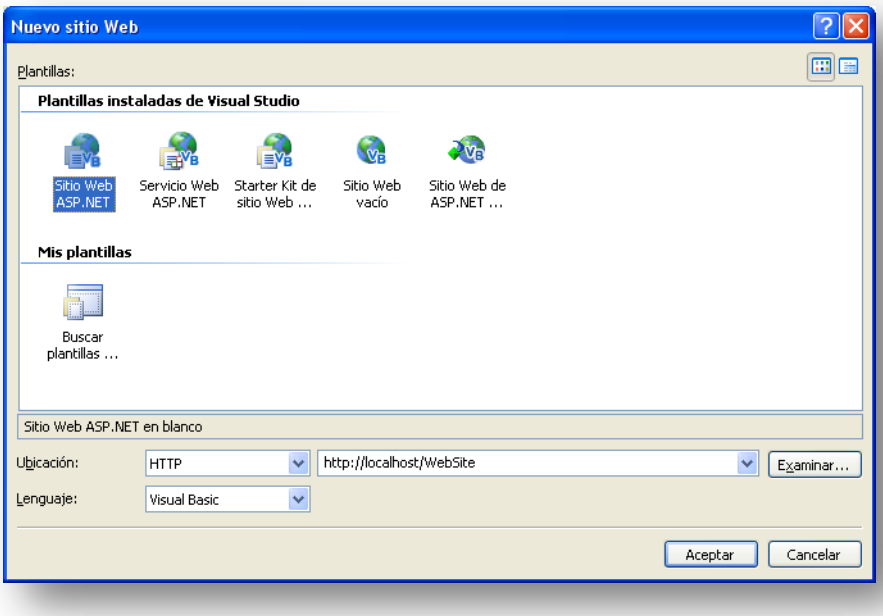
En este punto tenemos la estructura del IIS, el Sitio Web predeterminado, dentro del cual se irán generando nuestras páginas web que desarrollamos en Visual Studio.



Una vez generados los sitios web en Visual Studio vamos a configurar en el IIS, con una serie de opciones necesarias para poder ejecutar nuestras páginas desde el explorador de internet.

Creación de los servicios Web en Visual Basic .Net

En el entorno de Visual Studio ingresamos a la opción Archivo -> Nuevo Sitio Web y seleccionamos Sitio Web ASP .Net, en ubicación seleccionamos HTTP y como dirección **http://localhost/COBITWEB/login.aspx** y en lenguaje seleccionamos Visual Basic .



El sitio que generamos va a ser el que contiene los Servicios Web, ahora generamos un nuevo sitio web en la ubicación **http://localhost/COBITWEB/login.aspx** el cual va a contener la aplicación que va a consumir los servicios web creados anteriormente.

Cuando tenemos configurados los Servicios Web en Visual Studio y el IIS podemos ingresar desde el explorador de internet con la siguiente dirección: **http://localhost/COBITWEB/login.aspx**

6.6 Manual del Usuario

El manual del usuario se encuentra en el Anexo 2.

Capitulo 7
Conclusiones y Recomendaciones

Conclusiones

El modelo Cobit, actualmente es una de las herramientas más importantes a ser utilizada como guía para mantener el control de las actividades y procesos de TI. Este modelo exige que todos los procesos estén documentados, aprobados, en conocimiento, aplicados y evaluados por cada uno de los usuarios.

La utilización de una guía para la elaboración de la auditoría, nos permite evitar posibles olvidos u omisiones, al momento de realizar la tarea de auditoría, hechos que pueden ocurrir si no se tiene un esquema a seguir. Esto facilita la gestión del auditor, al tener de antemano los requisitos que serán solicitados al auditado, de forma que se pueda preparar con anterioridad y presentar la documentación de respaldo.

El modelo permite comparar una empresa o departamentos de TI, con otro de forma más fácil, esta retroalimentación ayuda a conseguir mejores resultados puesto que existe una interacción con experiencias externas.

Al utilizar una metodología de control cualquiera que esta sea, lo importante es la colaboración y predisposición de los involucrados en el mismo, ya que cualquier control que se implemente únicamente tendrá efecto el momento en que la gente tome conciencia de su importancia y el aporte que este brinde a su desempeño.

Recomendaciones

Para cualquier empresa que quiera iniciar o mantener un proceso de control, el primer paso es la capacitación del personal involucrado, por lo que se recomienda formar un grupo de personas especializadas, las cuales podrán posteriormente replicar sus conocimientos y técnicas hacia los demás participantes de la empresa.

Para realizar de forma efectiva la auditoría utilizando el modelo Cobit, se recomienda que las personas que van a realizar el trabajo revisen la mayor cantidad de documentación con respecto al marco de trabajo Cobit, procesos y herramientas de implementación de auditoría.

Es primordial tener presente la necesidad de la interacción permanente entre el grupo de auditoría y la gerencia de la empresa, especialmente en las entregas de los informes preliminares con el fin de evitar posibles errores u omisiones, que incurran en problemas de carácter legal contra la empresa Auditora.

Bibliografía

- Cobit 4.1 Control Objetives for information and related Technology, ISACA
- ISACA(1969-2011). *Trust in, a value from, information systems*

  Isaca: https://www.isaca.org/Pages/default.aspx 20/10/2011
- A-S Gobierno en TI.pptx Auditoría Informática MBA.

  Pablo Pintado
- A-S Aspectos Generales de Auditoría de Sistemas

  Ing. Diego Condo & MBA Pablo Pintado
- Information Systems Control and Audit Ron A. Weber
- Prentice Hall (October 29, 1998)1056 paginas
- Especificación de Requisitos de Software Proyecto SISCOOP Revisión 1.0 http://dspace.espoch.edu.ec/bitstream/123456789/188/1/EspecificacionRequerimientosSoftware.pdf 19/01/2012
- Implantación de Gobierno de TI - Resumen Ejecutivo Network Sec your IT Governace Partner

  http://www.network-sec.com/contenidos/Gobierno_TI.pdf 12/10/2011

Anexos

PLANEAR Y ORGANIZAR

	Alineacion Estrategica	Entrega de Valor	Administracion de Riesgos	Administracion de Recursos	Medicion del Desempeño	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Informacion	Infraestructura	Personas
PO1 Definir un plan estratégico de TI	P		S	S		P	S						X	X	X	X
PO2 Definir la arquitectura de la información	P	S	S	P		S	P	S	P				X	X		
PO3 Determinar la dirección tecnológica	S	S	S	P		P	P						X		X	
PO4 Definir los procesos, organización y relaciones de TI	S		P	P		P	P									X
PO5 Administrar la inversión en TI	S	P		S	S	P	P					S	X		X	X
PO6 Comunicar las aspiraciones y la dirección de la gerencia	P		P			P					S			X		X
PO7 Administrar recursos humanos de TI	P		S	P	S	P	P									X
PO8 Administrar la calidad	P	S	S			P	P		S			S	X	X	X	X
PO9 Evaluar y administrar los riesgos de TI	P		P			S	S	P	P	P	S	S	X	X	X	X
PO10 Administrar proyectos	P	S	S	S	S	P	P						X		X	X

ADQUIRIR E IMPLANTAR

	Alineacion Estrategica	Entrega de Valor	Administracion de Riesgos	Administracion de Recursos	Medicion del Desempeño	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Informacion	Infraestructura	Personas
AI1 Identificar soluciones automatizadas	P	P	S	S		P	S						X		X	
AI2 Adquirir y mantener software aplicativo	P	P	S			P	P		S			S	X			
AI3 Adquirir y mantener infraestructura tecnológica				P		S	P		S	S					X	
AI4 Facilitar la operación y el uso	S	P	S	S		P	P		S	S	S	S	X		X	X
AI5 Adquirir recursos de TI		S		P		S	P				S		X	X	X	X
AI6 Administrar cambios		P		S		P	P		P	P		S	X	X	X	X
AI7 Instalar y acreditar soluciones y cambios	S	P	S	S	S	P	S		S	S			X	X	X	X

ENTREGAR Y DAR SOPORTE

	Alineacion Estrategica	Entrega de Valor	Administracion de Riesgos	Administracion de Recursos	Medicion del Desempeño	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Informacion	Infraestructura	Personas
DS1 Definir y administrar los niveles de servicio	P	P		P	P	P	P	S	S	S	S	S	X	X	X	X
DS2 Administrar los servicios de terceros		P	P	S	S	P	P	S	S	S	S	S	X	X	X	X
DS3 Administrar el desempeño y la capacidad	S	S	S	P	S	P	P			S			X		X	
DS4 Garantizar la continuidad del servicio	S	P	P	S	S	P	S			P			X	X	X	X
DS5 Garantizar la seguridad de los sistemas			P					P	P	S	S	S	X	X	X	X
DS6 Identificar y asignar costos		S		P	S		P					P	X	X	X	X
DS7 Educar y entrenar a los usuarios	S	P	S			P	S									X
DS8 Administrar la mesa de servicio y los incidentes	S	P			S	P	P						X			X
DS9 Administrar la configuración		P	S			P	S			S		S	X	X	X	
DS10 Administrar los problemas		P	S			P	P			S			X	X	X	X
DS11 Administrar los datos		P	P	P					P			P		X		
DS12 Administrar el ambiente físico			P	S					P	P					X	
DS13 Administrar las operaciones				P		P	P		S	S			X	X	X	X

MONITOREAR Y EVALUAR

	Alineacion Estrategica	Entrega de Valor	Administracion de Riesgos	Administracion de Recursos	Medicion del Desempeño	Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Aplicaciones	Informacion	Infraestructura	Personas
ME1 Monitorear y evaluar el desempeño de TI					P	P	P	S	S	S	S	S	X	X	X	X
ME2 Monitorear y evaluar el control interno		P	P			P	P	S	S	S	S	S	X	X	X	X
ME3 Garantizar el cumplimiento regulatorio	P		P								P	S	X	X	X	X
ME4 Proporcionar gobierno de TI	P	P	P	P	P	P	P	S	S	S	S	S	X	X	X	X

Manual del Usuario

A continuación se describe la manera en la que el sistema para la Gestión de Recursos de TI basado en Cobit 4.1, nos permite navegar.

Como ya habíamos indicado anteriormente, existen cuatro perfiles de usuario en el sistema para controlar el acceso a las diferentes opciones del mismo.

En la pantalla de inicio podemos ver los campos para digitar el nombre y la contraseña de un usuario del sistema.

Página inicial del Sistema

Luego de que el usuario se identifica, será dirigido a una de las secciones siguientes:

1. **Perfil de Administración**

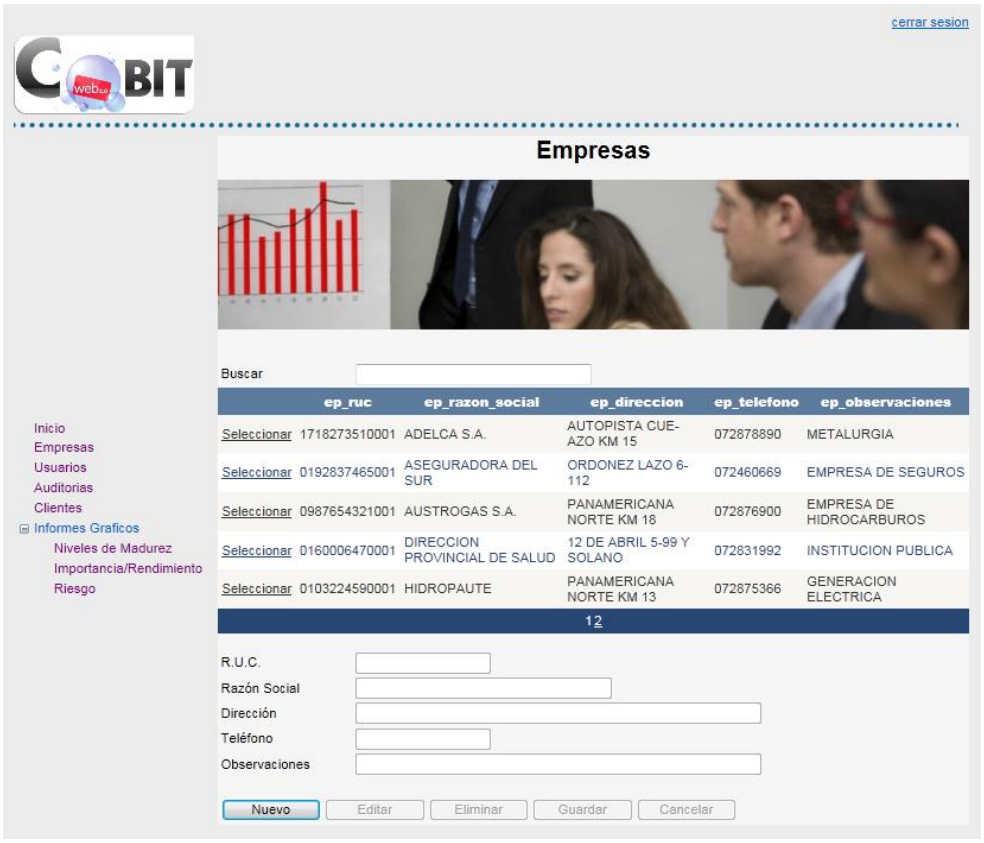
En este perfil el usuario puede realizar todas las operaciones de mantenimiento sobre el sistema, como es la creación, edición y eliminación de entidades y la revisión de informes gráficos.

Página de Inicio del Administrador

A la izquierda se puede ver el siguiente menú:

Menú del Administrador

1.1 Empresas



Página de Gestión de Empresas

Aquí podemos ver las empresas registradas o agregar una empresa nueva al sistema.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las empresas que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las empresas registradas con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente.

En la parte inferior se encuentran los campos de texto para escribir la información de las empresas:

R. U. C.: corresponde al Registro Único de Contribuyentes que identifica de forma única a una empresa, es de trece dígitos y debe finalizar en “001”.

Razón Social: es el nombre con el que se conoce a la empresa.

Dirección: es la ubicación de la empresa.

Teléfono: es el número telefónico para contactarse con la empresa, es de nueve dígitos y debe incluir el código de área sin espacios en blanco o guiones.

Observaciones: cualquier anotación adicional sobre la empresa.

Finalmente están los botones que permiten ejecutar diversas acciones:

Nuevo: habilita los campos para registrar una nueva empresa.

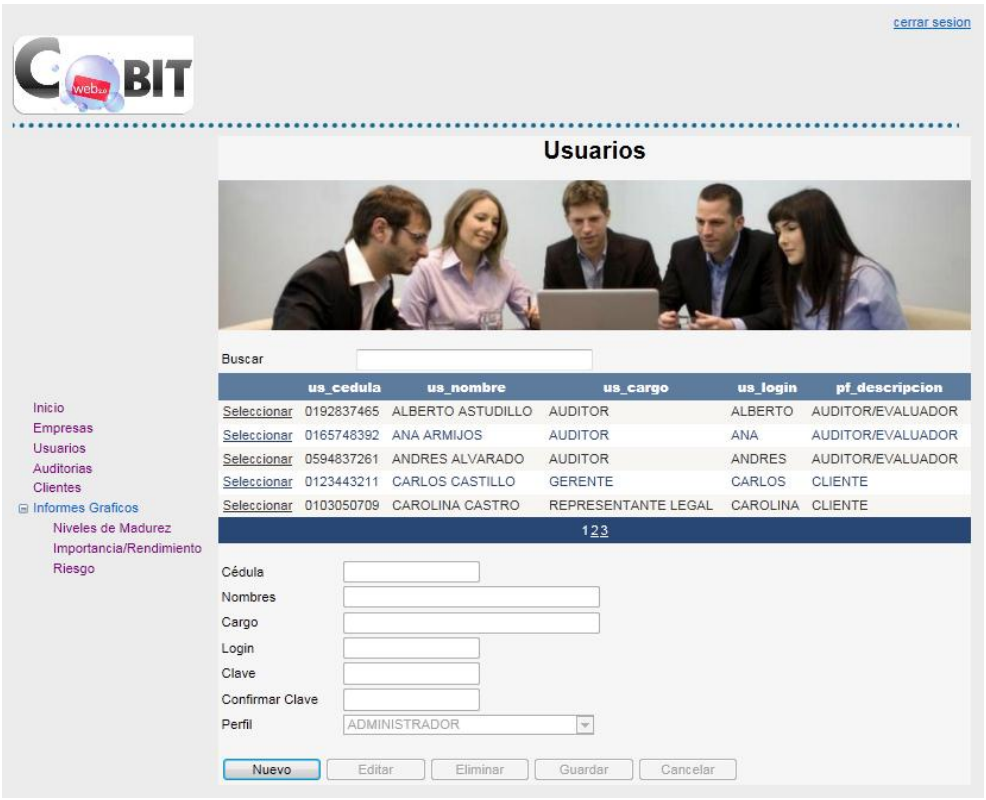
Editar: habilita los campos para editar la información de una empresa, previamente seleccionada.

Eliminar: suprime el registro seleccionado.

Guardar: almacena el nuevo registro o actualiza la información de un registro previamente seleccionado.

Cancelar: anula la acción que se encuentre realizando.

1.2 Usuarios



Página de Gestión de Usuarios

Aquí podemos ver los usuarios registrados o agregar un usuario nuevo al sistema.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de los usuarios que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de los usuarios registrados con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente.

En la parte inferior se encuentran los campos de texto para escribir la información de los usuarios:

Cedula: es el número que permite identificar de forma única a un usuario.

Nombre: el nombre completo del usuario del sistema.

Cargo: es el rol que desempeña en la empresa auditora o auditada.

Login: es el nombre que utilizará para ingresar al sistema.

Clave: es la contraseña que utilizará para ingresar al sistema.

Perfil: es el rol que tendrá al utilizar el sistema.

Finalmente están los botones que permiten ejecutar diversas acciones:

Nuevo: habilita los campos para registrar un nuevo usuario.

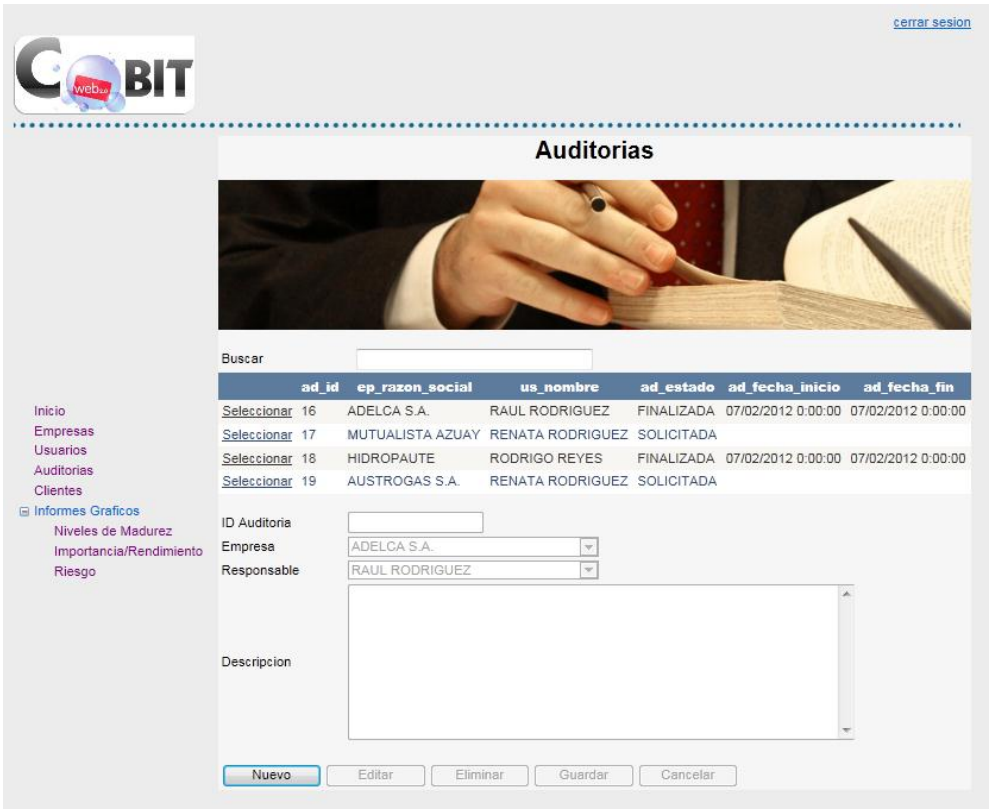
Editar: habilita los campos para editar la información de un usuario, previamente seleccionado.

Eliminar: suprime el registro seleccionado.

Guardar: almacena el nuevo registro o actualiza la información de un registro previamente seleccionado.

Cancelar: anula la acción que se encuentre realizando.

1.3 Auditorias



Página de Gestión de Auditorias

Aquí podemos ver las auditorias creadas o solicitar una nueva auditoría.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias solicitadas con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente.

En la parte inferior se encuentran los campos de texto para asociar la auditoria de una empresa con un responsable de la auditoria por parte de la empresa auditora y una breve descripción de la misma:

ID Auditoría: este es el número generado automáticamente por el sistema, de forma secuencial para identificar unívocamente una auditoría.

Empresa: es una lista desplegable para seleccionar la empresa que solicita la auditoría.

Responsable: es una lista desplegable para seleccionar al usuario responsable de la auditoría.

Descripción: permite indicar cualquier anotación relacionada con la auditoría.

Finalmente están los botones que permiten ejecutar diversas acciones:

Nuevo: habilita los campos para registrar una nueva auditoría.

Editar: habilita los campos para editar la información de una auditoria, previamente seleccionada.

Eliminar: suprime el registro seleccionado.

Guardar: almacena el nuevo registro o actualiza la información de un registro previamente seleccionado.

Cancelar: anula la acción que se encuentre realizando.

1.4 Clientes

Página de Gestión de Clientes

Aquí podemos ver las empresas registradas y los clientes asociados a las mismas, de modo que un usuario con el perfil cliente pueda acceder a la información correspondiente de una empresa determinada.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las empresas que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las empresas y los clientes asociados, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente.

En la parte inferior se encuentran los campos de texto para asociar una empresa con un cliente:

Empresa: es una lista desplegable para seleccionar la empresa a asociar con un cliente.

Cliente: es una lista desplegable para seleccionar al usuario del perfil cliente y asociarlo con una empresa.

Finalmente están los botones que permiten ejecutar diversas acciones:

Nuevo: habilita los campos para registrar una nueva relación.

Editar: habilita los campos para editar la información de una relación, previamente seleccionada.

Eliminar: suprime la relación seleccionada.

Guardar: almacena la nueva relación o actualiza la información de una relación previamente seleccionada.

Cancelar: anula la acción que se encuentre realizando.

1.5 Informes Gráficos

En esta sección el usuario podrá ver los resultados de las auditorias finalizadas a través de tres tipos de gráficos:

1.5.1 Niveles de Madurez

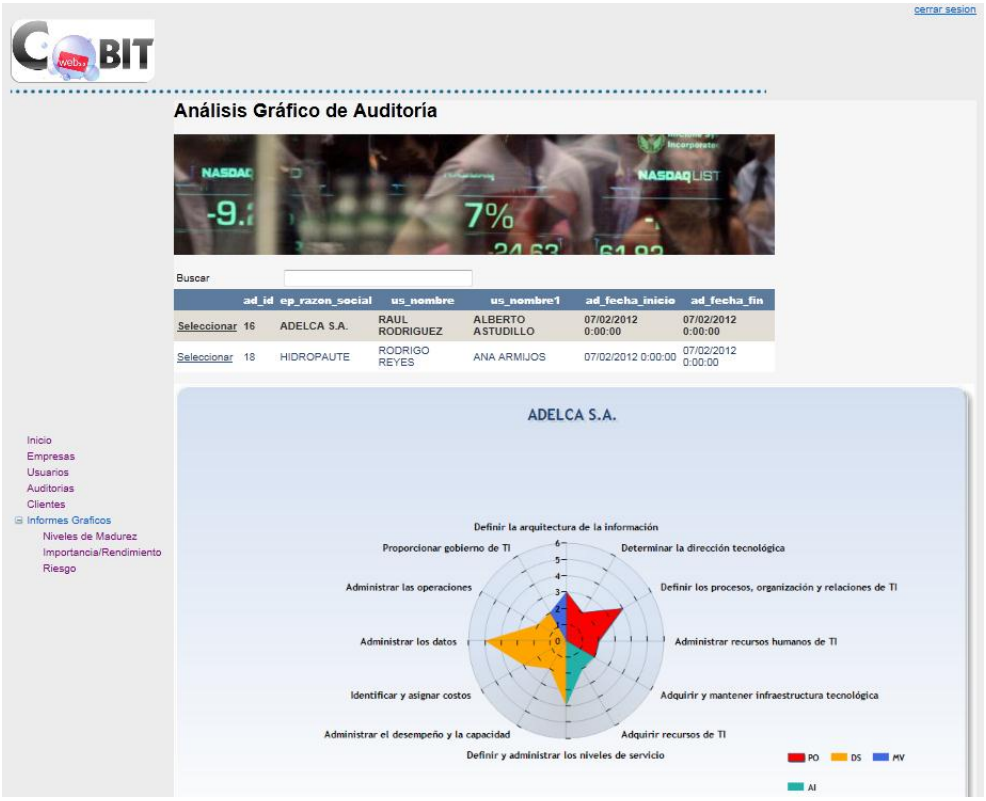


Grafico de Niveles de Madurez

El grafico Niveles de Madurez, de tipo radial, muestra la calificación de los procesos evaluados en una escala de 0 a 5 (determinada por el estándar Cobit 4.1), diferenciando los grupos por color

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico

1.5.2 Importancia/Rendimiento

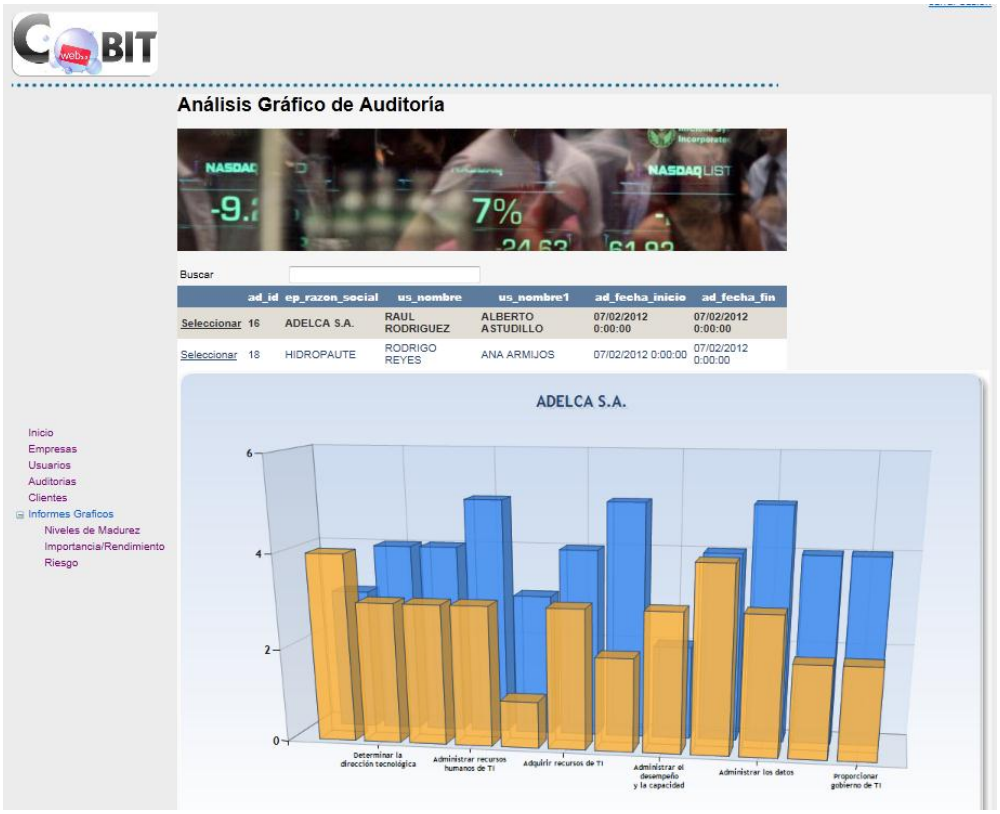


Grafico de Importancia/Rendimiento

El grafico Importancia/Rendimiento muestra la relación entre los valores de Importancia y Rendimiento de cada uno de los procesos Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

1.5.3 Riesgo

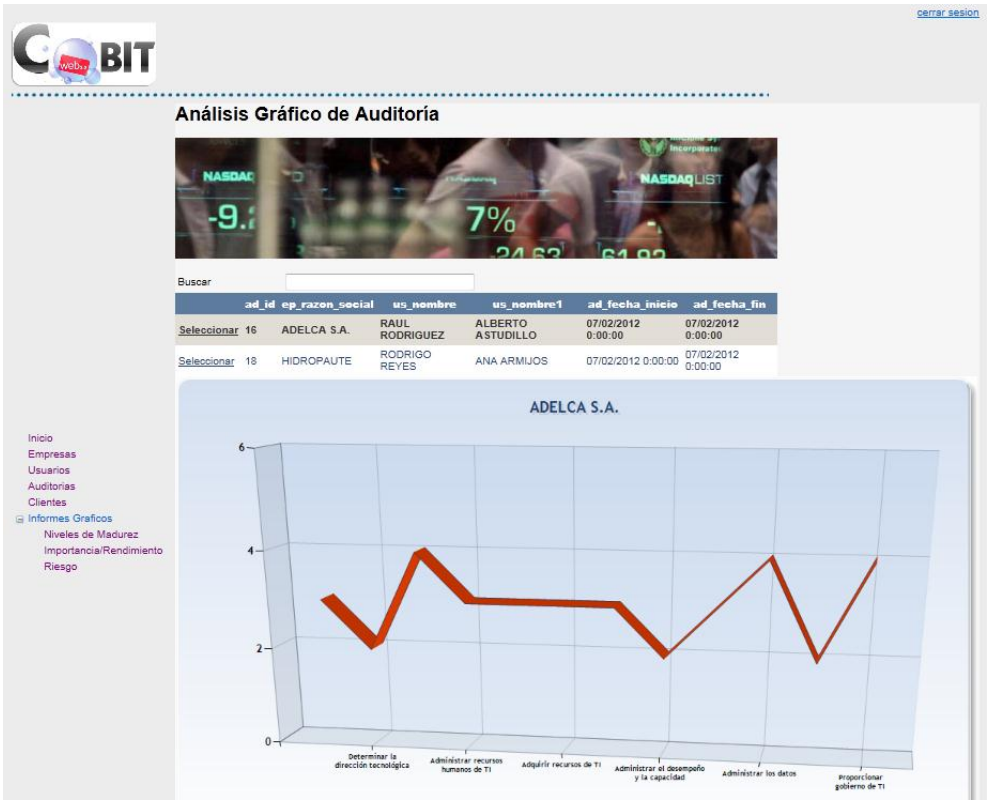


Gráfico de Nivel de Riesgo

El grafico Riesgo muestra la valoración de riesgo de cada uno de los proceso Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

2. Perfil de Responsable.

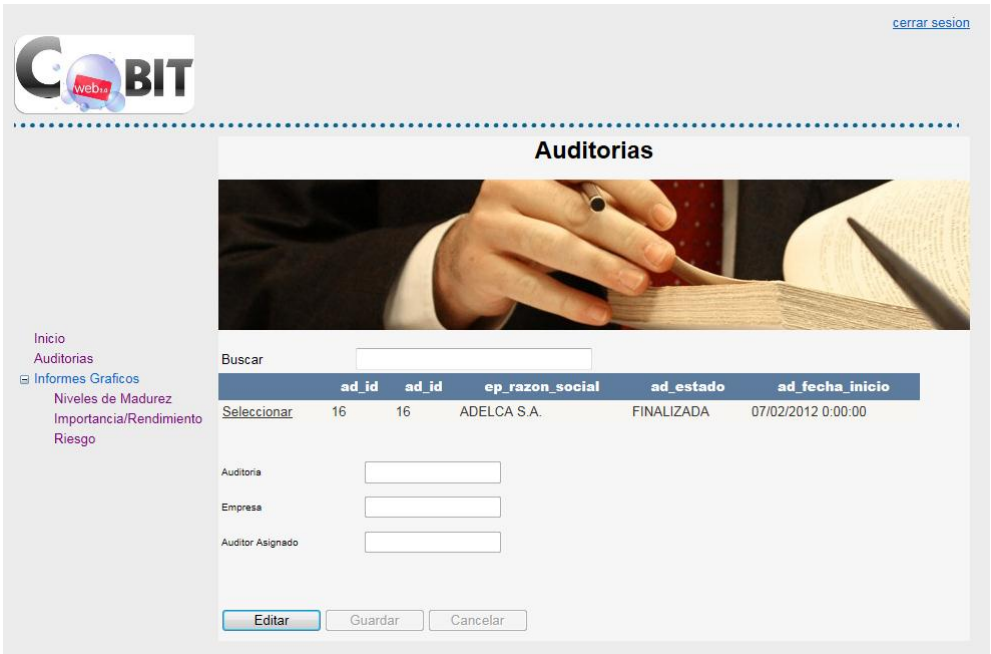
A través de este perfil, el usuario puede ver las auditorías asignadas a él, asociar un auditor para realizar la auditoría y ver los resultados gráficos de las auditorias finalizadas.

Página de Inicio del Responsable

A la izquierda se puede ver el siguiente menú:

Menú del Responsable

2.1 Auditorias



Página de Asignación de Auditores

Aquí podemos ver las auditorias creadas y de las que es responsable el usuario actual.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias solicitadas con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente.

En la parte inferior se encuentran los campos de texto para asociar la auditoria de una empresa con un responsable de la auditoria por parte de la empresa auditora y una breve descripción de la misma:

Auditoría: este es el número generado automáticamente por el sistema, de forma secuencial para identificar unívocamente una auditoría.

Empresa: muestra el nombre de la empresa auditada.

Auditor Asignado: muestra el nombre del usuario con perfil de auditor encargado de realizar la auditoría. Al editarse éste campo aparece una lista desplegable de auditores disponibles para asignar a la auditoría.

Finalmente están los botones que permiten ejecutar diversas acciones:

Editar: habilita los campos para editar la información de una auditoria, previamente seleccionada.

Eliminar: suprime el registro seleccionado.

Guardar: almacena el nuevo registro o actualiza la información de un registro previamente seleccionado.

Cancelar: anula la acción que se encuentre realizando.

2.2 Informes Gráficos

En esta sección el usuario podrá ver los resultados de las auditorias finalizadas a través de tres tipos de gráficos:

2.2.1 Niveles de Madurez

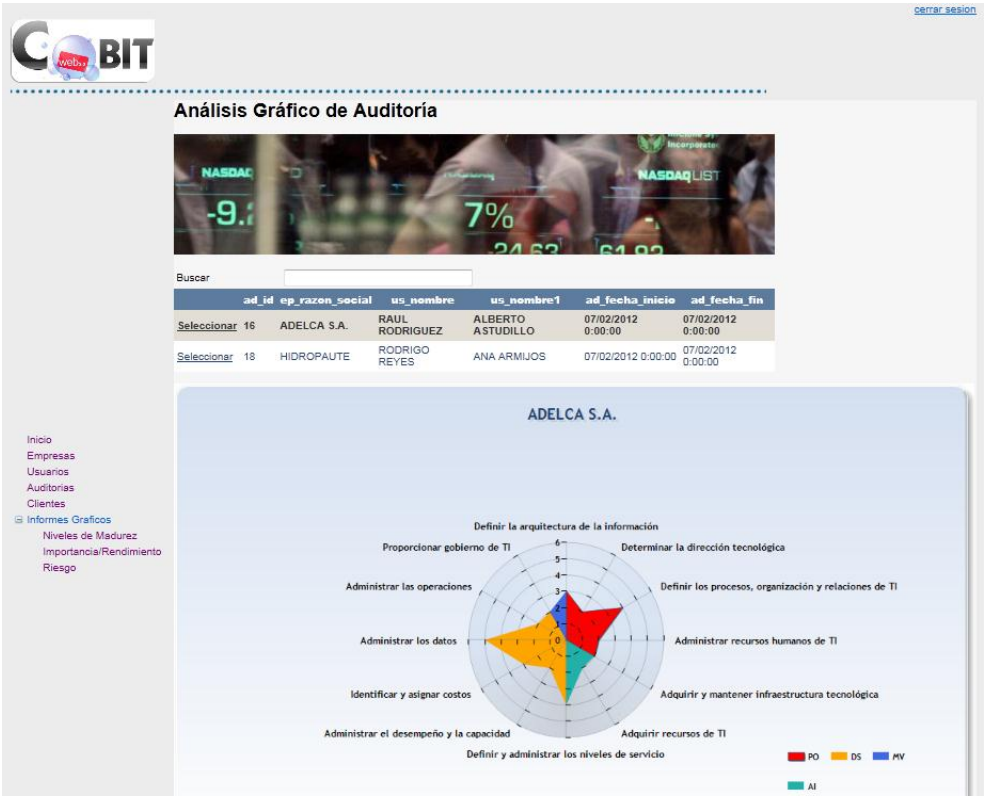


Gráfico de Niveles de Madurez

El grafico Niveles de Madurez, de tipo radial, muestra la calificación de los procesos evaluados en una escala de 0 a 5 (determinada por el estándar Cobit 4.1), diferenciando los grupos por color

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico

2.2.2 Importancia/Rendimiento

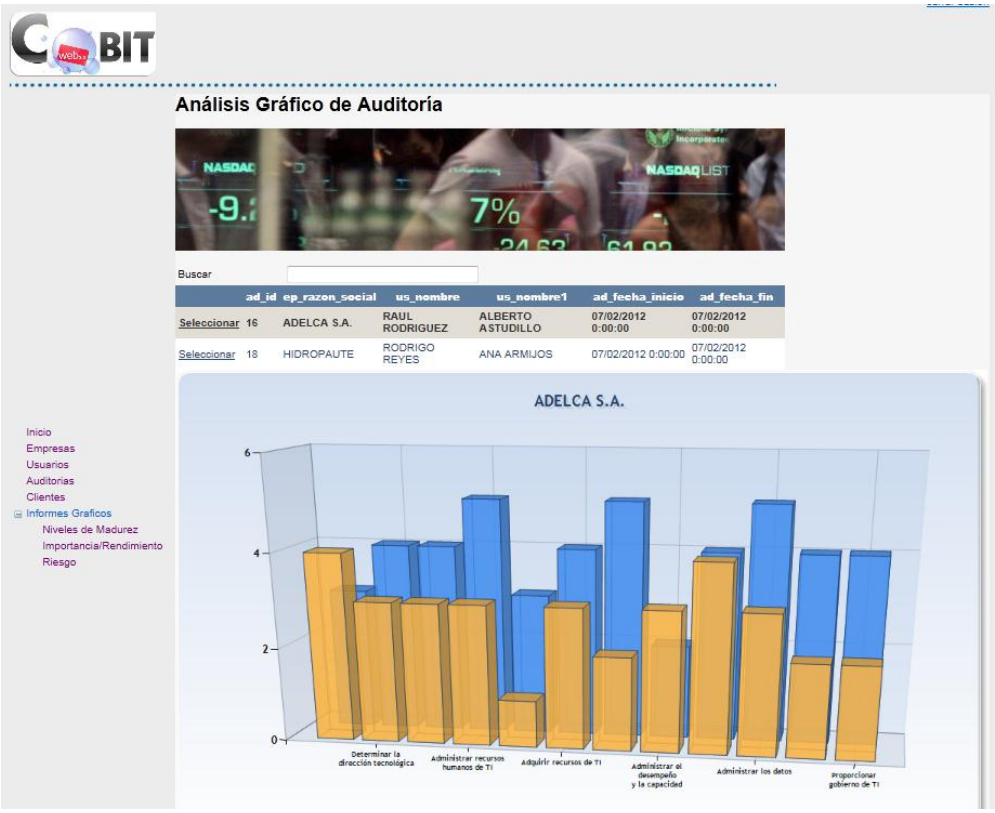


Grafico de Importancia/Rendimiento

El grafico Importancia/Rendimiento muestra la relación entre los valores de Importancia y Rendimiento de cada uno de los procesos Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

2.2.3 Riesgo

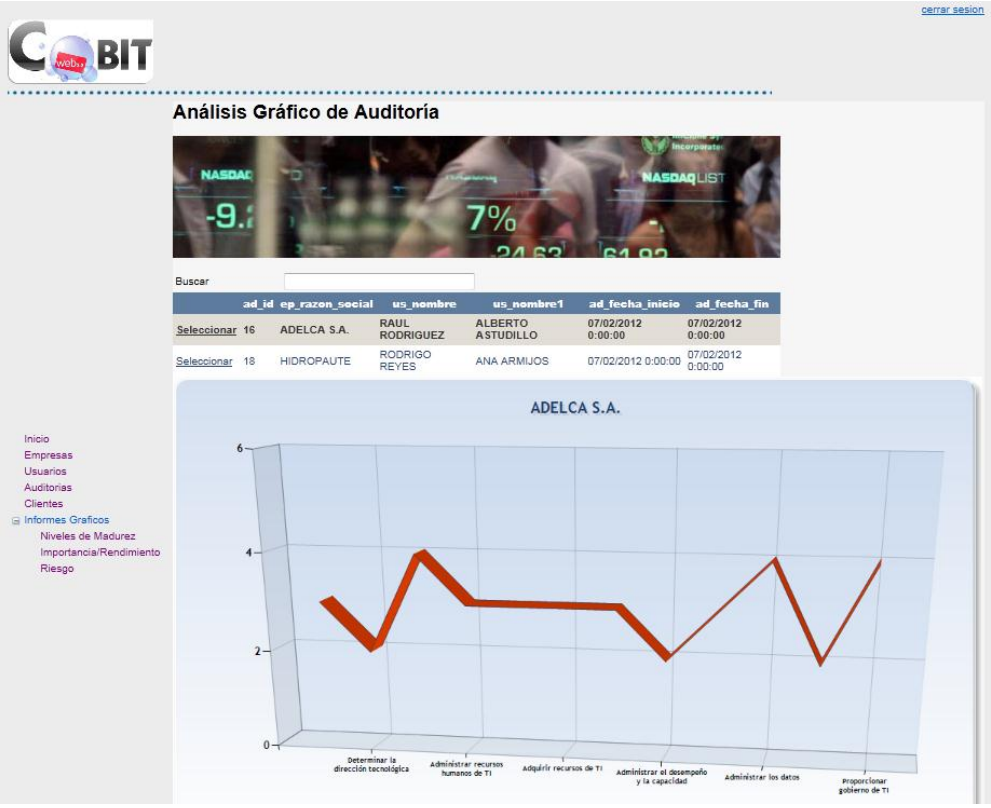


Grafico de Niveles de Riesgo

El grafico Riesgo muestra la valoración de riesgo de cada uno de los proceso Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

3. Auditor

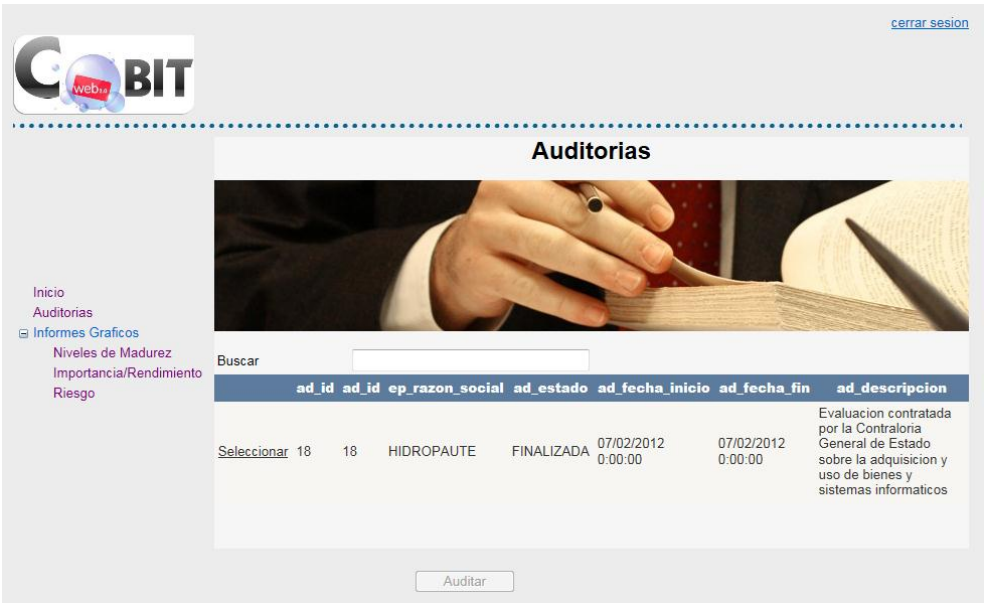
Mediante este perfil el usuario puede ver las auditorías a él asignadas y realizar el proceso de evaluación, así como también consultar los reportes gráficos de las auditorias finalizadas.

Página de Inicio del Auditor

A la izquierda se presenta el siguiente menú:

Menú del Auditor

3.1 Auditorías



Página de Auditorías Solicitadas

Aquí podemos ver las auditorias creadas y de las que es responsable el usuario actual.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias solicitadas con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente.

Si el estado de la auditoria es “SOLICITADA” o “INICIADA”, el botón “Auditar” se habilita para iniciar o continuar la auditoria seleccionada.

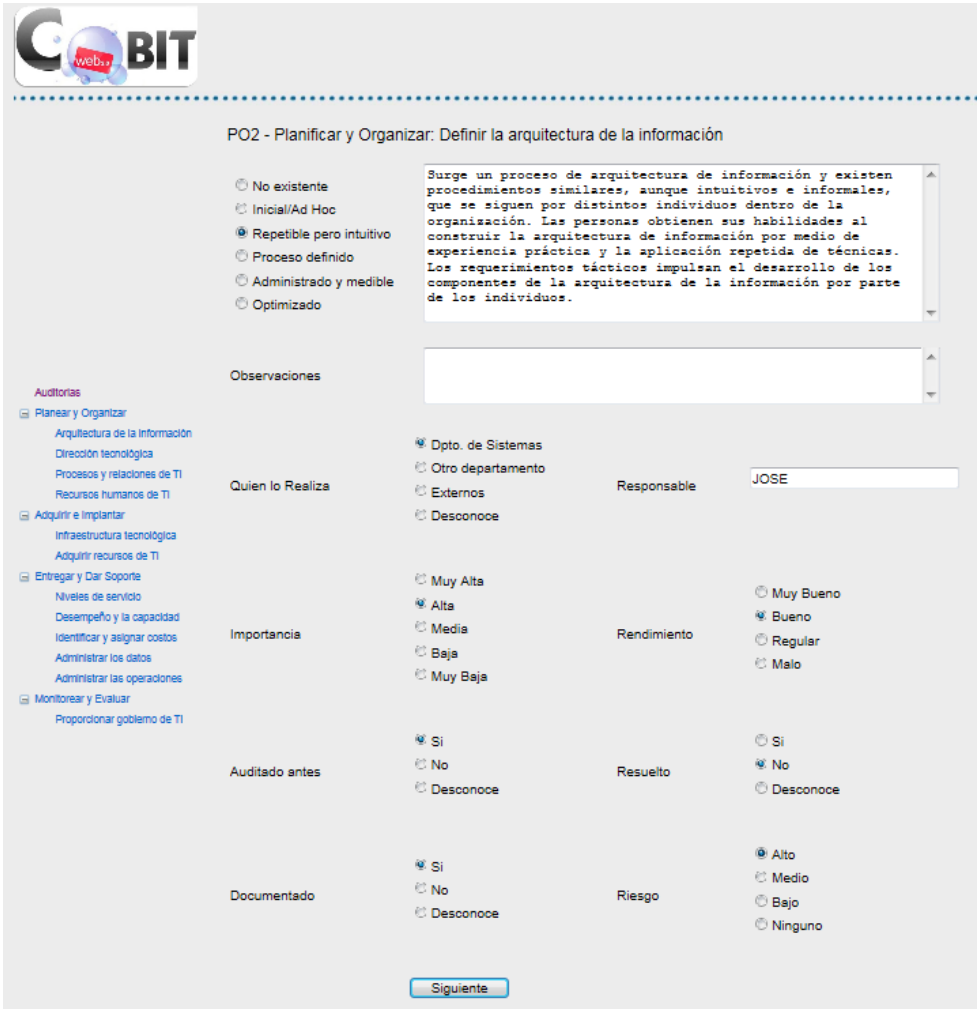
3.1.1 Auditoría

Página de Inicio de la Auditoría

En esta pantalla se muestra la información de la auditoria, tal como es el número, la empresa auditada, el estado en que se encuentra, la fecha de inicio de la auditoría, la fecha de finalización y la descripción de la misma.

En la parte inferior, el botón “Iniciar Auditoria” o lleva a la evaluación de los procesos Cobit.

3.1.2 Evaluación de Procesos.



Página de Evaluación de Procesos Cobit

Esta página se muestra para todos los procesos Cobit que se evaluarán.

En la parte superior se indica el código y nombre del grupo de procesos, seguido del nombre del proceso que se evalúa.

Seguidamente un grupo de botones que permiten seleccionar el nivel de madurez que el auditor identifique que posee el proceso, en la empresa que está evaluando. Al seleccionarlo, se muestra una descripción relativa al nivel de madurez seleccionado.

Luego dispone de un campo "Observaciones" para escribir cualquier anotación adicional relativa al proceso.

La sección "Quien lo Realiza" permite indicar que departamento está a cargo de las funciones relacionadas al proceso que se está evaluando.

El campo "Responsable" sirve para indicar el nombre del funcionario que está a cargo de las funciones relacionadas al proceso que se está evaluando.

En “Importancia” el evaluador indica el nivel de importancia que el proceso posee dentro de la empresa.

La sección “Rendimiento” indica el nivel de funcionalidad del proceso dentro de la empresa.

En la sección “Auditado antes” se indica si se ha realizado una auditoria previa al proceso actual.

“Resuelto” permite indicar si el proceso se considera íntegro o no.

La sección “Documentado” es para indicar si el proceso posee la documentación correspondiente.

En la sección “Riesgo” se indica el nivel de riesgo que posee el proceso dentro de la empresa.

Por último el botón “Siguiente” almacena los datos y avanza al siguiente proceso para evaluarlo del mismo modo.

Al llegar al último proceso, aparecerá el botón “Finalizar Auditoría” con el cual se da por terminado el proceso de evaluación y se almacena la fecha en la que se culminó el proceso.

3.2 Informes Gráficos

En esta sección el usuario podrá ver los resultados de las auditorias finalizadas a través de tres tipos de gráficos:

3.2.1 Niveles de Madurez

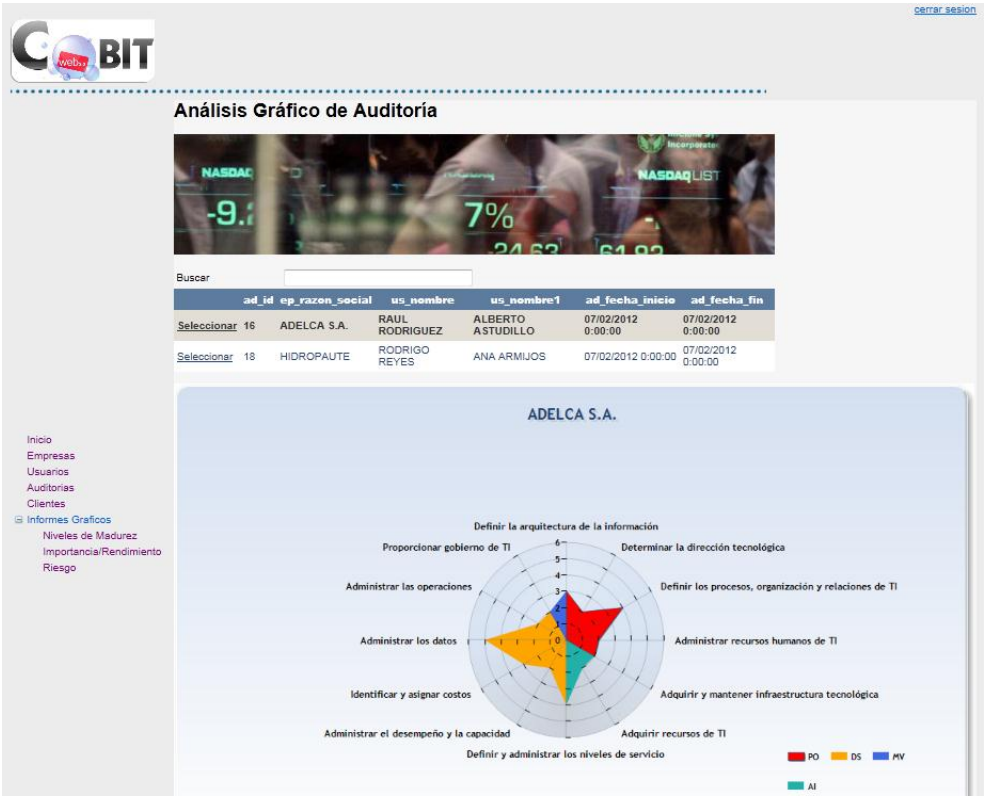


Grafico de Niveles de Madurez

El grafico Niveles de Madurez, de tipo radial, muestra la calificación de los procesos evaluados en una escala de 0 a 5 (determinada por el estándar Cobit 4.1), diferenciando los grupos por color

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico

3.2.2 Importancia/Rendimiento

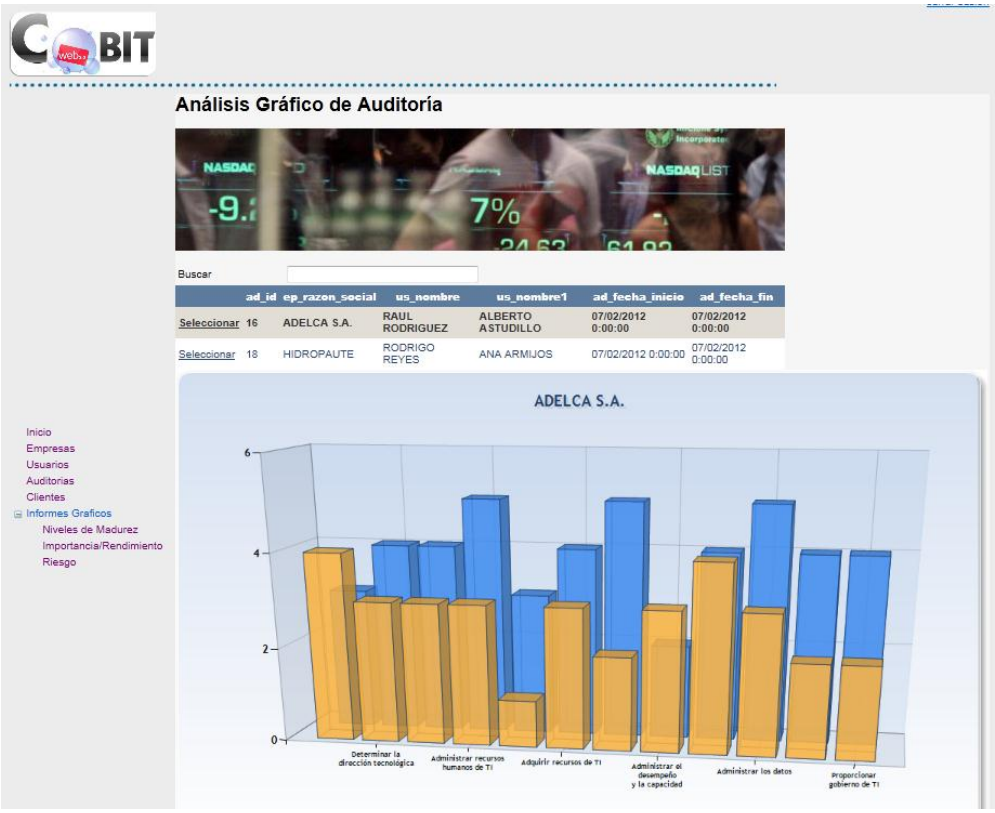


Grafico de Importancia/Rendimiento

El grafico Importancia/Rendimiento muestra la relación entre los valores de Importancia y Rendimiento de cada uno de los procesos Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

3.2.3 Riesgo

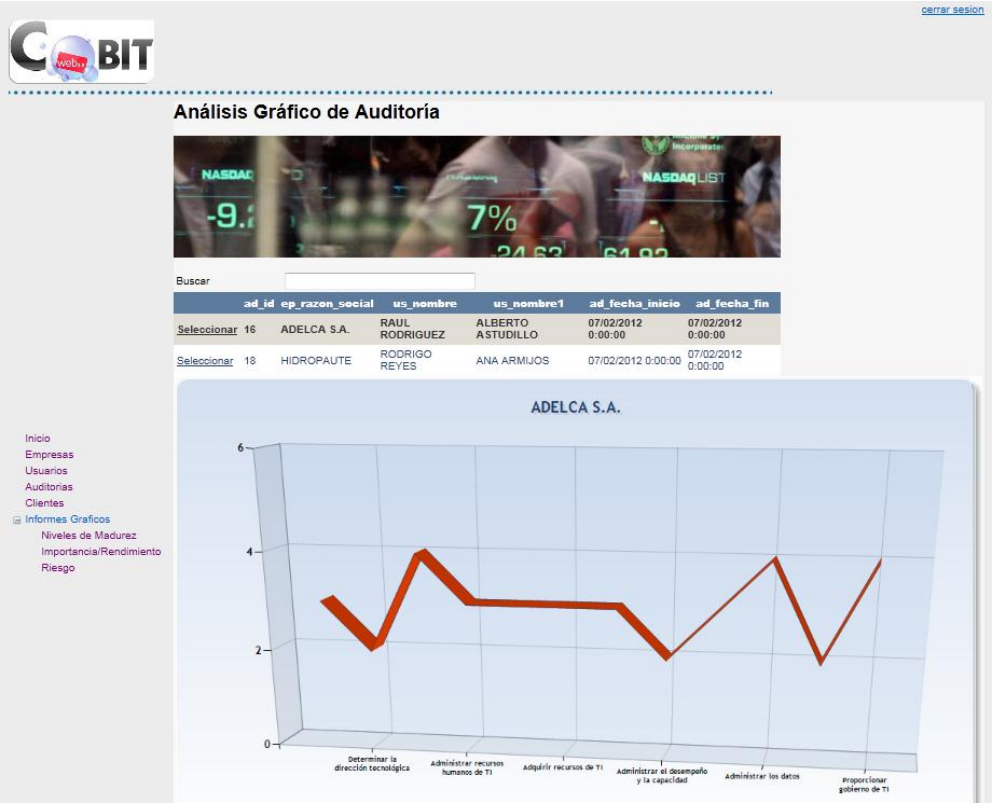


Gráfico de Nivel de Riesgo

El grafico Riesgo muestra la valoración de riesgo de cada uno de los proceso Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

4. Perfil de Cliente

En el perfil del Cliente, el usuario podrá acceder a la lista de reportes gráficos de las empresas a las que fue asociando previamente.

Página de Inicio del Cliente

En la parte izquierda se muestra el menú:

Menú del Cliente

4.1 Informes Gráficos

En ésta sección el usuario podrá ver los resultados de las auditorías a través de tres tipos de gráficos:

4.1.1 Niveles de Madurez

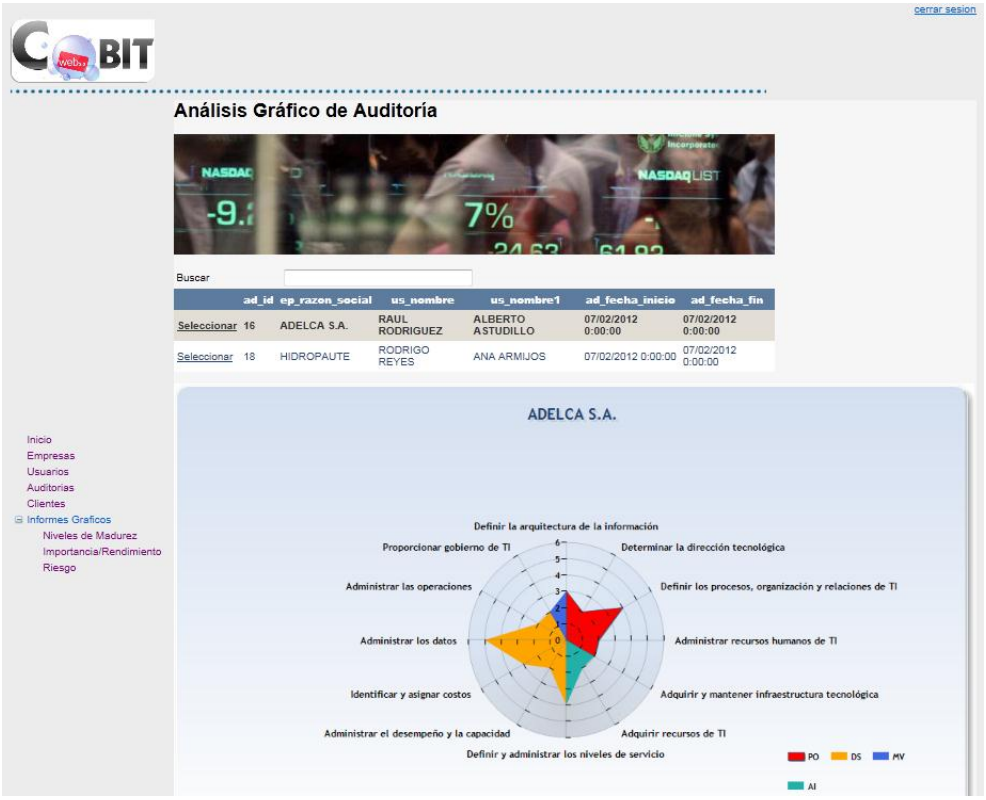


Gráfico de Niveles de Madurez

El grafico Niveles de Madurez, de tipo radial, muestra la calificación de los procesos evaluados en una escala de 0 a 5 (determinada por el estándar Cobit 4.1), diferenciando los grupos por color

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico

4.1.2 Importancia/Rendimiento

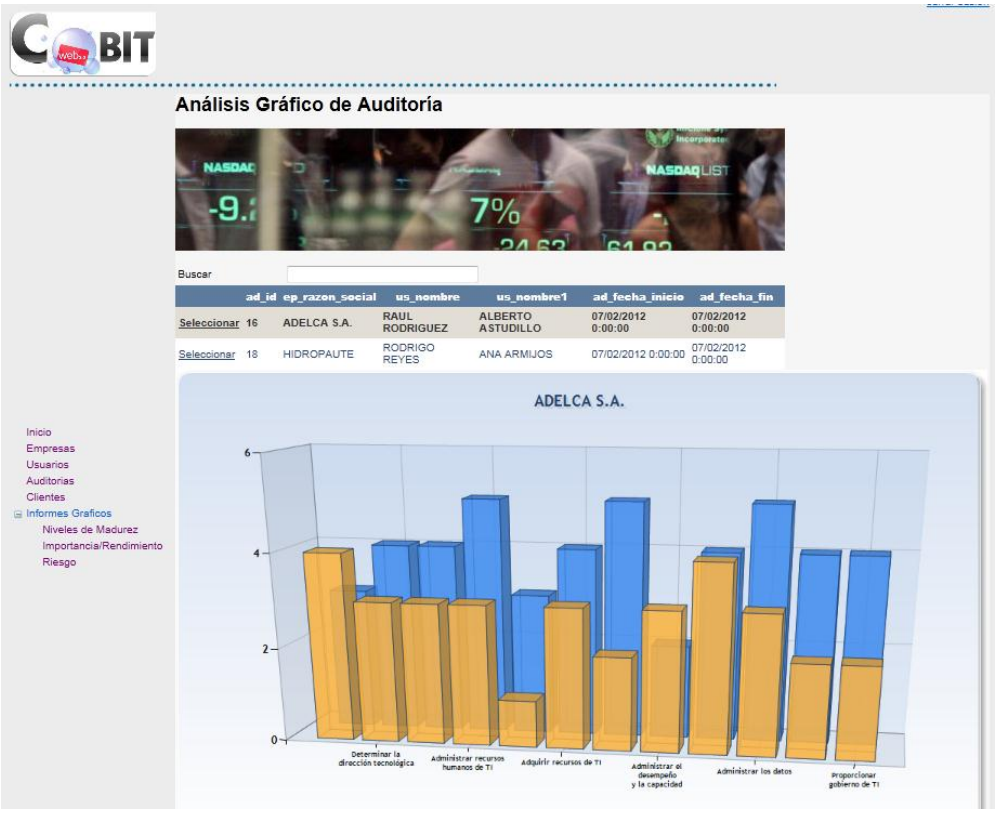


Grafico de Importancia/Rendimiento

El grafico Importancia/Rendimiento muestra la relación entre los valores de Importancia y Rendimiento de cada uno de los procesos Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.

4.1.3 Riesgo

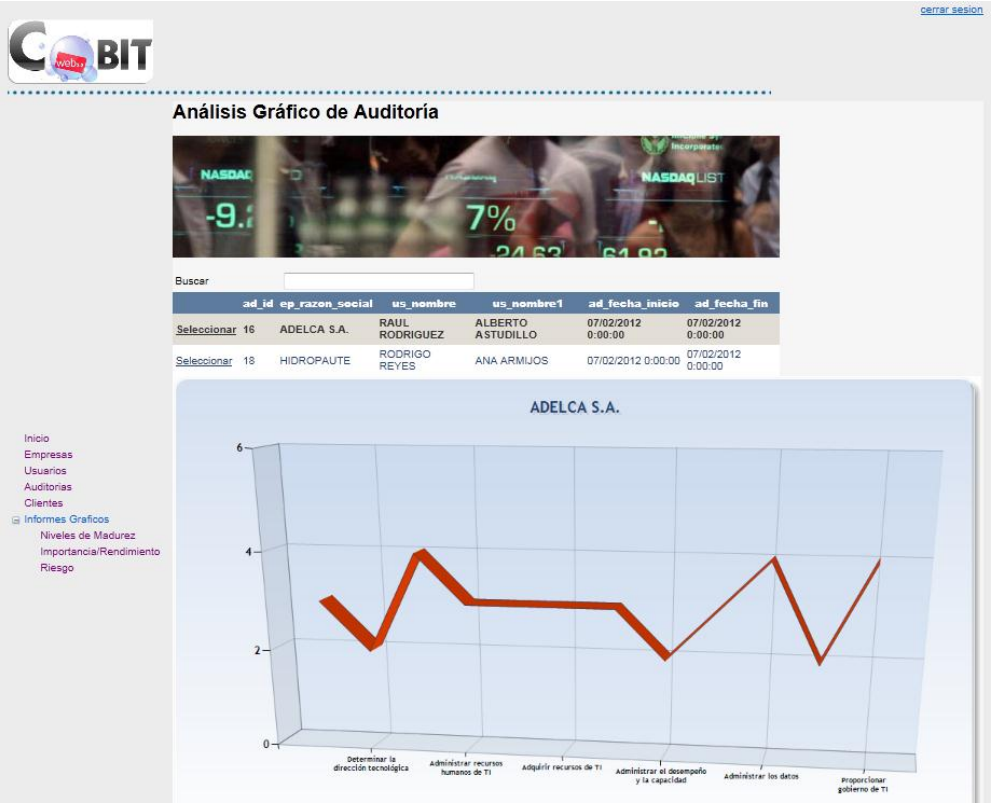


Grafico de Niveles de Riesgo

El grafico Riesgo muestra la valoración de riesgo de cada uno de los proceso Cobit evaluados.

En el centro tenemos el campo “Buscar”, el cual filtra el listado de las auditorias que se muestran, con cada pulsación del teclado.

Luego podemos ver el listado de las auditorias, con la opción “Seleccionar” en la primera columna, para seleccionar el registro correspondiente, y mostrar el grafico.