UNIVERSIDAD CARLOS III DE MADRID

ESCUELA POLITÉCNICA SUPERIOR

INGENIERÍA TÉCNICA EN INFORMÁTICA DE GESTIÓN

PROYECTO FIN DE CARRERA

AUDITORÍA PRÁCTICA DE BASES DE DATOS BAJO INFORMIX

Autor: Mª Isabel Romero Fernández

Tutor: Miguel Ángel Ramos González

Febrero, 2009

AGRADECIMIENTOS

Este proyecto ha constituido una meta muy importante a conseguir desde hace mucho tiempo, ya que debido a diversas circunstancias lo he tenido que ir posponiendo, pero con la ayuda de mis seres queridos, amigos y tutor, hoy es una realidad.

A todos mis amigos y familiares, pero muy en especial a mi madre que fue quien siempre me dio fuerzas y ánimos para luchar y conseguir las cosas que me propusiese, aunque ahora ya no está con nosotros, pero siempre estará en mi corazón, espero que desde donde esté se sienta orgullosa de mí.

A mi tutor, Miguel Ángel Ramos González, por la dedicación y colaboración en este Proyecto, ahora y en el pasado, así como por su interés y profesionalidad. Gracias a él me ha dado la ilusión de volver a intentarlo, muchas gracias.

Por último, y no menos especial, a mi marido, que ha estado ahí apoyándome y ayudándome para conseguirlo, esto y otros muchos momentos difíciles que nos ha tocado vivir, no tengo palabras para agradecérselo.

Gracias a todos.

INDICE

INDICE

CAPÍTULO 1

ORGANIZACIÓN DEL PROYECTO FIN DE CARRERA

1. ORGANIZACIÓN DEL PROYECTO FIN DE CARRERA

Antes de empezar a escribir este proyecto fin de carrera, uno de los objetivos que me planteé era que este trabajo fuera algo más técnico, que aportara una guía práctica al auditor para afrontar el estudio de un sistema de bases de datos, presentando aquellos aspectos más intrínsecos a Informix, así como una herramienta que lo llevase a cabo.

Aunque mi objetivo inicial fue el indicado anteriormente, a lo largo del proyecto y a través de mí experiencia profesional me he dado cuenta que la empresas tienen un control muy exhaustivo de los programas que se ejecutan en sus máquinas y sobre todo en aquellos que acceden directamente a los datos. Todos aquellos procesos que van contra la base de datos deben pasar un conjunto de pruebas muy exhaustivo y ejecutados por determinadas personas, que tienen dichos privilegios, y en horarios que no afecten al rendimiento del sistema. Además de la gran variedad de arquitecturas que existen, cada organización desarrolla un sistema que se ajusta a sus necesidades y en función de esto y de las decisiones estratégicas de la empresa desarrollan un entorno de almacenamiento y gestión de la información. Todo esto me ha demostrado que la probabilidad de que se permita ejecutar un programa en los sistemas de una empresa y la cantidad de parámetro a parametrizar para que se ajuste al entorno hace de esto que sea bastante baja. Creo que dicha tarea solo sería encomendada al equipo de auditoría interna del organismo o a una empresa especializada en base de datos Informix, bajo su exhaustiva supervisión.

Para poder conseguir mi objetivo inicial, aportar ayuda en el ámbito técnico, se exponen un conjunto de herramientas de Informix, que dan información del sistema y considero que no habría ninguna dificultad en su ejecución, ya que son propias del sistema Informix. Esta relación de herramientas, así como su funcionamiento y la información que aportan queda recogida tanto en el Proyecto Fin de Carrera como en la aplicación implementada del mismo.

Por todo lo expuesto con anterioridad, he desarrollado una aplicación que gestiona y ayuda a la creación de toda la documentación, pudiendo utilizar o diseñar plantillas que nos ayuden, permitiendo adaptarlos a las preferencias del equipo de auditoría.

Ésta documentación ya elaborada, permite al equipo de auditoría utilizarla como base y sólo tener que adaptarlas a las necesidades del estudio que se este llevando a cabo. Así como otro aspecto muy importante, el almacenamiento de todos aquellos estudios de auditoría llevado a cabo, lo que permite acceder de forma inmediata. Y en relación a Informix, objetivo principal del Proyecto Fin de Carrera, ayuda técnica clasificada en diferentes áreas de estudio y así como enlaces a manuales on-line alojados en la web oficial de Informix, donde poder ampliar la información.

Este Proyecto Fin de Carrera está enfocado a varios aspectos, por un lado la Auditoría de forma genérica, pero siempre enfocada en último término a las bases de datos y por otro lado Informix, como entorno, producto comercial muy importante en el mundo empresarial, actualmente disminuyendo su ámbito comercial, pero que ha sido y sigue siendo impulsor de las bases de datos. Y todo esto aplicado a la herramienta implementada.

CAPÍTULO 2

INTRODUCCION

2. INTRODUCCIÓN

En la actualidad, dados los altos niveles de complejidad que han alcanzado los procesos tecnológicos dentro de las empresas y la importancia de los sistemas de información se ha creado la necesidad de la existencia de una supervisión de los sistemas tanto por el departamento de Auditoría Interna como por Auditorías Externas.

Cabe aclarar que la Informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ello, debido a su importancia en el funcionamiento de una empresa, existe la Auditoría Informática.

Cada vez son más las empresas que sienten preocupación por la seguridad y protección de datos debido al auge del comercio electrónico y especialmente ante la aparición de legislación específica.

La Auditoría aporta una serie de información que hace que hoy sea necesaria en cualquier tipo de organización. Se deben realizar revisiones periódicas que garanticen la calidad y los niveles mínimos aceptables de control dentro de los sistemas de información, siempre adaptándose a la competitividad y necesidades de cada empresa.

El término de Auditoría se ha empleado incorrectamente con frecuencia ya que se considera como una evaluación cuyo único fin es detectar errores y señalar fallos. Sin embargo la auditoría es mucho más que esto, es un examen crítico pero no mecánico, que no implica la preexistencia de fallos en la entidad auditada y que persigue el fin de evaluar y mejorar la eficacia y eficiencia de una sección o de un organismo.

Pero la Auditoría requiere de personal con gran especialización, siendo necesarios mecanismos específicos sobre el área a tratar, que las hacen menos accesibles para todos los auditores. Por ello una solución es subcontratar los servicios de auditoría a terceras empresas a través de servicios de outsourcing.

Hoy en día no somos conscientes hasta que punto las bases de datos están integradas en nuestras vidas, incluso en muchas ocasiones no somos conscientes de estar utilizándolas. Por ejemplo, cuando utilizamos una biblioteca, una tarjeta de

crédito, realizamos la compra, alquilamos una película de vídeo, utilizamos Internet, o cualquier otra actividad de nuestra vida cotidiana. Todas estas acciones necesitan de una base de datos para poder llevarse a cabo, ya que el proceso supone conectarse y consultar o registrar cierta información para poder mostrarnos las películas, alquilar, permitirnos pagar con tarjeta, etc. Por ello la auditoría en esta área es prácticamente una actividad obligada a realizar toda organización.

La investigación sobre los sistemas de bases de datos ha tenido un impacto económico extraordinario. Con apenas 40 años de antigüedad como campo de investigación, se han conseguido grandes avances fundamentales en los sistemas de comunicación, transporte y logística, gestión financiera, sistemas de conocimiento, así como en otros campos de la ciencia, desde la informática a la biología. También hay que hacer mención especial al desarrollo de las capacidades del hardware, a la funcionalidad de éste y a las comunicaciones.

Las bases de datos constituyen en la actualidad el fundamento de todos los sistemas de información y han cambiado la forma en que muchas organizaciones operan. Cada vez se producen sistemas que son mucho más potentes e intuitivos de utilizar, llegando así a un mayor número de usuarios. Pero hay que tener cuidado, porque la creación de sistemas de información sin los suficientes conocimientos puede crear sistemas poco efectivos y eficientes. [SGBD Thomas M. Carolyn]

Por ello, es crucial el diseño de la base de datos. Una base de datos mal diseñada generará errores que pueden conducir a que se tomen decisiones incorrectas, lo cual podría tener repercusiones serias para la organización. Y por otro lado una base de datos bien diseñada proporciona la información correcta para que el proceso de toma de decisiones tenga éxito y funcione de manera eficiente.

También es importante hacer referencia a la calidad de los datos, es imprescindible obtener información veraz, si es inexacta la información proporcionada por la base de datos puede dar lugar a graves consecuencias a la organización. Algunas acciones, como son la estandarización, eliminación de duplicación, validación y enriquecimiento de la base de datos mejoran la calidad. Si se mejora la calidad de las bases de datos y teniendo datos de control de la calidad, las empresas puede generar información útil y actualizada que va a proporcionar una “fotografía” exacta de la eficiencia y

competitividad de la empresa, permitiendo maximizar la rentabilidad y reducir los costes, objetivos finales que persigue toda organización. Todo esto lleva a la necesidad de un control de las Bases de Datos y a la realización de un estudio para ver el control que se está realizado, por ello es necesario “Auditar”, nos va aportar una información de cómo está el sistema y las mejoras que necesitamos para obtener la calidad que nos permita ser competitivos en el mercado.

CAPÍTULO 3

AUDITORÍA

3. AUDITORÍA

3.1. INTRODUCCIÓN

Si nos remontamos al campo de la etimología se observa que auditoría viene del latín *auditorius*, que tiene la virtud de oír y revisar cuentas que están encaminados a un objetivo específico que es el de evaluar la eficiencia y eficacia con el que se operan los procesos, por medio de indicaciones de alternativas de acción, se tomen acciones que permitan corregir errores, en caso que existieran, o mejorar la forma de actuación.

La Auditoría Informática puede ser definida de diversas formas y una de sus definiciones la proporciona el diccionario Español Sopena, el cual define a la auditoría como "Revisor de Cuentas colegiado". Careciendo inicialmente de una definición donde se especifique el objetivo fundamental, es decir, no se indica en ningún momento la labor específica del auditor: evaluar la eficiencia y eficacia.

Para un mejor entendimiento de lo que significa la auditoría, vamos a detallar algunos conceptos realizados por expertos en la materia:

- La Auditoría es la verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad (eficiencia y eficacia) y presentar recomendaciones a la Dirección

- La Auditoría es una actividad que permite determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones y estándares la eficiencia de su implantación.

- Auditoría es una actividad dirigida a verificar y juzgar información en una empresa.

- Según ISO 19011:2002; Auditoría es el proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el grado de cumplimiento de los criterios de auditoría.

- Auditoría es un examen metódico de una situación relativa a un producto, proceso u organización, en materia de calidad, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado.

- Auditoría es el examen y evaluación de los procesos de todas las áreas de una empresa, utilización de los recursos que intervienen, establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las posibles deficiencias existentes y poder mejorarlas.

- Auditoría es un examen que se realiza con carácter objetivo, crítico, sistemático y selectivo con el fin de evaluar la eficacia y eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado soporte adecuado a los objetos y metas del negocio respecto a:

    - Eficiencia en el uso de recursos informáticos

    - Validez de la información

    - Efectividad de los controles establecidos.

Una vez expuesto diferentes definiciones que se han dado a la auditoría informática, podemos indicar que los principales objetivos de la misma son:

- El control de la función informática.

- El análisis de la eficacia del Sistema Informático.

- La verificación de la implantación de la Normativa.

- La revisión de la gestión de los recursos informáticos.

3.2. IMPORTANCIA DE LA AUDITORÍA

La Auditoría cumple una función muy valiosa e independiente, aunque no toma acciones facilita sugerencias y sus conclusiones deben tenerse en cuenta en el momento de la toma de una decisión. La auditoría se apoya con herramientas de análisis, verificación y exposición; conformando así elementos de juicio que permitirán determinar las debilidades y disfunciones del sistema.

La Auditoría aporta información sobre la situación informática de la empresa a la alta Dirección, que en muchos casos es desconocida. También descubre la existencia de algún tipo de delito efectuado, así como la falta de una planificación en el desarrollo normal y ante posibles situaciones de desastre. Identifica la falta de una política clara de actuación, objetivos, normas, metodología y estándares adecuados para la organización en el ámbito de los sistemas de gestión de la información.

Además, el hecho de realizar la auditoría informática es importante debido a que las herramientas que se utilizan pueden definir o marcar la diferencia con respecto a la competencia o al momento en que se está viviendo.

Una empresa no puede permitir que el software y el hardware presente falta de eficiencia porque va en contra de sus propios intereses. Además la seguridad supone un punto estratégico a tener especial atención.

La auditoría de datos es muy recomendable debido a que los sistemas pueden tener fallos en la información elaborada y por ello arrojar resultados erróneos.

Existen algunos aspectos que pueden determinar la necesidad de una Auditoría Informática, en estos casos las empresas acuden a las auditorías externas para que determinen donde se encuentran los fallos. Estos síntomas se pueden agrupar en clases:

- Cuando existe desorganización y descoordinación, es decir, los promedios conseguidos no se ajustan a los estimados o los objetivos previstos no coinciden con los resultados obtenidos.

- Cuando existe una insatisfacción del cliente, esto es, no se consigue cumplir las necesidades del cliente, se producen fallos en los sistemas que provocan el desconcierto del usuario o bien los resultados periódicos no son entregados en los plazos establecidos.

- Debilidades de carácter económico o financiero.

3.3. AUDITORÍA DE BASES DE DATOS

Cuando se enfrenta un auditor a la auditoría de una base de datos, deberá estudiar el Sistema Gestor de Base de Datos (SGBD) y su entorno. Como se señala el autor de origen británico Belden Menkus, *"en el desarrollo y mantenimiento de sistemas informáticos en entorno de BD, deberían considerarse el control, la integridad y la seguridad de los datos compartidos por múltiples usuarios. Esto debe abarcar todos los componentes del entorno de BD"*.

Cada Auditor o empresa de auditoría desarrolla su propia forma de trabajo, podemos decir que aunque existen distintas metodologías que se aplican, éstas se pueden agrupar en dos tipos:

- Metodología Tradicional

- Metodología de evaluación de riesgos

La metodología tradicional se caracteriza porque el auditor revisa el entorno con la ayuda de listas de control (checklist) que están formadas por un conjunto de cuestiones a verificar, que normalmente son contestadas con los valores simples: S (si), N (no) y NA (no aplicable).

Normalmente en las auditorías de base de datos se utilizan estas listas de control donde se recogen todos los aspectos a tener en cuenta: parámetros de instalación, seguridad, tipos de protección de los datos, copias de seguridad y restauración, etc.

La metodología de evaluación de riesgos, conocida también por "*risk oriented approach*", es la que propone ISACA (Asociación de Auditoría y Control de Sistemas

de Información), fija unos objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno.

Es muy importante la estructura orgánica de las unidades encargadas de la responsabilidad de la gestión y control de la base de datos. Para que funcione correctamente es imprescindible detallar las responsabilidades. No obstante, podemos clasificar las funciones entre las siguientes:

- El personal de desarrollo de sistemas y el de explotación
- Explotación y control de datos
- Administración de base de datos y desarrollo
- Seguridad de la base de datos

No significa que estas tareas deban ser realizadas por personas distintas (lo que no sería viable en muchas pequeñas y medianas empresas), pero si es un aspecto importante sobre el control a considerar, por lo que en el caso de que no pueda lograrse la separación de funciones, deberán establecerse controles compensatorios o alternativos.

El auditor no encuentra normalmente en las empresas una descripción detallada de los puestos de trabajo (que incluyan responsabilidades, conocimientos, etc.), por ello la separación de funciones es muy difícil de verificar.

Las Bases de Datos son un elemento muy importante en toda organización. Tanto el auditor como el profesional de seguridad son los encargados de llevarlas a cabo. Sin embargo, suelen encontrarse con problemas a la hora de realizarlas. La activación de logs para obtener información del sistema implica el uso de parte de los recursos del sistema, lo cual provoca una minoración de la capacidad de procesamiento del equipo. Por otro lado, también se ven afectados los medios de almacenamiento, que ven minorada su capacidad por almacenar dicha información. Estas dos características hacen, a veces, que los administradores de la Base de Datos opongan cierta resistencia a la implementación de la auditoría. Y es que implementar la auditoría afecta directamente el rendimiento de la base de datos.

3.4. TIPOS DE AUDITORÍAS

3.4.1. Auditoría Interna

La Auditoría Interna es realizada con recursos humanos propios de la empresa. Esta auditoría es una actividad que existe por decisión propia, es decir, que la empresa puede decidir el momento en que esta labor puede ser disuelta.

Este tipo de auditoría tiene algunos aspectos más ventajosos que la auditoría externa, ya que puede realizarse de forma periódica, y puede ser incluida en un plan anual de trabajo realizado una revisión completa de los sistemas y los equipos. Pero solo las empresas grandes pueden contar con una oficina de auditoría, debido a que es costoso contar con este servicio permanentemente, por ello generalmente las empresas pequeñas acuden a la auditoría externa.

Entre las ventajas que tiene la auditoría interna se encuentra que el personal que participa conoce el entorno, pero puede suponer un lastre porque el auditor no puede exigir calidad y documentación si meses antes él no la ha hecho, y si en general no ha cumplido lo que ahora recomienda. También es un inconveniente la relación con las personas, los auditados han sido sus compañeros, lo que genera una posible falta de independencia.

3.4.2. Auditoría Externa

La Auditoría Externa debe ser realizada por personal externo a la empresa que es objeto de la auditoría. La periodicidad suele ser anual o bianual, según se contrate. En este tipo de auditoría la delimitación vendrá dada por el objetivo del encargo, si bien los auditores podrán sugerir áreas complementarias de examen a la entidad, desde el principio o bien a la vista de los resultados parciales que se vayan encontrando.

Respecto a la selección de la empresa auditora deben considerarse varias entidades que cumplan las condiciones que se fijen y no seleccionar la entidad recomendada directamente por el Director de Informática.

En el contrato, es necesario especificar cláusulas de confidencialidad, porque la empresa contratada va obtener información vital y de gran valor para la entidad. Podrían incluirse cláusulas especiales cuando se prevea que el personal auditado no va a aportar las facilidades suficientes o que las personas clave no van a estar disponibles.

La auditoría informática externa normalmente será encargada por la Dirección General, por el Consejo de Administración o incluso por la mayoría de los accionistas. A veces es el propio Director de Informática quien solicita una auditoría externa con la intención de conocer la situación existente o para confirmar de forma independiente puntos que crea evidentes: falta de presupuesto, personal mal remunerado, saturación de equipos o cualquier otro aspecto que considere necesario.

Otros motivos por los que se puede producir que una organización que cuenta con una oficina de auditoría interna, solicite los servicios de una auditoría externa pueden ser:

- La falta de capacidad técnica para realizar la auditoría de materia especializada.
- Cruzar informaciones emitidas tanto de la auditoría interna como de la auditoría externa.
- La oficina de auditoría interna forma parte de la misma empresa, es por ello que es recomendable solicitar los servicios de una auditoría externa, lo cual permitirá tener una visión exterior de la empresa.

Tanto la auditoría externa como interna, deberán estar libres de toda influencia política, debido a que pueden afectar gravemente la estrategia y política general de la empresa. La oficina de auditoría puede actuar por decisión propia ya que es un órgano independiente de la empresa aún estando dentro de la misma, también actúa a solicitud de la dirección o de parte del cliente.

3.5. FASES DE LA AUDITORÍA INFORMÁTICA

A continuación planteamos una serie de fases que se desarrollan habitualmente durante una Auditoría dentro de una organización:

- Identificar el Alcance y los Objetivos de la Auditoría Informática
- Realizar un Estudio Inicial del entorno a auditar
- Determinar los Recursos necesarios para realizar la auditoría
- Elaborar el Plan de trabajo
- Realizar las actividades de auditoría
- Realizar el Informe Final
- Carta de Presentación y Carta de Manifestaciones

3.5.1. Alcance y Objetivos de la Auditoría

Al realizar una Auditoría es necesario indicar el alcance de la misma, es decir, definir con precisión el entorno y los límites en que va a desarrollarse la auditoría informática, y se complementa con los objetivos de ésta, indicando todos aquello que va a quedar exento de la auditoría. La no definición pondrá en peligro el éxito de la Auditoría Informática.

El alcance puede ir desde el estudio completo del sistema o sólo de una parte o la comprobación de las acciones correctivas de auditorías anteriores.

El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado, no solamente hasta que puntos se ha llegado, sino que materias fronterizas han sido omitidas. La indefinición de los alcances de la auditoría compromete el éxito de la misma.

Se realiza un acuerdo por escrito, entre el auditor y el cliente, donde se indica que se va a auditar, qué funciones, materias, Departamentos o Áreas, así como los temas que no van a ser auditados. El auditor debe comprender con exactitud los deseos y pretensiones del cliente de manera que pueda cumplir claramente los objetivos acordados previamente.

Con la Auditoría se pretende conseguir minimizar y evaluar los controles implantados frente a los posibles riesgos, comprobar que se produce el cumplimiento de la normativa, la consistencia y confiabilidad de los sistemas de información, grado de seguridad, confidencialidad y privacidad, así como mostrar la situación actual y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.

- Minimizar y evaluar los controles implantados frente a los riesgos en el uso de las tecnologías de información.
- Comprobar el uso adecuado de los recursos
- Comprobar el cumplimiento de la normativa que afecta el orden gubernamental e institucional.
- Comprobar la consistencia y confiabilidad de los sistemas de información con las que cuenta la organización.
- Evidenciar el grado de seguridad, confiabilidad y privacidad del ambiente informático de la empresa
- Aumentar la satisfacción de los usuarios de los sistemas computarizados asegurando una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Aumento de la calidad
- Disminución de costes y plazos.

3.5.2. Estudio Inicial

Es preciso examinar la situación general de funciones y actividades generales de la informática. Estudiar la estructura organizativa del departamento de informática a auditar, su entorno de trabajo así como las aplicaciones informáticas que utilizan: Bases de datos, ficheros, etc.

Cuando se estudia la organización se examinan las relaciones jerárquicas y funcionales, los flujos de información, la cantidad de personal que permita determinar si es correcta la distribución de los recursos o es necesario una reorganización.

El Auditor debe disponer de una referencia del entorno de trabajo a auditar, inventario de hardware y software, formas de comunicación y redes, procedimientos de trabajo que utilizan, volumen, antigüedad y complejidad de las aplicaciones, metodología de trabajo, cantidad y complejidad de la bases de datos y ficheros, detallando el tamaño de las mismos; así como el número de accesos y la frecuencias de actualización. A partir de este Estudio Inicial se determinan los recursos humanos y materiales que va a necesitar el auditor.

En este estudio inicial y a lo largo del proceso de auditoría es importante determinar si la empresa tiene definida una política de seguridad donde se indican los procedimientos y planes que salvaguardan los recursos del sistema contra pérdidas y daños. En general, el coste de proteger al sistema contra las amenazas debe ser menor que el de recuperación en caso de que se viera afectado por una amenaza de seguridad. Si la empresa no tiene el conocimiento suficiente de lo que está protegiendo y de las fuentes de amenaza, puede ser difícil alcanzar un nivel aceptable de seguridad.

Es importante hacer que en el diseño de la política de seguridad participe la gente adecuada, además de obtener su aceptación y su cooperación en la política de seguridad. En definitiva, de todo ello dependerá el éxito.

El análisis del riesgo de un sistema que deben llevar a cabo las empresas implica determinar ¿Qué necesitan proteger?, ¿De qué necesitan protegerlo? y ¿Cómo protegerlo? Los riesgos se clasifican por nivel de importancia y gravedad de la pérdida.

Esta actividad no se debe realizar una sola vez en la vida de la empresa, el entorno es cambiante y por ello debe llevarse a cabo con regularidad. Siendo la auditoría la que puede dar información sobre si se está llevando a cabo una correcta política de seguridad.

3.5.3. Plan de Auditoría

Con toda la información obtenida en las fases anteriores se puede ya establecer un calendario de actividades en el cual hay que tener en cuenta una serie de aspectos, entre los cuales se encuentran los recursos necesarios para llevarla a cabo.

La planificación de la Auditoría, según ISACA, organización a nivel mundial que establece para los responsables de la dirección, control, seguridad y auditoría de información, las siguientes pautas a seguir:

- Conocimiento de la organización y de sus procesos, para identificar problemas potenciales, alcance de los mismos, etc.
- Programa de auditoría: calendario de trabajo (tareas y recursos) y su seguimiento.

Evaluación interna del control, mediante pruebas de cumplimiento de controles.

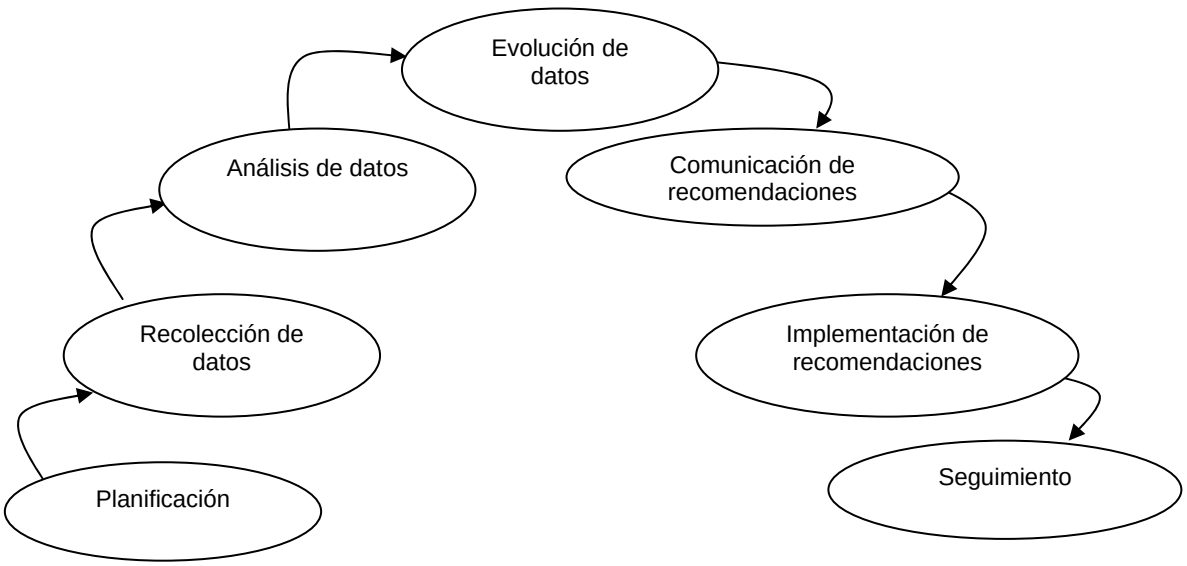


Ilustración 1.- Modelo del Plan de Auditoría

3.5.4. Técnicas y Herramientas en la Auditoría Informática

Durante el desarrollo de una auditoría informática se lleva a cabo una serie de actividades donde se analiza toda la información obtenida mediante una serie de herramientas tales como entrevistas, cuestionarios, muestreos, simulaciones (generadores de datos), paquetes de auditoría, revisiones de los controles existentes, etc.

Las principales técnicas y herramientas que se utilizan durante la ejecución de una auditoría informática se pueden resumir en:

- **Cuestionarios:**

  La auditoría informática se materializa recabando información y documentación de todo tipo. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global y objetivo, siempre amparado en hechos demostrables y evidentes.

  Los resultados que se obtienen con la auditoría se ven reflejados en los informes finales que éstos se emitan y su capacidad para el análisis de situaciones de debilidades o de fortaleza que se dan en los diversos ambientes. El denominado trabajo de campo consiste en que el auditor busca por medio de cuestionarios recabar información necesaria para emitir un juicio objetivo.

  Lo habitual es solicitar el cumplimento de formularios o cuestionarios que son dirigidos a las personas que el auditor considera más indicadas, no siendo necesario que dichas personas sean responsables de las áreas a auditar. Cada cuestionario es diferente y específico para cada una de las áreas y además debe ser elaborado teniendo especial cuidado en cuanto a la forma y el fondo.

- **Entrevistas:**

  Existen varias formas para que el auditor logre relacionarse con el personal auditado:

- La solicitud de la información debe ser concreta y sobre materias específicas de responsabilidad directa de la personal auditada.

- En la entrevista no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

- La entrevista es el medio por el que el auditor obtendrá información concreta.

Con la entrevista se obtiene mayor cantidad de información, además de ser más concreta que la proporcionada por otros medios técnicos como los cuestionarios. En el proceso de la entrevista el auditor deberá tener mucho cuidado, la entrevista debe ser de una forma muy cordial y bajo parámetros correctos, de manera que se pueda conseguir que sea lo menos tensa posible y el auditado conteste de la forma más natural.

- **Lista de comprobación**:

Como parte de la auditoría está la evaluación del personal, para ello existe el esta herramienta de auditoría. Es un cuestionario, el cual es archivado bajo estrictas medidas de seguridad, por considerarse información confidencial y activos muy importantes que respalda su actividad.

El auditor profesional es aquel que reelabora muchas veces sus cuestionarios en función de los escenarios auditados. Tiene claro qué necesita saber y por qué. Sus cuestionarios son vitales para el trabajo de análisis, contraste de la información y posterior síntesis de todo ello.

Hay opiniones que descalifican el uso de las listas de comprobación, ya que consideran que leer una serie de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático. Pero en realidad esta no es la forma de utilizar este tipo de herramientas por parte del auditor que actúa en esta línea de trabajo. El profesional realiza un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción

de puntos débiles y fuertes. Una ejecución profesional debe llevar a cabo preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas reciben el nombre de Listas de Comprobación. Salvo excepciones deben ser contestados oralmente, con ello se obtiene mayor cantidad de información. El personal auditado generalmente se encuentra familiarizado con el perfil técnico y lo percibe fácilmente, así como los conocimientos del auditor. Por ello es muy importante la forma y el orden en que se formulan.

Las listas de comprobación pueden ser de dos tipos atendiendo a su razonamiento para su evaluación:

- Lista de comprobación de rango: contendrá preguntas que se harán dentro de los parámetros establecidos, por ejemplo, 1 a 5, siendo 1 la respuesta más negativa y 5 la más positiva.

- Lista de comprobación binaria: preguntas que son formuladas con respuesta única y excluyente, Si o No; Verdadero o Falso.

- **Trazas o/y huellas**

Las funciones que deben realizar los programas, tanto de los sistemas como de los usuarios deberán ser las previstas y esto debe ser verificado por el auditor informático. Existen herramientas de software de dan información sobre el seguimiento de los datos a través de los programas.

Si por causas de las herramientas del auditor se da un aumento de carga en el sistema se podrá optar por darle uso en los momentos más adecuados.

Prácticamente todos los sistemas gestores de base de datos del mercado permite registrar ciertas operaciones realizadas sobre la base de datos, llamados pista de auditoría. El modelo de referencia de gestión de datos - ISO (1993), considera las pistas de auditoría como un elemento esencial de un Sistema Gestor de Base de Datos, señalando que “el requisito para la auditoría

es que la causa y el efecto de todos los cambios de la base de datos sean verificables".

La introducción de trazas o huellas puede hacerse de varias formas, con triggers se pueden lanzar procedimientos en el caso de detectar eventos, o la utilización de archivos de log o incluso modificar el código insertando en procedimientos almacenados en el código fuente. De esta forma podemos analizar los archivos de log y realizar las acciones pertinentes sin interferir en el flujo principal productivo.

- **Software de interrogación o auditoría**

Hasta hace algunos años se han utilizado productos software llamados genéricamente "paquetes de auditoría", capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos de software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados generalmente por los auditores externos, la auditores internos disponen del software nativo propio de la instalación.

Un ejemplo de estas herramientas son las que generan registros de auditoría, estos archivos son generados por unos scripts que se ejecutan después o en lugar de las instrucciones INSERT, UPDATE y DELETE. Los registros de auditoría son esenciales para las aplicaciones que trabajan con datos confidenciales o críticos, ya que realizan un seguimiento de la fecha y la hora en que se producen cambios de datos, así como de los usuarios que los realizan. De hecho, muchas aplicaciones financieras y de asistencia sanitaria deben emplear registros de auditoría por ley. Además, los registros de auditoría

son útiles a efectos de depuración, ya que proporcionan una ventana al estado de la base de datos en el momento que se produce un error.

- **Metodología de trabajo**

  Para la realización de la auditoría es importante utilizar un marco de referencia metodológico, que va a establecer un método de trabajo. La metodología usada por el auditor es generalmente es diseñada y desarrollada por el mismo y se basa en su grado de experiencia y habilidad. Son aplicados diferentes metodologías a los diversos aspectos definidos en el Plan de Auditoría.

  Como hemos indicado con anterioridad, la metodología de trabajo está basada en los profesionales de gran nivel de experiencia y formación, capaces de dictar recomendaciones técnicas, operativas y jurídicas.

  Todas las metodologías van encaminadas a establecer y mejorar un conjunto de medidas que reduzcan las amenazas lo más posibles o al menos se reduzcan de una forma razonable en coste-beneficio.

  Cualquier metodología de trabajo esta compuesta por un conjunto de fases, donde inicialmente se recopila y estudia los procesos de negocio o sistemas a auditar, posteriormente se analizan y evalúan los controles existentes para poder determinar la efectividad y eficiencia del mismo y por último se aplican pruebas de auditoría que verifican la efectividad de los controles o procesos. Este estudio genera un informe final donde se recogen un conjunto de sugerencias correspondientes a las oportunidades de mejoras.

  Con anterioridad hemos hecho referencia a la existencia de dos formas de llevar a cabo una auditoría, la Metodología Tradicional y la Metodología de evaluación de riesgos

  - Metodología Tradicional
  - Metodología de evaluación de riesgos

Es importante hacer referencia a ISACA (Information Systems Audit and Control Association), asociación internacional que elabora estándares que permiten a las organizaciones desarrollar proyectos de tecnología de información que cubren de manera adecuada las necesidades del cliente, en forma eficiente y oportuna y dentro del presupuesto establecido. El estándar internacional conocido como COBIT, sirve como guía para la buena práctica de la auditoría de las TI.

- **Lenguajes de cuarta generación**

Además de las herramientas que tiene integrado el Sistema Gestor de Base de Datos, el auditor puede encontrarse con un conjunto de generadores de aplicaciones o de informes que actúan sobre las base de datos y que, por tanto, también son un elemento importante a considerar en el entono del SGBD. El auditor deberá estudiar los controles disponibles en estas aplicaciones.

No obstante existe cierto riesgo con los lenguajes de cuarta generación, debido a que no se apliquen controles con el mismo rigor que al resto de programas desarrollados. La falta de código fuente tradicional hace más difícil el control de cambios en las aplicaciones. Además, también suelen ocurrir otros problemas asociados con este tipo de aplicaciones como son la ineficiencia o el elevado consumo de recursos.

3.5.5. El Informe

Podemos definir el “Informe de Auditoría” como el medio formal para comunicar los objetivos de la auditoría, las normas de auditoría utilizadas, los alcances, los resultados, las conclusiones y las recomendaciones de la auditoría.

Con todos los elementos de juicio recolectados, el Auditor podrá emitir un informe en el cual expresará el estado en el que se encuentran los sistemas, expondrá los fallos

existentes referentes al hardware y software, así como la correcta utilización del recurso informático.

En el informe se determinan los objetivos y alcances de la auditoría, enumerando los temas considerados. Indicando de manera exhaustiva los temas objeto de la Auditoría, antes de entrar profundamente en cada uno de ellos:

En la exposición de los temas evaluados se seguirá el siguiente orden:

- La situación actual, donde se dará a conocer el estado actual y real.
- Proyección de la evaluación futura.
- Exposición de puntos débiles y posibles amenazas.
- Se darán recomendaciones y planes de actuación; aquí es donde se detalla el verdadero objetivo de la auditoría informática, junto con la exposición de los puntos débiles.
- La carta de presentación o introducción, que es un resumen de la auditoría realizada, dirigida a la persona que se encuentra como responsable de la empresa, o la persona que pidió la auditoría.
- El Informe Final.

El Informe Final, debe contener los hechos realmente importantes, ya que los hechos irrelevantes no hacen más que distraer la atención del lector. Estos hechos deben estar documentalmente probados y soportados mediante una verificación objetiva, ya que esto puede indicar una debilidad que debería ser corregida. Por ello el Informe debe ser objetivo, claro, conciso, constructivo y oportuno.

La Asociación de Auditoría y Control de Sistemas de Información (ISACA) establece en su estándar 070.010, del cual hablaremos de manera más detallada a lo largo del presente proyecto, el contenido a incluir en el Informe de Auditoría:

- Alcance
- Objetivos
- Período de cobertura
- Naturaleza y extensión del trabajo de auditoría
- Organización
- Destinatarios del informe
- Restricciones
- Hallazgos
- Conclusiones
- Recomendaciones

Junto con el Informe Final se entrega una Carta Presentación que consiste en un resumen del contenido del Informe Final, donde se incluye la naturaleza, objetivos y alcance de la auditoría, se expone una conclusión general, concretando las áreas de gran debilidad y se indica su orden de importancia.

3.6. PERFIL DEL AUDITOR

La figura del auditor no se encuentra regulada en ningún manual y no existe ningún registro al respecto, por lo que el único requisito radica en su calificación y experiencia en diferentes proyectos. El Auditor debe ser una persona en constante formación debido a que la rapidez con la que progresan las nuevas tecnologías.

La auditoría y la seguridad en Base de Datos, son parte de los conocimientos imprescindibles de cualquier persona que quiera dedicarse plenamente a la profesión de Auditor Informático.

Es importante que un Auditor Informático tenga conocimientos de Auditoría y Seguridad en Base de Datos, porque hoy en día cualquier aplicación, independientemente del lenguaje en el que esté programada, consulta, modifica e introduce nuevos datos en una base de datos. Es, por tanto, primordial que el auditor sea capaz de auditar la metodología utilizada para el diseño de las bases de datos y los distintos entornos que utiliza, así como la explotación que se hace de la base de datos.

Cualquier ataque a un sistema se realiza con el único fin de la obtención de datos e información Hoy en día todos esos datos residen en bases de datos. Por tanto, un Auditor Informático tiene que saber que procedimientos utilizar para conocer los accesos no autorizados, los accesos de personas a información para la cual no tienen privilegios, así como el borrado o modificación de la información privilegiada. En la actualidad la creación e imposición de procedimientos de seguridad ayudan a proteger lo que se está convirtiendo rápidamente en el bien más importante y preciado de las empresas: los datos. Y, aunque el almacenamiento de esa información en una base de datos los hace más útiles y disponibles para toda la empresa, también los hace vulnerables a un acceso no autorizado. Será necesario, pues, prevenir y detectar dichos intentos de acceso.

Durante el desarrollo de una auditoría informática el auditor lleva a cabo una serie de actividades, donde analiza toda la información obtenida mediante una serie de herramientas tales como entrevistas, cuestionarios, muestreos, simulaciones (generadores de datos), paquetes de auditoría, etc.

Entre las personas que llevan acabo el plan de Auditoría en una determinada organización deben tener el siguiente perfil:

- Persona especializada que se dedica a evaluar la función informática.
- El auditor que evalúa la función informática debe tener conocimientos en tres áreas principales, Auditoría, Informática y Administración
- Expresarse con claridad tanto de forma oral como escrita

- Tener mente crítica que le permita analizar y cuestionar, con mucho cuidado, las diferentes actividades que evalúa.
- Amplio conocimiento del tipo de organización en la que realiza su labor que le permita ofrecer una asesoría constructiva.

Algunos autores definen el perfil ideal de un Auditor con los siguientes conocimientos y aptitudes.

Conocimientos	Aptitudes
Técnicas y procedimientos de auditoría.	Capacidad para planear y organizar las actividades de evaluación del control interno.
Ubicación adecuada de la función de la informática en la estructura organizacional.	Facilidad para analizar las funciones de la organización y determinar si el área de cálculo depende del nivel jerárquico superior.
Funciones, obligaciones y atribuciones de cada uno de los puestos técnicos y de apoyo del departamento de procesos.	Habilidad para evaluar las definiciones de los manuales de puestos para el departamento de procesos y capacidad de comprobación del funcionamiento de cada una de sus funciones.
Las distintas actividades que deben ejecutarse para alcanzar el adecuado procesamiento de los datos.	Capacidad para evaluar las tareas que se ejecutan en un sistema de procesamiento de datos y preparar lotes de datos que puedan someter a prueba las actividades del sistema.

Conocimientos	Aptitudes
Riesgos a que se enfrentan los datos, sistemas, equipos y recursos humanos en el ambiente de procesamiento.	Capacidad para discriminar entre los controles adecuados para la protección de los recursos informáticos y poder evaluar los controles de acceso lógico y físico.
Técnicas, políticas, recursos y procedimientos de respaldo y recuperación de operaciones.	Finalidad para evaluar las operaciones de respaldo sobre recursos de procesamiento y para revisar las actividades contempladas en los planes de contingencia y su factibilidad.
La metodología que debe ejecutarse para alcanzar un adecuado producto del desarrollo de los sistemas.	Participación activa en la evaluación de resultado de cada una de las fases del desarrollo de los sistemas automatizados.
Los avances tecnológicos y las tendencias de los recursos informáticos	Capacidad para verificar el análisis de los requerimientos de equipo, sistemas y otros recursos del área de informática.

3.7. ORGANISMOS Y NORMATIVA

3.7.1. Agencia Española de Protección de Datos

Es el organismo encargado de velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.

Se trata de un Ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada que actúa con independencia de las Administraciones

Públicas en el ejercicio de sus funciones. Por tanto es un referente a la hora de gestionar y controlar la información tratada en las bases de datos.

Entre algunas de sus principales funciones cabe destacar su capacidad de participación en la elaboración de normas, de manera que informa a los proyectos de desarrollo de la normativa sobre protección de datos. Así como dictar instrucciones y recomendaciones de adecuación de los tratamientos de dicha ley, además de facilitar recomendaciones en materia de seguridad y control de acceso a los ficheros.

Entre otro de sus cometidos está la potestad sancionadora, autorizar las transferencias internacionales de datos, emitir autorizaciones previstas en la ley y requerir medidas de corrección sobre la información contenida en las bases de datos.

Como desarrollo al cumplimiento de los objetivos de la Agencia Española de Protección de Datos dentro de su estructura orgánica debemos señalar dos Subdirecciones Generales, la primera encarga de la inspección de los datos que comprueba la legalidad en el tratamiento de la información; y la segunda la Subdirección General del Registro de Protección de Datos que vela por la publicidad de los tratamientos de datos (ficheros públicos y ficheros privados).

En 2007 la Agencia Española de Protección de Datos (AEPD) resolvió un total de 399 procedimientos sancionadores, incrementándose la cifra en un 32,5% respecto al año anterior.

Por último señalar que en España existen actualmente cuatro Agencias de Protección de Datos:

- La Agencia Española de Protección de Datos, regula a lo largo de todo el territorio español donde no exista una Agencia de Protección de Datos Autonómica y por lo tanto con competencias para realizar esta labor en esa determinada zona geográfica.
- La Agencia Catalana de Protección de Datos, regula y gestiona todo aquello relativo a la Protección de Datos en Cataluña.

- La Agencia de Protección de Datos de la Comunidad de Madrid, que regula y gestiona todo lo relacionado a la Protección de Datos en la Comunidad de Madrid.
- La Agencia Vasca de Protección de Datos, que regula y gestiona todo lo relativo a la Protección de Datos en el País Vasco.

Actualmente otras comunidades autónomas están desarrollando la creación de su propia agencia de Protección de Datos.

3.7.2. Ley Orgánica de Protección de Datos

La Constitución, norma básica y fundamental del estado de derecho de nuestra sociedad, que en su artículo 10 reconoce el derecho a la dignidad de la persona. Y en su artículo 18.4 dispone que "la ley limitará el uso de la informática para garantiza el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

En desarrollo del citado artículo 18.4 y como transposición al ordenamiento jurídico español de la Directiva 95/46/CE (Directiva sobre protección de datos), fue aprobada la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Esta ley tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

El Real Decreto 1720/2007 de 21 de Diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal, publicado en BOE n.17 de 19/1/2008 y entrando en vigor el 19 de abril. Se trata de un desarrollo de la Ley Orgánica de Protección de Datos que desarrolla tanto los principios de la ley, como las medidas de seguridad a aplicar en los sistemas de información. Se aplica tanto a ficheros en soporte automatizado, como en cualquier otro tipo de soportes.

Esta norma reglamentaria nace con la intención de no reiterar los contenidos de la norma superior y de desarrollo, incluye no sólo los mandatos contenidos en la Ley Orgánica, sino también aquellos que en estos años de vigencia de la Ley se ha demostrado que precisan de un mayor desarrollo normativo.

El objeto del presente desarrollo legislativo afecta a cualquier persona física o jurídica que trate datos personales fuera de la esfera puramente personal o doméstica. Se considera datos de carácter personal cualquier información numérica , alfanumérica, gráfica, fotográfica, acústica o de cualquier otro tipo concernientes a personas físicas identificadas o identificables. La ley considera que se trata de datos personales cuando hacen referencia a algunos de esta información: nombre y apellidos, fecha de nacimiento, dirección postal o dirección de correo electrónico, número de teléfono, número de identificación fiscal, huella digital, fotografías, número de la seguridad social, etc.
Existen una serie de excepciones que están recogidas en el artículo 2 del reglamento de desarrollo de la LOPD, según el cual no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal. Y por último tampoco será de aplicación a los datos referidos a personas fallecidas.

Los datos deben tratarse de manera legal y lícita. Deben recogerse con fines determinados, explícitos y legítimos. Y además deben ser adecuados, pertinentes y no excesivos en la relación con el ámbito y los fines para los que se han recogido.

El responsable de un fichero o tratamiento es la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales. Según el Tribunal Supremo se considera “Responsable del fichero” quien decide la creación del mismo, su aplicación, su finalidad, contenido y

uso. Y “Responsable del tratamiento” quien adopta decisiones sobre las actividades concretas de un determinado tratamiento de datos.

En el artículo 9 de la LOPD, se establece que, tanto el responsable del fichero como el encargado del tratamiento, deberán adoptar las medidas no sólo de índole técnico sino también de índole organizativo para garantizar la seguridad y evitar la pérdida, alteración y destrucción de ficheros con datos de carácter personal.

Sobre el responsable del fichero recaen las principales obligaciones establecidas por la LOPD y le corresponde velar por el cumplimiento de la Ley en su organización. En consecuencia el responsable debe:

- Notificar los ficheros ante el Registro General de Protección de Datos para que se proceda a su inscripción.
- Asegurarse de que los datos sean adecuados y veraces, obtenidos licita y legítimamente y tratados de modo proporcional a la finalidad para la que fueron recabados.
- Garantizar el cumplimiento de los deberes de secreto y seguridad.
- Informar a los titulares de los datos personales en la recogida de éstos.
- Obtener el consentimiento para el tratamiento de los datos personales.
- Facilitar y garantizar el ejercicio de los derechos de oposición al tratamiento, acceso, rectificación y cancelación.
- Asegurar que en sus relaciones con terceros que le presten servicios, que comporten el acceso a datos personales, se cumpla lo dispuesto en la LOPD.
- Cumplir, cuando proceda, con lo dispuesto en la legislación sectorial que le sea de aplicación.

En tratamientos de los datos por terceros se deberá regular mediante contrato escrito o cualquier otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado tratará los datos conforme a las instrucciones del responsable, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación a otras personas.

Los responsables tienen obligación de informar al interesado de forma previa, expresa, precisa e inequívoca de los siguientes aspectos:

- La existencia de un fichero o tratamiento con sus datos.
- Conocer para qué se utilizan sus datos.
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

El derecho a la protección de datos puede considerarse una condición preventiva para la garantía de otras libertades y derechos fundamentales. Así la LOPD reconoce específicamente a los ciudadanos los siguientes derechos en materia de protección de datos:

- Derecho de información en la recogida de datos
- Derecho de consulta al Registro General de Protección de Datos
- Derecho de acceso
- Derecho de rectificación
- Derecho de cancelación
- Derecho de oposición.

Por último mencionar la legislación existente, que trata ciertos aspectos relativos al almacenamiento de la información, la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (LJT) y la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI) que atribuyen a la Agencia Española de Protección de Datos la tutela de los derechos y garantías de abonados y usuarios en el ámbito de las comunicaciones electrónicas, en relación con las comunicaciones comerciales remitidas por correo electrónico o medios equivalentes y sobre el empleo de dispositivos de almacenamiento de la información en equipos terminales.

3.7.3. ISACA

A la hora de hablar de Auditoría hay que hacer mención especial a ISACA (Asociación de Auditoría y Control de Sistemas de Información). En 1967 un grupo de profesionales del sector de las Tecnologías de la Información decidieron desarrollar una guía de referencia central a la que todos pudieran consultar. Actualmente, más de 50 millones de miembros en todo el mundo confían en las pautas de gobernación, control, seguridad y auditoría de la información. ISACA se constituye de 170 sedes representativas que están situadas en más de 60 países.

El carácter especializado de la auditoría de sistemas de información y las habilidades necesarias para llevar a cabo dichas auditorías, requieren estándares aplicables globalmente que se adecuen específicamente a la auditoría de los sistemas de información. Es muy importante el desarrollo y la divulgación de los Estándares para la Auditoría de Sistemas de Información a la comunidad de auditores.

Los objetivos de los Estándares de ISACA para la Auditoría son informar a:

- Los auditores de los sistemas de información sobre el nivel mínimo requerido de rendimiento aceptable para cumplir con las responsabilidades profesionales establecidas en el Código de Ética Profesional para los Auditores de Sistemas de Información.

- Gerencia y a otros interesados sobre las expectativas de la profesión en relación con el trabajo de los auditores.

El marco de los Estándares de la Auditoría de Sistemas de Información de ISACA se compone de múltiples niveles:

- Los estándares definen los requisitos obligatorios para la auditoría y el informe de sistemas de información.

- Las directrices brindan una guía para aplicar los estándares de auditoría de sistemas de información. El auditor debe considerarlas para determinar cómo llevar a cabo la implementación de los estándares citados aquí anteriormente,

usar su juicio profesional al aplicarlas y estar preparado para justificar cualquier desviación de las mismas.

- Los Procedimientos ofrecen ejemplos de los procesos que deben ser seguidos por un auditor de sistema de información en un trabajo de Auditoría. Los documentos de procedimiento proporcionan información sobre la manera de cumplir con los estándares cuando se está realizando un trabajo de auditoría.

El objetivo de las directrices de ISACA para la auditoría de sistemas de información es proveer información adicional sobre cómo cumplir con los estándares de ISACA para la Auditoría de los Sistemas de Información.

A continuación enunciamos y desarrollamos brevemente los estándares aplicables a la auditoría de Sistemas de Información:

010 Estatuto de Auditoría

010.010 *Responsabilidad y Autoridad*. La responsabilidad y la autoridad de las funciones de auditoría de los sistemas de información deben estar documentadas de una forma apropiada mediante un estatuto o carta de compromiso de auditoría.

020 Independencia

020.010 *Independencia Profesional*. En todos los asuntos relacionados con la auditoría, el auditor de sistemas de información debe ser independiente del auditado tanto en actitud como en apariencia.

020.020 *Relación con la Organización*. La función de auditoría de sistemas de información debe ser lo suficientemente independiente del área que esté siendo auditada como para permitir que se logren los objetivos de la auditoría.

030 Ética Profesional y Estándares

030.010 *Código de Ética Profesional*. El auditor de sistemas de información debe acatar el Código de Ética Profesional de la Asociación.

030.020 *Debido Cuidado Profesional.* Se debe ejercer el debido cuidado profesional y se deben observar los estándares aplicables de auditoría profesional en todos los aspectos del trabajo del auditor de sistemas de información.

040 Competencia

040.010 *Destrezas y Conocimientos.* El auditor de sistemas de información debe ser competente desde el punto de vista técnico y debe tener las habilidades, destrezas y conocimientos necesarios para realizar el trabajo del auditor.

040.020 *Educación Profesional Continua*. El auditor de sistemas de información debe mantener su competencia técnica por medio de una educación profesional continua apropiada.

050 Planificación

050.010 *Planificación de la Auditoría.* El auditor de sistemas de información debe planificar el trabajo de auditoría de los sistemas de información para lograr los objetivos de la auditoría y para cumplir con los estándares aplicables de auditoría profesional.

060 Realización del Trabajo de Auditoría

060.010 *Supervisión.* El personal de auditoría de sistemas de información debe estar debidamente supervisado para garantizar que se logren los objetivos de la auditoría y que se observen los estándares aplicables de auditoría profesional.

060.020 *Evidencia.* En el curso de la auditoría, el auditor de sistemas de información debe obtener evidencias suficientes, confiables, relevantes y útiles para lograr los objetivos de una forma efectiva. Los hallazgos y las conclusiones de la auditoría deben estar respaldados por análisis apropiados y por una interpretación correcta de esta evidencia.

070 Informe

070.010 *Contenido y Forma del Informe.* El auditor de sistemas de información debe suministrar un informe, en una forma apropiada, a los destinatarios que corresponda al terminar el trabajo de auditoría. El informe de auditoría debe establecer el alcance, los objetivos, el período abarcado y la naturaleza y envergadura del trabajo de auditoría que se realizó. El informe debe identificar la organización, los destinatarios y cualquier restricción sobre su circulación.

El informe debe establecer los hallazgos, las conclusiones y las recomendaciones, así como también cualquier reserva o calificación según la opinión del auditor con relación a la auditoría

080 Seguimiento de las Actividades

080.010 *Seguimiento*. El auditor de sistemas de información debe solicitar y evaluar la información pertinente sobre los hallazgos, conclusiones y recomendaciones anteriores relevantes para determinar si se han implementado las medidas adecuadas de forma oportuna.

3.7.4. COBIT

El estándar COBIT es un conjunto de “mejores prácticas” para el manejo de la información creado por la Asociación para la Auditoría y Control de Sistemas de Información (ISACA) y el Instituto de Administración de las Tecnologías de la Información (ITGI).

COBIT ha proporcionado una ayuda a las organizaciones para salir adelante ante los desafíos que se presentan en sus negocios. Cada ve más, las empresas comprenden las ventajas de la tecnología de la información (TI) y reconocen la dependencia crítica de muchos procesos de negocio sobre la TI. Además del impacto significativo que la información puede tener sobre el éxito del negocio, y la obtención de una ventaja competitiva de su buen uso.

Originalmente fue desarrollado en 1992, pera la primera edición fue publicada en 1996; la segunda edición en 1998; la tercera edición en 2000 y la cuarta edición en

diciembre de 2005. En esta última edición, COBIT fijó 34 objetivos de alto nivel que cubren 318 objetivos de control (específicos o detallados) clasificados en cuatro dominios: Planificación y Organización, Adquisición e Implementación, Entrega y Soporte, y Supervisión y Evaluación.

Recientemente ha sido publicada la versión 4.1 de COBIT, se trata de una actualización significativa del marco mundial que asegura que las TI estén alineados con los objetivos de negocio, sus recursos sean usados responsablemente y sus riesgos se administren de forma apropiada. Esta versión puede utilizarse para mejorar el trabajo basado en versiones anteriores de COBIT.

Las actualizaciones en COBIT 4.1 incluyen: avances en la medición del desempeño; mejores objetivos de control y una excelente alineación entre objetivos de negocio y de las tecnologías de la información.

La misión de COBIT es investigar, desarrollar, publicar y promocionar un conjunto de objetivos de control generalmente aceptados para las tecnologías de la información que sean autorizados (dados por alguien con autoridad), actualizados e internacionales para el uso del día a día de los gestores de negocios (también directivos) y auditores. Gestores, auditores, y usuarios se benefician del desarrollo de COBIT porque les ayuda a entender sus Sistemas de Información (o tecnologías de la información) y decidir el nivel de seguridad y control que es necesario para proteger los activos de sus compañías mediante el desarrollo de un modelo de administración de las tecnologías de la información.

Se puede decir que COBIT es el único marco administrativo que comprende el ciclo de vida completo de la inversión en TI. Considera los logros en los objetivos de negocio, asegura alineación de las TI con el negocio y mejora la eficiencia y efectividad de las tecnologías de la información.

En resumen, el objetivo principal de COBIT consiste en proporcionar una guía a alto nivel sobre puntos en los que establecer controles internos con el propósito de:

- Asegurar el buen gobierno, protegiendo los intereses de los clientes, accionistas, empleados, etc.

- Garantizar el cumplimiento normativo del sector al que pertenezca la organización.
- Mejorar la eficiencia de los procesos y actividades de la organización.
- Garantizar la confidencialidad, integridad y disponibilidad de la información.

El estándar define el término control como: “políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proveer con seguridad razonable el logro de los objetivos del negocio y se prevendrán, detectarán y corregirán los eventos no deseables”.

Por tanto, la definición abarca desde aspectos organizativos (por ejemplo, flujo para pedir autorización a determinada información, procedimiento para reportar incidencias, selección de proveedores, etc.), hasta aspectos más tecnológicos y automáticos (como el control de acceso a los sistemas o la monitorización de los sistemas mediante herramientas automatizadas, entre otros).

Por otra parte, todo control tiene por naturaleza un objetivo. Es decir, es un propósito o resultado deseable como garantizar la continuidad de las operaciones ante situaciones de posibles contingencias.

En consecuencia, para cada objetivo de control de nuestra organización podremos implementar uno o varios controles: ejecución de copias de seguridad periódicas, traslado de copias de seguridad a otras instalaciones, etc., que nos garanticen la obtención del resultado deseable.

COBIT clasifica los procesos de negocio relacionados con las Tecnologías de la Información en cuatro dominios:

- Planificación y Organización
- Adquisición e Implementación
- Entrega y Soporte

- Supervisión y Evaluación

En definitiva, cada dominio contiene procesos de negocio, desglosado en actividades, para los cuales se pueden establecer objetivos de control e implementar controles organizativos o automatizados:

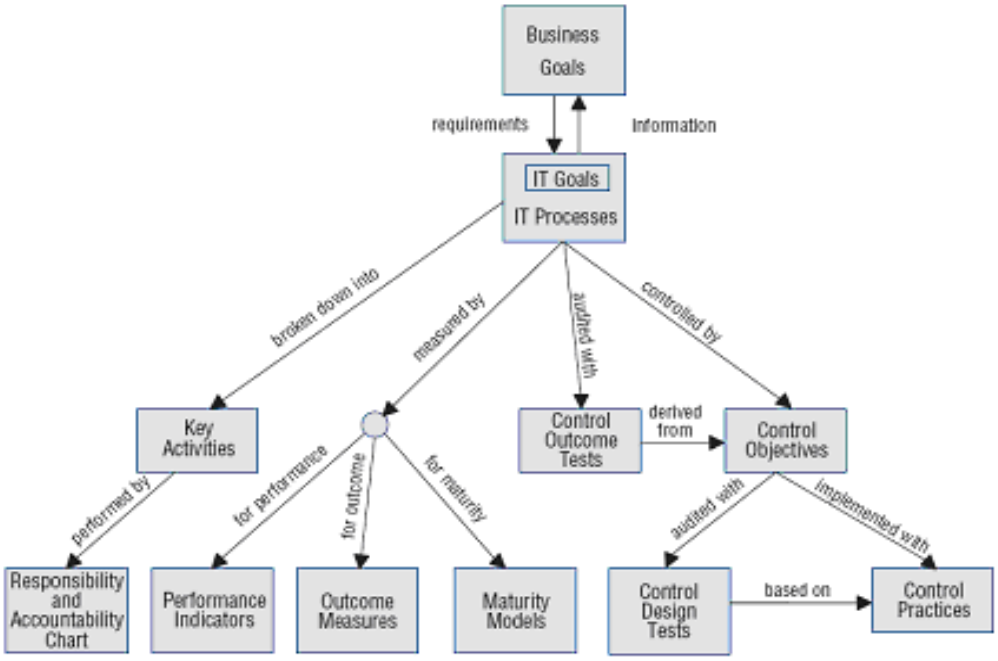


Ilustración 2. Las interrelaciones de los componentes de COBIT

Por otra parte, la organización dispone de recursos (aplicaciones, información, infraestructura y personas) que son utilizados por los procesos para cubrir los requisitos del negocio:

- Efectividad, es decir cumplimiento de objetivos.
- Eficiencia (consecución de los objetivos con el máximo aprovechamiento de los recursos).
- Confidencialidad.

- Integridad.
- Disponibilidad.
- Cumplimiento regular.
- Fiabilidad.

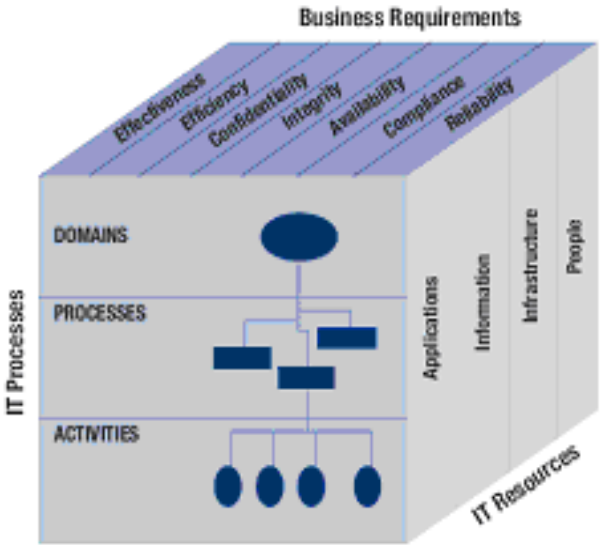


Ilustración 3. El Cubo COBIT

El estándar COBIT está formado por una serie de herramientas de implementación que proporcionan aspectos aprendidos por las empresas que de manera rápida y exitosa aplicaron este estándar en sus entornos de trabajo.

COBIT otorga especial importancia a aquellos requerimientos de negocio con respecto a su efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

Aunque anteriormente ya hemos hablado del modelo de COBIT (Control Objectives for Information and related Technology: Objetivos de Control para Tecnología de la información y relacionada), es importante profundizar en su modelo, ya que ayuda a

salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos. Proporciona “prácticas sanas” a través de un Marco de Referencia de dominios y procesos y presenta actividades en una estructura manejable y lógica. Las prácticas sanas de COBIT representan el consenso de los expertos, ayudarán a optimizar la inversión en información, y lo que es aún más importante, representa aquello sobre lo que será juzgado si las cosas no salen bien.

COBIT esta diseñado no solo para ser utilizado por los usuarios y auditores, sino para ser utilizado como una lista de verificación detallada para los propietarios de los procesos de negocio, proporcionándolos una herramienta que facilite el control. También se facilita la información que precisa la empresa para alcanzar sus objetivos.

Presenta 34 Objetivos de Control de alto nivel, uno para cada uno de los Procesos de TI, agrupados en cuatro dominios: planificación y organización, adquisición e implementación, entrega (de servicio) y monitoreo. Esta estructura cubre todos los aspectos de la información y de la tecnología que lo soporta. Adicionalmente junto a cada uno de los 34 objetivos de control de alto nivel, existe una guía de auditoría o aseguramiento que permite la revisión de los procesos de TI contra los 302 Objetivos detallados de control recomendados por COBIT para proporcionar a la Gerencia la certeza de su cumplimiento y/o una recomendación para su mejora.

COBIT contiene un conjunto de herramientas de implementación que proporciona experiencias de empresas que rápida y exitosamente lo aplicaron en sus organizaciones. Incluye un Resumen Ejecutivo para el entendimiento y la sensibilización de la alta gerencia sobre los principios y conceptos fundamentales de COBIT. La guía de implementación cuenta con dos útiles herramientas, Diagnóstico de Sensibilización Gerencial y Diagnóstico de Control en TI, para proporcionar asistencia en el análisis del ambiente de control en una organización.

El estándar COBIT está formado por una serie de herramientas de implementación que proporcionan aspectos aprendidos por las empresas que de manera rápida y exitosa aplicaron este estándar en sus entornos de trabajo.

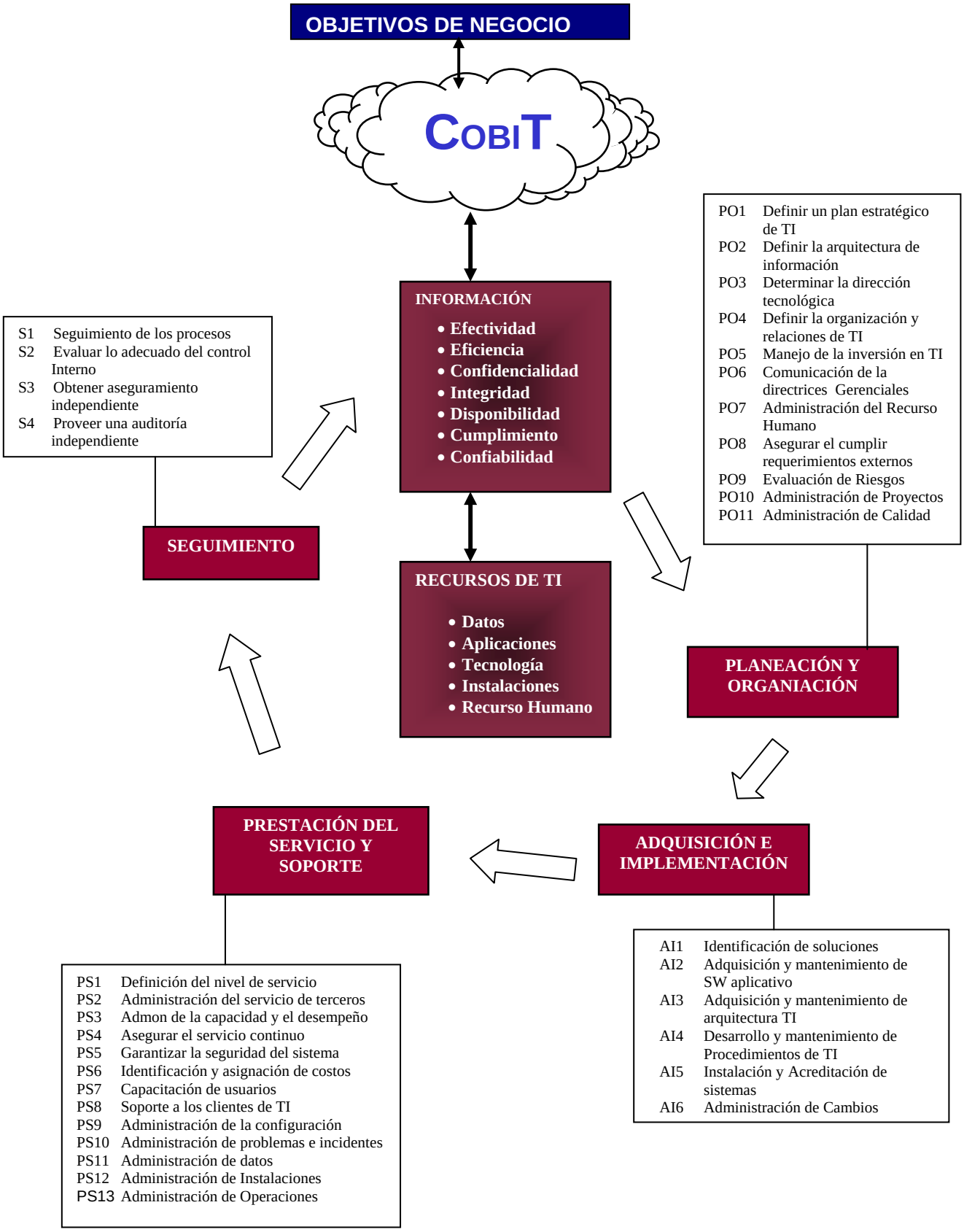


Ilustración 4. Objetivos del Negocio

COBIT ha sido desarrollado como un estándar generalmente aplicable y aceptado para la práctica del control de Tecnología Informática. Ha mejorado los estándares internacionales existentes tanto a nivel técnico y profesional, como específicos de la industria.

El desarrollo de COBIT ha tenido como resultado la publicación del Marco de Referencia general y de los Objetivos de Control detallados, y le seguirán actividades educativas. Estas actividades asegurarán el uso general de los resultados del Proyecto de Investigación COBIT.

COMPONENTES DEL PRODUCTO COBIT

El desarrollo de COBIT ha generado:

- Un Resumen Ejecutivo que consiste en una síntesis que proporciona a la alta gerencia entendimiento y conciencia sobre los conceptos clave y principios de COBIT.

- El Marco Referencial describe en detalle los 34 objetivos de control de alto nivel e identifica los requerimientos de negocio para la información.

- Objetivos de Control, los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de los 302 objetivos de control detallados y específicos a través de los 34 procesos de TI.

- Directrices de Auditoría, las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia unas indicaciones para la mejora de las aéreas analizadas.

- Conjunto de Herramientas de Implementación, que aportan lecciones aprendidas por organizaciones que han aplicado COBIT de manera rápida y exitosa en sus ámbitos de trabajo.

3.7.5. ISO/IEC 17799 (27002:2005)

ISO (Organismo Internacional para la Estandarización) es un organismo de alcance mundial encargado de coordinar y unificar las normas. Promueve el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas. Su función principal es buscar la estandarización de normas de productos y seguridad para las empresas y organizaciones a nivel internacional.

La norma de calidad, ISO/IEC 17799: 2005 (27002:2005) proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la Información se define en el estándar de la siguiente manera:

- Preservación de la confidencialidad: asegurando que sólo quienes estén autorizados pueden acceder a la información.
- Integridad: comprobando que la información y sus métodos de proceso son exactos y completos.
- Disponibilidad: asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Desde julio de 2007, ISO ha oficializado el cambio de nomenclatura de ISO/IEC 17799:2005, pasándose a llamar ISO/IEC 27002:2005. El cambio de nomenclatura viene a confirmar los esfuerzos que ISO está realizando para concentrar en la familia 27000 una serie de normas determinadas que guardan estrecha relación con la Seguridad de la Información. El cambio afecta únicamente al nombre de la norma, ya que los contenidos son exactamente los mismos que los anteriores.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

- Política de seguridad
- Aspectos organizativos para la seguridad

- Clasificación y control de activos
- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad de negocio
- Conformidad

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones, aunque cada organización debe considerar previamente cuantos serán realmente los aplicables según sus propias necesidades.

CAPITULO 4

BASES DE DATOS Y SISTEMA GESTOR DE BASE DE DATOS

4. BASE DE DATOS Y SISTEMA GESTOR DE BD

Definimos una Base de Datos como una colección de datos relacionados y el Sistema Gestor de Bases de Datos (SGBD) como el software que gestiona y controla el acceso a la base de datos. Una aplicación de bases de datos es un programa que interactúa con ésta en algún punto de su ejecución. Podemos considerar sistema de base de datos al conjunto de programas de aplicación que interactúan con la base de datos.

Las bases de datos proporcionan la infraestructura requerida para los sistemas de apoyo a la toma de decisiones y para los sistemas de información estratégicos, ya que éstos explotan la información contenida en las bases de datos de la organización para apoyar el proceso de toma de decisiones o para lograr ventajas competitivas. Por este motivo es importante conocer la forma que están estructuradas las bases de datos y su manejo.

Uno de los objetivos principales de un sistema de bases de datos consiste en proporcionar a los usuarios una visión abstracta de los datos, ocultando ciertos detalles acerca de cómo se almacenan y manipulan. Debemos tener en cuenta que se trata de un recurso compartido y cada usuario puede requerir una vista diferente de la información contenida en la base de datos.

El Sistema de Gestión de Bases de Datos (SGBD) constituye hoy en día la parte fundamental en los sistemas de información y ha provocado un cambio en las organizaciones, permitiéndoles una gestión más óptima de la información, así como un valor añadido a la empresa.

4.1. HISTORIA

Es importante hacer una referencia a la historia de las bases de datos, porque vamos a ver como IBM fue uno de los propulsores de la existencia de las bases de datos. De hecho IBM es la compañía que desarrolla y mantiene el producto del cual trata este proyecto, entornos Informix.

No se puede indicar una fecha concreta como inicio de la existencia de las bases de datos, pero se aduce que los sistemas de gestión de bases de datos tienen sus raíces en el proyecto lunar Apollo de la década de 1960, ya que era necesario gestionar y controlar la gran cantidad de información que el proyecto iba a generar.

North American Aviation, el contratista principal del proyecto, desarrolló un sistema de software denominado GUAM (*Generalized Update Acces Method*: método generalizado de acceso y actualización). A mediados de la década de 1960, IBM unió sus fuerzas a NAA para desarrollar GUAM, lo que dio como resultado lo que ahora se conoce con el nombre de IMS (*Information Management System*: sistema de gestión de la información).

A mediados de la década de los años sesenta, otro desarrollo significativo fue la aparición de IDS (*Integrated Data Store*, almacenamiento integrado de datos) de General Electric. Este desarrollo condujo a un tipo de sistema de base de datos denominado SGBD en red, que resuelven la necesidad de presentar relaciones de datos más complejas. También supuso la intención de establecer un estándar de base de datos. Para ayudar a establecer dicho estándar, la conferencia CODASYL (*Conference on Data System Languages*, conferencia sobre lenguajes de sistemas de datos) en la que participaron representantes del gobierno americano y del mundo empresarial. Se obtuvo un informe que no fue adoptado formalmente por ANSI (*American National Standards Institute*, Instituto nacional de estándares de los Estados Unidos), pero que sirvió como base para desarrollar diversos sistemas como CODASYL o DBTG, constituyendo la primera generación de sistemas de gestión de bases de datos.

En 1970, E. F. Codd, del laboratorio IBM Research Laboratory elaboró un artículo sobre el modelo de datos relacional, donde se indicaban las desventajas de las técnicas anteriores. Su idea fundamental era el uso de “relaciones”, además de no tener relevancia el lugar y forma en que se almacena los datos, a diferencia de otros modelos donde si era importante. Los primeros productos comerciales con este modelo aparecen a finales de la década de los años setenta y principios de los ochenta. Algunos de estos productos SGBD relacionales implementados con carácter comercial, fueron por ejemplo DB2 y SQL/DS y Oracle.

En 1976, Peter Chen presentó el modelo entidad-relación, que hoy en día constituye una técnica ampliamente aceptada para el diseño de base de datos. El modelo ER ha sido la base para diversas metodologías sobre análisis y diseño de sistemas, herramientas de ingeniería de software asistida por computador (CASE) y repositorios de sistemas. En este sentido, el Modelo ER ha sido utilizado por el IBM Repository Manager/MVS y por el DEC CDD/Plus.

Debido a la creciente complejidad de las aplicaciones de bases de datos, aparecen dos nuevos sistemas: los Sistema Gestor de Base de Datos orientados a objetos (OODBMS) y los Sistemas Gestor de Base de Datos objeto-relacionales (ORDBMS).

4.2. LAS BASES DE DATOS

Definimos base de datos como una colección compartida de datos lógicamente relacionados, junto con una descripción de estos datos, que están diseñados para satisfacer las necesidades de información de una organización. Se trata de un recurso compartido.

Según Henry F. Korth autor del libro “Fundamentos de Bases de Datos” se define una base de datos como una serie de datos organizados y relacionados entre sí, y un conjunto de programas que permitan a los usuarios acceder y modificar esa información.

La descripción de los datos se denomina catálogo del sistema o diccionario de datos o metadatos, es decir, información acerca de los datos. Así se consigue la independencia entre los programas y los datos.

Como venimos indicando a lo largo de este proyecto, los datos constituyen un valioso recurso que debe ser estrictamente controlado y gestionado, por ello ha de garantizarse su seguridad y confidencialidad.

4.2.1. Diseño y creación de Bases de Datos

Es importante la utilización de metodologías de diseño de datos. El equipo de analistas y diseñadores deben hacer uso de una misma metodología de diseño, la cual debe estar en concordancia con la arquitectura de Base de Datos elegida. A partir de distintos factores como el número de usuarios que accederá a la información, la necesidad de compartir información y las estimaciones de volumen se deberá elegir el SGBD más adecuado a las necesidades de la empresa o proyecto en cuestión.

En la fase de diseño de datos, deben definirse los procedimientos de seguridad, confidencialidad e integridad que se aplicarán a los datos y éstos deben ser implementados en la fase de creación. A continuación se exponen una relación de procedimientos a llevar a cabo:

- Procedimientos para las copias de seguridad y restauración de los datos en casos de caídas del sistema o corrupción de los archivos.

- Procedimientos para prohibir el acceso no autorizado a los datos, para ello deberán ser identificados.

- Procedimientos para restringir el acceso no autorizado a los datos. Debiendo identificar los distintos perfiles de usuario que accederán a los archivos de la aplicación y los subconjuntos de información que podrán modificar o consultar. Para ello existen dos posibles enfoques:

  - Confidencialidad basada en roles: consiste en la definición de los perfiles de usuario y las acciones que les son permitidas (lectura, actualización, alta, borrado, creación / eliminación de tablas o modificación de la estructura de las tablas).

  - Confidencialidad basada en vistas: consiste en la definición de vistas parciales de la base de datos, asignándolas a determinados perfiles de usuario.

- Procedimientos para mantener la consistencia y corrección de la información en todo momento.

La no implementación de mecanismos de control, de seguridad, pistas de auditoría y otros aspectos que pueda incluirse en esta fase producen un mayor coste cuando quieren incorporarse una vez concluía la implementación de la bases de datos y la programación de las aplicaciones.

El auditor debe, por tanto, en primer lugar, analizar la metodología de diseño con el fin de determinar si es o no aceptable, y luego comprobar su correcta utilización. Como mínimo una metodología de diseño de Base de Datos deberá contemplar dos fases de diseño: lógico y físico, aunque la mayoría de las empleadas en la actualidad contemplan tres fases; además de las dos anteriores, una fase previa de diseño conceptual tiene que ser abordada en este momento del ciclo de vida de la base de datos.

En esta fase de diseño se llevarán a cabo los diseños lógicos y físicos de la base de datos, por lo que el auditor tendrá que examinar si estos diseños se han realizado correctamente; determinando si la definición de los datos contemplan además de su estructura, las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y las cuestiones relativas a la seguridad. El auditor tendrá que tomar una muestra de ciertos elementos (tablas, vistas, índices) y comprobar que su definición es completa, que ha sido aprobado por el usuario y que el administrador de la base de datos participó en su establecimiento.

Es importante que la dirección del departamento de informática, los usuarios e incluso, en algunas ocasiones, la alta dirección, aprueben el diseño de los datos, al igual que el de las aplicaciones.

La tendencia de los SGBD es la implementación de los procedimientos, expuestos con anterioridad, en el esquema físico de datos, lo cual incide en un aumento de la fiabilidad y en una disminución del coste de programación, ya que el propio gestor de la base de datos controla la obligatoriedad de los atributos y las reglas de integridad referencial.

4.2.2. Explotación de la Base de Datos

Es necesaria la realización de inspecciones periódicas que comprueben que los procedimientos de seguridad, confidencialidad e integridad de los datos funcionan correctamente. Para ello, existen diversos métodos y utilidades, entre estos se encuentran los archivos de acceso y actividad (logs). Los Sistemas Gestores de Base de Datos actuales suelen tener archivos de auditoría, donde se registran las acciones realizadas sobre la base de datos, indicando los objetos modificados, fecha, usuario que lo ha llevado a cabo, resumiendo, los datos más relevantes para poder llevar a cabo seguimiento de las acciones efectuadas.

Dado que la base de datos es un elemento cambiante, es necesario realizar periódicamente un mantenimiento, ya que su estructura, volumen, comportamiento y apariencia se modifican con el paso de tiempo y generan nuevas necesidades. Así mismo deben revisarse los roles de los usuarios para adecuarlos a los posibles cambios que se vayan produciendo.

Es muy importante, también, el mantenimiento del diccionario de datos, ya que es el elemento que nos ayuda a determinar cuales son los mecanismos del sistema, así como proporcionarnos la definición y dónde son utilizados.

Los propios diccionarios se pueden auditar de manera análoga a las bases de datos (puesto que son bases de “metadatos”), la diferencia entre unos y otros, reside principalmente en que un fallo en una base de datos puede atentar contra la integridad de los datos y producir un mayor riesgo financiero, mientras que un fallo en un diccionario, suele llevar consigo una pérdida de integridad de los procesos, siendo más peligrosos los fallos en los diccionarios puesto que pueden introducir errores de forma repetitiva a lo largo del tiempo y son más difíciles de detectar.

Las diferentes etapas de vida de una base de datos, desde su diseño, creación, explotación, etc., aportan distintas funcionalidades.

COBIT dedica un apartado completo a detallar los objetivos de control para la gestión de datos, calificándolos en un conjunto de apartados.

- Procedimientos de preparación de datos

- Procedimiento de autorización de documentos fuente
- Recogida de datos de documento fuente
- Manejo de errores de documento fuente
- Retención de documento fuente
- Procedimiento de autorización de datos
- Verificación de exactitud, compleción y autorización.
- Manejo de errores de entrada de datos
- Integridad del procesamiento de datos
- Retención y manejo de salidas
- Distribución de salidas
- Reconciliación y balance de salidas
- Manejo de errores y revisión de salidas
- Medidas de seguridad para informes de salida
- Protección de información sensible
- Protección de información sensible dispuesto
- Gestión de almacenamiento
- Periodos de retención y términos de almacenamiento
- Sistema de gestión de biblioteca de medios
- Responsabilidades de gestión de la biblioteca de medios
- Copias de respaldo y recuperación
- Trabajos de copias de respaldo

- Almacenamiento de respaldo

El Auditor estudiará el rendimiento del sistema de BD, comprobando si se llevan a cabo las optimizaciones adecuadas que no sólo consisten en el rediseño físico o estricto de la BD, sino que también abarca ciertos parámetros del Sistema Operativo e incluso la forma en que acceden las transacciones a las Bases de Datos. Cabe recordar que "*la función del administrador de la base de datos debe ser el responsable de monitorizar el rendimiento y la integridad de los sistemas de BD*", - Moeller (1989).

A lo largo del ciclo de vida de la base de datos se deberán controlar la formación que precisan los usuarios informáticos (administrador, analista, programadores, etc) como los no informáticos, ya que la formación es una de las claves para minimizar el riesgo en la implantación de una base de datos. Ya que los usuarios poco formados constituyen uno de los peligros más importantes de un sistema. La formación deberá abarcar además del área de base de datos el control y la seguridad.

Es importante que la empresa tenga una política de calidad, cuyo principal objetivo debería consistir en asegurar la calidad. Aunque existen pocas medidas de calidad para una base de datos, no obstante hay ciertas técnicas bastantes difundidas que se pueden aplicar a una base de datos como es a teoría de la normalización.

4.2.3. Bases de Datos Orientadas a Objeto

Es importante realizar una breve referencia a este modelo, bastante reciente, implementado por la mayoría de las empresas dedicadas al mundo de las bases de datos.

El modelo de base de datos Orientado a Objetos ha surgido debido a las limitaciones existentes en el modelo relacional, como consecuencia de las mismas los investigadores las resolvieron con este nuevo modelo, almacenando en la base de datos los objetos completos (estado y comportamiento).

Las aplicaciones de bases de datos tradicionales consisten en tareas de procesamiento de datos, tales como la banca, seguros, ventas, gestión de recursos

humanos. Dichas aplicaciones presentan conceptualmente tipos de datos simples. Los elementos de datos básicos son registros bastante pequeños y cuyos campos son atómicos, es decir, no contienen estructuras adicionales.

Las BDOO ofrecen un mejor rendimiento de la máquina que las bases de datos relacionales, tanto para aplicaciones como para clases con estructuras complejas de datos. Está diseñada para ser eficaz, desde el punto de vista físico, de manera que pueda almacenar objetos complejos. De esta manera se evita el acceso a los datos, mediante los métodos almacenados en ella. Ofreciendo así una mayor seguridad al no permitir acceso a los datos. También hay que considerar, que al tratarse de recientes tecnologías, la inmadurez del mercado constituye una posible fuente de problemas, por ello es importante analizarlo antes de adoptar un producto basado en esta tecnología.

Una base de datos orientada a objetos es una base de datos que incorpora todos los conceptos importantes de la programación orientada a objetos:

- Encapsulación.- Ocultar datos del resto de datos.
- Herencia.- Reusabilidad del código
- Polimorfismo.- Sobrecarga de operadores o de métodos.

A finales de los años 80 aparecieron las primeras BDOO, considerada como una base de datos inteligente, que soporta el paradigma orientado a objetos, almacenando no solo datos sino también los métodos.

4.2.4. Ventajas de las Bases de Datos

Algunos autores, enumeran un conjunto de ventajas que aporta el uso de bases de datos, entre las cuales destacamos las siguientes:

- Globalización de la información, lo que permite a los diferentes usuarios considerar la información como un recurso corporativo que carece de propietarios específicos.
- Eliminación de información redundante.

- Eliminación de información inconsistente.
- Información compartida
- Mayor integridad de los datos
- Independencia de los datos y su tratamiento
- Incluir restricciones de seguridad en el acceso de los usuarios a los datos y operaciones sobre los mismos

Pero realmente son los SGBD, a través de sus utilidades, los que nos facilitan y ayudan a interactuar con la base de datos de una forma más sencilla y rápida, para la realización de tareas como son la definición de la base de datos, construcción, manipulación de los datos mediante la realización de consultas, actualizaciones y generación de informes, importar-exportar datos, reorganización de la información, control del rendimiento, seguridad y muchas otras tareas.

4.2.5. Problemas fundamentales de las Bases de Datos

En las bases de datos se plantean problemas de seguridad como la compartición de datos, acceso a estos, protección contra fallos o accesos no permitidos. El SGBD facilita mecanismos para prevenir los fallos, detectarlos y poder corregirlos.

Detallamos algunos aspectos fundamentales de la seguridad:

- Confidencialidad. No desvelar datos a usuarios no autorizados, también comprende la privacidad (protección de datos personales).
- Accesibilidad o disponibilidad. La información debe estar disponible, así como el acceso a los servicios.
- Integridad. - Permite asegurar que los datos no han sido falseado o modificados de forma indebida.

Existen dos tipos de mecanismos de seguridad contra el acceso no autorizado:

- Discrecionales, se usan para otorgar privilegios a los usuarios.
- Obligatorios, sirven para imponer seguridad de múltiples niveles, clasificando los datos de los usuarios en varias tipos de seguridad e implementando después la política de seguridad apropiada de la organización.

Además, se pueden crear cuentas de acceso a la base de datos para los distintos usuarios, las cuales se podrían agrupar según sus roles.

En una base de datos estadística no se debe permitir acceso a la información confidencial detallada sobre individuos específicos. En ocasiones es posible deducir ciertos hechos relativos a los individuos a partir de consultas, lo cual tampoco debe permitirse. Otra técnica de seguridad es el cifrado de datos, que consiste en codificar cierta información, dependiendo del grado de seguridad que necesite la información almacenada, se utiliza una clave de cifrado distinta para cada registro o una para todos.

A continuación se detallan posibles problemas que existen en las bases de datos, estos puntos son más sensibles de estudio en una auditoría. Podemos clasificarlos en varios grupos:

- La seguridad en las bases de datos, teniendo en cuenta no solo el contexto de la seguridad del propio Sistema Gestor de Base de Datos sino también la seguridad de su entorno.
- Aspectos de procesamiento y optimización del acceso a la información de la base datos, debido a la importancia de disponer de la información a tiempo.
- Todo sistemas de gestión de base de datos debe proporcionar las siguientes funciones que se detallan a continuación:
    - Gestión de transacciones
    - Control de concurrencia
    - Recuperación

Estas funciones tratan de garantizar que la base de datos sea viable y permanezca en estado coherente cuando múltiples usuarios acceden a ella.

Pero también hay que tener en cuenta otra serie de aspectos que muestran las desventajas que supone tener un entorno de base de datos:

- El coste elevado que supone la actualización del hardware y software.
- Coste económico de tener un Administrador de base de datos.
- El mal diseño de la Base de Datos puede originar problemas en un futuro.
- La falta de formación de los usuarios puede generar problemas.
- La falta de manual de sistema entorpece la solución de los problemas.
- La inexistencia o mala política de seguridad.

4.2.6. Evaluación de la Seguridad

La seguridad hace referencia a la protección de los datos contra una revelación, alteración o destrucción no autorizada. En otras palabras, seguridad implica garantizar que los usuarios están autorizados a realizar la acción que tratan de llevar a cabo.

Los problemas de seguridad tienen muchos aspectos, entre los que cabe destacar:

- Aspectos legales, sociales y éticos
- Controles físicos
- Cuestiones de política interna
- Problemas de operación
- Controles de equipo
- Seguridad del sistema operativo
- Materias de relevancia específica para el sistema de base de datos

Los objetivos susceptibles de la aplicación de un mecanismo de seguridad pueden ser desde bases de datos completas hasta valores específicos en una fila y columna concreta de una tabla. Los mecanismos de seguridad deben garantizar que los usuarios sólo pueden realizar aquellas operaciones para las que están autorizados sobre ciertos objetos particulares. Por otro lado, hay que tener en cuenta que distintos usuarios pueden tener diferentes tipos de autorizaciones sobre los mismos objetos.

Las medidas de seguridad de la información las toma el administrador de la base de datos, para lo que utiliza herramientas proporcionadas por el lenguaje de operación de base de datos.

En el caso de SQL (Structured Query Language), el sistema cuenta con dos mecanismos diferentes implicados en el mantenimiento de la seguridad: el sistema de gestión de vistas, y el subsistema de autorización mediante el cual los usuarios con derechos específicos pueden conocer de manera selectiva y dinámica esos derechos de otros usuarios y después revocarlos, si lo desean.

Los aspectos relativos al control de la Seguridad de la Información tienen varias líneas básicas en la auditoría de sistema de información. Aquellos aspectos relativos a la confidencialidad y seguridad, que no implican sólo la protección material o los soportes de información, sino también el control de acceso a la propia información. Así como aquellos aspectos jurídicos relativos a la seguridad de la información que tratan de analizar la adecuada aplicación del sistema de información en la empresa en cuanto al derecho a la intimidad y el derecho a la información.

Concretando sobre el aspecto de seguridad en una base de datos lo podemos definir como los mecanismos de protección que deben poseer para hacer frente a accesos no autorizados, ya sean intencionados o no. Los Sistemas Gestores de Bases de Datos son uno de los componentes principales encargados de la misma.

Esta necesidad de seguridad, aunque a veces no se ha prestado la suficiente atención en el pasado, es cada vez mejor comprendida por las organizaciones. La razón de este cambio de mentalidad es la gran cantidad de información que se almacenan en los sistemas informáticos y el reconocimiento de que cualquier pérdida o falta de disponibilidad de estos datos puede llegar a ser desastrosa.

Las organizaciones deben tratar de reducir los riesgos producidos por situaciones de robo, fraude, pérdida de confidencialidad, privacidad, integridad y disponibilidad. Aunque algunos riesgos no son resultado de cambios en la base de datos o en el sistema informático sino ataques externos al sistema.

Cuando hablamos de confidencialidad y privacidad parecen términos similares pero tratan sobre aspectos distintos. La confidencialidad es la necesidad de mantener en secreto ciertos datos, usualmente sólo aquellos que son críticos para la organización. Mientras que la privacidad hace referencia a la necesidad de proteger los datos acerca de las personas. Las implicaciones por la violación de la confidencialidad y privacidad originan distintos problemas. Una pérdida de confidencialidad, por ejemplo, puede originar una reducción de competitividad de la organización mientras que la pérdida de privacidad podría implicar que alguien iniciara acciones legales contra la organización que no ha sabido custodiar correctamente sus datos.

La pérdida de integridad de los datos provoca la aparición de datos inválidos o corrompidos, pudiendo afectar seriamente a la organización. La pérdida de disponibilidad implica que los datos, el sistema o ambos dejen de estar accesible pudiendo afectar seriamente a los resultados financieros.

Todos estos aspectos que pueden afectar a un organismo requieren de unas medidas de seguridad y planes de contingencia. Siendo éstos puntos muy importantes en el estudio a realizar por una auditoría.

Los datos constituyen un valioso recurso que debe ser estrictamente controlado y gestionado. Una parte de los datos corporativos, o todos ellos, pueden tener una importancia estratégica para la organización y debe, por tanto, garantizarse su seguridad y confidencialidad.

Como ya hemos detallado con anterioridad, los SGBD deben garantizar la seguridad de la base de datos, entre otros aspectos, y proporcionar mecanismos para verificar que sólo usuarios autorizados accedan a la información de la base de datos.

4.2.6.1. Seguridad Física y Seguridad Lógica

La seguridad no sólo se debe aplicar a las bases de datos, también puede afectar a otras partes del entorno de la organización. No obstante, nos vamos a centrar en la seguridad de las bases de datos y estudiar las medidas de seguridad proporcionadas por el SGBD Informix.

Podemos hacer la siguiente clasificación: seguridad física y seguridad lógica:

- La seguridad física se ocupa del hardware y de los soportes de datos, también de toda la estructura que forma parte de las instalaciones que alberga el hardware.

- La seguridad lógica se refiere al cuidado del software y la protección de datos, programas y demás procesos, así como las formas de acceso a la información por parte de los usuarios.

En los últimos años se ha observado un incremento en cuanto a los delitos informáticos y las agresiones a centros e instalaciones informáticas, dando lugar a que se tomen las medidas correspondientes con el fin de mejorar la seguridad lógica y el uso de medios criptográficos bastante desarrollados.

La seguridad debe considerar los siguientes aspectos:

- Definir la política de seguridad de la empresa.

- La seguridad física, como ciertas catástrofes: incendios, terremotos, etc.

- Ejecutar políticas de seguridad del personal.

- Seguridad de los equipos, de los sistemas de redes y terminales y de todos los elementos en general.

- Establecer planes de contingencia ante situaciones de desastre.

- Definir el rol que cumplirán los auditores internos y los externos.

4.2.6.2. Amenazas

Amenaza es cualquier situación o suceso, intencionado o accidental, que pueda afectar adversamente a un sistema y, consecuentemente, a la organización. La amenaza puede considerarse como una ruptura potencial de seguridad, que si tiene éxito producirá un cierto impacto. El grado de impacto dependerá de los planes de contingencia y contramedidas que posea la organización.

La organización necesita identificar los tipos de amenaza a los que tiene que hacer frente y establecer los planes apropiados, teniendo siempre presente el coste de su implementación.

En la siguiente tabla se presenta un resumen de las potenciales amenazas a las que se enfrentan los sistemas informáticos. Cabe destacar que las contramedidas que pueden aplicarse a los sistemas informáticos van desde controles físicos hasta procedimientos administrativos. También es necesario tener en cuenta que, generalmente, la seguridad de un SGBD depende en buena medida del sistema operativo, debido a lo estrechamente que están asociados.

Amenaza	Robo y Fraude	Perdida de confidencialidad	Pérdida de privacidad	Pérdida de integridad	Pérdida de disponibilidad
Utilizar los medios de acceso	✓	✓	✓		
Modificación o copia no autorizada de los datos	✓			✓	
Alteración de un programa	✓			✓	✓
Políticas y procedimientos inadecuados que permiten que se produzca la consulta de datos tanto confidenciales como no confidenciales	✓	✓	✓		

Amenaza	Robo y Fraude	Perdida de confidencialidad	Pérdida de privacidad	Pérdida de integridad	Pérdida de disponibilidad
Entrada ilegal por parte de un hacker	✓	✓	✓		
Creación de “puertas traseras” en un sistema	✓	✓	✓		
Robo de datos, programas y equipos	✓	✓	✓		✓
Fallos de los mecanismos de seguridad, proporcionando un acceso superior al normal		✓	✓	✓	
Formación inadecuada del personal		✓	✓	✓	✓
Visualización y divulgación de datos no autorizados	✓	✓	✓		
Corrupción de los datos debidos a cortes de suministros o sobretensiones				✓	✓
Introducción de virus				✓	✓

4.2.6.3. Controles de Seguridad

Es necesaria la existencia de una serie de controles que tengan como finalidad la seguridad de los sistemas de base de datos. A continuación vamos a enumerar y explicar de una forma más amplia información sobre cada uno de ellos.

- Autorización
- Controles de acceso

- Vistas
- Copias de seguridad y recuperación
- Integridad
- Cifrado
- Tecnología RAID

- **Autorización**

Definimos autorización como la concesión de un derecho o privilegio que permite a una persona acceder legítimamente a un sistema o a un objeto del sistema. Además de controlar el acceso también se puede regular que acciones está autorizado a llevar a cabo dentro del sistema.

El proceso de autorización implica la autenticación de los sujetos que soliciten acceso a los objetos, donde la palabra 'sujeto' representa tanto a un usuario como a un programa, mientras que 'objeto' representa una tabla de la base de datos, una vista, un procedimiento, un disparador o cualquier otro objeto que pueda crearse en el sistema.

- **Controles de accesos**

Los controles de accesos de un sistema de bases de datos se basan en la concesión y revocación de privilegios. Un privilegio permite a un usuario crear o acceder a algún objeto de base de datos, como por ejemplo una relación, vista ó índice, o ejecutar ciertas utilidades del SGBD. Los privilegios se conceden a usuarios para que puedan llevar a cabo las tareas requeridas por su trabajo. Una concesión excesiva de privilegios innecesarios puede poner en cuestión los mecanismos de seguridad. Sólo debe concederse un privilegio a un usuario si dicho usuario no puede llevar a cabo su labor sin disponer de dicho privilegio. El SGBD llevará el control de concesión de privilegios a los usuarios así como sus revocaciones, para garantizar en cada

momento que los usuarios disponen de los privilegios necesarios para acceder a los distintos objetos.

La mayoría de los SGBD comerciales proporciona una técnica para gestionar los privilegios que emplea un mecanismo de SQL conocido con el nombre de *control de acceso discrecional (DAC).* El estándar SQL lo soporta mediante los comandos GRANT y REVOKE. GRANT proporciona privilegios a los usuarios, mientras que REVOKE los elimina. Sin embargo, tiene ciertas debilidades, por lo que son necesarios mecanismos de seguridad adicionales para eliminar tales amenazas.

Existen unos mecanismos de "control de acceso obligatorio", soportados por algunos SGBD que se basan en políticas de nivel de sistema que no pueden ser modificadas por los usuarios individuales. A cada objeto de la base de datos se le asigna una clase de seguridad y a cada usuario se le asigna un nivel de autorización para cada clase de seguridad, imponiéndose una serie de reglas a la lectura y escritura de objetos de base de datos por parte de los usuarios. El SGBD determina si un usuario específico puede leer o escribir un objeto determinado basándose en una serie de reglas relacionadas con la clase de seguridad del objeto y el nivel de seguridad del usuario. Estas reglas tratan de garantizar que los datos confidenciales nunca puedan ser pasados a otro usuario que no disponga del nivel de seguridad adecuado. El estándar SQL no incluye soporte para este mecanismo.

- **Vistas**

Una vista es una relación virtual que no existe en realidad en la base de datos, sino que se genera en el momento en que un usuario concreto efectúa una solicitud.

Con las vistas se obtiene un sistema de seguridad potente y flexible, al ocultar partes de la base de datos a ciertos usuarios. El usuario no es consciente de la existencia de algún otro atributo o fila que no se presente en la vista. Así con la vista se consigue mayor restricción que con la concesión de privilegios al usuario.

- **Copia de seguridad y recuperación**

Realizar una copia de seguridad o copia de respaldo se refiere a la copia de los datos de tal forma que estas copias adicionales puedan restaurar un sistema después de una pérdida de información.

Un SGBD debe proporcionar facilidades de copia de seguridad para ayudar a la recuperación de la base de datos en caso de que se produzca un fallo. Es aconsejable realizar copias de seguridad de base de datos y del archivo de registro a intervalos regulares y garantizar que las copias se conserven en una ubicación segura. En caso de que se produzca un fallo que haga que la base de datos deje de ser utilizable, podrán usarse la copia de seguridad y los detalles capturados en el archivo de registro para restaurar la base de datos hasta el estado coherente más reciente.

El archivo de registro (o diario) es gestionado por el SGBD y almacena todos los cambios realizados en la base de datos, nos da información sobre el estado actual de las transacciones y de los cambios efectuados en la base de datos. Como ya hemos indicado con anterioridad, es utilizado para realizar la restauración de la base de datos.

- **Integridad**

El objetivo de la integridad es proteger la base de datos contra operaciones que introduzcan inconsistencias en los datos. Cuando los contenidos de una base de datos se modifican con sentencias INSERT, DELETE o UPDATE, la integridad de los datos almacenados puede perderse de muchas maneras diferentes.

Se puede clasificar en integridad semántica y en integridad operacional. Cada una de ellas puede producirse cuando concurren unas circunstancias o se produce un estado de la base de datos no normal.

La integridad semántica se da cuando existan operaciones que pueden violar restricciones definidas al diseñar la base de datos, como pueden ser restricciones sobre los dominios o sobre los atributos. Estas reglas se almacenan en el diccionario de datos. Es el SGBD quien debe comprobar la coherencia de las reglas que se

definan, controlar las distintas transacciones y detectar las violaciones de integridad, y en el caso de producirse, ejecutar las acciones pertinentes.

La integridad operacional se dar en sistemas multiusuarios donde es imprescindible un mecanismo de control de concurrencia para conservar la integridad de la base datos. Técnicas de control de concurrencia más habituales son: bloqueo, marcas de tiempo, transacciones anidadas y muchas otras más.

- **Cifrado**

En un sistema de base de datos que almacena datos particulares y confidenciales puede que sea necesario codificarlos como precaución frente a posibles amenazas externas. Algunos SGBD proporcionan esta funcionalidad. Con el cifrado se produce una cierta degradación del rendimiento debido a los tiempos necesarios para la decodificación. Con el cifrado también se protegen los datos transmitidos a través de líneas de comunicación.

- **RAID (Redundant Array of Independent Disk)**

El hardware en el que el SGBD se ejecute debe ser tolerante a fallos, lo que quiere decir que el SGBD debe poder continuar operando incluso aunque uno de los componentes de hardware, falle. Consiste en disponer de componente redundantes que pueden integrase de forma transparente en el sistema cada vez que se produzca un fallo del componente. Los principales componentes de hardware que deben ser tolerante a fallos son los discos duros, los controladores de disco, el procesador, las fuentes de alimentación y los ventiladores de refrigeración. Las unidades de disco son los componentes más vulnerables, presentando un tiempo más corto entre fallos que cualquier otro componente del hardware.

Con respecto al sistema de almacenamiento con múltiples discos duros entre los que se distribuye o replican los datos se obtiene una mayor integridad y tolerancia a fallos, en definitiva un mejor rendimiento y capacidad.

Existen diferentes niveles de RAID, donde cada nivel de RAID ofrece una combinación específica de tolerancia a fallos (redundancia), rendimiento y coste, diseñadas para satisfacer las diferentes necesidades de almacenamiento. La mayoría de los niveles RAID pueden satisfacer de manera efectiva sólo uno o dos de estos criterios. Cada uno es apropiado para determinadas aplicaciones y entorno informáticos. Oficialmente existen siete niveles (0-6), aunque existen posibles combinaciones de estos niveles.

En función de las necesidades del organismo, en lo que respecta a factores como seguridad, velocidad, capacidad, se implementa un nivel o la combinación de varios.

4.3. ESTRUCTURA DE LOS SISTEMAS DE BASE DE DATOS

En 1971 se elaboró una de las primeras propuestas de terminología estándar y de arquitectura general para los sistemas de bases de datos. Esta propuesta fue elaborada por DBTG (Data Base Task Group, grupo de trabajo en bases de datos) nombrado por la conferencia CODASYL, dispone de un enfoque en dos niveles: una vista del sistema denominada esquema y una serie de vistas de usuario denominadas subesquemas.

El comité SPARC (Standard Planning and Requirements Committee, comité de requisitos y planificación de estándares) de ANSI (American National Standars Institute) realizó una propuesta basada en tres niveles, en la que se añadía un catálogo de sistema.

Estas propuestas reflejaban las publicadas por determinadas organizaciones de usuarios de IBM años antes, con el fin de aislar los programas de los problemas de representación subyacentes. Aunque el modelo ANSI-SPARC no llegó a convertirse en un estándar, continúa proporcionando una base para comprender parte de la funcionalidad de un SGBD.

Podemos definir que el objetivo de los tres niveles es el de separar la vista que cada usuario tiene de la base de datos de la forma en que se representan y almacenan los datos físicamente. Es decir, la interacción del usuario con la base de datos debería ser independiente de las consideraciones de almacenamiento. Además las actuaciones

del Administrador de la Base de Datos (DBA) en lo referente a cambios en las estructuras de almacenamiento no deben afectar a las vistas de los usuarios.

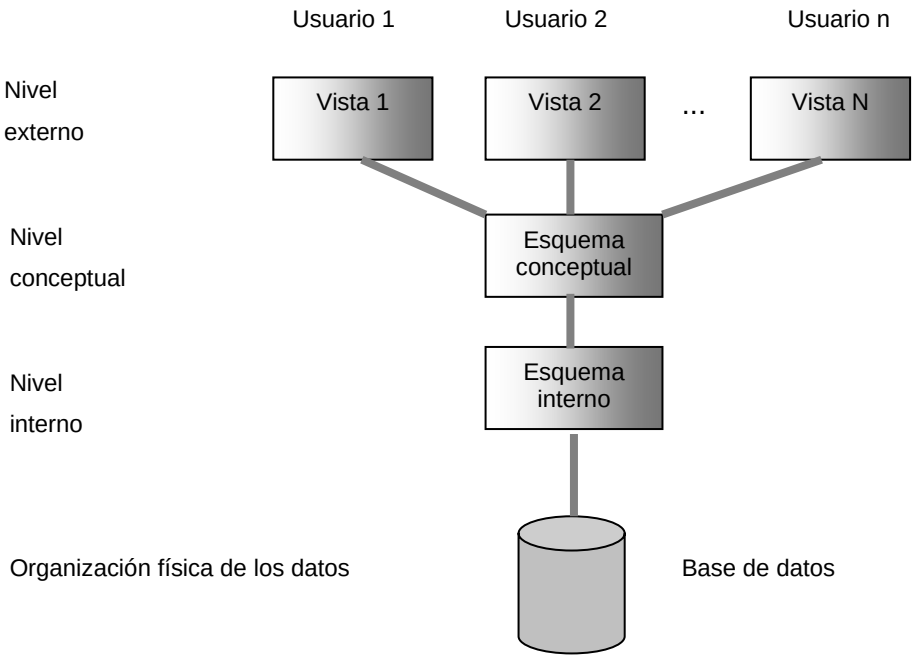


Ilustración 5. Arquitectura en tres niveles

En la figura se muestra una arquitectura en tres niveles, el nivel externo corresponde a la forma que los usuarios perciben los datos, el nivel interno es como lo perciben el SGBD y el sistema operativo, y el nivel conceptual proporciona tanto la correspondencia como la necesaria independencia entre los niveles externos e internos. Es además, donde se describen qué datos están almacenados en la base de datos y las relaciones existentes entre los mismos, en otras palabras es como lo ve el Administrador de la Base de Datos.

4.4. SISTEMA GESTOR DE BASE DE DATOS

El Sistema Gestor de Bases de Datos (SGBD) es el software que gestiona y controla el acceso a la base de datos, es decir, permite a los usuarios definir, crear, mantener y controlar el acceso, copias de seguridad, ficheros de logs, etc. Además ofrece información para optimizar el sistema, llegando a ser en determinadas ocasiones

verdaderos sistemas expertos que proporcionan la estructura óptima de la base de datos y de cientos de parámetros del SGBD y el Sistema Operativo. Podemos decir que uno de los objetivos más importantes del SGBD es proporcionar a los usuarios una visión abstracta de los datos.

Un sistema gestor de base de datos (SGBD) consiste en una colección de datos interrelacionados y un conjunto de programas para acceder a dichos datos. La colección de datos, normalmente denominada base de datos, contiene información relevante para una empresa. El objetivo principal de un SGBD es proporcionar una forma de almacenar y recuperar la información de una base de datos de manera que sea tanto práctica como eficiente.

En cuanto a las funciones de auditoría que ofrece el propio sistema, prácticamente todos los productos del mercado permiten registrar ciertas operaciones realizadas sobre la base de datos en un fichero (o en conjunto de tablas) de pistas de auditoría (audit trail). El propio Modelo de Referencia de Gestión de Datos, ISO (1993), considera las pistas de auditoría como un elemento esencial de un SGBD, señalando que “el requisito para la auditoría es que la causa y el efecto de todos los cambios de la base de datos sean verificables”.

El auditor deberá revisar, por tanto, la utilización de todas las herramientas que ofrece el propio SGBD y las políticas y procedimientos que sobre su utilización haya definido el administrador, para valorar si son suficientes o si deben ser mejorados.

Los Sistemas de bases de datos se diseñan para gestionar grandes cantidades de información. La gestión de los datos implica tanto la definición de estructuras para almacenar información como la provisión de mecanismos para su manipulación. Además los sistemas de bases de datos deben garantizar la fiabilidad de la información almacenada, a pesar de las caídas del sistema o de los intentos de accesos no autorizados.

El SGBD interactúa con los programas de aplicación del usuario y con la base de datos. Normalmente proporcionando la siguiente funcionalidad:

- Permite a los usuarios definir la base de datos, mediante *un lenguaje de definición de datos*, donde se especifican las estructuras y tipos de datos y las

restricciones aplicables a la información que hay que almacenar en la base de datos.

- Permite a los usuarios insertar, actualizar, borrar y extraer datos de la base de datos, mediante un lenguaje de manipulación de datos. El lenguaje SQL (Structured Query Language, lenguaje estructurado de consulta) que ahora es el estándar de facto para los SGBD relacionales.

- Acceso controlado a la base de datos de manera que pueda proporcionar:

  - Un sistema de seguridad, para evitar accesos no autorizados.

  - Un sistema de integridad que mantiene coherencia de los datos almacenados.

  - Un sistema de control de concurrencia que permite el acceso compartido a la base de datos.

  - Un sistema de control de recuperación que restaura la base de datos a un estado previo coherente después de un fallo e hardware o software.

Existe una funcionalidad de los SGBD que podríamos denominar mecanismo de vistas que permite que cada usuario tengo una visión de la base de datos, así sólo ve y tiene acceso a aquella información que necesita. Podemos decir que reducen la complejidad al permitir que se vean los datos en la forma que se desean. También las vistas ofrecen otras series de ventajas:

- Con las vistas se consigue cierto nivel de seguridad, ya que se puede no mostrar ciertos datos a usuarios que no los deban ver.

- Con las vista se permite personalizar la apariencia de la bases de datos.

- Se puede presentar una imagen coherente y estática de la estructura de la base de datos. Si se añaden o modifican campos que no son utilizados en la vista, éstas no se verán afectadas y se conseguirá una independencia entre programas y datos.

El programa de aplicación es el programa que interactúa con la base de datos emitiendo solicitudes dirigidas al SGBD.

En el siguiente esquema, se observa como se integran los elementos de un sistema de base de datos

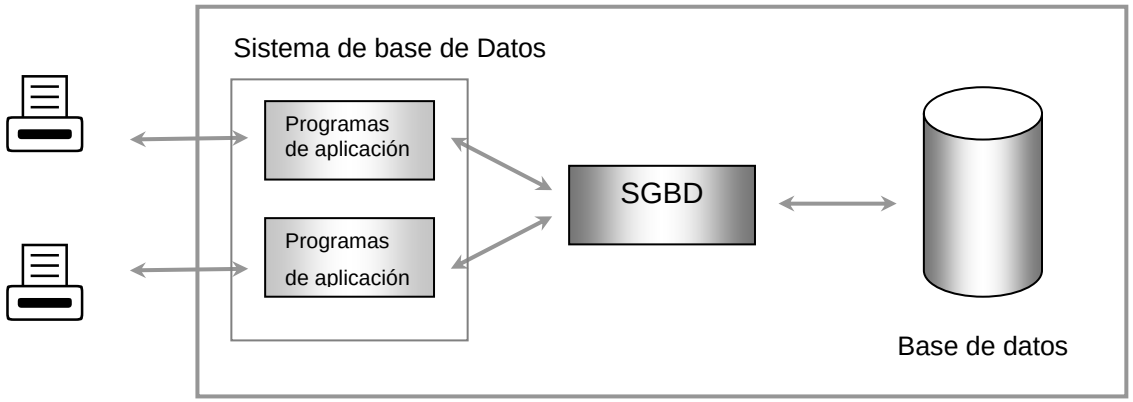


Ilustración 6. Elementos de un Sistema de Base de Datos

La anterior explicación es de carácter general, el nivel real de funcionalidad ofrecido por un SGBD difiere entre unos productos y otros. Los SGBD están continuamente evolucionando y expandiéndose para adaptarse a las nuevas necesidades de los usuarios, como son los nuevos tipos de información que es necesaria almacenar, imágenes, video, sonido, etc.

4.4.1. Ventajas y Desventajas

Podemos indicar las ventajas y desventajas que presentan los Sistemas Gestor de Bases de Datos y con ello observamos la importancia del mismo y lo que aporta al sistema de información de la organización:

Sistema Gestor de Base de Datos	
Ventajas	• Control de la redundancia de datos • Coherencia de los datos • Más información a partir de la misma cantidad de información • Compartición de datos • Mayor integridad de los datos • Mayor seguridad • Imposición de estándares, por ejemplo: formato de datos, convenios definición, etc, • Reducción de costes por tener una fuente de datos centralizada • Mejor accesibilidad a los datos y mayor capacidad de respuesta • Productividad mejorada • Mantenimiento mas sencillo debido a la independencia de los datos • Mayor nivel de concurrencia • Servicios mejorados de copia de seguridad y recuperación
Desventajas	• Complejidad • Tamaño • Coste del SGBD • Costes de hardware adicional • Costes de conversión • Mayor impacto de los fallos

4.4.2. Funciones de un SGBD

Codd, informático que definió las tres Formas Normales que se aplican para la normalización de sistemas de bases de datos, en 1982 enumeró una serie de funciones y servicios que debe proporcionar un SGBD, son los siguientes:

- Almacenamiento, extracción y actualización de datos
- Un catálogo accesible por el usuario
- Soporte para transacciones
- Servicios de control de concurrencia
- Herramientas y mecanismos para la planificación y realización de copias de seguridad
- Servicios de recuperación
- Servicios de autorización
- Soporte para la tramitación de datos
- Servicios de integridad

Almacenamiento, extracción y actualización de datos

Un SGBD debe proporcionar a los usuarios la capacidad de almacenar, extraer y actualizar los datos de la base de datos. Con ello se ocultan los detalles internos de implementación física a los usuarios.

Catálogo

Un SGBD debe proporcionar un catálogo donde se almacenen las descripciones de los elementos de datos. Podemos definir “catálogo de sistema” o “diccionario de datos” como un repositorio de información que describe los datos contenidos en la base de

datos. Cada SGBD aporta una información y una forma de trabajar con dicha información. El catálogo, normalmente almacena los siguientes datos:

- Los nombres, tipos y tamaños de los elementos de datos.
- Los nombres de las relaciones.
- Los nombres de los usuarios autorizados que tienen acceso a los datos
- Los elementos de datos a los que cada usuario puede acceder y los tipos de acceso permitidos.
- Los esquemas externos, conceptuales e internos y las correspondencias entre los distintos esquemas.
- Las estadísticas de uso, como las frecuencias de transacciones y el número de accesos realizados a los distintos objetos de la base de datos.

El catálogo del sistema es uno de los componentes fundamentales de un SGBD, la información contenida es utilizada por las aplicaciones, proporcionando una serie de ventajas:

- Se puede recopilar y almacenar de forma centralizada la información sobre los datos.
- Se define el significado de los datos.
- Se puede identificar a los usuarios que acceden a los datos.
- Es más fácil identificar la información redundante y las incoherencias, al estar los datos centralizados.
- Puede mantenerse un registro de cambios efectuados en la base de datos.
- Puede determinarse el impacto de un cambio antes de implementarlo, debido a que el catálogo del sistema almacena información de cada elemento de datos, de sus relaciones y de sus usuarios.

- Pueden establecerse mecanismos de seguridad.
- Puede garantizarse la integridad.
- Puede proporcionar información de auditoría.

Soporte de transacciones

Un SGBD debe proporcionar un mecanismo que garantice que se lleven a cabo todas las actualizaciones correspondientes a una determinada transacción, o que no se lleve a cabo ninguno. Ésta funcionalidad es muy importante, porque permite que tras una modificación en bloque de datos relacionados, la base de datos ante un posible fallo no quede en un posible estado incoherente.

Servicio de control de concurrencia

Un SGBD debe proporcionar un mecanismo para garantizar que la base de datos se actualice correctamente cuando haya múltiples usuarios actualizando de manera concurrente la base de datos.11111111

Servicios de recuperación

Un SGBD debe proporcionar un mecanismo para garantizar que sólo los usuarios autorizados puedan acceder a la base de datos. La seguridad es la protección de la base de datos frente a accesos no autorizados, ya sean intencionados o accidentales.

Soporte para la tramitación de datos

Un SGBD debe poder integrarse con un software de comunicación. Debido a que la mayoría de los usuarios acceden a la base de datos desde estaciones de trabajo, éstas pueden estar comunicadas directamente a la máquina donde se ejecuta el SGBD o a través de una red, porque estén situadas en ubicaciones remotas. El SGBD recibe peticiones que son gestionadas por un DCM (Data Communication Manager, gestor de comunicaciones), que aunque no forma parte del SGBD, si es necesario que el SGBD sea capaz de integrarse con estos.

Servicio de integridad

Un SGBD debe proporcionar un medio de garantizar que tanto los datos de la base de datos como los cambios efectuados en los mismos se adecuen a ciertas reglas. Podemos considerarlo como otro tipo de *protección* de la base de datos, donde se establecen reglas de coherencia que la base de datos no puede violar. Con ello se permite la calidad de la información.

4.4.3. Componentes de un SGBD

Entre los componentes de un SGBD podemos destacar el núcleo (kernel), el catálogo (componente fundamental para asegurar la seguridad de la base de datos) las utilidades para el administrador de la base de datos (entre las que se suelen encontrar algunas para crear usuarios, conceder privilegios y resolver otras cuestiones relativas a la confidencialidad); las que se encargan de la recuperación de la BD; rearranque, copias de respaldo, ficheros diarios (logs) etc. y algunas funciones de auditoría.

Los SGBD son programas software altamente complejos que tratan de proporcionar funcionalidades que nos permite trabajar y gestionar los datos de la base de datos. Resulta imposible generalizar la estructura de los componentes de un SGBD ya que varía enormemente de unos sistemas a otros, pero a continuación vamos a exponer una posible arquitectura genérica.

Podemos enumerar los siguientes componentes que forma parte de un entorno Sistema Gestor de Base de Datos:

- **Hardware**. Así el SGBD y las aplicaciones requieren de una plataforma hardware sobre la que ejecutarse. El hardware concreto dependerá de las necesidades de la organización y el SGBD utilizado. Ya que algunos SGBD sólo se ejecutan sobre una plataforma hardware concreta y sistemas operativos específicos.

- **Software.** El componente software comprende el propio software SGBD y los programas de aplicación junto con el sistema operativo. Normalmente los programas de aplicación se escriben en leguajes de tercera generación o

cuarta generación como SQL, incrustado dentro de un lenguaje de tercera generación. El SGBD puede disponer de sus propias herramientas de cuarta generación que permiten el desarrollo rápido de aplicaciones.

- **Datos**. Están contenidos en la base de datos y contiene los datos operacionales y los metadatos.

- **Procedimientos.** Son las instrucciones y reglas que gobiernan el diseño y utilización de la base de datos. Estos procedimientos pueden estar compuestos de instrucciones que dicen cómo llevar a cabo ciertas acciones:

  - Iniciar una sesión en el SGBD

  - Utilizar una funcionalidad del SGBD

  - Iniciar y detener el SGBD

  - Realizar copias de seguridad de la base de datos

  - Gestionar fallos de hardware y software

  - Cambiar la estructura de la tabla, reorganizar la base de datos, mejorar el rendimiento, archivar los datos en almacenamiento secundario

El siguiente cuadro nos muestra los diferentes componentes de un Gestor de Base de datos.

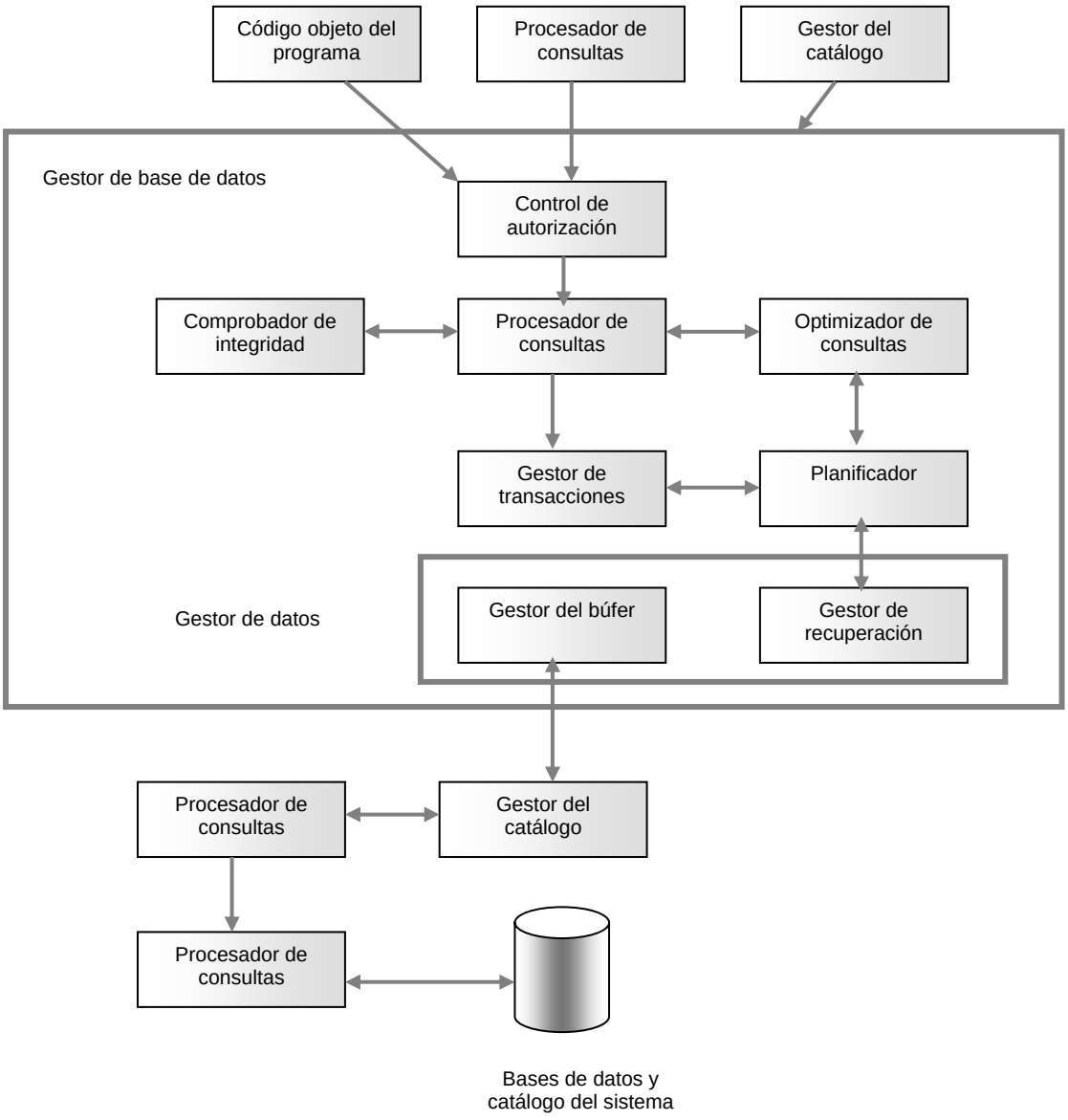


Ilustración 7. Componentes de un gestor de base de datos

4.4.4. Tipos de arquitectura de los SGBD

Estas arquitecturas constituyen la más comúnmente utilizadas para implementar sistemas de gestión de bases de datos multiusuario.

Teleprocesamiento

Se trata de un sistema formado por una única computadora con una unidad central de proceso y una serie de procesadores, llevando todo el procesamiento dentro de una misma computadora física, donde los terminales no pueden trabajar por sí mismos.

Con este sistema se produce una enorme carga de trabajo a la computadora central, que además de ejecutar los programas de aplicación y el SGBD también lleva a acabo otra serie de tareas por cuenta de los terminales.

Se han producido avances significativos en los últimos años en el desarrollo de computadoras personales de altas prestaciones y redes informáticas, así se consigue sustituir los caros ordenadores *mainframe* por redes más baratas de ordenadores personales que permiten conseguir los mismos resultados. Ha dado lugar al surgimiento de dos arquitecturas: servidor de archivos y el modelo cliente-servidor.

Arquitectura de servidor de archivos

En un entorno de servidor de archivos, el procesamiento está distribuido por toda la red. El servidor de archivos almacena los archivos que las aplicaciones y el SGBD necesitan, pero las aplicaciones y el SGBD se ejecutan en cada estación de trabajo, realizando peticiones de archivos al servidor cada vez que sea necesario.

Esta arquitectura tiene el problema de provocar alto nivel de tráfico y desencadenar problemas de rendimiento, además de que el control de concurrencia, de recuperación y de integridad son más complejos, ya que existen múltiples SGBD accediendo a los mismos archivos.

Arquitectura cliente-servidor en dos niveles

Con esta arquitectura se pretende resolver las desventajas que presentaban las dos anteriores. Consiste básicamente que un programa, el cliente, realice peticiones a otro programa, el servidor, que le da respuesta.

La separación entre cliente y servidor es una separación de tipo lógico, donde el servidor no se ejecuta necesariamente sobre una sola máquina ni es necesariamente un sólo programa. Los tipos específicos de servidores incluyen los servidores Web, los servidores de archivo, los servidores del correo, etc. Mientras que sus propósitos varían de unos servicios a otros, la arquitectura básica seguirá siendo la misma.

Con este tipo de arquitectura se consigue una serie de ventajas entre las que se encuentra un acceso más universal a las bases de datos existentes, mejores prestaciones, se reducen costes de hardware y comunicación, además de una mayor coherencia al permitir que el servidor pueda gestionar las comprobaciones de identidad, por lo que sólo es necesario definir y validar las restricciones en un único lugar.

Arquitectura cliente-servidor en tres niveles

Para mejorar la escalabilidad de los sistemas empresariales se propone una nueva variación del modelo tradicional en 1995, donde se proponen tres niveles, cada uno de los cuales puede ejecutarse en una plataforma distinta:

1. El nivel de interfaz de usuario, se ejecuta en la computadora del usuario final (el cliente).

2. El nivel de lógica de negocio y procesamiento de datos. Es el nivel intermedio, que normalmente se ejecuta en un servidor denominado servidor de aplicaciones.

3. Un SGBD que almacena los datos requeridos por el nivel intermedio. Se ejecuta en un servidor independiente, denominado servidor de base de datos.

Con esta arquitectura se consiguen más ventajas, dado que el hardware necesario es menos costoso ya que los clientes son “simples”. El mantenimiento de aplicaciones está centralizado, al transferirse la lógica de negocio desde las plataformas de los usuarios finales a un único servidor de aplicaciones y más facilidad para equilibrar el procesamiento al separar la lógica principal de negocio de las funciones de base de datos.

Otra ventaja adicional es que la arquitectura en tres niveles se adapta de forma bastante natural a los entornos web, donde un explorador web actúa como cliente “simple” y un servidor web actúa como servidor de aplicaciones.

Monitores de procesamiento de transacciones

Consiste en un programa que controla la transferencia de datos entre clientes y servidores para proporcionar un entorno coherente, particularmente para el procesamiento de transacciones en línea. Suele utilizarse en entornos que tienen un volumen muy alto de transacciones, donde el monitor *Transaction Processing* (TP) puede emplearse para descargar tareas de procesamiento del servidor SGBD.

Un monitor de procesamiento de transacciones (TP) es un componente *middleware* que proporciona acceso a los servidores de una serie de gestores de recursos. El monitor TP constituye el nivel intermedio de una arquitectura en tres niveles, que proporciona el encaminamiento de las transacciones, la gestión de transacciones distribuidas, equilibrado de carga y mejora de la fiabilidad.

Algún ejemplo de monitor TP es CICS de IBM (utilizado principalmente en IBM AIX o Windows NT y que ahora se incluyen en los productos IBM TxSeries) y Tuxedo de BEA Systems.

4.5. SISTEMAS DE MONITORIZACIÓN Y AJUSTE DEL SISTEMA

El ajuste de rendimiento de un sistema implica ajustar varios parámetros y opciones de diseño para mejorar el rendimiento en una aplicación concreta. Existen varios aspectos del diseño de los sistemas de bases de datos que afectan al rendimiento de las aplicaciones, aspectos de alto nivel como el esquema y el diseño de las transacciones, parámetros de las bases de datos como los tamaños de memoria intermedia y aspectos de hardware como el número de discos. Cada uno de estos aspectos puede ajustarse de modo que se mejore el rendimiento.

En la auditoría también es importante monitorizar el sistema para mejorar las prestaciones. Uno de los objetivos principales del diseño físico de la base de datos consiste en almacenar y acceder a los datos de una manera eficiente. Existen una serie de factores que se pueden utilizar para medir la eficiencia:

- *Tasa de procesamiento de transacciones*. Es el número de transacciones que pueden procesarse en un intervalo de tiempo determinado.
- *Tiempo de respuesta*. Es el tiempo que transcurre en completar el procesamiento de una única transacción. Hay ciertos factores que influyen en el tiempo de respuesta y de comunicación, por ejemplo la carga que tenga el sistema o los tiempos de comunicación.
- *Almacenamiento en disco*. Es la cantidad de espacio en disco requerida para almacenar los archivos.

Sin embargo, no hay un único factor que sea el que se aplique con mayor frecuencia, hay que establecer un compromiso entre los distintos factores con el fin de conseguir un adecuado equilibrio.

Los SGBD proporcionan al Administrador de la Base de Datos una serie de utilidades para monitorizar la operación del sistema y optimizar éste.

Son diversos los beneficios que pueden obtenerse optimizando la base de datos:

- La optimización puede evitar tener que comprar hardware adicional
- Puede que sea posible reducir la configuración del hardware. Esto influye en el ahorro de dinero en componentes y, consecuentemente, que el mantenimiento sea también más económico.
- Un sistema bien optimizado proporciona tiempos de respuestas más rápidos y una mayor tasa de procesamiento, lo que a su vez hace que los usuarios, y por tanto la organización, sean más productivos.
- Los tiempos de respuesta mejorados aumenta la satisfacción de los usuarios.
- Los tiempos de respuesta mejorados aumenta la satisfacción de los clientes.

Los accesos a memoria principal son significativamente más rápidos que los accesos al almacenamiento secundario, por ello es aconsejable que el SGBD y las aplicaciones de bases de datos tengan suficiente memoria. Es aconsejable que tengan disponible un 5%, y resulta desaconsejable tener más del 10% porque el sistema operativo transferirá páginas de los proceso a disco con el fin de liberar memoria. Si la transferencia de páginas o el intercambio de procesos son excesivos, puede originar problemas con la memoria principal.

Por ello es importante comprender el modo en que el SGBD elegido utiliza dicha memoria principal, que búferes mantiene en memoria principal y qué parámetros existen para ajustar el tamaño de estos búferes.

Con respecto al procesador, hay que tener en cuenta que es el recurso que controla las tareas de los otros recursos del sistema y ejecuta los procesos, además de ser el recurso más caro del sistema. Es importante conocer la carga de trabajo que tiene en un periodo de 24 horas, ya que es necesario garantizar que hay recursos suficientes disponibles no sólo para la carga de trabajo normal sino también para los picos de carga. Una opción para garantizar que hay suficiente recursos en los picos de trabajo es que no se ejecute ninguna tarea no imprescindible durante los excesos de carga.

Cualquier SGBD complejo, necesita realizar una cantidad significativa de operaciones Entrada/Salida para almacenar y extraer datos. Aunque en los últimos años ha incrementado la velocidad de procesado, sin embargo esta no ha aumentado de forma proporcional con los dispositivos de E/S, y por tanto puede surgir la “contienda de disco”, fenómeno que se produce cuando múltiples procesos tratan de acceder a un mismo disco simultáneamente. La mayoría de los discos tienen una serie de límites tanto en el número de accesos como en la cantidad de datos, por ello los procesos pueden tener que esperar para acceder al disco. Una posible solución es distribuir equitativamente los datos entre los discos disponibles, para reducir la probabilidad de que se produzcan problemas de rendimiento.

Por tanto, podemos indicar como una configuración típica de distribución de los datos entre los discos:

- Los archivos del sistema operativo deben estar separados de los de base de datos.
- Los archivos principales de la base de datos deben estar separados de los archivos de índice.
- El archivo del registro de recuperación debe estar separado del resto de la base de datos.

Los mecanismos utilizados para optimizar el sistema deben estar perfectamente documentados, junto con las razones para optimizarlos de la manera elegida.

Cabe destacar que la optimización de un sistema, no sólo implica al SGBD, existen otros puntos fatídicos relacionados con el rendimiento. En la siguiente figura se observa que un alto porcentaje, correspondiente al tiempo invertido, se lo lleva la optimización de las sentencias SQL que forman parte de las aplicaciones, mientras que un porcentaje bastante inferior se invierte en optimizar tanto la base de datos como los recursos del sistema operativo.

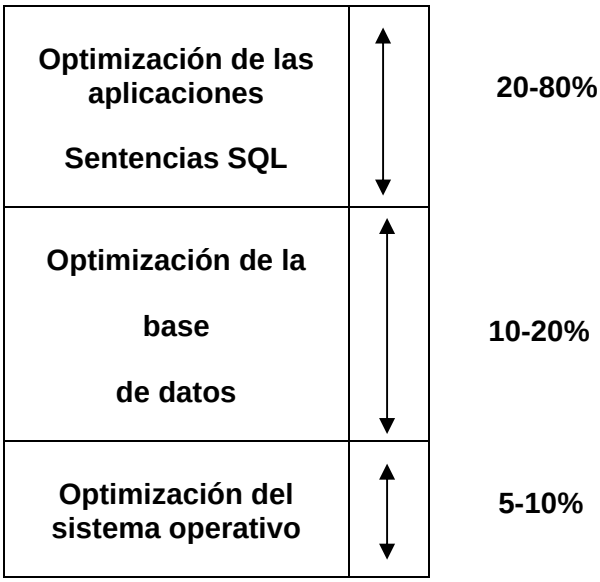


Ilustración 8. Porcentajes de optimización

Teniendo en cuenta esto, se puede afirmar que la mayoría de los problemas que se generan en un SGBD son por causa de un mal diseño de las aplicaciones que atacan la información de la base de datos, aunque evidentemente no va a ser la única causa.

El Sistema Operativo es una pieza clave del entorno, el SGBD se apoya en el en mayor o menor medida, según se trate de un SGBD dependiente o independiente, en los aspectos de control de memoria, gestión de áreas de almacenamiento intermedio (buffer), manejo de errores, control de confidencialidad, mecanismos de ínter bloqueo, etc. Esta información es difícil de estudiar porque es reservada de los fabricantes de los productos, además de requerir unos conocimientos excepcionales que entran en el campo de la técnica de sistema.

Los administradores de bases de datos pueden ajustar los sistemas de bases de datos en tres niveles. El nivel inferior es el nivel de hardware, donde las opciones para el ajuste de los sistemas incluyen añadir discos o usar sistemas RAID (si la E/S de disco constituye un cuello de botella), añadir más memoria si el tamaño de la memoria intermedia de disco no es suficiente y ralentiza el sistema o aumentar la velocidad del procesador.

El segundo nivel consiste en los parámetros de los sistemas de base de datos, como el tamaño de la memoria intermedia y los intervalos de puntos de revisión. La mayoría

de los sistemas de bases de datos poseen manuales que proporcionan información sobre los parámetros del sistema de bases de datos que pueden ajustarse y el modo en que deben escogerse los valores de esos parámetros.

El tercer nivel es el superior, incluye el esquema y las transacciones. El administrador puede ajustar el diseño del esquema, los índices que se crean y las transacciones que se ejecutan para mejorar el rendimiento.

Como hemos indicado con anterioridad, tienen que ajustarse cada uno de estos aspectos en conjunto, porque el ajuste de uno puede originar desajustes en otros.

- Ajuste del hardware
- Ajuste del esquema
- Ajuste de los índices
- Uso de vistas
- Ajuste automático del diseño físico
- Ajuste de las transacciones

4.6. LA FIGURA DEL ADMINISTRADOR

Las bases de datos y el SGBD es un recurso corporativo que debe gestionarse de igual forma que cualquier otro recurso. El Administrador es una figura muy importante porque es el responsable de gestionar los datos que incluye planificación de la base de datos, desarrollo y mantenimiento de políticas, estándares y procedimientos. Siendo el responsable del sistema, tanto mantenimiento como seguridad, control, integridad, fiabilidad del sistema así como la garantía de que las aplicaciones tengan un rendimiento adecuado y satisfactorio. Es por ello que en el proceso de auditoría de sistemas de bases de datos, es muy importante obtener parte de la información del Administrador, que como ya hemos visto es quien la posee y la utiliza, en definitiva en sus manos está el control del sistema.

El Administrador de Base de Datos (DBA) además ser la persona encargada en definir y controlar las bases de datos corporativas, proporcionar asesoría a los usuarios y ejecutivos que lo requieren. A continuación detallamos algunas de sus principales funciones:

- Establecer la estructura de la base de datos en el sentido de determinar que información va a ser necesaria almacenar en la misma, después de haber analizado los requerimientos de los usuarios.

- Establecer los estándares por los que se va a regir la organización en el ámbito de la documentación de la bases de datos, metodología de diseños, etc.

- Establecer la estrategia de transición cuando se pasa de un sistema a otro nuevo, de tal forma que las decisiones tomadas causen el mínimo trastorno a los usuarios y a la organización.

- Gestión de los permisos de explotación y uso, estableciendo la normativa necesaria para la utilización de la base de datos, forma de solicitar acceso, actualización, etc.

- Gestión y control de aspectos relativos a la seguridad, incluyendo los procedimientos de control y auditorías.

- Mantenimiento rutinario de la base de datos, revisando que se cumplan, entre otras, las siguientes actividades:

  - Copia de seguridad periódica de la base de datos

  - Controlar que existe suficiente espacio libre de almacenamiento para las operaciones normales.

- Supervisar los trabajos que se realizan sobre la base de datos y verificar que el rendimiento no se degrada debido a tareas muy costosas realizadas por ciertos usuarios.

CAPÍTULO 5

AUDITORÍA, SEGURIDAD Y CONTROL EN INFORMIX

5. AUDITORÍA, SEGURIDAD Y CONTROL EN INFORMIX

A lo largo del Proyecto se ha presentado información sobre que es una Auditoría y como se lleva a cabo. No obstante podemos tratarlo bien desde un enfoque general o bien orientado específicamente al área de informática. Debido a que habitualmente el término Auditoría, para toda persona ajena al mundo de las tecnologías de la información, se identifica con el área contable a las que están sometidos con frecuencia cualquier entidad u organismo.

Por otro lado, se han mostrado todos aquellos aspectos relacionados con una base de datos y su entorno: qué es una base de datos, que componentes la forman y su funcionalidad, atendiendo en todo momento a la seguridad, control y rendimiento, parámetros que las hacen diferente entre los distintos productos existentes en el mercado.

La unión de Auditoría y Bases de Datos, se materializa en este siguiente capítulo, donde se va a exponer como abordar la Auditoría de una base de datos, pero no cualquiera, sino Informix, producto comercial que se podría decir que fue propulsor de esta forma de tratar y gestionar la información.

Es importante añadir un concepto más al desarrollo de este capítulo, la seguridad. Se demuestra que existe una especial relación entre la auditoría y seguridad de la información, la auditoría nos va a aportar información sobre la seguridad del sistema, uno de los objetivos finales que se pretende obtener, el nivel de seguridad que posee el sistema. A través de alguno de los siguientes puntos se puede comprobar:

- Control de acceso a los sistemas (a priori).
- Auditoría de la seguridad (a posteriori).
- Independencia de las aplicaciones.
- Auditar de forma selectiva, porque sino puede causar ciertos problemas de almacenamiento y rendimiento del sistema:

- Las necesidades de almacenamiento aumentan.
- El rendimiento de la Base de Datos y del propio sistema se resiente ostensiblemente.

El proceso de auditoría del entorno a estudiar, se puede identificar, a grandes rasgos, en dos actividades bien diferencias: la recogida de la información que servirá de base para el análisis de auditoría y el procesamiento de la información tomada que es la función de la auditoría.

Para la tarea de recogida de información, se expone a continuación un detalle de todas aquellas sentencias que nos permiten controlar el acceso e integridad de los datos. Indicadores que nos van a proporcionar información del sistema. Los ficheros de logs que proporciona Informix, muestran las huellas que ha dejado el sistema cuando han interactuado los usuarios.

5.1. PRODUCTOS DE INFORMIX

Para afrontar una proceso de auditoría es importante comenzar con una pequeña descripción sobre los productos que posee Informix para poder obtener la información del sistema, así como las herramientas y métodos que permiten mantener un nivel de seguridad aceptable en todos aquellos entornos que contienen Informix.

El Sistema de Gestión de Bases de Datos (DBMS) de Informix fue concebido y diseñado por Roger Sippl a finales de los años 70. La compañía Informix fue fundada en 1980 y salió a bolsa en 1986. Durante parte de los años 90 fue el segundo sistema de bases de datos más popular después de Oracle. Sin embargo, su éxito no duró mucho y en el año 2000 una serie de tropiezos en su gestión debilitaron seriamente la compañía desde el punto de vista financiero.

En 2001 IBM adquirió Informix, impulsada por una sugerencia de Wal-Mart (el mayor cliente de Informix). IBM tenía planes a largo plazo tanto para Informix como para DB2,

compartiendo ambas bases de datos tecnología una de la otra. A principios de 2005, IBM lanzó la versión 10 del Informix Dynamic Server (IDS).

Se muestra a continuación una tabla de las herramientas que posee Informix por categorías. Es importante conocer de las herramientas que se dispone para afrontar el estudio de un sistema, aunque nos centremos posteriormente solo en aquellas que nos aportan mayor información sobre las bases de datos.

Herramienta	**Desarrollo de aplicaciones**	**Administración de Base de Datos**	**Integración de la información**	**Proceso**	**Desarrollo Web**
Informix 4GL	✓				
Informix Client Software	✓				
Development Kit	✓				
Informix Connect	✓				
Informix Data Director for Web					✓
Informix Enterprise Gateway Manager			✓		
Informix Enterprise Gateway Manager with DRDA			✓		
Informix ESQL/C	✓				
Informix ESQL/COBOL	✓				
Informix I-Spy				✓	
Informix JDBD	✓				
Informix MaxConnect 1.0				✓	
Informix Server Administrator		✓			
Informix SQL	✓				

Herramienta	Desarrollo de aplicaciones	Administración de Base de Datos	Integración de la información	Proceso	Desarrollo Web
Server Studio	✓	✓		✓	
Sentinel		✓		✓	

5.1.1. Estrategia de IBM con respecto a Informix Dynamic Server

A través de la siguiente tabla se presenta el pasado, el presente y el futuro de Informix Dynamic Server (IDS) de IBM:

Continuidad del Negocio con Seguridad IDS 11 2007	Disponibilidad continua & Escalabilidad Cheetah2 2008	Dynamic Enterprise OLTP DataServer* vNext 2010	Enterprise OLTP con Cero Administración* vNext + 2012

A continuación se detalla las principales características que se dan en cada una de las etapas por las que va pasando y que se espera se desarrolle sobre Informix Dynamic Server (IDS):

IDS v.11 (2007) se caracteriza por lo siguiente,

- Alta disponibilidad y mejoras en disponibilidad continua
- Mejoras significativas en Seguridad y Cifrado, LBAC y Common Criteria certification.
- Mejoras especiales y servicios web para la localización.
- Reducción del TCO con mejoras en la administración.
- Avanzado desarrollo de aplicativos, SOA.
- Mejoras en la integración API'S Admin, footprints modificable.

Cheetah2 (2008) se caracteriza por:

- Alto potencial de escalabilidad y disponibilidad de soluciones cluster.
- Mejora en el Cifrado de Datos
- Mejoras para el desarrollo avanzado de aplicativos
- Soporte de Mac OS
- Mejoras en el 4GL
- Administración integrada servidores

Dynamic Enterprise OLTP Data Server (2010) se caracterizará por:

- Siempre disponible
- Compresión
- Aprovisionamiento dinámico
- Mejor rendimiento
- Nuevas opciones en la gestión de la Seguridad
- Mejoras en las herramientas de gestión.
- Mejoras XML.

Y por último, ***Enterprise OLTP Cero Administración (2012)***:

- Continúa replicación heterogénea.
- 100% Disponibilidad
- Clusters de alta escalabilidad

- Totalmente autogestionado
- Mejora en el soporte de aplicaciones

5.1.2. Características del nuevo producto de Informix

Cabe destacar el producto “Informix Dynamic Server 11.5” que IBM ha presentado recientemente, en mayo de 2008. Se trata del primer servidor que sin ser un *mainframe* proporciona a los centros de datos disponibilidad continua y recuperación ante posibles desastres. Este servidor de base de datos es capaz de reducir los costes de gestión de la información hasta un 33%.

Otras ventajas de IDS son, según IBM, que permite gestionar la misma cantidad de datos con menos servidores y por tanto se necesitan menos licencias de software. Esto puede reducir los costes de administración y permite conseguir importantes ahorros de energía y espacio.

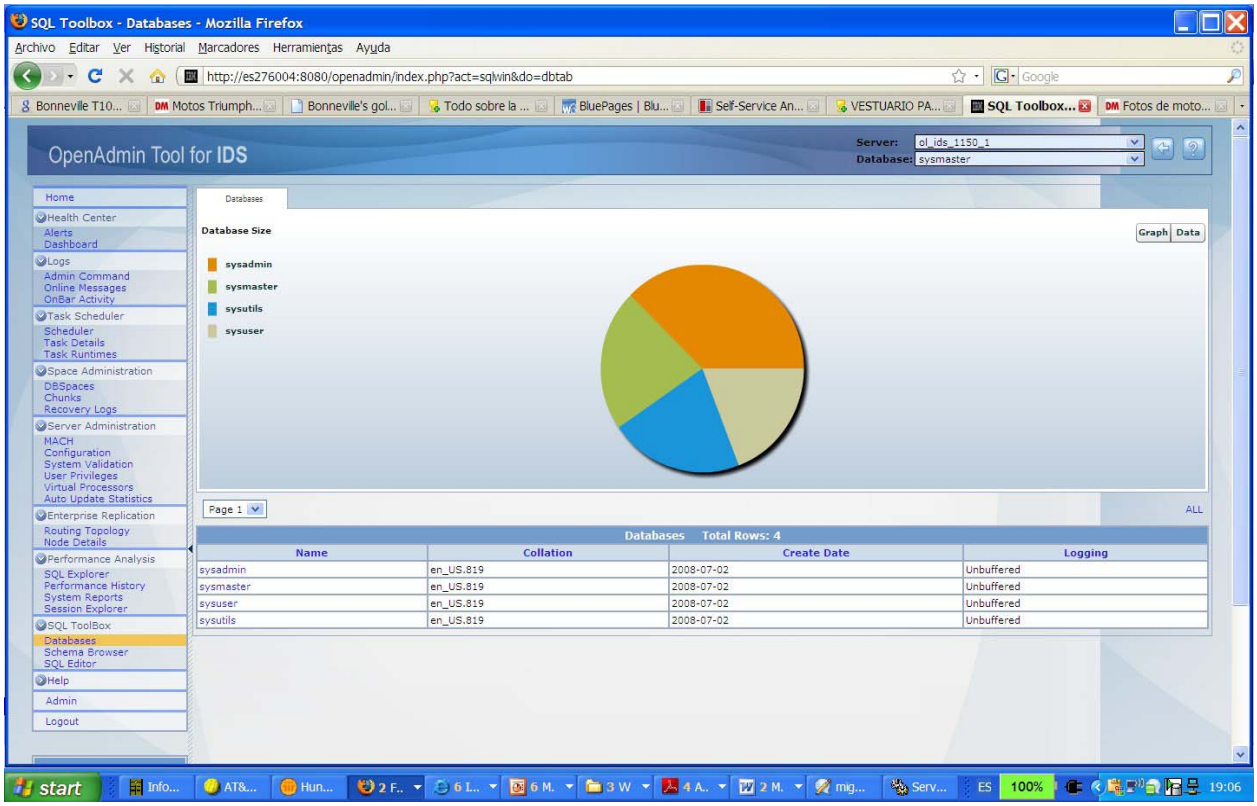
La nueva versión del Informix Dynamic Server (IDS) v11.5 ofrece un servidor flexible de datos que supone importantes mejoras de rendimiento, réplica, disponibilidad, escalabilidad y seguridad que proporcionan un excelente sistema informático de proceso de transacciones en línea. Además, IDS disminuye aún más la complejidad, el tiempo, los conocimientos del Administrador de Base de Datos y los costes relacionados con la gestión, ya que simplifica y automatiza la mayoría de las tareas asociadas al mantenimiento de la base de datos de una empresa.

Podemos definir a IDS v11.5 con las siguientes características:

- Manejable
- Veloz
- Robusto y fiable
- Abierto y extensible

Considerando que es "*manejable*" por las facilidades que da en las tareas de administración. Se han conseguido mejoras con respecto a las API SQL de Administración, un planificador interno, almacenar un historial con el rendimiento y monitor de salud. Además posee una mayor autonomía que implica menor dedicación por parte del Administración de la base de datos y por último permite la posibilidad de seleccionar qué módulos se desean seleccionar, así como guardar las respuestas en un fichero para su posterior ejecución y la instalación silenciosa.

La nueva herramienta de administración *Open Admin Tool* , que facilita la administración es otra de la nuevas características de IDS v11.5. A continuación se presenta una imagen con el aspecto de dicha herramienta.



Además también hay mejoras en el ámbito del desarrollo, como son:

- Queries distribuidas que permiten tipos de datos extendidos.

- Soporta XML, de tal forma que se puede generar XML a partir del resultado de una select y también se puede extraer parte de un documento XML.
- Soporta múltiples *triggers* por operación de insert/update/delete.
- Soporta el nivel de aislamiento de transacción "*Set isolation to read committed"*, que determina este nivel de aislamiento de transacción para la siguientes transacciones, globalmente o para la sesión actual.
- SQL dinámico en SPL.

Con respecto a la Replicación también se han producido mejoras, HDR (High-Availability Data Replication). Esto se consigue con dos servidores idénticos en dos máquinas distintas: Servidor primario y Servidor secundario.

- Servidor Primario: es un servidor plenamente funcional, lleva acabo toda la actividad de la bases de datos (insert/update/deletes) y realiza envío de logs al servidor secundario.
- Servidor Secundario: se accede en modo lectura para la realización de consultas y creación de tablas temporales. Además recibe los logs del servidor primario y va ejecutando sus transacciones, de tal forma que mantiene un sincronismo con el servidor primario. De esta manera si el primario se cae, el secundario toma el control y se convierte en el servidor estándar.

5.2. SEGURIDAD EN INFORMIX

Todo sistema precisa de un conjunto de medidas de seguridad frente a los posibles ataques externos e internos. Podemos decir que todo ataque a un sistema tiene como único fin la obtención de datos e información. Y como venimos indicando a lo largo del proyecto es vital para la existencia de la empresa, por ello es tan importante la seguridad tanto del sistema como de los datos.

Un Auditor informático tiene que saber los procedimientos para conocer los accesos no autorizados, los accesos de personas a información para la cual no tienen privilegios, así como el borrado o modificación de información privilegiada de la base de datos

Un aspecto muy importante que requiere una atención especial por parte del Administrador de la Base de Datos y por el Auditor Informático son las copias de seguridad de la información y la recuperación en caso de que se produzcan fallos. El Administrador de la base de datos suele ser el encargado de realizar las copias y su recuperación y el Auditor debe revisar todos los procedimientos de copia y recuperación para poder recuperar la Base de Datos en caso de fallo.

Se puede hablar de seguridad en los diferentes elementos que conforman el entorno de la organización: la seguridad del sistema, la seguridad de los datos y sobre otros aspectos que sean objeto de ataque en una empresa. Informix proporciona una serie de herramientas y métodos que abordan estos aspectos.

La Seguridad y Control de acceso a los datos en Informix podemos esquematizarla a través de las siguientes sentencias SQL que nos aportan dicha funcionalidad:

- La utilización de las sentencias GRANT y REVOKE otorga o deniega el acceso a una tabla determinada de la base de datos, es una forma de control de los usuarios sobre la base de datos.

- La utilización de las sentencias CREATE PROCEDURE o CREATE FUNCTION permite la creación de rutinas definidas por el Administrador de Base de Datos o la persona encargada de dicha tarea, que controlen y supervisen los usuarios que pueden leer, modificar o crear tablas en la base de datos.

- La utilización de la sentencia CREATE VIEW permite crear una vista restringida o modificada de los datos. La restricción puede ser vertical que excluye determinadas columnas, o bien horizontal que excluye determinadas filas, o ambas.

- La combinación de las sentencias GRANT y CREATE VIEW permite conseguir un control preciso sobre las partes de una tabla que el usuario puede modificar y con qué datos.

- Con uno de los servidores de datos que proporciona Informix, “Dynamic Server”, se puede utilizar la sentencia SET ENCRYPTION PASSWORD y las funciones de SQL incorporadas para cifrar y descifrar con la finalidad de implantar el cifrado de los datos personales a nivel de columna. Aquellos usuarios no autorizados que puedan ver un valor de una columna, no podrán recuperar el texto plano de los datos sin la clave de cifrado DES o triple-DES, que no está almacenada en la base de datos.

Diferentes estudios y el trabajo diario han detectado en ciertos productos de Informix algunos problemas de seguridad que se han ido solucionando. A modo de resumen se indican algunos de ellos:

- Situaciones en las que se pueden producir al desbordamiento de búfer, como pueden ser los errores de límites hallados en la funciones BINFO(), FILETOCLOB(), GETNAME(), IFX-FILE-TO-FILE() y LOTOFILE(). También puede producirse el desbordamiento a través de la introducción de nombres de usuario muy largos

- La ejecución arbitraria de comandos a través de procedimientos de exportación “dbexp” e importación “dbimp” en la base e datos. También se pueden dar casos de una errónea permisividad en la directiva “SET DEBUG FILE” destinada a la asignación de ficheros para el depurado.

- Otros errores generados bajo ciertas condiciones que han conducido a la denegación de servicio y aumento de privilegios, incluso que usuarios no autorizados puedan crear bases de datos, siendo posible también que las contraseñas de usuario queden almacenada en memoria compartida sin ningún tipo de cifrado.

Las versiones de Informix Dynamic Sever 7.31.xD9, 9.40.xC8 ó 10.00.xC4 son vulnerables a este tipo de errores, por ello se aconseja su actualización.

5.3. CONTROL Y GESTIÓN DE BASES DE DATOS

El control y la gestión de una Base de Datos es una tarea que suele recaer en el Administrador, sus decisiones e implantación de estrategias puede determinar en muchas ocasiones una mayor eficiencia en el sistema. La fragmentación de las tablas y accesos a las mismas son aspectos importantes que deben ser estudiados y comprobados por una auditoría.

Principalmente las amenazas contra la seguridad de la base de datos implican el acceso no autorizado o la modificación de información reservada, por ello el Administrador de Seguridad-Auditoría debe asegurar que todos los usuarios de la base de datos están identificados y autentificados antes del uso o acceso a los programas o datos. Por ello, todos los usuarios deben tener asociado una identificación. Además, el acceso a la información puede ser permitida o suprimida a diferentes niveles: a nivel de base de datos, tabla, procedimiento almacenado, rol o fragmentación.

Informix recoge en sus manuales en línea de *IBM Informix: Administrator's Reference y Performance Guide* una lista de tareas a realizar en la base de datos para su óptimo rendimiento y mantenimiento.

- Trabajar con las tablas de la base de datos sysmaster
- Calcular el tamaño de las tablas y gestionar las extensiones de tabla
- Modificar tablas (truncar, alterar, modificar columnas, cargar, conectar fragmentos)
- Desnormalizar los datos para mejorar el rendimiento.
- Establecer las modalidades de bloqueo y los bloqueos de supervisor correspondientes.
- Diseñar y mantener estrategias de fragmentación
- Fragmentar índices y tablas temporales

5.3.1. Acceso a las Bases de Datos

En el estudio de un sistema, uno de los aspectos más importantes a comprobar es la seguridad. Como los datos son uno de los activos más importante de toda empresa, es necesario verificar que el acceso a los mismos es el correcto. Informix proporciona diferentes niveles de acceso, y es función del auditor comprobar que el acceso es el correcto.

Informix, mediante SQL, puede restringir el acceso y modificación de los datos, para ello se establecen los siguientes niveles:

- Otorgar o denegar acceso a la base de datos o tablas específicas, además de la forma en la que los usuarios utilizaran la base de datos (mediante privilegios).
- Control y supervisión de las funciones de lectura, modificación o creación de tablas de la base de datos (mediante procedimientos y funciones)
- Creación de vistas que muestren los datos de forma restringida o modificada (puede ser vertical que excluye columnas, horizontal que excluye determinadas flags, o ambas).
- Con la combinación de ciertas sentencias de manipulación de datos nos permite lograr el control necesario sobre la tabla que el usuario puede llegar a modificar.
- Con sentencias y funciones de SQL que cifran y descifran la información relativa a los datos de carácter personal.

5.3.1.1. Privilegios

La autorización para utilizar una base de datos se denomina privilegio de acceso. Se pueden crear funciones para asignar privilegios a usuarios, de forma que los usuarios con tareas de trabajo parecidas puedan realizar el conjunto de privilegios de acceso

que sus tareas de trabajo requieren. Asignando privilegios a las funciones y funciones a los usuarios se puede simplificar la gestión de privilegios.

Existe un principio de Mínimos Privilegios, que es posiblemente el más lógico y fundamental para una buena gestión de la seguridad. Pero a pesar de que se tengan muy claro cuales son los principales motivos de la utilización de este principio, es importante mencionar que un usuario con privilegios amplios, potencia el impacto ante un incidente. Aunque es muy aconsejable que se aplique este principi0o y resulta básico, es poco frecuente verlo en las organizaciones, o dentro del diseño de aplicaciones, donde siempre impera la funcionalidad sin tener en cuenta los riesgos asociados a ésta práctica y mucho menos la clasificación de la información que esta procese.

La implementación de este principio favorece la segregación de funciones, otro pilar en la gestión de la Seguridad de la Información. Y se puede garantizar que su correcta aplicación es totalmente transparente para el usuario y con un gran valor agregado.

Como hemos comentado, los privilegios determinan en gran medida la seguridad del sistema, junto con otros tipos de controles. Una falta de aplicación y planificación de los mismo provoca debilidades en el sistema. Por ello es un punto muy importante a estudiar en el desarrollo de la auditoría.

En INFORMIX, se establecen los siguientes grupos de privilegios que controlan las acciones que puede llevar a cabo un usuario sobre los datos y sobre sus objetos de base de datos:

- Privilegios a nivel de base de datos.
- Privilegios a nivel de propiedad.
- Privilegios a nivel de tabla.
- Privilegios a nivel de columna.
- Privilegios a nivel de tipo.
- Privilegios a nivel de rutina.

- Privilegios a nivel de lenguaje de *Dynamic Server*.

Además, se puede llevar a cabo la automatización de los privilegios, debido a que con mayor o menor urgencia se realizan cambios de privilegios a diario, o incluso cada hora, en cualquier modelo que contenga datos importantes. Si se anticipa a este requisito se pueden preparar algunas herramientas automáticas que ayuden a mantener los privilegios.

La automatización se puede llevar a cabo mediante un script de mandatos, que consiste en la ejecución de un archivo que contiene un conjunto de sentencias SQL que llevan a cabo la tarea a realizar. Además existe otra forma de agilizar el cambio de privilegios mediante la utilización de funciones que se pueden crear en la base de datos.

- **TIPOS DE PRIVILEGIOS**

- **Privilegios a nivel de base de datos**

Los privilegios a nivel de bases de datos proporcionan un método general para controlar quién accede a una base de datos. Sólo los usuarios individuales, y no las funciones pueden tener privilegios a este nivel.

Los mecanismos de control del acceso a base de datos se basan en las sentencias GRANT y REVOKE que, además de otorgar o denegar el acceso a la base de datos, pueden controlar la forma que los usuarios utilizarán la base de datos. Sin embargo, a veces se pueden utilizar los recursos del sistema operativo como un modo adicional de controlar el acceso a una base de datos.

Mediante la sentencia GRANT se otorga privilegios sobre una base de datos, tabla, vista o procedimiento, o para otorgar una función a un usuario o a otra función. La sentencia REVOKE sirve para suprimir los privilegios sobre una base de datos o un objeto de base de datos, o para eliminar una función de un usuario o de otra función.

A continuación detallamos los comandos que otorgan los diferentes tipos de privilegios:

- **Connect**, privilegio que proporciona al usuario capacidad básica de consultar y modificar las tablas. Un usuario puede llevar a cabo las siguientes funciones:

  - Ejecutar las sentencias SELECT, INSERT, UPDATE y DELETE, siempre que tenga los privilegios necesarios a nivel de tabla.

  - Ejecutar una rutina SPL (Lenguaje de Procedimientos Almacenados), siempre y cuando tenga los privilegios necesarios a nivel de tabla.

  - Crear vistas, en caso de que tenga permisos para consultar las tablas en las que se basan las vistas.

  - Crear tablas temporales y crear índices sobre estas tablas.

  Normalmente en una base de datos, que no contengan datos muy importantes, se otorga el privilegio GRANT CONNECT TO PUBLIC justo después de crear la base de datos. Si no se otorga el privilegio Connect a PUBLIC, los únicos usuarios que pueden acceder a la base de datos a través del servidor de base de datos son aquellos a los que se le otorgue de forma específica. (Con PUBLIC los privilegios son otorgados a todos los usuarios).

- **Resource**, privilegio que comporta la misma autorización que el privilegio connect, además los usuarios con este privilegio pueden crear tablas nuevas, permanentes, índices y rutinas SPL, asignando así espacio de forma permanente.

- **Privilegios de administrador de base de datos**, comportan el nivel superior de privilegios, al crear la base de datos automáticamente se asigna este nivel al DBA. Las funciones que se pueden llevar a cabo con este nivel son:

- Ejecutar sentencias DROP DATABASE, START DATABASE y ROLLFORWARD DATABASE.

- Modificar cualquier objeto independientemente de quién sea su propietario.

- Crear tablas, vistas e índices para que los posean otros usuarios.

- Otorgar privilegios de base de datos, incluido el privilegio DBA, a otro usuario.

- **Privilegios a nivel de tabla**

Normalmente el servidor de base de datos, como parte de la creación de la tabla, otorga automáticamente a PUBLIC todos los privilegios excepto ALTER y REFERENCES, a menos que la variable de entorno NODEFDAC se haya establecido en "si" para denegar todos los privilegios a PUBLIC. Por ello una tabla recién creada será accesible a cualquier usuario que tenga el privilegio CONNECT.

- **Privilegios de acceso**, son los que controlan el modo en que los usuarios pueden acceder a una tabla. Son SELECT, INSERT, UPDATE y DELETE. Informix almacena la información sobre los privilegios en tablas del catálogo del sistema: sysusers y systabauth. El acceso a estas tablas lo tiene cualquier usuario con el privilegio CONNECT, pero solo de consulta. A través de la consulta puede conocer que privilegios se han otorgado y a quién.

- **Index, Alter y References**. El privilegio INDEX permite crear y modificar índices en una tabla. Se otorga de forma automática a PUBLIC cuando se crea una tabla aunque sólo puede ejercitarse si se tiene el privilegio RESOURCE. Esta limitación es debido a que un índice puede llenar gran cantidad de espacio de disco.

  El privilegio ALTER permite utilizar la sentencia ALTER TABLE. El privilegio REFERENCES permite imponer restricciones de referencia en una tabla.

Ambos privilegios deben otorgarse únicamente a usuarios que comprendan el modelo de datos y en los que confíe para ejecutar esta capacidad de manera cuidadosa.

- **Privilegios sobre fragmentos de datos**. Cuando las tablas contienen una gran cantidad de registros, Informix permite la partición de la tabla, que consiste en dividir la tabla en fragmentos que suelen ubicarse en dbspaces diferentes. Con la sentencia GRANT FRAGMENT se permite otorgar privilegios de INSERT, UPDATE y DELETE sobre fragmentos individuales. Esto solo es soportado para aquellas tablas que estén fragmentadas con esquemas de distribución basados en extensiones.

- **Privilegios a nivel de columna**

Son SELECT, UPDATE y REFERENCES con los nombres de columnas específicas. El hecho de nombrar columnas específicas le permite otorgar acceso específico a una tabla. Puede permitir que un usuario vea únicamente determinadas columnas, que actualice únicamente determinadas columnas o que imponga restricciones de referencia en determinadas columnas. Esto se consigue con las sentencias GRANT y REVOKE.

Esta característica soluciona el problema de que sólo determinados usuarios deben conocer el valor de ciertas columnas, un ejemplo sería el salario u otros atributos personales o confidenciales.

Para la implementación de privilegios a nivel de columna, es necesario inicialmente suprimir todos los privilegios que posee una tabla cuando es creada, esto se realiza a través de REVOKE ALL. Con las sentencias GRANT SELECT y GRANT UPDATE se otorga a usuarios o roles específicos, la capacidad de poder ver o modificar determinadas columnas de la tabla.

```
REVOKE ALL ON <nombre tabla> FROM PUBLIC
GRANT SELECT ON <nombre tabla> TO <usuario o grupo de usuarios>
GRANT UPDATE (columna, ..) ON <nombre tabla> TO <usuario ó grupo usuarios,...>
```

Todas aquellas sentencias, como por ejemplo SELECT COUNT(*), que intenten acceder a columnas a las que no se tengan permiso generarán un mensaje de error y no devolverá los datos.

- **Privilegios a nivel de tipo**

Dynamic Server da soporte a los tipos de datos definidos por el usuario, de manera que solo el Administrador de la Base de Datos y el propietario del tipo de datos puede otorgar o revocar privilegios de uso. Para limitar quien puede utilizar un tipo, primero debe suprimir el privilegio USAGE correspondiente a PUBLIC y luego especificar los nombres de los usuarios a los que desea otorgar dicho privilegio.

```
REVOKE USAGE ON <nombre tipo> FROM PUBLIC
GRANT USAGE ON <nombre tipo> TO <usuario o grupo de usuarios, ..>
```

- **Privilegios a nivel de rutina**

El privilegio EXECUTE se puede aplicar sobre una rutina definida por un usuario para autorizar a los que no son propietarios. Existe una tabla de catálogos del sistema sysprocauth donde se registran los privilegios a nivel de rutina,

```
GRANT EXECUTE ON <nombre rutina> TO <usuario o grupo de usuarios, ..>
```

Privilegios a nivel de lenguaje

El Dynamic Server da soporte a rutinas escritas en el Lenguaje de Procedimientos Almacenados (SPL), es una extensión de SQL que proporciona control del flujo con operaciones de bucle y ramificaciones. Existen procedimientos y funciones, ambas

están escritas en SPL y SQL, pero se diferencian que las funciones devuelven un valor y los procedimientos no. Los usuarios pueden escribir rutinas en los lenguajes SPL, C, Java y almacenarlas en la base de datos. En los siguientes manuales de IBM se describe su utilización y sintaxis: *IBM Informix: Guide to SQL Tutorial, Guide to SQL Syntax y Performance Guide*.

Para poder crear rutinas se debe tener privilegios RESOURCE en la base de datos. Además, para crear una UDR (denominadas rutinas externas) en el lenguaje SPL, un usuario debe tener también el privilegio USAGE sobre el lenguaje SPL.

El usuario informix y los que tienen privilegios de DBA tienen los privilegios USAGE de lenguaje sobre las UDR. Con las siguientes instrucciones se muestra como el usuario informix puede revocar a PUBLIC y dar permisos a otros usuarios para crear UDR en SPL.

```
REVOKE USAGE ON LANGUAGE SPL FROM PUBLIC
GRANT USAGE ON LANGUAGE SPL TO <usuario o grupo de usuarios, ..>
```

- **MANTENIMIENTO DE LOS PRIVILEGIOS**

Los privilegios requieren un mantenimiento constante, ya que las personas cambian de trabajo. Un empleado cuando deja su puesto es necesario revocar el privilegio UPDATE lo antes posible, porque un empleado insatisfecho podría realizar cambios en la base de datos que alterasen la información existente.

En las organizaciones se requiere realizar cambios de privilegios a diario, o incluso cada hora, en cualquier modelo que contenga datos importantes. Es necesario que se puedan especificar clases de privilegios que se basen en los trabajos de los usuarios, no en la estructura de las tablas. Así que cuando cambia una persona de puesto, por ejemplo un ascenso, se le revocan los privilegios del antiguo grupo al que pertenecía y se otorga un nuevo grupo de privilegios.

Por ello deben definirse clases de privilegios y para cada clase se debe especificar las bases de datos, tablas y columnas a las se que desea proporcionar acceso. Luego es

necesario crear dos rutinas automáticas para cada clase, una para otorgar la clase y otra para revocarlos.

La automatización con un script, recoge en un archivo las instrucciones que modifican los privilegios, así como el usuario a quién aplicarlo. Otra forma de facilitar esta tarea es mediante el uso de funciones. Una función es una característica de las bases de datos que permiten al Administrador de la Base de datos estandarizar y modificar los privilegios de varios usuarios, tratándolos como miembros de una clase. Mediante la sentencia CREATE ROLE se crea una nueva función. Cabe destacar que el ámbito de actuación de una función es únicamente la base de datos actual.

A veces, no se conocen las funciones que existen porque fue otra persona quien las creó. Está información queda recogida en las tablas de catálogo sysroleauth y sysusers, que nos indican quién tiene autorización sobre determinada tabla y cuántas funciones existen.

Es necesario un mantenimiento continuo de estas tablas, por ello en el proceso de auditoría es posible descubrir que algunas funciones ya no resultan útiles y sea necesario eliminarlas, para ello se utiliza la sentencia DROP ROLE.

Normalmente el sistema operativo da soporte a la ejecución automática de scripts de mandatos. En la mayoría de los entornos, las herramientas interactivas de SQL, como *DB-Access*, aceptan que los mandatos y sentencias SQL se ejecuten desde la línea de mandato. Se pueden combinar estas dos características para automatizar el mantenimiento de los privilegios.

Los detalles dependen del sistema operativo y de la versión de la herramienta interactiva de SQL que se utilice. El script de mandatos tiene que llevar a cabo las siguientes instrucciones:

- Tomar la identificación del usuario (ID), cuyos privilegios hay que modificar, que se recibirá como parámetro.

- Preparar un archivo de sentencias GRANT o REVOKE personalizado que contendrá el ID de usuario.

- Invocar la herramienta interactiva de SQL (por ejemplo DB-Access) con parámetros que indiquen que seleccione la base de datos y ejecute el archivo preparado de sentencias GRANT o REVOKE.

5.3.1.2. Rutinas SPL y rutinas externas

El acceso a las tablas y columnas individuales de la base de datos también se puede controlar mediante rutina SPL. Una potente característica de SPL es la posibilidad de diseñar una rutina con privilegio DBA, de esta forma se consigue que los usuarios con pocos o ningún privilegio, cuando ejecuten la rutina, tengan los mismos privilegios de DBA. Es una forma donde los usuarios pueden llevar a cabo tareas con privilegio de DBA temporalmente.

La rutina con privilegio de DBA le permite realizar las siguientes tareas:

- Puede restringir la cantidad de información que usuarios individuales pueden leer de una tabla.
- Puede restringir todos los cambios que se realizan en la base de datos y asegurar que las tablas enteras no se vacían o modifican accidentalmente.
- Puede supervisar una clase entera de cambios realizados en una tabla, como supresiones o inserciones.
- Puede restringir la acción de creación de objetos (definición de datos) que se produce dentro de una rutina SPL para conseguir un control completo sobre el modo en que se crean tablas, índices y vistas.

Por lo tanto, con la utilización de rutinas SPL se pueden canalizar todos los cambios y realizar un seguimiento de los mismos, tanto en la base de datos como a nivel de usuario. La rutina SPL realiza los cambios en lugar de los usuarios, lo cual permite un mayor control y evita posibles errores accidentales sobre las tablas que puedan cometer los usuarios.

Con la utilización de procedimientos, se puede crear un registro de cambios realizados en una base de datos, de manera que se recojan las acciones realizadas por los usuarios. Es una forma de supervisar los cambios realizados. Cabe destacar que todo control implica ciertas penalizaciones en el rendimiento.

Un ejemplo de procedimiento SPL que suprime filas de una tabla:

```
CREATE DBA PROCEDURE <nombre_procedimiento> (<parámetros entrada>)
        DELETE FROM <nombre_tabla>
        WHERE nombre_columna = <parámetro entrada>;
END PROCEDURE;
```

5.3.1.3. Vistas

Podemos definir vista como una tabla ficticia que puede consultarse como si fuera una tabla, y en algunos casos, puede actualizarla como si fuera una tabla. Sin embargo no es una tabla propiamente definida, es una síntesis de los datos existentes en tablas reales y en otras vistas.

La base de una vista es la sentencia SELECT y cuando se crea, define una sentencia SELECT que genera el contenido de la vista en el momento que accede a la misma.

Mediante las vistas se obtiene otra forma de seguridad y control de la base de datos, es decir de la información, ya que nos muestra sólo parte de los datos a los que se puede acceder.

Las vistas pueden utilizarse para:

- Restringir a los usuarios a determinadas columnas de tablas.
- Restringir a los usuarios a determinadas filas de tablas.
- Restringir los valores a determinados rangos.

- Proporcionar acceso a datos derivados sin tener que almacenar datos redundantes en la base de datos.

- Ocultar detalles de una sentencia SELECT complicada.

A continuación describimos dos tipos de privilegios sobre las vistas, por un lado los referentes a la creación de la vista y por otro aquellos que están asociados al cambio de los datos procedentes de la vista.

- Los niveles de privilegios asociados a los usuarios y las tablas se comprueban cuando se crea una vista, se verifica que el usuario que desea realizar la vista tiene privilegios sobre las tablas y vistas subyacentes.

- Cuando una vista es potencialmente modificable, es decir, permite modificar el contenido de sus datos mediante inserciones, modificaciones o borrado, es el servidor de base de datos quien otorga dichos privilegios sobre la vista, siempre y cuando el usuario tenga dichos privilegios sobre la tabla o vista subyacente.

Las sentencias de Informix que se muestran a continuación corresponden a la creación de una vista donde aparecen las columnas indicadas en la SELECT y restringen las filas según la condición indicada en el WHERE.

```
CREATE VIEW  <nombre_vista> AS
        SELECT <nombre_columna alias, ...>
         FROM <nombre tabla>
        WHERE <nombre columna> = <valor>

CREATE VIEW <nombre_vista> (nom_col_vista, ....) AS
SELECT <nombre_columna, ....>
        FROM <nombre tabla>
        WHERE <nombre columna> = <valor> ..
```

Al no ser una tabla, la vista no se puede indexar y, por tanto, ser el objeto de sentencias como ALTER TABLE y RENAME TABLE. Tampoco puede cambiar los nombres de las columnas con RENAME COLUMN. Y si se desea modificar, la única forma de llevarlo a cabo consiste en eliminarla (DELETE) y volver a crearla.

Una vista puede producir filas duplicadas, incluso cuando la tabla origen sólo tiene filas exclusivas. Para evitar este problema se puede especificar DISTINCT en la lista de proyección, pero su utilización implica realizar modificaciones sobre la vista. La alternativa consiste en seleccionar filas exclusivas, es decir, se seleccionan las columnas de una clave primaria.

En una vista se puede modificar su contenido mediante las sentencias DELETE, UPDATE ó INSERT si la sentencia que la ha definido no contenía ninguno de los siguientes elementos:

- Una unión de dos o más tablas.
- Una función de agregación o cláusula GROUP BY.
- La palabra DISTINTC o su UNIQUE sinónimo.
- La palabra clave UNION.

Cuando una vista no contiene ninguna de estas características restringidas, cada fila de la vista corresponde exactamente a una fila de una tabla.

Para evitar la inserción y la actualización de una fila en una vista que no satisfaga las condiciones de la vista; es decir, una fila que no resulte visible a través de la vista, se añaden las palabras claves WITH CHECK OPCTION cuando se crea la vista. Esta cláusula solicita al servidor de base de datos que pruebe cada fila insertada o actualizada para asegurarse de que cumple las condiciones establecidas por la cláusula WHERE de la vista. El servidor de base de datos rechaza la operación con un error si no cumplen las condiciones.

```
CREATE VIEW  <nombre_vista> AS
        SELECT <nombre_columna alias, ...>
      FROM <nombre tabla>
        WHERE <nombre columna> = <valor>
WITH CHECK OPTION
```

También se aplican los privilegios a las vistas creadas, de tal forma que el servidor de base de datos realiza pruebas para asegurarse que el usuario tiene los privilegios que necesita para ejecutar la sentencia SELECT en la definición de la vista. En caso que no sea posible, el servidor de base de datos no crea la vista. De esta manera se asegura que los usuarios no puedan crear una vista en la tabla y consultar la vista para obtener acceso no autorizado a una tabla. Después de crear la vista, el servidor de bases de datos otorga al usuario, el creador y propietario de la vista, al menos el privilegio Select sobre la misma. No se otorga automáticamente ningún privilegio a PUBLIC, como ocurre cuando se crea una tabla.

5.3.2. Integridad: control de seguridad de la información

La integridad de los datos es provista mediante alguno de los siguientes medios:

- Las transacciones.
- Los audit. trails, pistas de auditoría.
- Bloqueos: control de concurrencia

- **Transacciones**

Las transacciones son un conjunto de operaciones que deben ser tratadas como una unidad de trabajo.

Para su implementación debe contarse con un archivo de auditoría de la actividad en la base de datos (el *transaction-log file*), que puede ser generado al momento de crear

la base de datos (con la cláusula WITH LOG IN) o en cualquier momento con la sentencia START DATABASE.

Para indicar el inicio de una transacción, se utiliza la sentencia BEGIN WORK, de tal forma que todas las filas involucradas permanecen bloqueadas para los demás usuarios. El fin de una transacción se indica con la sentencia COMMIT WORK, que produce la liberación de todas aquellas filas que estaban bloqueadas y actúa como la confirmación de todas las operaciones.

Si el usuario detecta un error que invalide las operaciones efectuadas dentro de una transacción, puede cancelarlas con la sentencia ROLLBACK WORK, esto produce la vuelta de la base de datos al estado en que estaba al momento previo del inicio de la transacción y la liberación de las filas que estaban bloqueadas. De todos modos hay operaciones que no pueden ser canceladas como las de definición de datos o las de conceder o revocar permisos.

En caso de producirse problemas externos, se puede recuperar la base de datos mediante la utilización de la sentencia ROLLFORWARD DATABASE, que carga la copia de back-up de la base de datos y con el archivo de transacciones, existente desde el momento en que se hizo dicho back-up, se recupera la base de datos.

Hay un límite para el número de bloqueos simultáneos, por lo que una transacción muy grande puede ocasionar problemas, por ello será necesario dividirla en dos transacciones o hacer LOCK TABLE (bloqueo de la tabla).

Como el archivo de auditoría crece muy rápidamente es necesario inicializarlo periódicamente, mediante START DATABASE, después de haber hecho una copia de seguridad de la base de datos.

- **Audit trail**

Un *audit trail* es un archivo que registra todos los cambios producidos en una tabla de una base de datos.

Para iniciar un *audit trail* o fichero de pistas, se utiliza la sentencia CREATE AUDIT. Puede hacerse en cualquier momento, y su funcionalidad consiste en que todas las

operaciones que se lleven a continuación se hagan sobre la tabla y sean registradas en el fichero. Para eliminar un fichero de pistas se usa la sentencia DROP AUDIT.

Si existiera un problema con una tabla que deba ser recuperada, se puede hacer mediante la sentencia RECOVER TABLE, una vez que llevó a cabo la copia de back-up y siempre que hubiera creado el fichero de pistas justo antes de hacer la copia de seguridad.

Los ficheros de pistas no son muy utilizados por los inconvenientes que traen aparejados:

- Disminuye el rendimiento del sistema.
- Inciden en el número máximo de tablas abiertas simultáneamente.
- No proveen protección contra operaciones que involucran más de una tabla.

La sentencias que se utilizan para crear un archivo de seguimiento de auditoría y comenzar el registro en el mismo, así como borrarlo se detallan a continuación.

```
CREATE AUDIT FOR {Nombre-Tabla | Sinónimo} IN "pathname
DROP AUDIT FOR {Nombre-Tabla | Sinónimo}
```

Con la sentencia RECOVER TABLE permite recuperar una tabla cuando ocurre un fallo en el sistema, permite recuperar la tabla en cuestión desde una copia backup y un archivo de auditoría.

```
RECOVER TABLE Nombre-Tabla
```

Para poder llevar a cabo las instrucciones anteriores se requiere tener privilegio de Administrador de Base de Datos o ser el propietario.

- **Bloqueos: control de concurrencia**

El acceso de múltiples usuarios a los datos puede producir problemas de consistencia, para evitar estas situaciones, se cuenta con diferentes niveles de bloqueos, *locking*, que proporciona un adecuado nivel de control de concurrencia. En SQL hay dos niveles de bloqueo, a nivel de tabla o a nivel de fila o registro.

- **A nivel de Tabla**

  Si se utiliza de este modo, los demás usuarios pierden toda posibilidad de modificar o ver cualquier fila de la tabla, dependiendo el modo en el que se hizo el bloqueo. Si se efectuó en modo SHARE, los demás usuarios podrán seleccionar datos de la tabla, pero si se hizo en modo EXCLUSIVE no podrán insertar, borrar o actualizar filas de la tabla.

  El usuario deberá tener cuidado con los bloqueos a este nivel, y reservarlos para los casos en los que resulten necesarios por las características de las operaciones a ejecutar, como por ejemplo, demasiadas filas involucradas, operaciones que afecten a más de una tabla, etc.

- **A nivel de Fila o de registro**

  Previsto para operaciones que involucren sólo algunas filas y hay dos posibilidades:

  a) Bloqueos de una fila individual. SQL hace un bloqueo automático de una fila cuando la misma es invocada en una sentencia UPDATE o se trabaja en modo UPDATE desde el menú.

  b) Bloqueos de un grupo de filas. Se utiliza para tratar un conjunto de operaciones como una transacción, lo que además inhibe a los demás usuarios de acceder a esas filas mientras dura la transacción. Para ello se dispone de las sentencias BEGIN WORK y COMMIT WORK para abarcar el conjunto de operaciones. Todas las filas involucradas en las operaciones que allí se efectúan permanecen bloqueadas para los demás usuarios.

También las sentencias de actualización de datos que involucran múltiples filas implican bloqueos sobre las mismas.

Cuando un usuario intenta una operación sobre filas en una tabla que fue bloqueada en modo EXCLUSIVE, SQL retorna un error. Para evitarlo, el usuario puede utilizar la sentencia SET LOCK MODE TO WAIT, con lo que SQL permanecerá en espera hasta que las filas implicadas sean liberadas.

5.3.3. Optimización del rendimiento

Una de las tareas más importantes del Administrador de Base de Datos o el especialista encargado en dicha tarea, es mantener el rendimiento óptimo del servidor de base de datos y de las aplicaciones de bases de datos, esto se consigue mediante las siguientes operaciones:

- Supervisar los recursos del sistema que sean importantes para el rendimiento.
- Identificar las actividades de base de datos que afectan a los recursos importantes.
- Identificar y supervisar las consultas que sean importantes para el rendimiento.
- Utilizar los programas y utilidades del servidor de bases de datos dedicados a supervisar y ajustar el rendimiento.
- Optimizar la ejecución de consultas.
- Eliminar cuellos de botella que afectan al rendimiento llevando a cabo las siguientes tareas:
    - Equilibrar la carga en los recursos del sistema
    - Ajustar la configuración del servidor de base de datos
    - Ajustar la organización de los datos

- Asignar los recursos necesarios para las consultas de soporte de decisiones
- Crear índice que agilicen la recuperación de los datos

Existen varias utilidades que proporciona IBM para mejorar y gestionar el rendimiento del sistema. La mejora del rendimiento se puede abordar desde varios aspectos como son, gestión de la memoria, fragmentación, paralelización y optimización de consultas. En los *Manuales de Informix On-line* se recogen más ampliamente como se pueden utilizar e implementar estas técnicas que pueden mejorar el rendimiento del sistema.

Informix dispone del comando *onstat* para ver y monitorizar que está ocurriendo en el sistema. Por otro lado, con respecto a la configuración del sistema es importante hacer referencia al archivo de configuración ONCONFIG, debido a que los valores de los parámetros que contiene van a determinar el rendimiento del sistema. En la documentación de Ayuda Técnica que proporciona la Aplicación, AGAI, se presenta una tabla donde se indican los valores aconsejables para cada uno de los parámetros en función de las características del sistema. Esta información también aparece en el Manual de Usuario de la aplicación, que está incorporado en este Proyecto de Fin de Carrera (apartado 8.1).

Uno de los aspectos a evaluar es el coste de las consultas que se realizan en la base de datos, esto se consigue mediante el comando SET EXPLAIN O*N*, que inicia la grabación en un fichero denominado *sqexplain.out*, donde se recoge el coste que le ha supuesto al sistema las consultas realizadas y también indica como se accede a la información a través de las tablas, de tal forma que se puede saber si se están combinando correctamente la tablas o si son necesarios nuevos índices que permitan un acceso más rápido y con menor coste. Esta tarea permite mejorar el rendimiento de forma considerable.

También es importante ejecutar el siguiente comando, UPDATE STATISTICS, sincroniza la tabla que se especifique. La forma de llevarlo a cabo es básicamente recorriendo la tabla indicada y actualizando los campos en las tablas de catálogo

correspondientes, que son las utilizadas por el optimizador de la base de datos para elegir el mejor plan a la hora de ejecutar las *queries*. Por ello es recomendable utilizarlo frecuentemente en aquellas tablas cuya tasa de modificación sea alta.

- **FRAGMENTACIÓN**

Para mejorar el rendimiento de las consultas y bloqueos de los datos, una de las técnicas utilizada es la fragmentación. Esta función, que proporciona el servidor de base de datos, permite controlar donde se almacenan los datos a nivel de tabla. La fragmentación permite definir grupos de filas o claves de índice dentro de una tabla, según algún algoritmo o esquema y almacenar cada grupo o fragmento (también denominado partición) en un *dbspace* distinto asociado a un disco físico específico.

Desde la perspectiva del usuario final o aplicación cliente, una tabla fragmentada es idéntica a una tabla no fragmentada. Las aplicaciones cliente no necesitan ninguna modificación para permitirles acceder a los datos de las tablas fragmentadas. Por tanto, con la fragmentación se consiguen mejorar algunos aspectos como son: tiempo de respuesta de un solo usuario, concurrencia, disponibilidad, características de copia de seguridad, restauración y carga de datos.

La estrategia de fragmentación que se implante tendrá diferentes implicaciones en los objetivos indicados anteriormente. Hay que tener en cuenta que la fragmentación requiere cierta actividad adicional de administración y supervisión. Por este motivo es importante antes de crear una tabla fragmentada, elegir una estrategia de fragmentación adecuada, para ello es necesario conocer que procesos acceden a la información de la tabla.

Un esquema de distribución es un método que utiliza el servidor de base de datos para distribuir filas o entradas de índice a fragmentos. Los servidores de bases de datos Informix dan soporte a los siguientes esquemas de distribución:

- *Basado en expresiones*: se colocan filas que tienen valores especificados en el mismo fragmento.

- *Circular*: se colocan las filas una tras otra en fragmentos, rotando por las series de fragmentos para distribuir las filas de forma uniforme. (Se especifica FRAGMENT BY ROUND ROBIN en la sentencia CREATE TABLE).

- *Distribución por rango*: se distribuyen las filas entre fragmentos según valores enteros mínimos y máximos que especifica el usuario. (Se especifica FRAGMENT BY RANGE en la sentencia CREATE TABLE).

- *Hash* definido por el sistema: se utiliza una norma interna definida por el sistema que distribuye las filas con el objetivo de conservar el mismo número de filas en cada fragmento. (Se especifica FRAGMENT BY HASH en la sentencia CREATE TABLE).

- *Híbrido*: sistema de distribución que combina dos esquemas de distribución. (Se especifica FRAGMENT BY HYBRID en la sentencia CREATE TABLE).

La fragmentación se indica en la sentencia de creación, a continuación se presenta un ejemplo de un tipo de fragmentación de tabla:

```
CREATE TABLE  <nombre_tabla>  (<nombre_columna, ...>
FRAGMENT BY EXPRESSION
        <nombre_columna> <operador> <valor> IN dbaspace_x
         <nombre_columna> <operador> <valor> IN dbaspace_y
         ...
```

El operador en la sentencia anterior, puede ser un operador relacional o lógico de SQL, y define los límites de cada fragmento en una tabla. Puede contener los siguientes operadores:

- Operadores relacionales >, >, <=, >=

- Operadores lógicos AND y OR

- Expresiones algebraicas, incluyendo las funciones incorporadas

La forma de actuación de una inserción y actualización de una fila del servidor de base de datos cuando una tabla está fragmentada, consiste inicialmente en evaluar las expresiones de los fragmentos para comprobar si la fila pertenece a alguno de los fragmentos. Si es así, el servidor de base de datos inserta o actualiza la fila en el fragmento correspondiente. Si la fila no pertenece a ninguno de los fragmentos, se colocará en el fragmento que especifica la cláusula restante. Si no se incluye ninguna cláusula restante y la fila no coincide con los criterios correspondientes a ninguna de las expresiones de fragmento existentes, el servidor de base de datos devuelve un error.

La fragmentación, como hemos indicado anteriormente, se puede definir al mismo tiempo que se crea la tabla, pero también se puede realizar sobre tablas ya existentes no fragmentadas. Los párrafos anteriores dan una visión general de los diferentes tipos de fragmentación que se pueden llevar a cabo. Existen varios casos en los que es necesario convertir tablas no fragmentadas en tablas fragmentadas:

- Cuando tiene una versión implantada por una aplicación de fragmentación de tablas. Probablemente se desea convertir varias tablas pequeñas en una tabla fragmentada.

- Cuando tiene una tabla grande que desea fragmentar.

Las sentencias en INFORMIX que permiten combinar dos o más tablas no fragmentadas en una sola tabla fragmentada es la cláusula ATTACH de la sentencia ALTER FRAGMENT, es necesario que las tablas no fragmentadas tengan idénticas estructuras y deben estar almacenadas en distintos *dbspaces*.

Y en el caso que se desee fragmentar una tabla a partir de una no fragmentada, se utiliza la cláusula INIT en la sentencia ALTER FRAGMENT.

```
ALTER FRAGMENT ON TABLE <nombre_tabla>  INIT
        FRAGMENT GY ROUND ROBIN IN dbsapece1, dbspace2, dbspace3
```

También, se puede modificar la fragmentación de una tabla o un índice, para ello *Dynamic Server* utiliza las cláusulas ADD, DROP y MODIFY que combinan la estrategia de fragmentación, añaden, eliminan o modifican los fragmentos existentes.

ALTER GRAGMENT ON TABLE <*nombre* tabla> ADD <*dbespace*>.

ALTER GRAGMENT ON TABLE <*nombre* tabla> DROP <*dbespace*>.

ALTER GRAGMENT ON TABLE <*nombre*tabla> MODIFY <*dbespace*> TO <*condición*>

Las tablas que utilizan la fragmentación HASH no soporta las opciones anteriores, sino INIT, DETACH y ATTACH. Que consiste que cuando se requiere un cambio la estrategia de fragmentación de la tabla es necesario un movimiento de datos, y con la cláusula INIT el servidor de base de datos crea una copia de la tabla con el nuevo esquema de fragmentación e inserta filas procedentes de la tabla original en la nueva tabla y se utiliza DETACH y ATTACH cuando sólo es necesario modificar las expresión de un fragmento existente, eliminando o volviéndolo a conectar.

A los fragmentos se les pueden otorgar y revocar privilegios, pero en fragmentaciones basadas en expresiones, mediante la utilización de las sentencias GRANT FRAGMENT y REVOKE FRAGMENT.

5.4. AUDITORÍA EN INFORMIX

5.4.1. Introducción

El objetivo fundamental de la auditoría es obtener información de las operaciones que cada usuario realiza sobre los objetos de una base de datos.

La auditoría de base de datos debe incluir en su ámbito las modificaciones de la estructura de objetos de la base de datos. Debido a que dichas operaciones pueden tener una influencia importante en el nivel de acceso a los datos.

La auditoría puede establecerse sobre distintos aspectos:

- Las basadas en estadísticas sobre el número de operaciones realizadas sobre un objeto de Base de Datos, por cada usuario. O bien, se toma la información de todas las operaciones que recibe el gestor o bien registra esos datos de forma periódica.

- Aquellas que incluyen todas las operaciones realizadas sobre cada objeto, los cambios producidos sobre el contenido de los datos y/o la estructura y los accesos al contenido.

- Y las referentes a las copias de seguridad y reconstrucción de los datos.

5.4.2. Análisis de la Auditoría

Los mecanismos de auditoría están diseñados para detectar y revisar los intentos de violaciones de seguridad. Los datos que se generan en la auditoría solamente son útiles si son analizados y revisados, de no ser así es equivalente a tener deshabilitado la auditoría en el sistema.

Con el análisis y revisión de los datos generados por la auditoría, se detectan actividades sospechosas. Esto constituye el primer paso para identificar posibles

violaciones de seguridad que se estén produciendo. Mediante las pistas de auditoría nos permiten reconstruir los eventos que han llevado a la violación.

Existen dos formas de analizar los registros de auditoría, una forma más simple consiste en mostrar los datos que aparecen en dichos archivos y tratar la información con herramientas de análisis de auditoría. La otra manera consiste en descargar la información en un formato que pueda ser cargado en una tabla, de manera que sea tratado mediante sentencias SQL y así generar informes basados en estos datos. La utilidad ONSHOWAUDIT extrae la información de los registros de auditoría y la deja preparada para ser vista o manipulada por cualquiera de las dos formas indicadas anteriormente.

La siguiente imagen presenta de forma gráfica las formas de extraer la información generada por la auditoría.

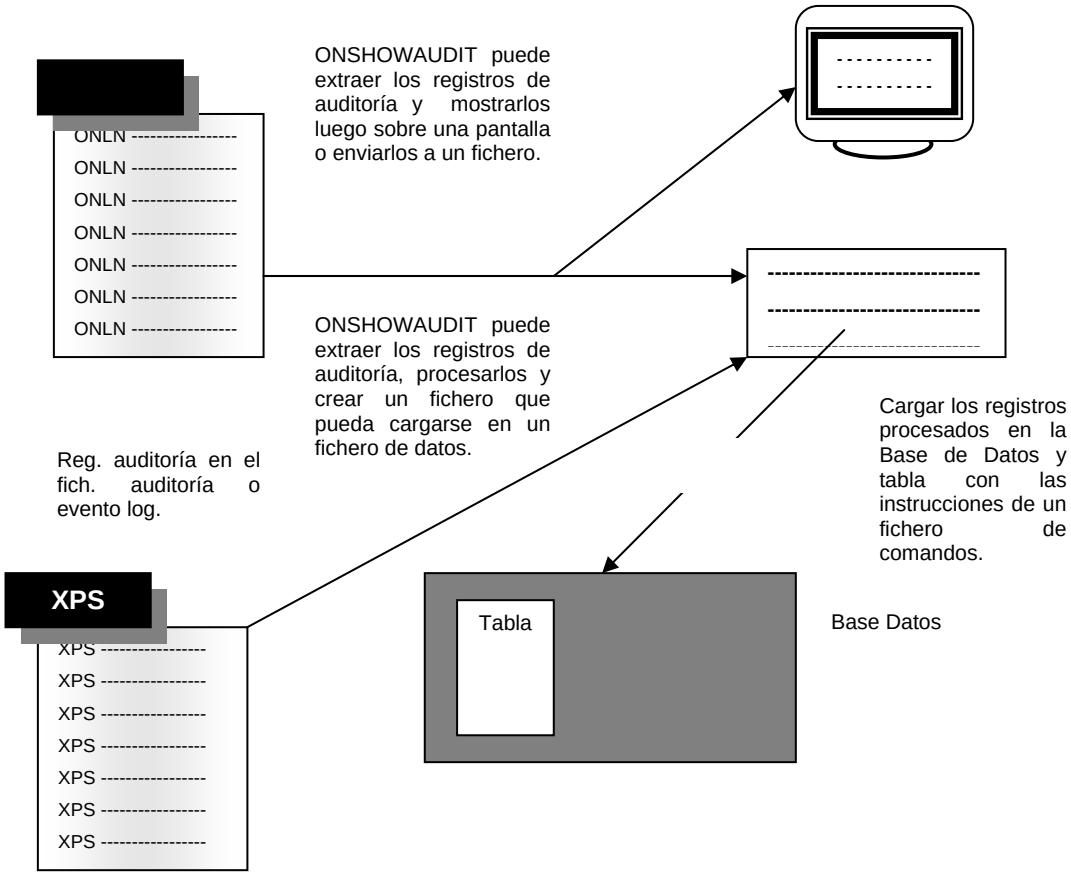


Ilustración 9. Extracción de información del fichero de auditoría

Las operaciones fallidas son el indicador más común cuando existe un problema de seguridad, aunque de igual importancia es la realización de una operación de forma correcta que corresponde a una actividad inusual para un determinado usuario.

La primera amenaza a la seguridad de una base de datos es el acceso no autorizado o la modificación de información reservada. Por ello son importantes los registros de auditoría que indican intentos fallidos, por ejemplo, accesos a datos por usuarios que no tienen permiso sobre ellos. También existen ataques internos, se trata de usuarios no autorizados con intenciones maliciosas que intentan obtener información reservada. Existen otro tipo de usuarios que buscan a través de los datos almacenados, localizar u obtener información sin una legítima necesidad. Normalmente estos usuarios ejecutan un gran número de similares consultas, muchas de las cuales son fallidas porque no tienen los suficientes privilegios. Estas indicaciones hacen que se relativamente fácil identificarlos en el fichero de pistas de auditoría.

Una vez identificados el usuario o usuarios que son responsables de irregularidades en la seguridad, a través de las pistas de auditoría *(trail file*), es necesario llevar a cabo un conjunto de acciones que nos permita encontrar la solución, como por ejemplo:

- Habilitar nuevos controles de auditoría para identificar el problema.
- Desarrollar un plan con la supervisión de los usuarios para tratar el problema.
- Hacer frente el caso de forma individual.
- Desconectar el servidor de base de datos para que no fluya la información no autorizada.

5.4.3. Roles para la Auditoría

Informix contempla la existencia de un rol "*Auditing Analysis Officer*" (AAO) que realiza las auditorías de los registros de los tipos específicos de actividades de la base de datos. De tal forma que si alguien intenta burlar o corromper los mecanismos de seguridad de la base de datos, se podrían rastrear estas acciones.

Durante la instalación de Informix se solicitará crear grupos y usuarios adicionales y añadir usuarios a los grupos. Informix propone una serie de grupos, con los siguientes nombres por defecto, cada uno ellos abarca una funcionalidad en la base de datos. A continuación se detallan, así como su funcionalidad:

Nombre de grupo por omisión	Categoría de función	Funcionalidad
Ix_dbsa **(INFORMIX-ADMIN)**	Administrador de base de datos	Realiza tareas administrativas generales como, por ejemplo, el almacenamiento y restauración de datos, la supervisión del uso y su rendimiento, así como el ajuste del sistema
Ix_aao	Auditing Analysis Officer (AAO)	Realiza una auditoría de los registros de los tipos específicos de actividades de la base de datos. Si alguien intenta corromper el mecanismo de seguridad de la base de datos, se podrán rastrear estas acciones.
Ix_dbsso	Database System Security Officer (DSSO)	Mantiene la seguridad del servidor de bases de datos. El objetivo de esta función incluye el ajuste de auditorías y el cambio de características de seguridad de objetos de almacenamiento.
Ix_users	Usuarios de la base de datos	Accede a la base de datos para realizar tareas de usuario. Con la separación de funciones habilitadas, sólo los usuarios que están designados como miembros del grupo ix_users pueden acceder a la base de datos.

El encargado de la auditoría necesita especificar y mantener la configuración de la auditoría, que debe incluir:

- El modo de auditoría. (Se puede establecer diferentes forma de llevarla a cabo, por ejemplo indicar tipo de gestión, realizada por el sistema operativo o por el servidor, de forma automática o no, etc)
- El directorio donde se van a ubicar las pistas de auditoría.
- El tamaño máximo de un fichero de auditoría antes de empezar automáticamente otro fichero.
- Como se va a comportar el Servidor si ocurre un error cuando está generando el registro de auditoría.

Existen varias posibilidades para configurar los parámetros de auditoría, mediante la utilidad ONAUDIT o directamente sobre el fichero que contiene toda la información de la auditoría, ADTCFG, que en los próximos puntos se explicará con más detalle.

Para obtener más información sobre los parámetros de configuración del sistema se puede ver a través del archivo ONCONFIG, existe uno para cada servidor de base de datos.

5.4.4. Tipos de gestión de la auditoría

5.4.4.1. Pistas de Auditoría

La información que se genera en una auditoría es almacenada e un "*audit trail*" (pistas de auditoría), es un archivo que contiene información de todas las inserciones, modificaciones, supresiones, actualizaciones y manipulaciones de las tablas de la base de datos. Este fichero tiene un propósito similar a un log, es utilizado para mantener una historia de las operaciones sobre la base de datos y su restauración.

Mediante el siguiente comando se crea un archivo de pistas de auditoría, es aconsejable, si se dispone de más de un disco almacenarlo en lugar diferente a donde se encuentran la base de datos.

```
CREATE AUDIT  FOR nombre_tabla IN “ruta”

DROP AUDIT FOR nombre_tabla
```

Se debe realizar una copia de la tabla antes de empezar la auditoría. Además de otra copia del propio fichero “*audit trail*”, para poder hacer la recuperación en caso de producirse algún problema. La sentencia para recuperar la tabla en caso de que exista algún tipo de problema se lleva a cabo desde la copia de seguridad y el archivo de auditoría.

```
RECOVER TABLE
```

Hay que tener en cuenta, que todo control adicional sobre el sistema tiene un coste en rendimiento, por ello en muchas ocasiones no son muy utilizados los “*audit trails*” u otras herramientas.

5.4.4.2. Las máscaras de Auditoría

En Informix la auditoría se puede implementar a través de eventos, que se define como la actividad que podría potencialmente alterar o revelar un dato. Existe un registro de eventos donde se guarda aquellos hechos que se han realizado correctamente o han sufrido algún fallo.

Estos eventos son implementados mediante máscaras de auditoría, de tal forma que una mascara tiene asociado un identificador de usuario y una acción específica, que quedará registrada cuando dicho usuario la lleve a cabo.

Existen cuatro tipos de máscara de auditoría:

Tipo	Nombre máscara
Máscaras para usuarios de forma individual	Nombre_usuario
Máscara por defecto	_default
Máscaras obligatorias	_require y _exclude
Plantilla de máscaras	_nombremáscara

Las máscaras que proporciona Informix son _default, _require y _execute, son para todos los usuarios del sistema. Además de estas se pueden definir máscaras específicas para determinados usuarios. Con las máscaras de usuarios se permite auditar más a unos usuarios que a otros.

La forma como aplica las máscaras Informix es la siguiente, cuando un usuario accede a la base datos el Servidor comprueba si existe una máscara individual con el mismo nombre de usuario que está siendo utilizado por el usuario. Si existe, se aplican las instrucciones de auditoría de la máscara encontrada, si no existe el Servidor lee y aplica las instrucciones de la máscara _default. Las máscaras _require y _exclude se aplican a todos los usuarios.

La máscara _require audita a cada uno de los usuarios del servidor de bases de datos, con esta se puede realizar la mayoría de la auditoría, además de permitir realizar los cambios de configuración, añadiendo y eliminando elementos desde esta máscara, de forma más rápida.

La máscara _exclude es la última que se lee, como su nombre indica, los eventos que se especifican son excluidos de la auditoría. Un buen candidato para incluir en esta máscara es el evento “Read Row”, lectura de una fila, es un evento que genera una gran cantidad de registros y a menos que se desee auditar los datos, no suele ser necesario dicha información.

Las máscaras y sus eventos son denominados instrucciones de auditoría.

Como hemos indicado con anterioridad los eventos son almacenados en un fichero de forma abreviada, con un nemotécnico formado por cuatro letras. La siguiente tabla muestra los eventos auditables por Informix, indicando su nemotécnico y significado.

Nemotécnico	Nombre Evento	Nemotécnico	Nombre evento
ACTB	Acceso Tabla	**GRTB**	Dar permiso acceso tabla
ADCK	Añadir Chunk	**INRW**	Insertar fila
ADLG	Añadir Log de transacciones	**LGDB**	Cambio log modo BD
ALFR	Modificar Fragmentos	**LKTB**	Bloquear tabla
ALIX	Modificar Indice	**LKTB**	Listar marcas de auditoría
ALME	Modificar método de acceso	**LSDB**	Listar Bases de datos
ALOP	Modificar cluster optico	**MDLG**	Modificar log transacción
ALTG	Modificar Tabla	**ONAU**	Onaudit
BGTX	Inicio Transacción	**ONCH**	Oncheck
CLDB	Cerrar Base de Datos	**ONIN**	Oninit
CMTX	Commit transacción	**ONLG**	Onlog
CRAM	Crear Máscara de auditoría	**ONLO**	Onload
CRBS	Crear Blobspace	**ONMN**	Onmonitor
CRBT	Crear Tipo opaco	**ONMO**	Onmode
CRCT	Crear Cast	**ONPA**	Onmparams
CRDB	Crear Base de Datos	**ONSP**	Onspaces
CRDS	Crear Dbspace	**ONST**	Onstat
CRDT	Crear tipo distinct	**ONUL**	Onunload
CRIX	Crear Indice	**OPDB**	Abrir Base de Datos

Nemotécnico	Nombre Evento	Nemotécnico	Nombre evento
CRME	Crear método de acceso	**RDRW**	Leer fila
CRNRT	Crear tipo nombramiento fila	**RLOP**	Cluster
CROC	Crear clase operador	**RLTX**	Rollback transacción
CROP	Crear Cluster	**RMCK**	Limpieza chunks espejos
CRRL	Crear Rol	**RNBD**	Renombrar base de datos0
CRSN	Crear sinónimo	**RNTC**	Renombrar Tabla/Columna
CRSP	Crear procedimiento almacena	**RSOP**	Reservar cluster
CRTB	Crear tabla	**RVDB**	Borrar acceso base de datos
CRTR	Crear trigger	**RVFR**	Borrar acceso a fragmento
CRVW	Crear vista	**RVRL**	Borrar rol
DLRW	Borrar fila	**RVTB**	Borrar acceso a tabla
DNCK	Trayendo Chunck fuera de line	**SCSP**	Comando del sistema, procedimiento almacenadc
DNDM	Deshabilitar disco espejo	**STCN**	Establecer restricciones
DRAM	Borrar mascara de auditoría	**STDF**	Establecer fichero debuf
DRBS	Borrar blobspace	**STDP**	Establecer password base datos
DRCK	Borrar chunk	**STDS**	Establecer puntos de ruptura
DRCT	Borrar cast	**STEX**	Establecer explain
DRDB	Borrar base de datos	**STIL**	Establecer nivel insolation
DRDS	Borrar dbspace	**STLM**	Establecer modo bloqueo
DRIX	Borrar índice	**STOM**	Establecer modo objeto
DRLG	Borrar Log transaction	**STOP**	Detener estamento

Nemotécnico	Nombre Evento	Nemotécnico	Nombre evento
DRME	Borrar método de acceso	**STPR**	Establecer prioridad
DRNRT	Borrar nombrado tipo fila	**STRL**	Establecer rol
DROC	Borrar clase operador	**STRT**	Iniciar instrucción
DROP	Borrar cluster	**STSA**	Establecer sesión autorización
DRRL	Borrar rol	**STSN**	Establecer nueva sesión
DRSN	Borrar sinónimo	**STIX**	Establecer modo transacción
DRSP	Borrar procedim. almacenado	**TMOP**	Tiempo cluster
DRTB	Borrar tabla	**ULTB**	Desbloqueo tabla0
DRTR	Borrar trigger	**UPAM**	Modificar mascara de auditoría
DRTY	Borrar tipo	**UPCK**	Traer chunck on-line
DRVW	Borrar vista	**UPDM**	Habilitar espejo del disco
EXSP	Ejecutar procedim. almacenado	**UPRW**	Modificar fila actual
GRDB	Dar permiso acceso BD	**USSP**	Modificar estadísticas, procedimiento almacenadc
GRFR	Dar permito acceso fragmentad	**USTB**	Modificar estadísticas, tabla
GRRL	Dar permiso rol		

En la tabla anterior se ha incluido la palabra *chunk*, que definimos como la unidad mínima de disco que el Sistema Operativo puede asignar. Teniendo en cuenta que un *dbspace* es la unidad de asignación de espacio de informix, de tal forma que a un *dbspace* se le puede asignar uno o más chunks, que irán aumentando en número a medida que se vaya necesitando más espacio en el *dbspace*.

Informix, establece un tamaño máximo de 2GB. La forma de agregar a un *dbspace* es utilizando la herramienta ONMONITOR, accediendo a la opción *dbspaces* y por último "Add Chunk".

Todas las máscaras utilizadas por el Servidor son almacenadas en la tabla sysaudit en el sysmaster de la base de datos. Aunque esta información se puede acceder a través de sentencias SQL, también existe la utilidad ONAUDIT para la creación y mantenimiento de todas las máscaras de auditoría.

En el proceso de auditoría consiste en almacenar los registros en un fichero denominado "fichero de auditoría" donde se almacenan la información generada que es gestionada por el sistema operativo o el Servidor Universal.

5.4.4.3. Los ficheros de Auditoría

La auditoría genera unos ficheros que recogen las pistas de auditoría. Informix proporciona unas utilidades que permiten extraer la información, se puede especificar un formato determinado que permite cargarlo en la base de datos y posteriormente manipularla mediante sentencias SQL.

Los ficheros de auditoría están localizados en un directorio que puede indicarse con la utilidad onaudit o mediante el parámetro ADTPATH en el fichero $INFORMIXDIR/aaodir/adtcfg.

Con respecto a la nomenclatura que reciben los ficheros de auditoría esta definida en el fichero ONCONFIG, y a medida que se van generando ficheros se le añade un número, comenzando con el 0.

El encargado de administrar el proceso de auditoría, debe determinar el tamaño óptimo, teniendo en cuenta la configuración del sistema y la auditoría a realizar. Es importante indicar que ficheros con gran capacidad genera menor número de archivos pero son más difíciles de manipular.

Un aspecto muy importante es el control de acceso a estos ficheros, los cuales no deberían estar disponibles para ser vistos o modificados por los usuarios estándar, debido a que cualquier imprudencia puede originar pérdida de información. Por ello el

encargado de administrarlos debe almacenarlos en directorios donde este implementado el correcto nivel de permisos de accesos.

5.4.5. Configuración

Para que Informix lleve a cabo la auditoría del sistema, según la configuración fijada, es necesario habilitarla. De esta forma el Servidor Universal o el Sistema Operativo, en función de la configuración, generará los registros de auditoría por cada evento que se haya especificado en las instrucciones de auditoría.

Si son gestionados por el Servidor Universal los registros de auditoría son almacenados en un fichero llamado "*audit. trail*". El *audi. trail* (pistas de auditoría) puede estar formado por más de un fichero de auditoría. Si es gestionado por el Sistema Operativo, la información es almacenada en unos ficheros del sistema operativo.

La configuración de la auditoría está recogida en los parámetros del fichero $INFORMIX/aaodir/adtcfg, también conocido como el fichero ADTCFG. Los parámetros son ADTERR, ADTMODE, ADTPATH y ADTSIZE.

También puede utilizarse la utilidad "onaudit" para realizar cambios en la configuración de la auditoría, que son escritos en un fichero denominado adtcfg.servernum, donde SERVERNUM es un parámetro que se encuentra en el fichero ONCONFIG. El Administrador o encargado de la auditoría debe copiar manualmente los cambios desde el fichero adtcfg.servernum al fichero ADTCFG.

La utilidad "onaudit" permite realizar las siguientes tareas:

- Mostar, crear, modificar y borrar las máscaras de auditoría
- Empezar un nuevo fichero de auditoría
- Mostrar la configuración de la auditoría
- Cambiar de forma genérica las actividades de la auditoría
- Habilitar y deshabilitar la auditoría

- Establecer el modo de actuación ante errores
- Establecer ubicación de donde colocar el fichero de auditoría y tamaño máximo
- Determinar si gestiona el fichero de auditoría el Servidor o el sistema operativo

La sentencia y formato en que se presenta la actual configuración de la auditoría de un sistema es la siguiente:

```
onaudit –c

Onaudit -- Audit Subsystem Control Utility
Copyright (c) Informix Software, Inc., 1997

Current audit system configuration:
        ADTMODE = 1
        ADTERR = 0
        ADTPATH = /tmp
        ADTSIZE = 20000
        Audit file = 64
```

Los parámetros que admite “onaudit” y pueden cambiar la configuración son los siguientes, se encuentran en el fichero ADTCFG y en el parámetro que se indica a continuación:

-e	**Manejo de errores**	Admite los valores 0, 1 y 3. Parámetro ADTERR. Valor 0: continúa procesando y anota el error en el log. Valor 1: suspende el procesamiento cuando no puede grabar un registro en el fichero de auditoría actual, continua hasta que lo consigue.

		Valor 3: El servidor está desconectado.
-l	**Modo de auditoría**	Admite los valores 0, 1, 2, 3, 4, 5, 6, 7, 8. Parámetro ADTMODE. Valor 1: Cambio para ser gestionado por el Servidor la auditoría, pero no de forma automática. Valor 2: Cambio para ser gestionado por el S.O. la gestión de auditoría, pero no de forma automática. Valor 3: Cambio para ser gestionado por el Servidor la auditoría automáticamente. Valor 4: Cambio para ser gestionado por el S.O. la auditoría automáticamente. Valor 5: Cambio para ser gestionado por el Servidor y automáticamente auditar acciones el administrador del servidor. Valor 6: Cambio para ser gestionado por el S.O. y automáticamente auditar las acciones el administrador del servidor. Valor 7: Cambio para ser gestionado por el Servidor la auditoría y automáticamente auditar las acciones el administrador del Servidor y el DBSSO (The Database System Security Officer). Valor 8: Cambio para ser gestionado por el S.O. y automáticamente auditar las acciones el administrador del Servidor y el DBSSO.
-p	**Nombre del directorio donde crear el fichero auditoría.**	Parámetro ADTPATH.
-s	**Tamaño máximo del fichero de auditoría.**	Parámetro ADTSIZE.

La utilidad “onshowaudit” permite realizar las siguientes tareas:

- Extraer información de auditoría del fichero de auditoría
- Preparar la información del fichero para realizar dbload (descarga en un fichero)

Si se ha realizado una separación de roles, solamente puede ejecutar esta utilidad el AAO, pero si no se ha realizado, solo la podrá realizar los usuarios informix y root.

Sintaxis:

Onshowaudit –I -f path -u username -s servername -l –O

- I /O	utiliza las pistas de auditoría de Informix / del Sistema Operativo
- f	el nombre de fichero de pistas de auditoría a examinar, puede ser omitido si con la utilidad onaudit o en el fichero ADTCFG se ha indicado el parámetro que contiene esta información.
-s	Nombre del Servidor de Base de datos de donde extraer la información de auditoría.
-u	Especificar el nombre del login de un usuario acerca del cual extraer la información de auditoría.
- l	Directiva para formatear la información extraída y poder realizar un dbload.

5.4.6. Administración de la Auditoría

El conjunto de tareas que el administrador de la auditoría debe realizar, podemos considerar que las más importantes son las siguientes:

- Administración y separación de los roles.
- Mantenimiento de las máscaras de auditoría.
- Establecer configuración de la auditoría.

Informix aconseja la existencia de tres roles que participen en la auditoría, el Administrador del Servidor, la persona responsable de la seguridad del sistema de la base de datos y el de la Auditoría.

El Administrador del Servidor es el encargado de configurar la seguridad en la base de datos durante la instalación y definir los roles. Las roles que lleven a cabo el control de la auditoría deberían ser personas que tengan los permisos necesarios sobre la base de datos, esto se consigue mediante la designación de cuentas de usuarios con dichos privilegios.

La persona encargada de la seguridad de la base de datos es quien lleva a cabo tareas relacionadas con el mantenimiento de la seguridad de la base de datos, entre estas se incluye: mantener las máscaras de auditoría, resolver los problemas de seguridad y educar y formar a los usuarios. Estas tareas pueden ser llevadas a cabo mediante la utilidad **onaudit.**

Este rol, DBSSO (*Database System Security Officer*) debe diseñar las cuentas de usuario y conocer los requerimientos de control de acceso, sus acciones deben ser auditadas, debido al poder que le da el acceso y herramientas que posee y así reducir posibles riesgos. La figura del encargado de analizar la Auditoría se encarga de configurar el sistema para la auditoría, leer y analizar las pistas de auditoría. Estos ficheros pueden ser cargados en la base de datos para ser analizados mediante la utilización de SQL, incluso se pueden desarrollar aplicaciones con Informix SQL API que lo lleven a cabo. Estas tareas son llevadas a cabo con las utilidades **onaudit** y **onshowaudit**.

Con respecto a las máscaras, es muy importante su configuración y mantenimiento, nos permite tener un control sobre ciertos tipos de actividades realizadas por usuarios determinados, así como otras acciones que requieran su control.

Con respecto a la configuración de la auditoría no es una tarea que se inicia de forma automática, antes de que las acciones de los usuarios sean auditadas debe realizarse una serie de tareas de configuración como son: especificación de los eventos a auditar, usuarios y máscaras a utilizar, indicar el directorio donde guardar los logs, especificar como debe comportarse el sistema ante un error mientras se está escribiendo en un fichero de auditoría, determinar el nivel de auditoría y activar o

desactivar controles de auditoría. También, muchas de estas tareas son realizadas con la utilidad **onaudit**.

5.4.7. Implicaciones de la Auditoría

La auditoría nos proporciona información y seguridad en el sistema, pero tiene efectos directos sobre la cantidad de recursos del sistema operativo, la base de datos y los dispositivos de almacenamiento que son utilizados. Si se generan una gran cantidad de registros de auditoría se necesita mucho espacio libre de almacenamiento, gran cantidad de tiempo de procesador para procesar los registros de auditoría.

Los siguientes factores determinan en gran medida la cantidad de recursos del sistema a utilizar:

- Número de usuarios /eventos auditados
- Configuración del procesador
- Sistema y carga de usuarios
- Espacio de disco
- Carga de trabajo

Informix puede activar o desactivar la auditoría del sistema, y en caso de estar activado determinar el nivel de auditoría, entre los valores de 0 a 8, recogido en el parámetro ADTMODE del fichero ADTCFG.

5.4.8. Recomendaciones

Informix recomienda que las acciones del administrador de auditoría o el usuario informix, sean siempre auditadas, para reducir el riesgo de usuarios sin escrúpulos que abusen del poder que poseen. También considera importante una separación de tareas a realizar, mediante la asignación de roles diferentes.

Así como configurar, administrar y estudiar las máscaras, pistas de auditoría y otros mecanismos que se hayan implementado, porque son la fuente de información que va a determinar los errores o malas prácticas que se estén produciendo en el sistema.

Todas estas tareas en gran medida son llevadas a través de las utilidades onaudit y onshowaudit. No obstante, es aconsejable la creación de programas en informix que automatice el control del sistema, de tal forma que el tiempo de solución ante problemas sea el menor posible, así como los costes en recursos humanos que son también muy elevados.

CAPÍTULO 6

COPIAS DE SEGURIDAD Y RESTAURACIÓN

6. COPIAS DE SEGURIDAD Y RESTAURACIÓN

6.1. INTRODUCCIÓN

Un sistema de recuperación permite hacer una copia de seguridad de los datos del servidor de base de datos, para posteriormente poder restaurarlos si los datos actuales se dañan o dejan de ser accesibles. Los datos se pueden dañar o perder debido a causas que pueden comprender desde un error de programa o un error de disco hasta un desastre que afecte a todo el sistema.

6.1.1. Las copias de Seguridad

Una copia de seguridad es una copia de uno o más espacios de la base de datos (también denominados espacios de almacenamiento) y de los archivos de anotaciones lógica que mantiene el servidor de base de datos y que contiene registrada la actividad del servidor de base de datos que se ha producido entre procesos de copias de seguridad.

La copia de seguridad se escribe normalmente en un soporte de almacenamiento secundario, como puede ser un disco, una cinta magnética o un disco óptico. Es recomendable guardar el soporte de almacenamiento fuera de línea y conservar una copia fuera del lugar de trabajo.

Es importante indicar que las copias de seguridad de bases de datos no sustituyen a las copias de seguridad normales realizadas por el sistema operativo, que copia archivos diferentes a los archivos de la base de datos de Informix.

No siempre es necesario hacer una copia de seguridad de todos los espacios de almacenamiento. Aquellas tablas que cambian con poca frecuencia no es necesario que se copien cada vez que se realiza una copia de seguridad de los datos del servidor de base de datos. Por tanto, es necesario planificar detenidamente un plan de copias de seguridad para evitar largas esperas durante el proceso.

Todo sistema de copias de seguridad para el servidor de bases de datos requiere una planificación adecuada, para ello es necesario analizar la configuración y actividad de su servidor de bases de datos y los tipos de soporte de copia de seguridad disponibles en el sistema.

Los sistemas de bases de datos proporcionan programas de utilidad para realizar las copias de seguridad y restauración de los datos en un servidor de base de datos.

6.1.2. La recuperación de una base de datos

Un sistema de recuperación permite hacer una copia de seguridad de los datos del servidor de base de datos y luego restaurarlos si los datos actuales se dañan o dejan de ser accesibles. El Administrador de la Base de datos tiene entre sus tareas la realización de las copias de seguridad y la recuperación en caso de que se produzcan fallos. Debe conocer con anticipación los tipos de fallos que pueden ocurrir y devolver la base datos a su estado normal lo más rápidamente posible.

El Auditor de Bases de Datos, al igual que el Administrador de la Base de Datos, debe conocer todos estos procedimientos para poder supervisarlos y revisarlos durante una auditoría de Base de Datos.

El Administrador de Base de datos, para realizar de forma satisfactoria las recuperaciones, debe anticiparse a los tipos de fallo que pueden ocurrir, escoger el método de backup, comprobar que se realizan correctamente las copias y estar familiarizado con las estrategias de recuperación.

Los datos se pueden dañar o perder debido a causas que pueden comprender desde un error de programa o un error de disco hasta un desastre que afecte a todo el sistema. Un sistema de recuperación permite recuperar datos que se han perdido debido a esas anomalías. A continuación se presenta una posible clasificación:

- Errores de usuario
- Error en la ejecución de una sentencia
- Fallo del SGBD

- Fallo de medio

El proceso de restauración reconstruye los datos del servidor de base de datos a partir de espacios de almacenamiento y archivos de anotaciones lógicas de copia de seguridad. La restauración reconstruye los datos que han pasado a ser inaccesibles por alguna de las razones que continuación se van a exponer.

Para restaurar datos al estado que tenían cuando se produjo el error, debe existir como mínimo una copia de seguridad completa de cada espacio de almacenamiento antes del error y los archivos de anotaciones lógicas donde residen todas las transacciones producidas desde la realización de esas copias de seguridad.

Para realizar todo este proceso, el SGBD proporciona una serie de funcionalidades que ayudan a la recuperación de la base de datos, entre las que se encuentra:

- Mecanismo de copia de seguridad mediante el cual se hagan copias de seguridad periódicas de la base de datos.
- Registro que mantengan el control del estado actual de las transacciones y de los cambios realizados en la base de datos.
- Una funcionalidad de puntos de comprobación que permita que las actualizaciones de la base de datos que están llevándose a cabo se hagan permanentes.
- Un gestor de recuperación que permita al sistema restaurar la base de datos a un estado coherente después de un fallo.

El SGBD debe proporcionar un mecanismo que permita realizar copias de seguridad de la base de datos y del archivo de registro a intervalos periódicos sin necesidad de detener el sistema. Esta copia de la base de datos puede ser completa o incremental, compuesta sólo por las modificaciones realizadas desde la última copia incremental o completa.

El problema de recuperación y concurrencia en un sistema de base de datos está muy ligado a la noción de *procesamiento de transacciones*. A continuación ampliamos este aspecto, así como su funcionamiento, que nos va a permitir entender mejor como es posible la restauración de la información a un punto después de haber ocurrido un fallo que la ha dejado inconsistente. También es importante para la Auditoría y monitorización de rendimiento, el registro de anotaciones que se va completando y que aporta información que permite conocer el sistema y así, localizar posibles errores.

- **TRANSACCIONES**

Las transacciones representan la unidad de recuperación básica en un sistema de base de datos. Dicho de otra forma, una transacción es una secuencia de operaciones en una base datos mediante la cual un estado consistente de la base de datos se transforma en otro estado consistente, sin conservar por fuerza la consistencia en todos los estados intermedios.

Para controlar las transacciones de la base de datos que se van ejecutando, el SGBD mantiene un archivo especial denominado *registro* que contiene la información sobre todas las actualizaciones realizadas en la base de datos. Las operaciones en SQL COMMIT Y ROLLBACK son la clave de su funcionamiento. COMMIT indica que una transacción ha finalizado con éxito al SGBD, mientras que ROLLBACK indica al SGBD que debe recuperar su estado justo en el momento anterior a comenzar la transacción que no ha podido finalizar.

Para garantizar la integridad de los datos se necesita que el sistema de base de datos mantenga las siguientes propiedades en las transacciones:

- Atomicidad. Todas las operaciones de la transacción se realizan adecuadamente en la base de datos, o ninguna de ellas.

- Consistencia. La ejecución aislada de la transacción (es decir, sin otra transacción que se ejecute concurrentemente) conserva la consistencia de la base de datos.

- Aislamiento. Aunque se ejecuten varias transacciones concurrentes, el sistema garantiza cada transacción. De tal forma que cada transacción ignora el resto de las transacciones que se ejecuten concurrentemente en el sistema.

- Durabilidad. Tras la finalización con éxito de una transacción, los cambios realizados en la base de datos permanecen, incluso si hay fallos en el sistema.

En ausencia de fallos, todas las transacciones se completan con éxito. Sin embargo, una transacción puede que no siempre termine su ejecución con éxito, en este caso se denomina abortada. Si se pretende asegurar la atomicidad, una transacción abortada no debe tener efecto sobre el estado de la base de datos. Así, cualquier cambio que haya hecho la transacción abortado sobre la base de datos debe deshacerse. Es responsabilidad del gestor de recuperación garantizar dos de las cuatro propiedades de las transacciones, la atomicidad y la permanencia en presencia de fallos.

El registro de transacciones contiene:

- Identificador de la transacción.
- Tipo de entrada de registro (inicio de transacción, inserción, actualización, borrado, aborto de la transacción y confirmación).
- Identificador del elemento de datos afectado por la operación de base de datos.
- Imagen anterior del elemento de datos.
- Imagen posterior del elemento de datos.
- Información de gestión del registro, como por ejemplo un puntero a las entradas anterior y siguiente del registro correspondiente a dicha transacción.

El registro de transacciones se utiliza con frecuencia para otros propósitos distintos a la recuperación, como por ejemplo la auditoría o la monitorización del rendimiento. Por ello a veces se registra información adicional en el archivo de registro.

Debido a la importancia del archivo de registro de transacciones, es posible que el registro esté *duplexado* o *triplexado* (es decir, que mantengan dos o tres copias independientes) de modo que si una de las copias está dañada, se pueda utilizar otra.

También debe tenerse en cuenta que el archivo de registro es un cuello de botella potencial y que la velocidad de escritura en el archivo de registro puede ser crítica a la hora de determinar las prestaciones globales del sistema de base de datos.

Cuando se produce un fallo de la base de datos se utiliza la información del archivo de registro, pero es necesario limitar las operaciones de búsqueda en el registro, para ello se utiliza una técnica denominada establecimiento de puntos de comprobación (checkpointing). Son los puntos de sincronización entre la base de datos y el archivo de registro de transacciones. Estos puntos se programan a intervalos predeterminados que implican las siguientes operaciones:

- Escribir en el almacenamiento secundario todas las entradas de registro de la memoria principal.
- Escribir en el almacenamiento secundario los bloques modificados de los búferes de la base de datos.
- Escribir una entrada de punto de comprobación en el archivo de registro. Esta entrada contendrá los identificadores de todas las transacciones que estén activas en el punto de comprobación.

Si las transacciones se realizan en serie, cuando se produzca un fallo comprobaremos el archivo de registro para localizar la última transacción que se iniciara antes del último punto de comprobación. Todas las transacciones anteriores ya habrán sido escritas en la base de datos en el punto de comprobación, por lo que sólo será necesario rehacer la transacción que estuviera activa en dicho punto y todas las transacciones subsiguientes para las que el registro contenga tantas entradas de inicio como entradas de comprobación. Si una transacción estuviera activa en el momento del fallo, dicha transacción deberá ser anulada. En el caso de que las transacciones se ejecutaran concurrentemente, se tendrán que rehacer todas las transacciones que

se hayan confirmado desde el punto de comprobación y deshacer aquellas que estuvieran activas en el momento del fallo.

6.1.3. Técnicas de recuperación

El procedimiento de recuperación concreto que hay que utilizar dependerá de los daños que la base de datos haya sufrido, así podemos considerar dos casos:

- Si la base de datos sufre daños considerables es necesario restaurar la última copia de seguridad de la base de datos y volver a aplicar las operaciones de actualización de las transacciones confirmadas utilizando el archivo de registro. Siempre que no haya sido dañado también el archivo de registro. Es muy importante almacenar este archivo en un disco independiente de los archivos principales de la base de datos para reducir el riesgo de que ambos archivos resulten dañados al mismo tiempo.

- La base de datos no ha resultado físicamente dañada pero ha quedado en un estado incoherente, este caso puede ocurrir cuando se produce una parada catastrófica y se estaban ejecutando transacciones. Para volver a un estado coherente es necesario deshacer los cambios que han provocado la incoherencia, también puede ocurrir que sea necesario rehacer algunas transacciones. En este supuesto no es necesario utilizar la copia de seguridad de la base de datos, únicamente podemos restaurar ésta a un estado coherente utilizando las imágenes anteriores y posteriores almacenadas en el archivo de registro.

Cuando la base de datos ha de recuperarse de esta última situación, el caso en el que la base de datos no haya resultado destruida pero haya quedado en un estado incoherente, existen varias técnicas denominadas actualización diferida, actualización inmediata y páginas en espejo, se diferencian en la forma que escriben las actualizaciones en almacenamiento secundario.

También hay que tener en cuenta el momento en el que realizar el proceso de recuperación, dependiendo de la gravedad del error la restauración de los datos puede

aplazarse para realizarse en horas de poca activada, pero si la gravedad es alta debe ser restaurada inmediatamente.

- **Actualizaciones diferidas**

La técnica de recuperación utilizando actualizaciones diferidas consiste en que las actualizaciones no se escriben en la base de datos hasta después de que una transacción alcance su punto de confirmación. Si la transacción falla antes de alcanzar este punto, no se habrá modificado la base de datos y no será necesario deshacer el cambio. Pero si puede ser necesario rehacer las actualizaciones de las transacciones confirmadas, ya que su efecto puede haber alcanzado la base de datos. En este caso, utilizamos el archivo de registro para protegernos frente a fallos del sistema.

En el registro se escribe cuando se inicia una transacción, la operación de escritura, la confirmación y si se aborta, se ignoran las entradas de registro de la transacción y no se realizan las escrituras.

Pero hay que tener en cuenta que se escribe en el registro antes de que la transacción sea confirmada, de tal forma que si se produce un fallo del sistema mientras que se están llevando a cabo las actualizaciones de la bases de datos, las entradas de registro persistirán y las actualizaciones pueden volver a ser aplicadas posteriormente. En caso de fallo, debe examinarse el registro para identificar las transacciones que se estaban llevando a cabo en el momento del fallo. Se comienza por la última entrada del archivo de registro, recorriendo hacia atrás hasta alcanzar la entrada más reciente del punto de comprobación, y todas aquellas transacciones con entrada de registro de inicio y confirmación de transacción deben rehacerse.

El proceso de restaurar consiste en llevar a cabo todas las escrituras en la base de datos utilizando las entradas de registro de imagen posterior correspondientes a las transacciones, en el orden en que fueron escritas en el registro. Así si ya fue realizado anteriormente esta escritura no pasa nada, pero con ello se garantiza que todos los elementos estén actualizados correctamente.

- **Actualización inmediata**

La técnica de recuperación utilizando una actualización inmediata consiste en que las actualizaciones se aplican a la base de datos según van teniendo lugar, sin esperar a alcanzar el punto de confirmación. De tal forma que ante un fallo, es necesario deshacer los efectos de las transacciones que no hubieran sido confirmadas en el momento del error. El archivo de registro actúa de la siguiente manera para su protección contra fallos, escribiendo al comienzo de una transacción, cuando se realiza una operación de escritura, posteriormente escrito el archivo de registro, se escribe la actualización en los búferes de la bases de datos y las actualizaciones de la base de datos se escriben cuando posteriormente se vuelcan los búferes en el almacenamiento secundario y por último cuando se confirma la transacción, ésta se escribe en el registro.

Es muy importante que las entradas de registro se escriban antes de la correspondiente escritura en la base e datos, ya que si se realizase primero la actualización en la base de datos y ocurriera después un fallo, por lo tanto antes de escribir en el registro, no habría forma alguna de recuperar la información y no se podría saber lo que se ha realizado en la base de datos.

- **Página espejo**

A diferencia de las técnicas anteriores, ésta no se basa en el archivo de registro. Consiste en mantener dos tablas de páginas durante la vida de la transacción: una tabla de páginas actuales y otra de páginas espejo. Cuando se inicia la transacción, las dos tablas de página son iguales. La tabla de página en espejo nunca cambia a partir de ahí y se utiliza para restaurar la base de datos en caso de fallo del sistema. Durante la transacción, la tabla de páginas actuales se utiliza para registrar todas las actualizaciones realizadas en la base de datos y cuando se completa la transacción, la tabla de páginas actuales se convierte en tabla de páginas en espejo.

Las páginas en espejo tienen diversas ventajas sobre los sistemas basados en registro: se elimina el coste adicional de mantener el archivo de registro y la recuperación es significativamente más rápida, ya que no existe necesidad de rehacer

y deshacer operaciones. Pero también tiene ciertas desventajas, como son la fragmentación de datos y la necesidad de realizar una recolección periódica de memoria para reclamar los bloques inaccesibles.

6.2. COPIAS DE SEGURIDAD EN INFORMIX.

Es importante conocer el sistema de copias de seguridad y restauración de Informix para poder auditarlo. Saber si está correctamente configurado para obtener la máxima eficiencia y mínimo consumo de recursos. Además de saber prever ante posibles desastres planes de contingencia, preparados y verificados para poderlos llevar a cabo.

Informix dispone de IBM Informix Enterprise Replication, herramienta asíncrona basada en la anotación cronológica para duplicar datos entre servidores de bases de datos IBM Informix Dynamic Sever. La forma de funcionamiento consiste en un servidor fuente, Entreprise Replication, captura las transacciones que deben ser duplicadas leyendo la anotación lógica, almacenando las transacciones y transmitiendo de forma fiable a los servidores de destino cada transacción como datos de duplicación. En cada servidor de destino, Enterprise Replication recibe cada transacción contenida en los datos de duplicación y la aplica a las bases de datos y tablas como una transacción normal anotada cronológicamente.

Dynamic Server utiliza los siguientes mecanismos de anotaciones cronológicas y recuperación que protegen la integridad de los datos y su coherencia si se produce una anomalía del sistema operativo o del soporte de almacenamiento:

- Copia de seguridad y restauración
- Recuperación rápida (expuesto en el apartado de Restauración de datos)
- Duplicación de disco
- Duplicación de datos de alta disponibilidad (HDR)

A continuación se explica cómo está estructurado dicho sistema, como funciona y que ficheros contienen información sobre la actividad del mismo y como en caso de desastre nos permite restaurar el sistema.

6.2.1. Sistemas de copias y restauración de Informix

Los programas de utilidad que ofrece IBM para gestionar los servidores de bases de datos Informix son ON-Bar y ontape. La diferencia entre ambas utilidades es que ON-Bar requiere un gestor de almacenamiento, Informix Storage Manager (ISM), y ontape no lo requiere.

6.2.1.1. Informix Storage Manager (ON-Bar)

El producto de IBM que se encarga de gestionar los dispositivos y soportes de almacenamiento para el servidor de bases de datos Informix es “Informix Storage Manager” (ISM), para las copias de seguridad y restauración de datos del servidor de bases de datos se utiliza ISM con la utilidad ON-Bar. También proporciona otra utilidad, denomina ontape.

Informix Storage Manager está formado por el servidor ISM para el intercambio de información de copia de seguridad y recuperación entre los dispositivos de almacenamiento, ON-Bar y por el catálogo de Informix Storage Manager, encargado de mantener los registros actualizados de las operaciones de copia de seguridad que se hayan realizado y los soportes en los que están almacenados los datos copiados.

El servidor ISM reside en el mismo sistema que ON-Bar y que el servidor de base de datos Informix; así como los dispositivos de almacenamiento que deben estar conectados al sistema.

El manual de IBM que recoger información sobre este gestor es IBM Informix: Storage Manager Guía del Administrador.

Informix Storage Manager realiza las siguientes funcionalidades:

- Proporciona servicios de gestión de almacenamiento de datos para el servidor de base de datos Informix.

- Recibe peticiones de copia de seguridad y de restauración desde ON-Bar y dirige los datos a y desde los volúmenes de almacenamiento que están montados en dispositivos de almacenamiento ISM.

- Realiza el seguimiento de los datos copiados a través de un ciclo de vida de los datos determinado por el administrador de bases de datos o del sistema y puede gestionar automáticamente los dispositivos y volúmenes de almacenamiento.

- Mantiene el catálogo de ISM y crea y guarda la información que es necesaria para restaurar el estado del servidor ISM después de una anomalía de disco.

La figura presenta la interacción entre ON-Bar, el servidor Informix Storage Manager y los mandatos de este.

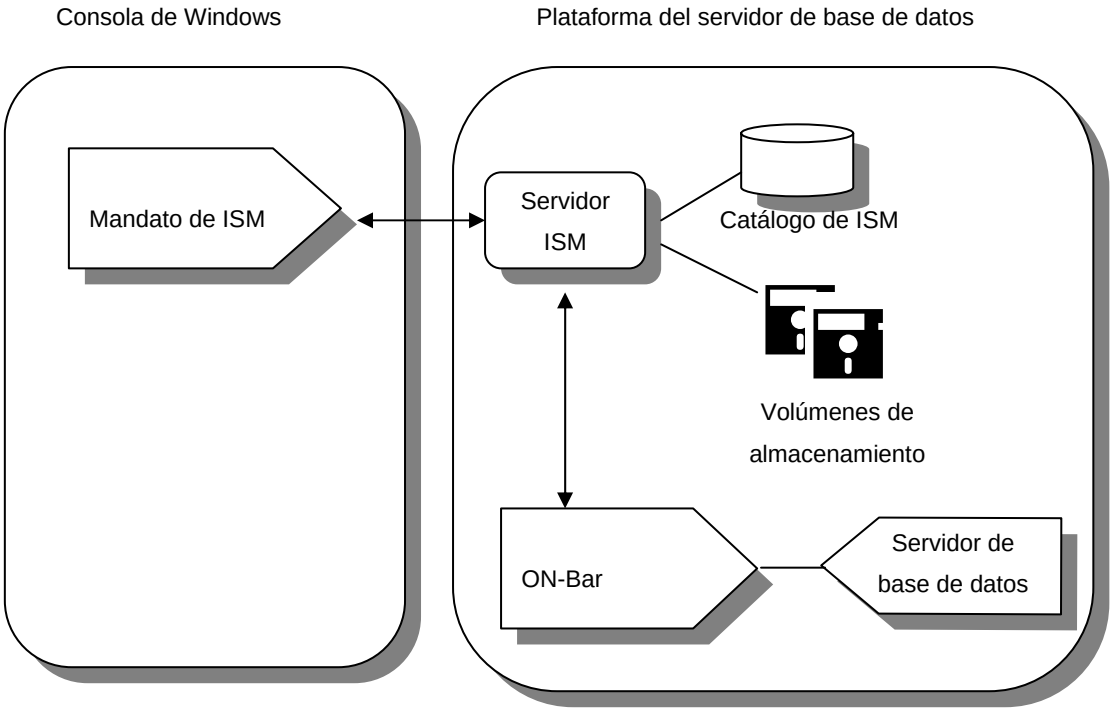


Ilustración 10. Interacción entre ISM y ON-Bar

El Informix Storage Manager (ISM) como hemos indicado con anterioridad está formado por estos tres componentes que explicamos más en profundidad a continuación.

- El servidor de ISM
- El catálogo de ISM
- On-Bar

- **Servidor ISM**

El servidor ISM es el componente de ISM que conecta el servidor de bases de datos Informix con los dispositivos de almacenamiento y permite supervisar el proceso de las operaciones de copia de seguridad y restauración, gestionar los datos copiados y controlar los soportes y dispositivos de almacenamiento. El comando "*ism_config"* nos permite configura las propiedades del servidor ISM.

En el proceso de copia de seguridad y restauración Informix utiliza diversos archivos de anotaciones cronológicas, donde se recoge información de gran valor ante situaciones de error. Existe un mandato "*ism-chk.pl"* que recopila información sobre el estado actual del ISM, los procesos de ON-Bar y el servidor de base de datos de los ficheros de anotaciones cronológicas

En el proceso de copias de seguridad es muy importante el mantenimiento y configuración adecuada de los archivos de anotaciones cronológicos que mantiene ISM. Por ello es necesario controlar el tamaño y el número de archivos de anotaciones cronológicas:

ISM_MAXLOGSIZE	Contiene el valor del tamaño máximo de la anotación cronológica. El valor 0, se interpreta como sin límite.
ISM_MAXLOGVERS	Establece el número máximo de archivos de anotaciones cronológicas de actividades que debe

	conservar el servidor ISM. El valor por defecto es cuatro.
ISM_COMPRESSION	Determina si ISM utiliza compresión o cifrado al realizar una copia de seguridad.
ISM_ENCRYPTION	Si se estable en TRUE o XOR, el servidor ISM utiliza el cifrado para almacenar o recuperar los datos especificados en esa petición.
ISM_DEBUG_LEVEL	Controla el nivel de detalle de información que se registra en la anotación cronológica de mensajes XBSA. (Valor 0 suprime todos los registros de depuración de XBSA y valor 1 solo informa acerca de las anomalías de XBSA).

Es muy importante la información incluida en la secuencia inicial de instrucciones del servidor ISM para la recuperación de errores muy graves, es fundamental guardar de forma segura la salida impresa de la secuencia más reciente.

El servidor ISM mantiene archivos de anotaciones cronológicas donde se registran sus actividades. Se registran las peticiones recibidas y las operaciones que efectúa el servidor. Estos archivos de anotaciones cronológicas de actividad se encuentran en los siguientes directorios:

```
En UNIX
        $INFORMIXDIR/ism/logs/daemon.log
        $INFORMIXDIR/ism/applogs/xbsa.mssage   (anotaciones del XBSA)
  En WINDOWS
        %ISMDIR%\logs\daemon.log
        c:\nsr\applogs\xbsa.message  (anotaciones del XBSA)
```

En el caso de disponer de diferentes servidores de bases de datos Informix instalados en distintos directorios del mismo sistema, se podrá saber la ubicación de la anotación cronológica de actividades del servidor ISM activo con el mandato "*ls -ls/nsr*".

Como venimos diciendo Informix utiliza diversos archivos de anotaciones cronológicas, donde se recoge información de gran valor ante situaciones de error.

Cuando se están estudiando problemas con una copia de seguridad o restauración este comando genera un informe que puede ser presentado en pantalla o redirigido a un archiv. *Ism_chk.pl* posee una serie de parámetros que nos permite seleccionar ciertas anotaciones: aquellas que estén en un intervalo de fechas, informes separados sobre el servidor de base de datos, de ON-Bar y de ISM, estado de la red, etc. En los manuales de Informix se puede obtener de forma detallada todos los parámetros que posee.

Un breve ejemplo de cómo generar un informe sobre las anotaciones cronológicas durante un periodo de tiempo se especificaría de la siguiente manera:

```
Ism_chk.pl –s "2008-06-01 08:00:00" –e "2008-06-02 21:00:00"
ism_chk.pl –s "2008-06-01" –e "2008-06-02"  (de forma abreviada)
```

El informe generado por ism_chk.pl es útil para investigar problemas de las operaciones de copia de seguridad o restauración.

```
"onstat –a ", muestra el estado del servidor de base de datos
"netstat"      informa sobre la carga y los recursos de la red
```

Toda esta información que aportan estos mandatos es muy importante para el auditor, puesto que le permite controlar si se están produciendo errores, forma que tiene de corregirlos y tiempos de respuesta ante dichas situaciones, ya que como sabemos el proceso de restauración y copias de seguridad es muy importante y requiere una atención especial.

- **El Catálogo ISM**

El catálogo de Informix Storage Manager (ISM) se encarga de mantener los registros actualizados de las operaciones de copia de seguridad que se han realizado y los soportes en los que se están almacenados los dato.

El catálogo de ISM es utilizado por el servidor ISM para efectuar el seguimiento de los conjuntos guardados y los volúmenes en los que se han copiado.

- **ON-Bar**

ON-Bar realiza una petición de copia de seguridad al servidor ISM, quien graba los datos en volúmenes de almacenamiento, que están montados en dispositivos de almacenamiento conectados a éste. Informix utiliza agrupaciones de volúmenes para clasificar los datos específicos de los volúmenes de almacenamiento. Por ejemplo ISMData es el volumen que va a contener datos del espacio de la base de datos o ISMLogs contiene archivos de anotaciones lógicas, etc.

Las tareas que lleva a cabo ON-Bar son:

- Determina qué datos deben copiarse.
- Hace copias de seguridad a diferentes niveles (nivel 0, nivel 1, nivel 2).
- Recupera los datos de los espacios de almacenamiento o anotaciones lógicas correspondientes en el servidor de base de datos Informix, crea una lista de los objetos de copia de seguridad y lo envía al servidor ISM.
- Se conecta al servidor ISM para realizar las copias de seguridad o restauración.
- Crea un conjunto que recibe el nombre de “secuencia inicial de instrucciones del servidor ISM” que contiene información de configuración sobre el servidor ISM para la recuperación de errores muy graves”. Por ello es muy importante guardar de forma segura la salida impresa de la secuencia más reciente.

- ON-Bar graba información sobre la copia de seguridad en la anotación cronológica de mensajes del servidor de bases de datos y en la anotación cronológica de actividades de ON-Bar.

- Hace una copia de seguridad de los archivos de anotaciones.

- Verifica las copias de seguridad con el programa de utilidad archecker.

La forma de funcionamiento de la herramienta ON-Bar es mediante la utilización de las siguientes tablas de catálogo de la base de datos sysutils para supervisar las copias de seguridad y restauración:

- *Bar_server*: contiene una lista de los servidores de la base de datos, además supervisa las instancias del servidor de base de datos. La estructura de registro de la tabla es (srv_name, srv_mode), donde el primer campo es el nombre del servidor online y el segundo el nombre del nodo.

- *Bar_object*: describe cada objeto de copia de seguridad. Donde un objeto de copia de seguridad es una copia de seguridad de un espacio de base de datos, espacio de BLOB, espacio de SB o archivo de anotaciones lógicas. La estructura de registro de la tabla es (obj_serv_name, obj_oid, obj_name, obj_type). Los posibles valores que puede tomar el tipo de objeto de copia de seguridad obj_type son: R: espacio de base de datos raíz, CD: espacio de base de datos crítico, ND: espacio de base de datos no crítico, B: espacio de BLOB, L: anotación lógica.

- *Bar_action*: contiene todos los intentos de copia de seguridad y restauración satisfactorios que se han producido para cada objeto de la copia de seguridad, excepto algunos sucesos de recuperación de archivos de anotaciones y restauración en frío. La tabla tiene la siguiente estructura: act_aid, act_oid_act_type, act_status, act_star_act_end. El campo act_type puede contener los siguientes tipos de acción: 1- copia de Seguridad, 2- restauración, 3-restauración remota o importada, 4- copia de seguridad ficticia, 5- copia de seguridad del sistema completo, 6- restauración del sistema completo, 7- copia de seguridad para objetos caducados o suprimidos, 8- restauración externa.

- *Bar_instante*: La estructura del registro de la tabla es: ins_aid (identificador de accion), ins_oid (identif. objeto), ins_time (hora de producirse desde el servidor), ins_copyid_hi (Id. de copia desde Storage Manager), ins_copyid_lo (Id. de copia desde Sotorage Manager), ins_req_aid (prerequisite del id. el objeto), ins_first_log (Primer log lógico requerido), ins_verify (Verificación), ins_verigy_date (fecha-hora de archivo de validación).

La relación entre las cuatro tablas principales que residen en la base de datos de sysutils: bar_Server, bar_objetc, bar_action y bar_instance, se puede presentar mediante el siguiente esquema:

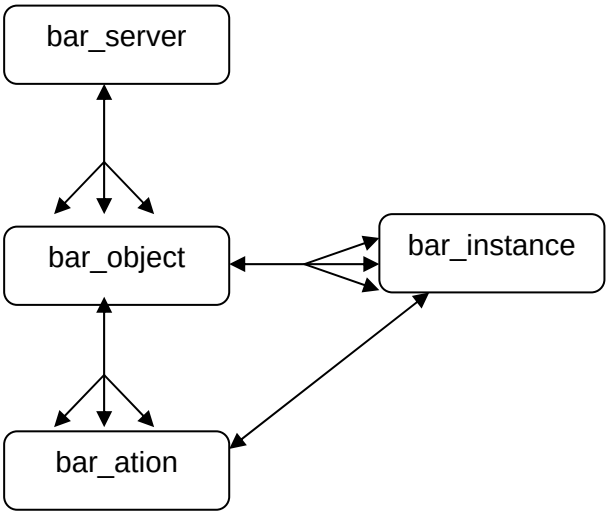


Ilustración 11. Tablas que utiliza ON-Bar

6.2.1.2. Ontape

Ontape es un programa de utilidad que no requiere un gestor de almacenamiento, a diferencia de ON-Bar que si lo necesita. Se utiliza para realizar las siguientes tareas:

- Realiza copias de seguridad y restauraciones de los espacios de almacenamiento y anotaciones lógicas.

- Cambia el estado de las anotaciones de la bases de datos
- Inicia las copias de seguridad de anotaciones lógicas continuas
- Utiliza la duplicación de datos.
- Renombra fragmentos de almacenamiento utilizando nombres distintos de vías de acceso y desplazamientos.

6.2.2. Duplicación de disco

Cuando se utiliza la duplicación de disco, el servidor de bases de datos graba cada elemento de datos en dos ubicaciones. La duplicación de disco es una estrategia que empareja un fragmento de almacenamiento primario de un espacio de almacenamiento con un fragmento de almacenamiento duplicado de igual tamaño. Cada grabación en el fragmento primario va acompañada automáticamente de una grabación idéntica en el fragmento duplicado. Si se produce una anomalía en el fragmento primario, la duplicación del disco le permitirá leer y grabar en el fragmento duplicado hasta que se recupere el fragmento primario y todo ello sin interrumpir el acceso del usuario a los datos.

6.2.3. Duplicación de datos

La duplicación de datos genera y gestiona diversas copias de los datos en uno o más sitios, lo cual posibilita el compartimiento de datos corporativos de una empresa en toda su organización. La duplicación de datos brinda un sistema de copia de seguridad en caso de producirse una anomalía muy grave.

6.2.4. Enterprise Replication

La duplicación de datos de alta disponibilidad (HDR) proporciona la duplicación síncrona de datos para Dynamic Server. HDR permite duplicar datos de las bases de datos durante la ejecución simultánea en un segundo sistema. Si un sitio experimenta

un error muy importante, el usuario puede obligar inmediatamente a las aplicaciones a que utilicen el segundo servidor de base de datos que compone el par de duplicación de datos. Para mayor detalle se puede consultar el manual online IBM Informix Administrator's Guide.

Enterprise Replication capta transacciones que deben duplicarse en toda la empresa. En el servidor de bases de datos fuente, Enterprise Replication lee las anotaciones lógicas y transmite cada transacción a los servidores de bases de datos destino. En cada servidor de base de datos destino, Enterprise Replication recibe las transacciones y las aplica a las bases de datos y tablas adecuadas. Enterprise Replication puede combinarse con HDR. Se puede ampliar esta información en el manual online IBM Dynamic Server Guía de Enterprise Replication.

6.3. GESTIÓN DE COPIAS DE SEGURIDAD

6.3.1. Tipos de Copias de Seguridad

Informix proporciona un entorno de copia de seguridad más flexible, "*ON-Bar*" y "*ontape"*, ya detallado anteriormente, estos permiten 3 niveles de copias de seguridad:

Nivel 0 Hace una copia de seguridad de todas las páginas utilizadas que contienen datos para los espacios de almacenamiento especificados

Nivel 1 Hace una copia de seguridad únicamente de los datos que han cambiado desde la última copia de seguridad de nivel 0 de los espacios de almacenamiento especificados. Se hace copias de seguridad de todas las páginas de tabla y de índice cambiadas, incluidas la que contiene datos suprimidos. Los datos que se copian en la copia de seguridad reflejan el estado que tenían los datos modificados en el momento de comenzar la copia de seguridad del nivel 1.

Nivel 2 Hace una copia de seguridad de solo los datos que han cambiado desde la última copia de seguridad de nivel 1 de los espacios de almacenamiento especificados. La copia de seguridad de nivel 2 contiene cada página de

tabla y de índice perteneciente a un espacio de almacenamiento que ha cambiado desde la última copia de seguridad de nivel 1.

Informix, en concreto ON-Bar, graba un archivo con las notaciones lógicas, que son el registro de la actividad del servidor de base de datos que se ha producido entre procesos de copia de seguridad. Estos archivos también se les realizan una copia en disco o cinta una vez que están llenos.

Es importante realizar copias de seguridad de los archivos que contienen las anotaciones lógicas por varias razones:

- Para minimizar la pérdida de datos si falla un disco que contiene archivos de anotaciones lógicas
- Para asegurar que las restauraciones contengan transacciones coherentes y las más recientes.

Informix recomienda guardar las copias de seguridad de archivos de anotaciones lógicas desde las dos últimas copias de seguridad de nivel 0 para poder utilizarlas en una restauración.

A continuación se muestra una tabla que compara ON-Bar con ontape. Si conmuta a ON-BAR e ISM desde ontape, se observa que se comporta de forma diferente:

¿Puede el programa de utilidad?	**ON-Bar**	**Ontape**
¿Utilizar un gestor de almacenamiento para supervisar las copias de seguridad y los soportes de almacenamiento?	si	no
¿Hacer copia de seguridad de todos los datos del servidor de bases de datos?	si	si

¿Puede el programa de utilidad?	ON-Bar	Ontape
¿Hacer copia de seguridad de espacios de almacenamiento seleccionados?	si	no
¿Hacer copia de seguridad de archivos de anotaciones lógicas?	si	si
¿Hacer copia de seguridad mientras el servidor de bases de datos está en línea?	si	si
¿Hacer copia de seguridad mientras el servidor de bases de datos está fuera de servicio?	si	si
¿Restaurar todos los datos del servidor de bases de datos?	si	si
¿Restaurar espacios de almacenamiento seleccionados?	si	si
¿Inicializar la duplicación de datos de alta disponibilidad?	si	si
¿Restaurar datos hasta un punto determinado en el tiempo?	si	no
¿Efectuar restauraciones físicas y lógicas separadas?	si	no
¿Hacer copia de seguridad y restaurar espacios de almacenamiento diferentes en paralelo?	si	no
¿Utilizar simultáneamente varias unidades de cinta para las copias de seguridad y restauraciones?	si	no
¿Reiniciar una restauración?	si	no
¿Cambiar la modalidad de registro de anotaciones para bases de datos?	no	no

6.3.2. Planificación de las copias de seguridad

Todo sistema que requiera la realización de copias de seguridad y restauración, debe realizar una planificación. El plan de copias se ajustará a las necesidades del sistema. Cuanto más a menudo cambien los datos y más importantes sean éstos, con mayor frecuencia necesitará hacer una copia de seguridad de ellos.

Las siguientes preguntas pueden ayudar a determinar con qué frecuencia y cuándo se pueden llevar a cabo las copias de seguridad de los datos:

- ¿Existe en la empresa un periodo de inactividad en el que se pueda restaurar el sistema?
- Si el sistema trabaja 24 horas, los 7 días de la semana (ningún periodo de inactivad) ¿existe algún tiempo de menor actividad en el que se pueda realizar una restauración?
- Si la restauración se debe realizar durante un periodo de gran actividad, ¿cómo de crítico es el tiempo?
- ¿Qué datos se pueden restaurar mientras el servidor de base de datos está en línea?, y ¿Qué datos se deben restaurar fuera de línea?
- ¿Cuántos dispositivos de almacenamiento están disponibles para hacer copias de seguridad y restaurar datos?

Es aconsejable crear un plan de copia de seguridad que mantenga un volumen pequeño de copias de seguridad de nivel 1 y nivel 2, y planificar la ejecución frecuente de copias de seguridad de nivel 0. Con un plan de copia de seguridad de esta tipo, evitará tener que restaurar copias de seguridad de nivel 1 y nivel 2 de gran volumen o muchas copias de seguridad de archivos de anotaciones lógicas.

Las copias de seguridad de nivel 0 pueden exigir mucho tiempo, pues ON-Bar escribe todas las páginas de disco en el soporte de copia de seguridad. Las copias de seguridad de nivel 1 y nivel 2 pueden necesitar casi el mismo tiempo que una copia de seguridad de nivel 0, pues el servidor de bases de datos debe examinar todos los

datos para determinar qué ha cambiado desde la última copia de seguridad. Requiere menos tiempo restaurar datos a partir de copias de seguridad de nivel 0, de nivel 1 y de nivel 2 que a partir de copias de seguridad de nivel 0 y una larga serie de copias de seguridad de archivos de anotaciones lógicas.

Las copias de seguridad de nivel 1 ocupa menos espacio y puede necesitar menos tiempo que una copia de seguridad de nivel 0, pues en el gestor de almacenamiento solo se copian los datos que han cambiado desde la última copia de seguridad de nivel_0.

Las copias de seguridad de nivel 2 ocupa menos espacio y puede necesitar menos tiempo que una copia de seguridad de nivel 1, pues en el gestor de almacenamiento solo se copian los datos que han cambiado desde la última copia de seguridad de nivel_1.

Es necesario recoger información sobre el sistema antes de realizar una copia de seguridad sobre:

- La configuración del servidor de base de datos. Los siguientes archivos contienen dicha información: sqlhost, oncfg, archivos de inicio de emergencias, ONCONGIG, sm_versions.

- Verificación de la integridad de los datos. Se debe comprobar periódicamente que todos los datos del servidor de base de datos sean coherentes antes de hacer una copia de seguridad de nivel 0.

- Con carácter opcional se puede obtener un seguimiento del número de filas de cada tabla.

Cuando se produce un cambio en el esquema físico, se debe realizar una copia de seguridad del espacio de base de datos raíz y de los espacios de almacenamiento modificados.

También hay que supervisar que existe espacio suficiente en el archivo de anotaciones lógicas, ya que si no hay espacio suficiente el servidor de base de datos dejará de responder.

Es importante hacer una copia de seguridad de cada espacio de almacenamiento al menos una vez, ya que la herramienta ON-Bar no puede restaurar espacios de almacenamiento para los que no ha creado nunca una copia de seguridad.

6.3.3. Verificación de las copias de seguridad

Informix proporciona la utilidad *archecker* para comprobar la validez e integridad de las copias de seguridad, esto es debido a que es necesario asegurarse que se puede restaurar sin problemas una copia de seguridad.

El programa de utilidad *archecker* se accede desde el mandato "*onbar –v*". Esta utilidad verifica que todas las páginas necesarias para restaurar una copia de seguridad están presentes en el soporte de almacenamiento en la forma correcta. Este comando se puede utilizar mientras el servidor de base de datos se encuentra funcionando.

Cuando finaliza el examen, *archecker* utiliza el mapa de bits para verificar la copia de seguridad y registra el estado en el archivo de anotaciones de mensajes de *archecker.*

El programa *archecker* necesita un espacio para almacenar los archivos temporales. Si la copia de seguridad no pasa la verificación, los archivos temporales se conservan. Es aconsejable copiarlos en otra ubicación para que los responsables puedan examinarlos. De tal forma que si la copia de seguridad se verifica satisfactoriamente, los archivos temporales se suprimen.

Cuando el usuario verifica una copia de seguridad, ON-Bar escribe mensajes que quedan guardados en el archivo *bar_act.logs*, y que indican qué espacios de almacenamiento se verificaron y si ésta se realizó satisfactoriamente o no. El archivo donde se almacena esta información detallada será chequeado por el equipo técnico para diagnosticar los problemas que hayan surgido en las operaciones de copia de copia de seguridad y restauración.

Un ejemplo de anotaciones de la herramienta "ON-Bar", sobre una verificación que fue satisfactoria y otra que no (copia de seguridad de nivel 0) es el siguiente:

```
Begin backup verification of level0 for dbs2.2 (Storage Manager Copy ID:##)
Completed level-0 backup verification successfully.

Begin backup verification of level0 for rootdbs (Storage Manager Copy ID:##).
 ERROR: No se puede cerrar la comprobación física: mensaje de error.
```

A continuación se muestra un ejemplo de las anotaciones que se encuentran en el archivo de mensajes generado por *archecker* donde se puede observar que el nivel de detalle ofrecido es mayor:

```
STATUS: Scan PASSED
STATUS: Control page checks PASSED
STATUS: Starting checks of dbspace dbs2.2.
STATUS: Checking dbs2.2:TBLSpace . .
STATUS: Tables/Fragments Validated: 1
Archive Validation Passed
```

Es muy importante saber si una copia de seguridad no pasa las verificaciones, ya que no se pueden restaurar los datos copiados y los resultados pueden ser imprevisibles. No obstante, puede ocurrir que la restauración pueda parecer satisfactoria, y sin embargo oculte algún problema real existente en los datos o en el soporte de almacenamiento.

6.3.4. Dispositivos de almacenamiento

Se puede optar por varios tipos de dispositivos de almacenamiento, cada uno aporta una serie de ventajas e inconvenientes. Por ejemplo, la velocidad de la copia de seguridad y restauración son puntos muy importantes a tener en cuenta cuando se

planifique su estrategia de copia de seguridad, pero existen otros aspectos también a tener en consideración.

- La utilización de unidades de cintas o unidades de disco óptico como dispositivos de almacenamiento proporciona una forma económica de almacenar los datos a largo plazo. Permite almacenar las cintas y los discos ópticos en una ubicación externa o en un contenedor protegido. Además posee una capacidad ilimitada, ya que pueden adquirirse nuevos soportes. Pero tienen el inconveniente de la velocidad, estos dispositivos acceden a los datos secuencialmente, método que ralentiza la actividad de copia de seguridad y recuperación.

- Los dispositivos de almacenamiento de tipo de archivo, como, por ejemplo, sistemas de archivos o la unidad de disco duro, copian los datos con mayor rapidez que algunos dispositivos de cintas. Esta característica es especialmente importante si tienen un tiempo limitado para la copia de seguridad. También podrá accederse a los datos con mayor rapidez durante las operaciones de restauración porque los sistemas de archivos permiten el acceso aleatorio a los datos. Pero tiene como inconveniente que este tipo de dispositivo de almacenamiento es más caro que las cintas y además de la imposibilidad de almacenar los datos del dispositivo de almacenamiento de tipo de archivo en una ubicación externa. Aunque este inconveniente podría subsanarse mediante la clonación consiste en que una vez lleno un dispositivo de tipo archivo se clonen los datos a una cinta a fin de poder grabar el dispositivo de tipo archivo con nuevos datos.

Los volúmenes clonados proporcionan seguridad añadida, ya que permiten recuperar los datos en el caso que los volúmenes originales se dañen o se destruyan.

Informix recomienda utilizar una serie de nombres para las agrupaciones de volúmenes, por ello es una posible recomendación del auditor:

ISMData	Para almacenar espacios de almacenamiento en dispositivos que no son de tipo archivo.

ISMDiskData	Para almacenar espacios de almacenamiento en dispositivos que son de tipo archivo.
ISMLogs	Para almacenar anotaciones lógicas en dispositivos que no son de tipo archivo.
ISMDiskLogs	Para almacenar anotaciones lógicas en dispositivos que son de tipo archivo.

6.4. Restauración de datos

Informix posee dos programas de utilidad, “ON-Bar” y “ontape”, con los que se lleva a cabo la restauración del sistema. En función del tipo de dato a restaurar permite realizar varios tipos de restauraciones: en caliente, en frío o mixta.

La recuperación se realiza a partir de espacios de almacenamiento y archivos de anotaciones lógicas. Informix Dynamic Server proporciona un tipo de restauración rápida.

6.4.1. Recuperación rápida

Dynamic Server proporciona un tipo de recuperación rápida, se trata de un procedimiento automático que restaura el servidor de base de datos a un estado coherente después de que éste quede fuera de línea bajo condiciones controladas. Así mismo, este procedimiento recupera en avance todas las transacciones confirmadas desde el último punto de control y retrocede cualquier transacción que no esté confirmada.

Cuando el servidor de bases de datos arranca, comprueba las anotaciones físicas, las cuales contiene páginas que todavía no se han grabado en disco. Si las anotaciones físicas están vacías, significa que el servidor de base de datos se cerró de forma controlada. Si las anotaciones físicas no están vacías, el servidor de base de datos realizará automáticamente una recuperación rápida.

El manual online que recoge esta funcionalidad es IMB Informix: Administrator’s Guide.

6.4.2. Planificación de una estrategia de recuperación

Ante una situación de recuperación de datos, es necesario realizar una planificación, el primer paso es determinar qué volumen de pérdida de datos. Pueden producirse varios tipos de pérdidas de datos:

- Supresión de:
  - Filas, columnas, tablas o bases de datos
  - Bloques de datos, espacios de almacenamiento o archivos de anotaciones lógicas
- Corrupción de los datos o creación de datos incorrectos
- Error de hardware
- Error del servidor de bases de datos
- Desastre natural

Una vez determinado los objetivos de la recuperación, se define el plan de recuperación, existen varios niveles de error en función de la gravedad del error:

- Baja, se ha producido pérdida de datos no críticos. La restauración de los datos se puede aplazar para realizarla en horas de poca actividad. Se utiliza la restauración en caliente.
- Media, los datos perdidos son críticos para la empresa, pero no residen en un espacio de base de datos críticos. Se realiza una restauración en caliente de estos datos lo antes posible.
- Alta, pérdida de espacios de base de datos críticos. Se utiliza una restauración mixta para restaurar los datos no críticos durante las horas de poca actividad.
- Desastre, pérdida de todos los datos. Se realiza una restauración en caliente o restauración mixta lo antes posible.

6.4.3. Tipos de restauración

Informix permite realizar varias modalidades de restauración, la elección de una u otra depende de la decisión de cuando se desea hacerlo Mientras que el servidor de base de datos está fuera de servicio, en línea o fuera de línea, se puede hablar de tres tipos de restauración:

- *Restauración en caliente*, se restauran datos no críticos mientras el servidor de base de datos está en línea o fuera de servicio.

- *Restauración en frío*, se recuperan los archivos de anotaciones lógicas y restaura los espacios de la bases de datos críticos, otros espacios de almacenamiento y los archivos de anotaciones lógicas.

- *Restauración mixta*, es una restauración en frío de algunos espacios de almacenamiento seguida de una restauración en caliente de los espacios de almacenamiento restantes.

La restauración que realiza ON-Bar y ontape de los datos de un servidor de base de datos se realiza en dos fases:

- La primera fase es la restauración física, se restauran los datos a partir de copias de seguridad de todos los espacios de almacenamiento o solo de algunos seleccionados.

- La segunda fase es la restauración lógica, restaura las transacciones a partir de las copias de seguridad de los archivos de anotaciones lógicas, que se produjeron desde la última copia de seguridad. El servidor de base de datos detecta de forma automática qué archivos de anotaciones lógicas debe restaurar.

Durante el proceso de restauración se producen una serie de actuaciones, el administrador u operador del servidor de la base de datos utiliza la utilidad ON-Bar para solicitar esta operación. El servidor ISM recibe esta petición e ISM busca en el catálogo para identificar los volúmenes de almacenamiento que se necesitan. Cuando ISM recupera los datos, solicita el volumen de almacenamiento específico por su nombre.

La comunicación entre ON-Bar e ISM se realiza a través de X/Open Backup Services Aplication (XBSA) Programming Interface, que permite a ISM proporcionar servicios de gestión de soportes para el servidor de base de datos.

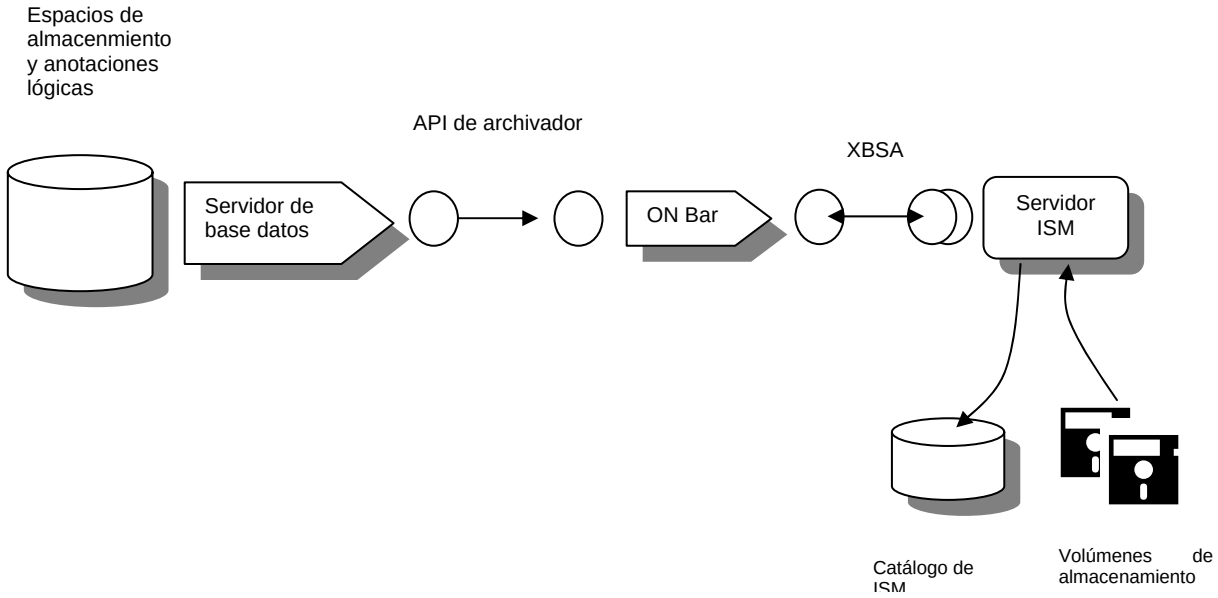


Ilustración 12 – Movimientos de los datos durante una restauración de ON-Bar

6.4.4. Programas de utilidad de Informix Storage Manager

El servidor ISM da soporte a varios programas de utilidad de línea de mandatos para gestión de los usuarios administrativos, del catálogo de ISM, de los dispositivos de almacenamiento y los volúmenes de soporte. A continuación se muestra una tabla con todos los mandatos disponibles.

ism_add	Añade usuarios admin. y dispositivos de almacenamiento.
ism_catalog	Vuelve a crear entradas en el catálogo de ISM, o recupera, crear una nueva secuencia inicial de instrucciones o busca la secuencia inicial de instrucciones del servidor ISM.

ism_chk.pl	Recopila información sobre ISM, ON-Bar y el servidor de bd.
Ism_clone	Inicia una operación de clonación con un volumen de almacenamiento o un conjunto guardado.
Ism_config	Configurar las propiedades del servidor ISM y cambiar los parámetros de los volúmenes de almacenamiento.
Ism_op	Etiqueta, monta y desmonta volúmenes de almacenamiento.
Ism_rm	Elimina un usuario administrativo o un dispositivo de almacenamiento del servidor ISM o elimina un volumen de almacenamiento de catálogo de ISM.
Ism_show	Visualiza la información sobre los administradores, volúmenes de soporte y dispositivos de almacenamiento de ISM.
Ism_shutdown	Cierra el servidor ISM.
Ism_startup	Inicia un servidor ISM.
Ism_watch	Visualiza un programa de utilidad de pantallas, donde se supervisa el servidor ISM.

CAPITULO 7

LISTAS DE COMPROBACIÓN

7. LISTAS DE COMPROBACIÓN

A continuación presentamos una amplia relación de listas de comprobación sobre diversos aspectos a tener en cuenta a la hora de realizar una auditoría, debido a que es una de las herramientas más importantes y utilizadas por la mayoría de las metodologías, con la intención de obtener información del sistema, entorno y otros elementos que sean objeto del estudio que se lleve a cabo.

En el apartado de "Herramientas" se expone ampliamente la utilidad de esta herramienta, así como de los diferentes tipos que existen. Pudiendo clasificarlos, además de por la materia que versan, también por el formato, lista de comprobación de rango y lista de comprobación binaria.

- **Lista de Comprobación de Rango**

Pregunta	1	2	3	4	5

- **Lista de Comprobación Binaria**

Pregunta	S	N	N/A

Estas listas de comprobación pueden versar sobre multitud de aspectos, en función del entorno que se desee estudiar, y se adaptarán para obtener el objetivo final, es decir, conseguir la mayor cantidad de información del sistema de tal forma que nos permita determinar cuales son las debilidades del sistema, formas de trabajo, etc, y poder así indicar si son las correctas o no.

A continuación se presenta un conjunto de listas de comprobación enfocados al entorno de un sistema de base de datos, pero no solo versan sobre el sistema de base de datos, sino también sobre todo el entorno que la rodea, que en gran medida determinan la configuración de la base de datos.

La forma de dar un resultado a cada uno de las siguientes listas de comprobación es mediante una regla de tres para cada tipo de respuesta.

7.1. DIRECCIÓN

Con la realización del estudio sobre la Dirección se pretende obtener información sobre un conjunto de aspectos, que a continuación detallamos, para poder obtener un Informe de Auditoría donde se muestren los riesgos y deficiencias detectados en la Dirección del área de Informática.

- Organización y calificación de la dirección de Informática
- Plan Estratégico de los Sistemas de Información
- Análisis de los puestos
- Planes y Procedimientos
- Normativa
- Gestión Económica

Los objetivos que se pretende conseguir es determinar la utilidad de las políticas, planes y procedimientos, así como su nivel de cumplimiento. Examinar el proceso de

planificación de sistemas de información y evaluar si cumplen los objetivos de los mismos. Verificar si el comité de Informática existe y cumple su papel adecuadamente. Revisar el emplazamiento del departamento de Informática y evaluar su dependencia frente a otros. Evaluar la existencia de estándares de funcionamiento, procedimientos y descripciones de puestos de trabajo adecuados y actualizados. Evaluar las características de la comunicación entre la Dirección de Informática y el personal del Departamento. Y por último verificar la existencia de un sistema de reparto de costes informáticas y que este sea justo.

PREGUNTAS (Dirección)	S	N	N/A
¿La dirección de los servicios de Información desarrolla regularmente planes a corto, medio y largo plazo que apoyen el logro de la misión y las metas generales de la organización?			
¿Dispone su entidad de un plan Estratégico de Tecnología de Información?			
¿Durante el proceso de planificación, se presta adecuada atención al plan estratégico de la empresa?			
¿Las tareas y actividades en el plan tiene la correspondiente y adecuada asignación de recursos?			
¿Existe un comité de informática?			
¿Existen estándares de funcionamiento y procedimientos que gobiernen la actividad del área de informática por un lado y sus relaciones con los departamentos usuarios por otro?			
¿Existen estándares de funcionamiento y procedimientos y descripciones de puestos de trabajos adecuados y actualizados?			

PREGUNTAS (Dirección)	S	N	N/A
¿Los estándares y procedimientos existentes promueven una filosofía adecuada de control?			
¿Las descripciones de los puestos de trabajo reflejan las actividades realizadas en la práctica?			
¿La selección de personal se basa en criterios objetivos y tiene en cuenta la formación, experiencia y niveles de responsabilidad?			
¿El rendimiento de cada empleado se evalúa regularmente en base a estándares establecidos?			
¿Existen procesos para determinar las necesidades de formación de los empleados en base a su experiencia?			
¿Existen controles que tienden a asegurar que el cambio de puesto de trabajo y la finalización de los contratos laborales no afectan a los controles internos y a la seguridad informática?			
¿Existe un presupuesto económico? ¿y hay un proceso para elaborarlo?			
¿Existen procedimientos para la adquisición de bienes y servicios?			
¿Existe un plan operativo anual?			
¿Existe un sistema de reparto de costes informáticos y que este sea justo?			
¿Cuentan con pólizas de seguros?			

PREGUNTAS (Dirección)	S	N	N/A
¿Existen procedimientos para vigilar y determinar permanentemente la legislación aplicable?			

7.2. CALIDAD

Con la siguiente lista de comprobación sobre Calidad se pretende comprobar que los procesos aplicables del programa de calidad han sido desarrollados y documentados correctamente.

PREGUNTAS (Calidad)	S	N	N/A
¿Se reflejan el software codificado tal como en el diseño en la documentación?			
¿Se probaron con éxito los productos de software usados en el centro de procesos?			
¿Se cumplen las especificaciones de la documentación del usuario del software?			
¿Los procesos de gestión administrativa aplicados en el área de informática de la institución son lo suficientemente óptimos?			
¿El funcionamiento del software dentro del área de trabajo está de acuerdo con los requerimientos específicos?			

PREGUNTAS (Calidad)	S	N	N/A
¿Los productos de software que utilizan en el área de informática esta de acuerdo con los estándares establecidos?			
¿Los dispositivos de trabajo en el área de informática se les realizan una revisión técnica correcta?			
¿Los costes fijados en la revisión técnica se encuentran dentro de los límites fijados?			

7.3. SEGURIDAD

Además de obtener información sobre los riesgos y deficiencias en el Sistema de Seguridad. Realiza un análisis sobre la organización y calificación del persona, sus planes y procedimientos, sistemas técnicos de detección y comunicación, análisis de puestos, mantenimiento y normativa.

Una segunda parte expone una relación de cuestiones sobre personal encargado de la seguridad, acceso a los recursos y en particular a la Base de Datos, gestión y control de cambios y todos aquellos aspectos que puedan incidir en la seguridad del sistema.

A la vista de los resultados obtenidos al realizar la Lista de Comprobación sobre seguridad, podremos comprobar la existencia de los procedimientos, normas y conductas de seguridad necesarias para un buen funcionamiento del Repositorio, y así evitar posibles fallos en el funcionamiento de las aplicaciones e incluso posibles fallos catastróficos para el negocio, la empresa y sus clientes.

PREGUNTAS (Seguridad)	S	N	N/A
¿Existen medidas, controles, procedimientos, normas y estándares de seguridad?			
¿Existe un documento donde este especificado la relación de las funciones y obligaciones del personal?			
¿Existen procedimientos de realización de copias de seguridad y de recuperación de datos?			

7.3.1. Seguridad Lógica

¿Existe un administrador de sistemas que controla a los usuarios?			
¿Dicho Administrador gestiona los perfiles de los usuarios?			
¿Existe una relación del personal autorizado a conceder, alterar o anular el acceso sobre datos y recursos?			
¿Existe una relación de controles periódicos a realizar para verificar el cumplimiento del documento?			
¿Se realizan periódicamente revisiones del perfil de los usuarios?			
¿Existen medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado?			
¿Existe una relación del personal autorizado a acceder a los locales done se encuentran ubicados los sistemas que tratan datos personales?			

PREGUNTAS (Seguridad)	S	N	N/A
¿Existe una relación de personal autorizado a acceder a los soportes de datos?			
¿Existe un periodo máximo de vida de las contraseñas?			
¿Existe una relación de usuarios autorizados a acceder a los sistemas y que incluyen los tipos de acceso permitidos?			
¿Los derechos de acceso concedidos a los usuarios son los necesarios y suficientes para el ejercicio de las funciones que tienen encomendadas, las cuales a su vez se encuentran o deben estar-documentadas en el Documento de Seguridad?			
¿Hay dadas de alta en el sistema cuentas de usuario genéricas, es decir, utilizadas por más de una persona, no permitiendo por tanto la identificación de la persona física que las ha utilizado?			
¿En la práctica las personas que tienen atribuciones y privilegios dentro del sistema para conceder derechos de acceso son las autorizadas e incluidas en el Documento de Seguridad?			
¿El sistema de autenticación de usuarios guarda las contraseñas cifradas?			
¿En el sistema están habilitadas para todas las cuentas de usuario las opciones que permiten establecer? • Un número máximo de intentos de conexión • Un período máximo de vigencia para la contraseña, coincidente con el establecido en el Documento de Seguridad			

PREGUNTAS (Seguridad)	S	N	N/A
¿Existe procedimiento de asignación y distribución de contraseñas?			

7.3.2. Seguridad Física

¿Existe un acceso restringido a la sala de servidores?			
¿Existen mecanismo de seguridad física en las salas de servidores?			
¿Se dispone de equipos auxiliares en caso de caída o avería del equipo principal?			
¿Se dispone de generador de energía auxiliar para asegurar la corriente a los servidores?			
¿Existen procedimientos para la realización de las copias de seguridad?			
¿Existen procedimientos que aseguran que, de todos los ficheros con datos de carácter personal, se realiza copia al menos una vez cada semana?			
¿Hay procedimientos que aseguran la realización de copias de todos aquellos ficheros que han experimentado algún cambio en su contenido?			
¿Existen controles sobre el acceso físico a las copias de seguridad?			
¿Sólo las personas con acceso autorizado en el documento de seguridad tienen acceso a los soportes que contienen las copias de seguridad?			

PREGUNTAS (Seguridad)	S	N	N/A
¿Las copias de seguridad de ficheros de nivel alto incluyen los ficheros cifrados, si estas copias se transportan fuera de las instalaciones?			
¿Las copias de seguridad de los ficheros de nivel alto se almacenan en lugar diferente al de los equipos que las procesan?			
¿Existe un inventario de los soportes existentes?			
¿Dicho inventario incluye las copias de seguridad?			
¿Las copias de seguridad, o cualquier otro soporte, se almacenan fuera de la instalación?			
¿Existen procedimientos de actualización de dicho inventario?			
¿Existen procedimientos de etiquetado e identificación del contenido de los soportes?			
¿Existe procedimientos en relación con la salida de soportes fuera de su almacenamiento habitual?			
¿Se evalúan los estándares de distribución y envío de estos soportes?			
¿Se obtiene una relación de los ficheros que se envían fuera de la empresa, en la que se especifique el tipo de soporte, la forma de envío, el estamento que realiza el envío y el destinatario?			

PREGUNTAS (Seguridad)	S	N	N/A
¿Se obtiene una copia del Registro de Entrada y Salida de Soportes y se comprueba que en él se incluyen: • Los soportes incluidos en la relación del punto anterior • Los desplazamientos de soporte al almacenamiento exterior (si existiera)			
¿Se verifica que el Registro de Entrada y Salida refleja la información requerida por el Reglamento: • Fecha y hora • Emisor/Receptor • Nº de soportes • Tipo de información contenida en el soporte • Forma de envío • Persona física responsable de la recepción/entrega			
¿Existen controles para detectar incidencias referentes a la falta de actualización de los Registros Entrada/Salida?			
¿Se determina que personas tienen llaves de acceso, tarjetas, etc de acceso a la sala?			
¿Existen procedimientos de realización de copias de seguridad del Registro de Acceso y el período de retención de las copias?			
¿Se comprueba que le Registro de Accesos se encuentra bajo el control directo del Responsable de Seguridad pertinente?			

PREGUNTAS (Seguridad)	S	N	N/A

7.3.3. Seguridad referente a la Administración de la Base de Datos

¿Están monitorizados los acceso de usuarios a la base de datos?			
¿Se comprueba periódicamente los registros de accesos de los usuarios?			
¿Existe un acceso restringido a las instancias que contienen el Repositorio?			
¿Existen listados de intentos de accesos no satisfactorios o denegados a estructuras, tablas físicas y lógicas del repositorio?			
¿Existen un diseño físico y lógico de la Base de Datos?			
¿El Diccionario de datos dispone de diseño físico y lógico?			
¿Existe una instancia con copia del Repositorio para el entorno de desarrollo?			
¿Está restringido el acceso al entorno de desarrollo?			
¿Se utilizan datos reales en el entorno de desarrollo?			
¿Existe un formulario de petición de cambio o modificación en el Repositorio?			
¿Es necesaria la autorización del Administrador para realizar cambios en el repositorio?			

PREGUNTAS (Seguridad)	S	N	N/A
¿Se realiza la modificación sobre la copia de seguridad del Repositorio?			
¿Existe algún fichero log que almacene todos los cambios realizados en el repositorio?			
¿Se realizan pruebas sobre el cambio para comprobar que la aplicación funciona correctamente?			
¿Se comprueba que el cambio solicitado se corresponde con lo realizado?			
¿Existe documentación escrita sobre el cambio (formulario de petición, script del cambio realizado, aprobación del solicitante)?			

7.4. EVALUACIÓN DE LAS ÁREAS CRÍTICAS DE LA SEGURIDAD

Con la siguiente relación de preguntas se obtiene una evaluación de las áreas críticas del la seguridad del sistema, con ello se consigue otra forma de obtener más información. Son preguntas cuya finalidad es determinar el grado de cumplimiento y efectividad de aspectos muy importantes en la seguridad, como son:

- Seguridad en el acceso al sistema
- Seguridad en el área física
- Planes de contingencia informático

- Seguridad en los sistemas computacionales
- Protección contra el robo y la piratería de información
- Protección contra virus informáticos
- Seguridad del hardware
- Seguridad del software

Preguntas	100% Excelente	80% Bueno	60% Regular	40% Mínimo	20% No cumple
Evaluación de la seguridad en el acceso al Sistema					
Evaluar los atributos de acceso al sistema.					
Evaluar los niveles de acceso al sistema.					
Evaluar la administración de contraseñas al sistema.					
Evaluar el monitoreo en el acceso al sistema.					
Evaluar las funciones del administrador del acceso al sistema.					
Evaluar las medidas preventivas o correctivas en caso de siniestros en el acceso.					

Evaluación de la seguridad en el Área Física					
Evaluar el acceso del personal al centro de procesos.					
Evaluar el acceso de los usuarios y terceros al centro de procesos.					
Evaluar el control de entradas y salidas de bienes informáticos del centro de procesos.					
Evaluar la vigilancia del centro de procesos.					
Analizar las políticas de la instalación en relación con los accesos ocasionales a la salida.					
Evaluación de los planes de contingencias informáticos					
Evaluar la existencia, difusión, aplicación y uso de contra contingencias de sistemas.					
Evaluar la aplicación de simulacros, así como el plan contra contingencias.					
Evaluar la confidencialidad, veracidad y oportunidad en la aplicación de las medidas del plan contra contingencias.					

Evaluación de la seguridad en los sistemas computacionales					
Evaluar el rendimiento y uso del sistema computacional y de sus periféricos asociados.					
Evaluar la existencia, protección y periodicidad de los respaldos de bases de datos e información importante de la organización.					
Evaluar la configuración, instalación y seguridad del equipo de cálculo, mobiliario y demás equipos.					
Evaluar la seguridad en el procesamiento de la información.					
Evaluar los procedimientos de captura, procesamiento de datos y emisión de resultados de los sistemas computacionales.					
Evaluación de la protección contra robo y piratería de información					
Medidas preventivas					
Protección de archivos					
Limitación de accesos					
Protección contra robos					

Protección ante copias ilegales					
Evaluación de la protección contra virus informáticos					
Medidas preventivas y correctivas					
Uso de vacunas y buscadores de virus					
Protección de archivos, programas e información.					
Evaluación de la seguridad del hardware					
Realización de inventarios de hardware, equipos y periféricos asociados.					
Evaluar la configuración del equipo de procesos (hardware).					
Evaluar el rendimiento y uso del sistema computacional y sus periféricos asociados.					
Evaluar el estado físico del hardware, periféricos y equipos asociados.					
Evaluación de la seguridad del Software					
Realización de inventarios de software, paqueterías y desarrollos empresariales.					

Evaluar las licencias permisos y usos de los sistemas computacionales.					
Evaluar el rendimiento y uso del software de los sistemas computacionales.					
Verificar que la instalación del software, paqueterías y sistemas desarrollados en la empresa sea la adecuada para cubrir las necesidades de esta última.					

7.5. BASES DE DATOS

Con la realización de las siguientes Listas de Comprobación se pretende estudiar la explotación, mantenimiento, diseño, carga, post implementación de sistema de bases de datos así como el SGBD, software de auditoría y el resto de sistemas.

PREGUNTAS (Bases de Datos)	S	N	N/A
¿Existe equipos o software de SGBD?			
¿La organización tiene un sistema de gestión de bases de datos (SGBD)?			
¿Los datos son cargados correctamente en el interfaz gráfica?			
¿Se verificará que los controles y relaciones de datos se realizan de acuerdo a las políticas establecidas en la organización?			

PREGUNTAS (Bases de Datos)	S	N	N/A
¿Existe personal restringido que tenga acceso a la BD?			
¿El SGBD es dependiente de los servicios que ofrece el Sistema Operativo?			
La interfaz que existe entre el SGBD y el SO es el adecuado			
¿Existen procedimientos formales para la operación del SGBD?			
¿Están actualizados los procedimientos de SGBD?			
¿La periodicidad de la actualización de los procedimientos es Anual?			
¿Son suficientemente claras las operaciones que realiza la BD?			
¿Existe un control que asegure la justificación de los procesos en el ordenador? (Que los procesos que están autorizados tengan una razón de ser procesados)			
¿Se procesa las operaciones dentro del departamento de procesos?			
¿Se verifican con frecuencia la validez de los inventarios de los archivos magnéticos?			
¿Existe un control estricto de las copias de estos archivos?			
¿Se borran los archivos de los dispositivos de almacenamiento, cuando se desechan estos?			

PREGUNTAS (Bases de Datos)	S	N	N/A
¿Se registran como parte del inventario las nuevas cintas magnéticas que recibe el centro de procesos?			
¿Se tiene un responsable del SGBD?			
¿Se realizan auditorías periódicas a los medios de almacenamiento?			
¿Se tiene relación del personal autorizado para manipular la BD?			
¿Se lleva control sobre los archivos transmitidos por el sistema?			
¿Existe un programa de mantenimiento preventivo para el dispositivo del SGBD?			
¿Existen integridad de los componentes y de seguridad de datos?			
De acuerdo con los tiempos de utilización de cada dispositivo del sistema de procesos, ¿existen equipos capaces de soportar la carga de trabajo?			
¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?			
¿La capacidad de almacenamiento máximo e la BD es suficiente para atender el proceso por lotes y el proceso remoto?			

7.6. ADMINISTRADOR DE LA BASE DE DATOS

La figura del Administrador de Base de Datos es muy importante, es la encargada de mantener el correcto funcionamiento de la base de datos, así como establecer las medidas necesarias para su rendimiento y seguridad.

Puede existir empresas, que no posean esta persona o equipo, debido a costes, y sea una persona del departamento informático que se atribuya dicha funcionalidad además de la suya propia.

El Administrador de Bases de Datos es la persona que nos puede aportar información muy útil para poder llevar a cabo la auditoría, debido a que es la persona que posee dicha información. Por ello es importante poner una especial atención a las preguntas que se les realiza.

PREGUNTAS (Administrador de la Base de Datos)	S	N	N/A
¿Existe Administrador de Base de la Base de Datos?			
¿Posee utilidades para administrar la base de datos?			
¿Existen tablas o registros de auditoría?			
¿Se mantienen las pistas de auditoría?			
¿Se utilizan las utilidades de Informix, onaudit y onshowaudit, para estudiar las anotaciones recogidas en los ficheros de auditoría?			
¿Considera que son suficientes las herramientas que posee para gestionar y mantener la base de datos?			
¿Utiliza las herramientas que proporciona Informix, a través privilegios, vistas, funciones, roles u otros mecanismos, para gestionar el control de acceso a la base de datos?			

PREGUNTAS (Administrador de la Base de Datos)	S	N	N/A
¿Es usted la persona encargada de realizar las copias de seguridad?			
¿Considera que el plan de copias de seguridad que existen en la actualidad necesita ser mejorada?			
¿Tienen un Plan de Contingencias y continuidad que garanticen el buen funcionamiento del Repositorio o Diccionario e Datos?			
¿En el Plan se identifican los riesgos y sus posibles alternativas?			
¿Revisa o está implicada la Dirección en la implantación y en el control de modificaciones que se realizan sobre el sistema de base de datos?			
¿Les pide información la Dirección sobre la calidad del sistema?			
¿Se han hecho algún estudio que releve la forma más sencilla y menos costosa de cambiar y mejorar el sistema?			
¿Se someten los elementos más críticos a pruebas especiales?			
En caso de si: ¿Se contrata personal externo especializado para realizarlo, como puede ser un auditor, consultor o experto en informática?			
¿Cuándo se realizan pruebas de aplicaciones o software, se asegura que los datos que se utilizan so ficticios o no relevantes?			
¿Si son reales, se comprueba que sean eliminados después de la prueba?			

PREGUNTAS (Administrador de la Base de Datos)	S	N	N/A
¿Si no se pueden borrar, se asegura que sólo algunos empleados tienen la autoridad y acceso para poder llevarlas a cabo y quedan debidamente registrados todos los acceso que realizan?			

7.7. EL SISTEMA

El siguiente cuestionario pretende estudiar la organización y cualificación del personal de Seguridad, el entorno de trabajo, los planes y procedimientos utilizados así como los sistemas técnicos de seguridad y protección existentes. Todo ello para poder verificar la seguridad, confianza, privacidad, utilidad en el entorno informático de la entidad. Parte de esta información será aportada por el Administrador de bases de datos.

PREGUNTAS (Sistema)	S	N	N/A
¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?			
¿Existe una persona responsable de la seguridad?			
¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?			
¿Existe personal de vigilancia en la institución?			
¿Existe una clara definición de funciones entre los puestos clave?			

PREGUNTAS (Sistema)	S	N	N/A
¿Se investiga a los vigilantes cuando son contratados directamente?			
¿Se controla el trabajo fuera de horario?			
¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar lo sistemas?			
¿Existe vigilancia en el departamento de procesos las 24 horas?			
¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?			
¿Se ha instruido a estas personas sobre qué medidas tomar en caso de que alguien pretenda entrar sin autorización?			
¿El centro de procesos tiene salida exterior?			
¿Son controladas las visitas y demostraciones en el centro de procesos?			
¿Se registra el acceso al departamento de procesos de personas ajenas a la dirección de informática?			
¿Se vigila la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar posible fraude?			
¿Se ha adiestrado el personal en el manejo de los extintores?			
¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?			

PREGUNTAS (Sistema)	S	N	N/A
¿Si es que existen extintores automáticos son activados por detectores automáticos de fuego?			
¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?			
¿Saben que hacer los operadores del departamento de procesos, en caso de que ocurra una emergencia ocasionada por el fuego?			
¿El personal ajeno a operación sabe que hacer en caso de una emergencia (incendio)?			
¿Existe una salida de emergencia?			
¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?			
¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?			
¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de procesos para evitar daños al equipo?			
¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?			
¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?			
¿Se tienen establecidos procedimientos de actualización a estas copias?			

PREGUNTAS (Sistema)	S	N	N/A
¿Existe departamento de auditoría interna en la institución?			
¿Este departamento de auditoría interna conoce todos los aspectos de los sistemas?			
¿Se cumplen?			
¿Se auditan los sistemas en operación?			
Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?			
¿Existe control estricto en las modificaciones?			
¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?			
¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?			

7.8. EXPLOTACIÓN DE LOS SISTEMAS

Se pretende obtener información sobre el personal, organización, normas y procedimientos en el área informática.

PREGUNTAS (Explotación del Sistema)	S	N	N/A
¿Existe personal con conocimiento y experiencia suficiente que organiza el trabajo para que resulte lo más eficaz posible?			
¿Existen procedimientos de salvaguardar, fuera de la instalación en relación con ficheros maestros, manuales y programas, que permitan construir las operaciones que sean necesarias?			
¿Se aprueban por personal autorizado las solicitudes de nuevas aplicaciones?			
¿Existe personal con autoridad suficiente que es el que prueba los cambios de unas aplicaciones por otras?			
¿Existen procedimientos adecuados para mantener la documentación al día?			
¿Tienen manuales todas las aplicaciones?			
¿Existen controles que garanticen el uso adecuado de discos y cintas?			
¿Existen procedimientos adecuados para conectarse y desconectarse de los equipos remotos?			

PREGUNTAS (Explotación del Sistema)	S	N	N/A
¿Se aprueban los programas nuevos y lo que se revisan antes de ponerlos en funcionamiento?			
¿Revisan y evalúan los departamentos de usuarios los resultados de las pruebas finales dando su aprobación antes de poner en funcionamiento las aplicaciones?			
Al poner en funcionamiento nuevas aplicaciones o versiones actualizadas ¿funcionan en paralelo las existentes durante un periodo de tiempo?			
¿Se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento, al personal autorizado?			
¿Se tiene relación del personal autorizado para firmar la salida de archivos confidenciales?			
¿Existen parámetros de control?			

7.9. COPIAS DE SEGURIDAD Y RESTAURACIÓN

PREGUNTAS (Copias de Seguridad y Restauración)	S	N	N/A
¿Existe una política de copias de seguridad?			
¿Se realizan copias de seguridad de la base de datos periódicamente?			

PREGUNTAS (Copias de Seguridad y Restauración)	S	N	N/A
¿Se realizan copias de seguridad de los archivos de anotaciones?			
¿Se guardan las copias de seguridad fuera del entorno?			
¿Existe en la empresa un periodo de inactividad en el que se pueda restaurar el sistema?			
En caso de que el sistema trabaja las 24 horas, los 7 días de la semana (ningún periodo de inactividad) ¿Existe algún tiempo de poca actividad en el que se pueda realizar una restauración?			
¿Cada copia de seguridad contiene todas las tablas de la Base de Datos?			
¿Se realizan copias de Seguridad Incremental?			
¿Se utilizan las herramientas que proporciona Informix, ontape y ON-Bar para realizar las copias de seguridad?			
¿Se utiliza ontape?			
¿Se utiliza ON-Bar?			
¿Se utiliza la utilidad archecker para comprobar la validez e integridad de las copias de seguridad?			
Si no se utilizan las herramientas de Informix, ¿Dispone de algún producto comercial que las lleve a cabo?			

7.10. RENDIMIENTO DE LA BASE DE DATOS

PREGUNTAS (Rendimiento Base de Datos)	S	N	N/A
¿La Base de Datos posee tablas fragmentadas?			
En caso afirmativo - ¿Comprueban periódicamente si están balanceadas?			
¿Se han hecho estudios sobre pruebas de rendimiento de las aplicaciones en el acceso a los datos?			
¿Se consigue con la fragmentación alguno de los objetivos: tiempo de respuesta, concurrencia, disponibilidad?			
¿Considera que la fragmentación que tiene considera que es la más adecuada?			
¿Se utiliza la herramienta de Informix, onstat, para observar y monitorizar el rendimiento del sistema?			
¿Considera que los parámetros de recogidos en el fichero ONCONFIG pueden ser mejorados para aumentar el rendimiento del sistema?			
¿Se comprueba que las consultas a la base de datos por parte de las aplicaciones están optimizadas?			

7.11. PERSONAL INFORMÁTICO

PREGUNTAS (Personal Informático)	S	N	N/A
¿La formación que recibe es suficiente para mantener y mejorar el sistema?			
¿La documentación que posee el personal informático es suficiente?			
¿Existe una política de mejora de la calidad?			
¿Existen niveles de privilegio en el acceso al sistema y base de datos?			
¿Las medidas tomadas para la mejora de la calidad consideran que son suficientes?			
Si es diseñador.- ¿En la fase de desarrollo se incluye mecanismos de control, de seguridad, pistas de auditoría y otros aspectos que puedan realizarse?			
¿Existe un inventario en la compañía de sistemas, hardware y datos?			
¿Se revisa periódicamente el inventario?			
¿Se sabe quiénes son los usuarios de los elementos del inventario?			
¿Existe un criterio para valorar cuáles son los elementos críticos del inventario?			

PREGUNTAS (Personal Informático)	S	N	N/A
¿Tiene un Plan de Pruebas que incluya, al menos, una especificación del tipo de pruebas, la fecha de comienzo de las pruebas, los recursos (hardware, humanos y tiempo) para realizar las pruebas y la especificación de uno de los casos?			
¿Los responsables de realizar las pruebas tiene la formación adecuada?			
¿El personal de la organización sabe que tiene soporte si ocurren problemas?			

7.12. DESARROLLO

La siguiente lista de preguntas pretende obtener información sobre las metodologías utilizadas, el control interno de las aplicaciones y el ciclo de vida del desarrollo del software. Todo esto es muy importante, y es necesario que desde el momento del desarrollo se introduzcan controles que van a ayudar a las auditorías y a la integridad del sistema.

PREGUNTAS (Desarrollo)	S	N	N/A
¿Existe un documento que contenga las funciones que son competencia del área de desarrollo, está aprobado por la dirección de informática y se respeta?			
¿Se comprueban los resultados con datos reales?			
¿Existe un organigrama con la estructura de organización del área?			

PREGUNTAS (Desarrollo)	S	N	N/A
¿Existe un manual del organización que regulas las relaciones entre puestos?			
¿El plan existe, es claro y realista?			
¿El personal de área de desarrollo cuenta con la formación adecuada y son motivados para la realización de su trabajo?			
¿Las personas seleccionadas cumplen los requisitos del puesto al que acceden?			
¿El personal esta motivado en la realización de su trabajo?			
¿Existe algún mecanismo que permita a los empleados hacer sugerencias sobre mejoras en la organización del área?			
¿Existe rotación de personal y existe un buen ambiente de trabajo?			
¿Los cambios en los planes de los proyectos se comunican al responsable de mantenimiento del plan de sistemas?			
¿Existe un procedimiento de aprobación de nuevos proyectos?			
¿Se tiene implantada una metodología de desarrollo de sistemas de información soportada por herramientas de ayuda?			
¿Las metodologías y las técnicas asociadas a la misma están adaptadas al entorno tecnológico y a la organización del área de desarrollo?			
¿Existe catálogo de aplicaciones disponibles en el área?			

7.13. MANTENIMIENTO

El conjunto de preguntas que contiene el apartado tiene como objetivo poder realizar una evaluación del mantenimiento correctivo y preventivo del software. Para ello se desea obtener referencias acerca de los planes y procedimientos de mantenimiento que se tienen y la normativa.

PREGUNTAS (Mantenimiento)	S	N	N/A
¿Existe un contrato de mantenimiento?			
¿Existe un programa de mantenimiento preventivo para cada dispositivo del sistema de cálculo?			
¿Existe plan de mantenimiento preventivo?			
¿Se notifican los errores?			
¿Se les da seguimiento?			
¿Las variaciones en el diseño son supervisadas durante el desarrollo para establecer su impacto sobre el mantenimiento?			
¿Se realizan varios tipos de medidas para poder estimar la calidad del software?			
¿El mantenimiento se tiene en cuenta antes de empezar el desarrollo?			
¿Durante el análisis de requerimientos, los siguientes aspectos que afectan al mantenimiento, son tomados en cuenta? • Identificación y definición de funciones, especialmente las opcionales.			

PREGUNTAS (Mantenimiento)	S	N	N/A
• Exactitud y organización lógica de los datos. • Los Interfaces (de máquina y de usuario). • Requerimientos de rendimiento • Requerimientos impuestos por el entorno (presupuesto). • Granularidad (detalle) de los requerimientos y su impacto sobre la trazabilidad. • Énfasis del Plan de Aseguramiento de Calidad del Software en el cumplimiento de las normas de documentación.			
¿La responsabilidad del mantenimiento se transfiere a una organización distinta, se elabora un Plan de Transición?, ¿qué es lo que incluye este plan? • La transferencia de hardware, software, datos y experiencia desde el desarrollador al mantenedor. • Las tareas necesarias para que el mantenedor pueda implementar una estrategia de mantenimiento del software.			
El Plan de Mantenimiento es preparado por el mantenedor durante el desarrollo del software.			
¿Los elementos software reflejan la documentación de diseño?			
¿Los productos software fueron suficientemente probados y sus especificaciones cumplidas?			
¿Los informes de pruebas son correctos y las discrepancias entre			

PREGUNTAS (Mantenimiento)	S	N	N/A
resultados actuales y esperados han sido resueltas?			
¿Los costes y calendarios se ajustan a los planes establecidos?			

CAPITULO 8

APLICACIÓN

8. APLICACIÓN

AGAI, Aplicación para la Gestión de Auditorías de Sistemas de Bases de Datos Informix, constituye un entorno de trabajo que permite gestionar y realizar todas aquellas tareas que lleva a cabo el Auditor así como su equipo de trabajo, durante el estudio y desarrollo de una Auditoría.

El volumen de documentación se que maneja en toda auditoría es muy importante y por ello considero que es necesario facilitar el acceso a dicha documentación así como un apoyo en la realización de la misma.

El objetivo de esta aplicación es tener una herramienta de trabajo que permita ayudar en el desarrollo y gestión de las auditorías que lleve a cabo el auditor. Así como su almacenamiento y accesibilidad a todas aquellas auditorías que hayan sido llevadas a cabo.

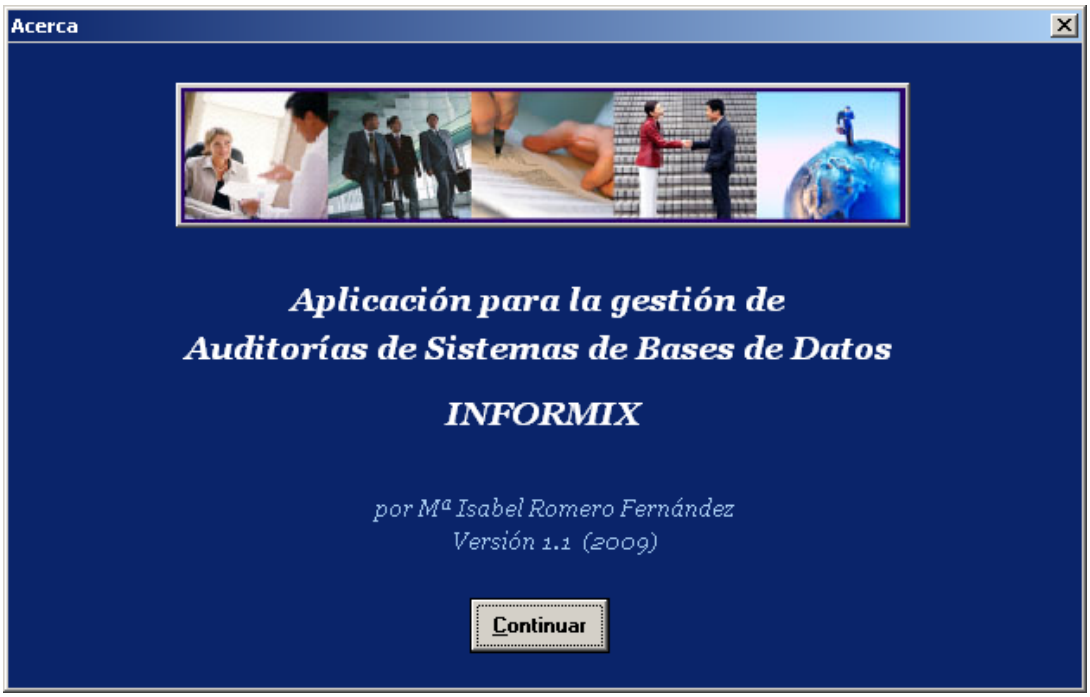
Esta aplicación, está desarrollada en el lenguaje de programación PowerBuilder, entorno de desarrollo de programación orientado a objetos, que ha sido muy importante en el desarrollo de este trabajo, permitiendo utilizar conceptos de orientación a objetos como la herencia. El conjunto de tablas en las que se apoya ésta herramienta han sido creadas en Informix, de tal forma que la información se obtiene de la base de datos Informix.

A continuación, en el Manual de Usuario, se exponen un conjunto de ventanas correspondientes a mantenimientos, ubicadas en la opción del Menú *Mantenimiento* que es imprescindible su carga inicial para poder poner en funcionamiento la aplicación. Así como los parámetros de configuración que van a recoger los lugares de almacenamiento de la documentación generada, y se encuentran recogidos en la pantalla *Configuración aplicación* alojada en la opción de Menú Administración.

Como toda aplicación, se puede adaptar a las necesidades de los usuarios o auditores, de tal forma que se ajuste a sus requerimientos y entorno de trabajo. En este caso, las características del entorno y necesidades abordadas han sido conclusiones obtenidas poco a poco a lo largo del desarrollo del Proyecto Fin de Carrera que he llevado a cabo.

8.1. MANUAL DE USUARIO

La aplicación se inicia a través del ejecutable “agai.exe” donde aparece la siguiente pantalla de presentación. Se podría añadir la funcionalidad de control de acceso, mediante dos campos donde se identifique el código de usuario y la password, la finalidad podría ser que cada usuario pudiera configurar la aplicación y guardarla, además también podría ser utilizado para que solo el auditor o grupo de auditoría que creó la auditoría tuviera acceso a su gestión y el resto de usuarios sólo tuvieran acceso en modo consulta.



Cabe destacar algunos aspectos generales de la aplicación, como son un acceso rápido, una buena ayuda y una correcta metodología de trabajo.

Muchas de las opciones del menú de la aplicación contienen una letra subrayada, por ejemplo “Salir”, son teclas de acceso rápido que nos permite activar una opción de forma rápida mediante la combinación de dos teclas, por ejemplo en este caso Ctrl + S. De esta forma la opción se activará sin necesidad de utilizar el ratón o las teclas de control y la letra correspondiente.

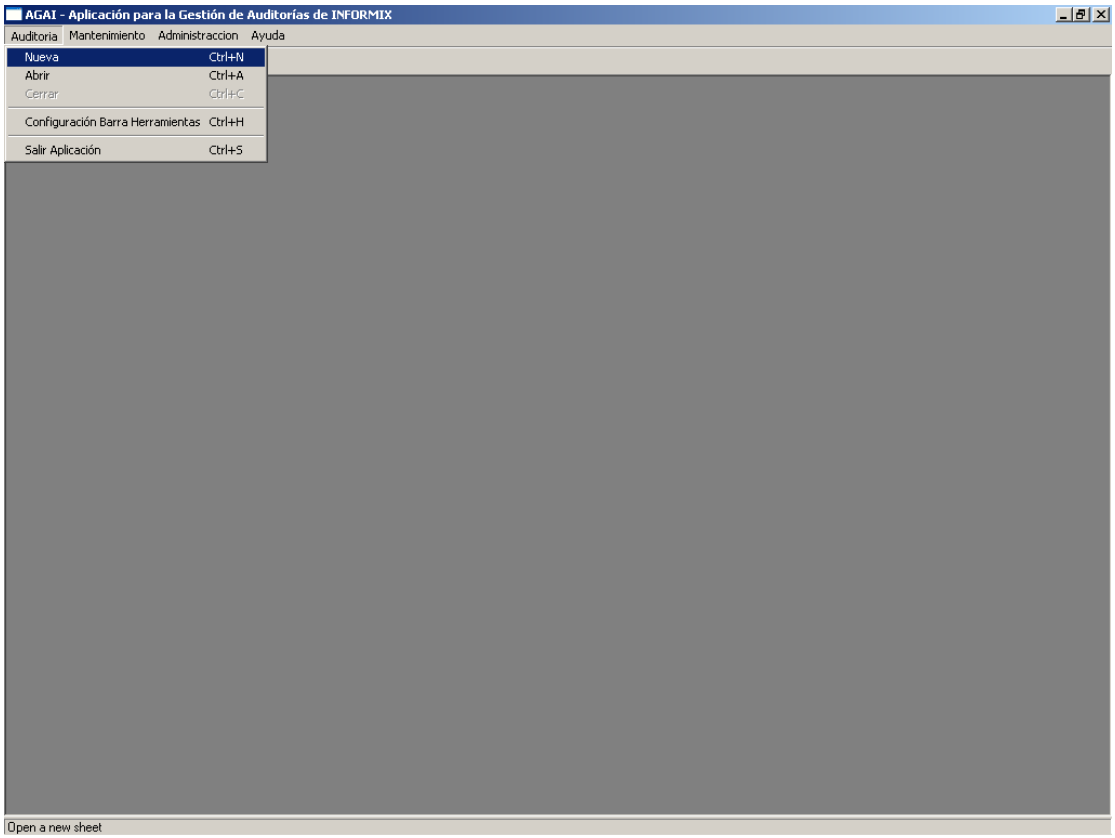
El sistema de Ayuda que proporciona la aplicación es a través de un botón que aparece en la parte derecha de cada ventana, con una interrogación amarilla  , donde se explica brevemente la funcionalidad de la ventana y algún otro aspecto que sea importante.

Esta aplicación gestiona la información de un Proyecto de estudio de auditoría a través de un conjunto de tablas y un conjunto de informes de Word, se presentan una relación de plantillas iniciales que podrán ser configuradas por el usuario, y que sirven de base para la realización de informes y almacenamiento de información. En la opción de Menú "Administración" se permite configurar donde se quiere localizar estos documentos, así como los archivos generados.

Cuando se inicia por primera vez la aplicación es aconsejable configurar los lugares de almacenamiento a través de las opciones presentadas en el Menú de *Administración* y además la carga de las tablas recogidas en el Menú *Mantenimiento*, donde se pueden grabar información que es necesaria a lo largo de la gestión de una auditoría. En algunos casos hay información que no se conoce de antemano, para estos casos se puede acceder cuando se disponga de ella.

8.1.1. Ventana principal

La ventana inicial da paso a la siguiente pantalla con acceso a los menús. Inicialmente sólo aparecen unas opciones básicas de la aplicación, creación, apertura o cierre de un proyecto de auditoría, mantenimiento de un conjunto de tablas con datos genéricos a todos los proyectos y configuración de los directorios de trabajo que está recogido en el menú Administración. La selección o creación de una Auditoría ampliará el conjunto de opciones de menús que nos permitirán trabajar con una auditoría determinada.



8.1.2. Opciones del Menú Auditoría

Auditoría: Donde se gestiona la selección, creación o cierre de un Proyecto de Auditoría para poder iniciar o finalizar la gestión del mismo. El submenú contiene las siguientes opciones:

Nueva Auditoría: Dar de Alta un Proyecto de Auditoría

Abrir Auditoría: Seleccionar un Proyecto de Auditoría de los existentes.

Cerrar Auditoría: Cerrar el Proyecto de Auditoría activo.

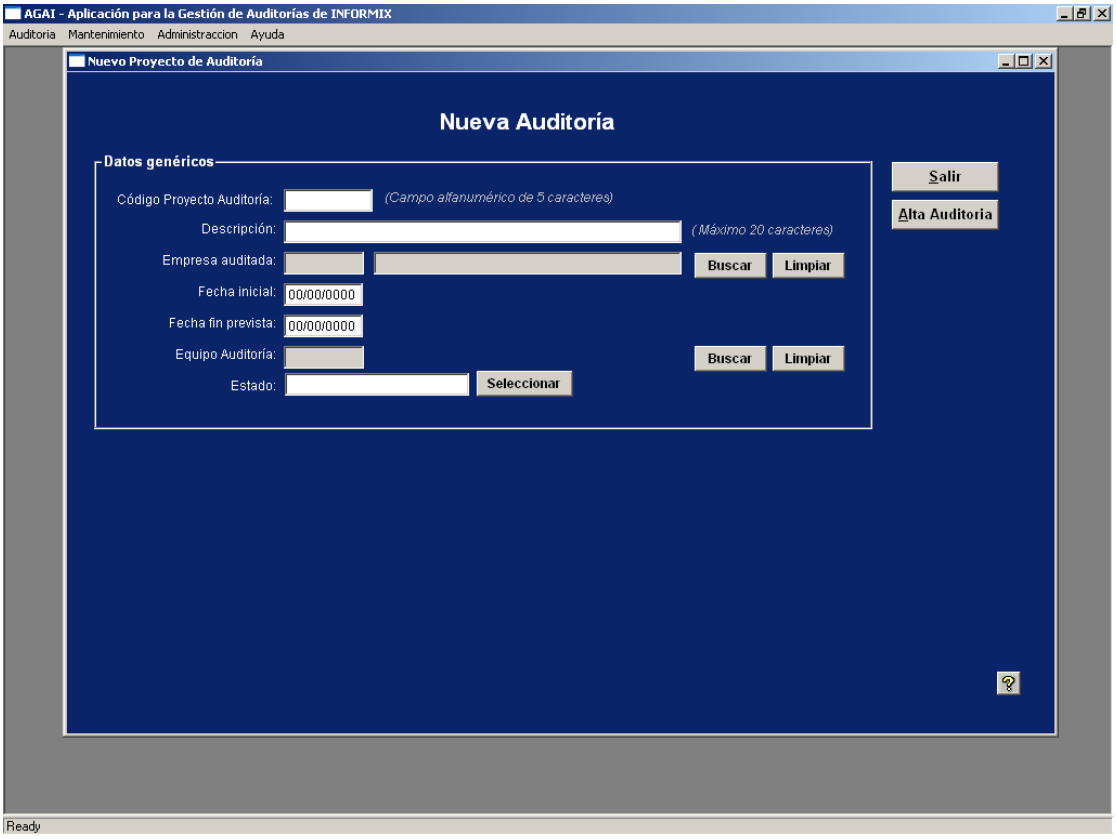
Configurar Barra de Herramientas: Cambiar de localización la barra.

Salir Aplicación: Salir de la aplicación,

Se puede observar que la opción *"Cerrar Auditoría"* permanece deshabilitada, esto se debe que no está activo ningún proyecto de Auditoría, se habilitará dicha opción cuando se esté trabajando con alguna auditoría.

- **Nueva**

Esta opción presenta la siguiente pantalla y es donde se piden todos los datos genéricos de un nuevo Proyecto de Auditoría, como son nombre, datos de la empresa de auditar, fechas de inicio y fin prevista, estado actual de la auditoría y datos del equipo de trabajo.



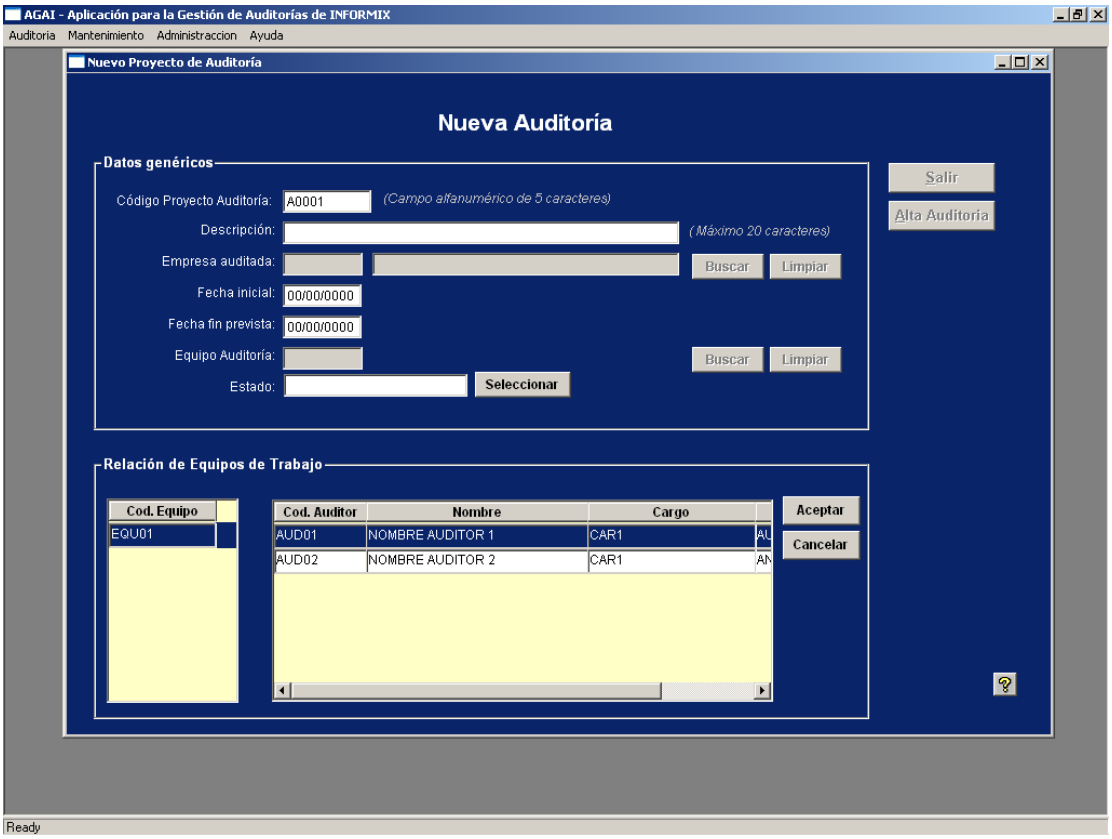
Junto a los campos “Empresa auditada” y “Equipo Auditoría” hay dos botones, Buscar y Limpiar, si pulsa el botón limpiar se quita el contenido de campo y si se pulsa el botón Buscar se presenta en la parte inferior de la pantalla, a continuación de los campos de entradas correspondientes a datos genéricos, un conjunto de tablas donde se puede seleccionar el equipo de trabajo o la empresa a auditar. Si no se encuentran los datos que se desean, es porque no están dados de alta y es necesario acceder a la opción de menú *Mantenimiento* y opciones *Empresas Auditadas* ó *Auditores* ó *Equipos de trabajo*, para proceder a su grabación.

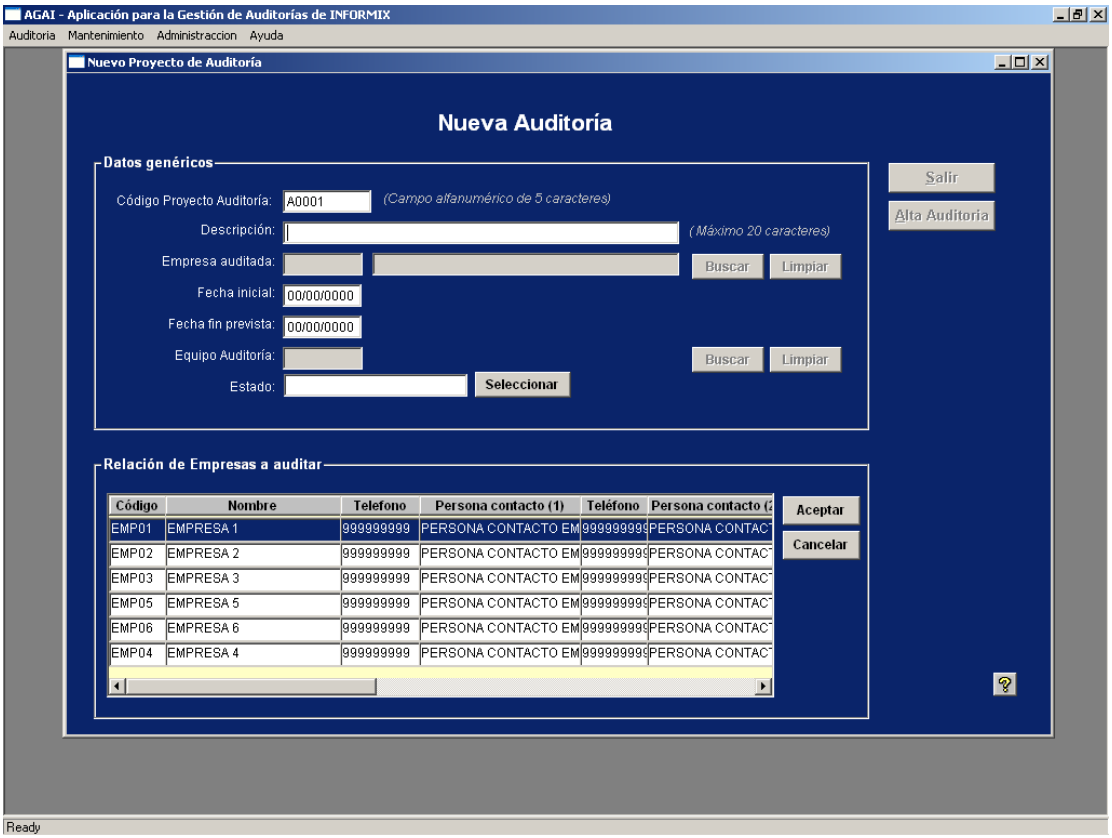
Como hemos indicado al pulsar el botón Buscar se muestra el detalle, donde sólo se puede abandonar y regresar a los datos generales, mediante la selección de un elemento y pulsar el botón aceptar o pulsando el botón cancelar.

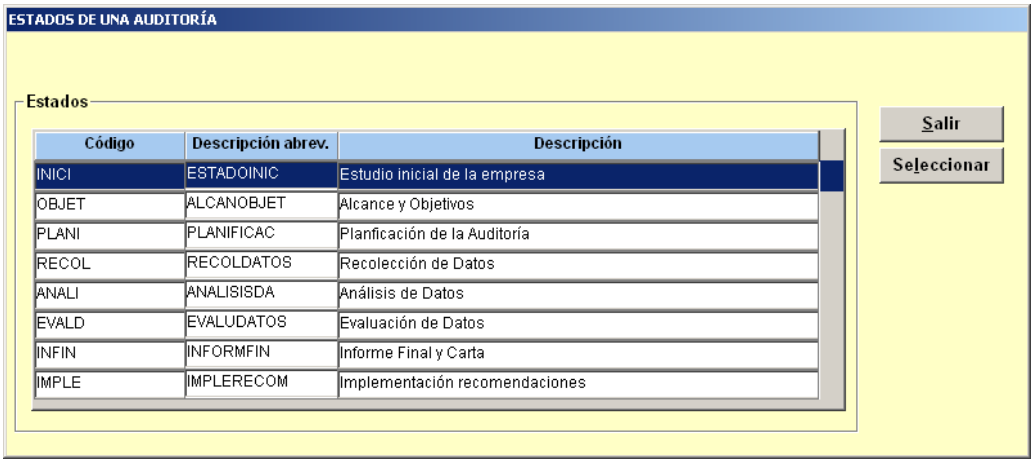
También junto al campo Estado se encuentra un botón, Seleccionar, que permite asignar un estado al proyecto. Este campo es muy importante darle valor, porque va a ser el que nos indique en qué fase se encuentra la Auditoría. El estado puede ser cambiado en dos pantallas más, en Modificar Auditoría y Cambio de Estado, más adelante se mostrará estas dos opciones.

Las pantallas de mantenimiento recoger la información de forma más detallada sobre éstos aspectos. Y como hemos comentado al inicio del manual, esta información corresponde a tablas básicas del proyecto, al igual que muchas otras que más adelante indicaremos. En la parte inferior derecha hay un botón que corresponde a la ayuda, donde se muestra de forma breve el objetivo de la ventana y como es su funcionamiento.

A continuación se muestra el aspecto de la ventana cuando se pulsan los botones de buscar o de seleccionar:



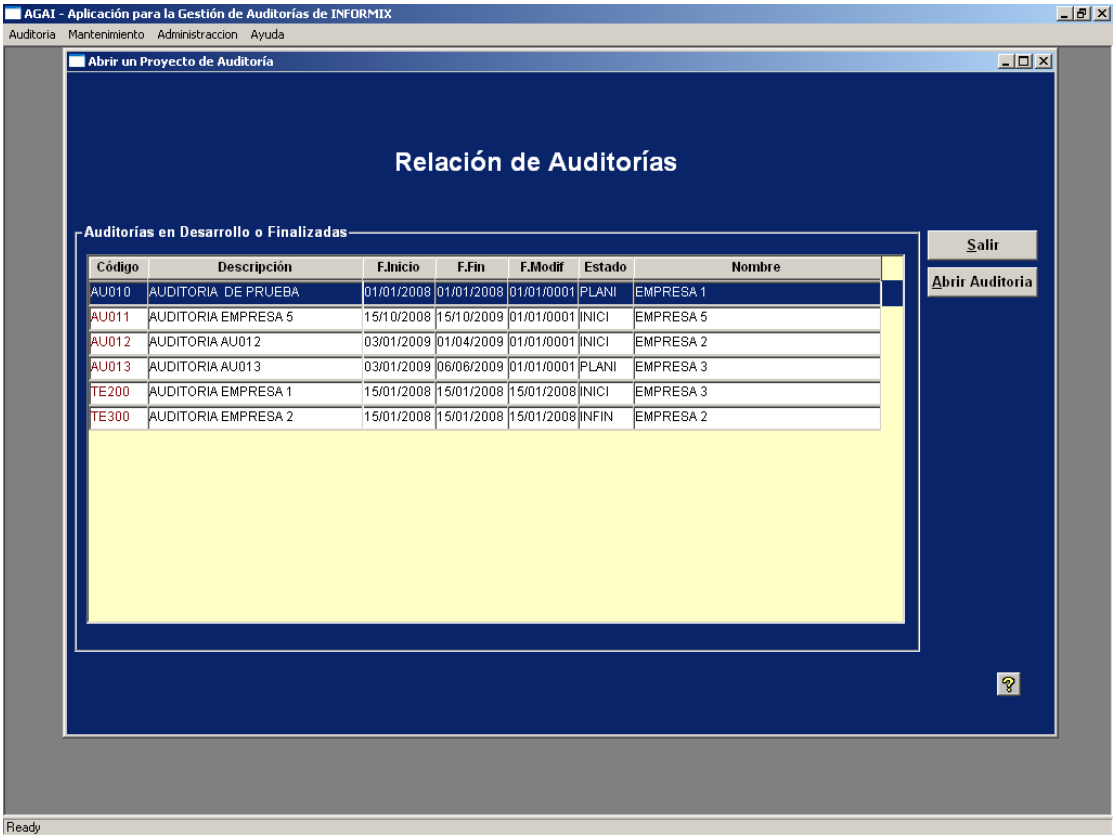




- **Abrir**

El acceso a la pantalla que abre una Auditoría puede realizarse de dos formas, desde el menú Abrir o desde el un icono que aparece en la barra de herramientas En la siguiente pantalla muestra una relación de las Auditorías gestionadas por la aplicación, donde se indica el código, descripción, fecha de inicio, fin y última modificación, estado y nombre

de la empresa auditada. Se presentan tanto las auditorías que se están gestionando en la actualidad como las ya finalizadas. Si ya existe una Auditoría abierta no se puede abrir otra, si ocurre dicho caso aparecerá un mensaje en la pantalla indicándolo.



Código	Descripción	F.Inicio	F.Fin	F.Modif	Estado	Nombre
AU010	AUDITORIA DE PRUEBA	01/01/2008	01/01/2008	01/01/0001	PLANI	EMPRESA 1
AU011	AUDITORIA EMPRESA 5	15/10/2008	15/10/2009	01/01/0001	INICI	EMPRESA 5
AU012	AUDITORIA AU012	03/01/2009	01/04/2009	01/01/0001	INICI	EMPRESA 2
AU013	AUDITORIA AU013	03/01/2009	06/06/2009	01/01/0001	PLANI	EMPRESA 3
TE200	AUDITORIA EMPRESA 1	15/01/2008	15/01/2008	15/01/2008	INICI	EMPRESA 3
TE300	AUDITORIA EMPRESA 2	15/01/2008	15/01/2008	15/01/2008	INFIN	EMPRESA 2

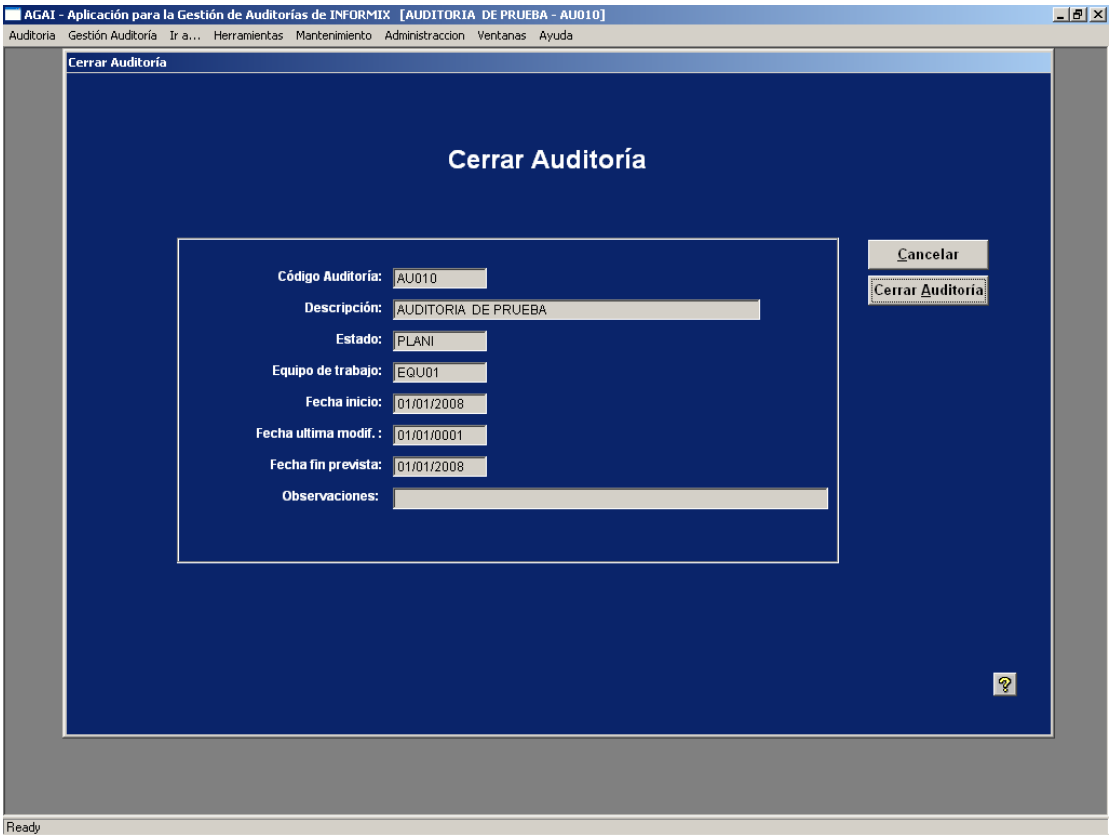
- **Cerrar**

Esta opción de Menú sólo permanecerá habilitada en el caso de que exista una Auditoría abierta, es decir, se haya accedido a la opción *Abrir* localizada en el menú de Auditoría. El acceso a esta opción puede realizarse por el menú o por el icono que aparece en la barra de herramientas, una cruz.

El significado de tener que Cerrar una Auditoría para poder acceder a otra es debido a que el conjunto de opciones de menú que aparecen en la barra de menú, excepto *Mantenimiento*, *Administración* ***y*** *Ayuda*, son correspondiente a una Auditoría en

particular, de tal forma que todas las gestiones que se realicen siempre hacen referencia al mismo proyecto de Auditoría. Es necesario ésta forma de trabajo debido a la gran cantidad de documentación y gestión que requiere una Auditoría.

En la barra de título de la aplicación, junto al nombre del programa, aparece el código y descripción de la auditoría que está activa.



- **Configuración Barra de Herramientas**

Esta opción permite cambiar la barra de herramientas, donde se encuentra un acceso rápido a las principales opciones de la aplicación.

- **Salir de la aplicación**

Mediante esta opción se abandona la aplicación, cerrando la auditoría en la que se estuviera trabajando.

8.1.3. Opciones del Menú Gestión Auditoría

Gestión Auditoría: Donde se gestiona y obtiene información de la Auditoría activa. El submenú contiene las siguientes opciones:

Modificar: Permite cambiar los datos particulares de la auditoría, como son descripción, fechas, estado, equipo de trabajo, etc.

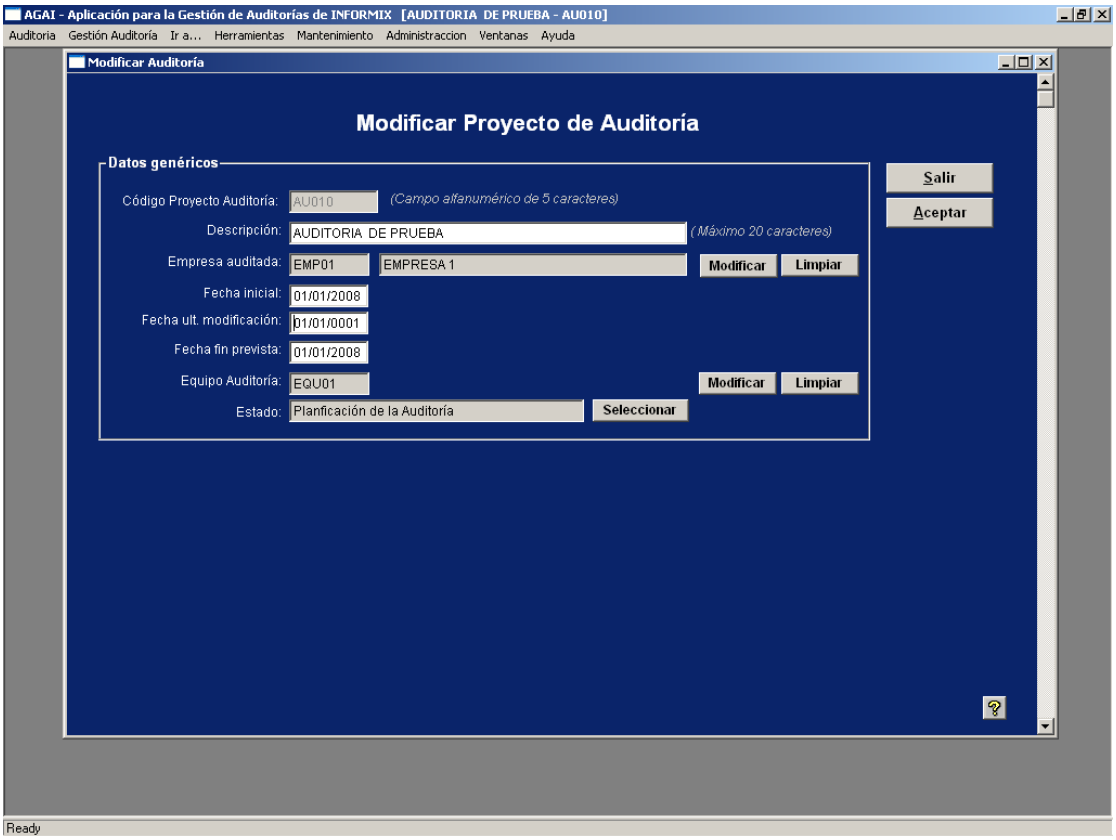
Cambiar Estado: Cambio de estado de una Auditoría.

Resumen Datos: Muestra datos significativos a la Auditoría.

- **Modificar**

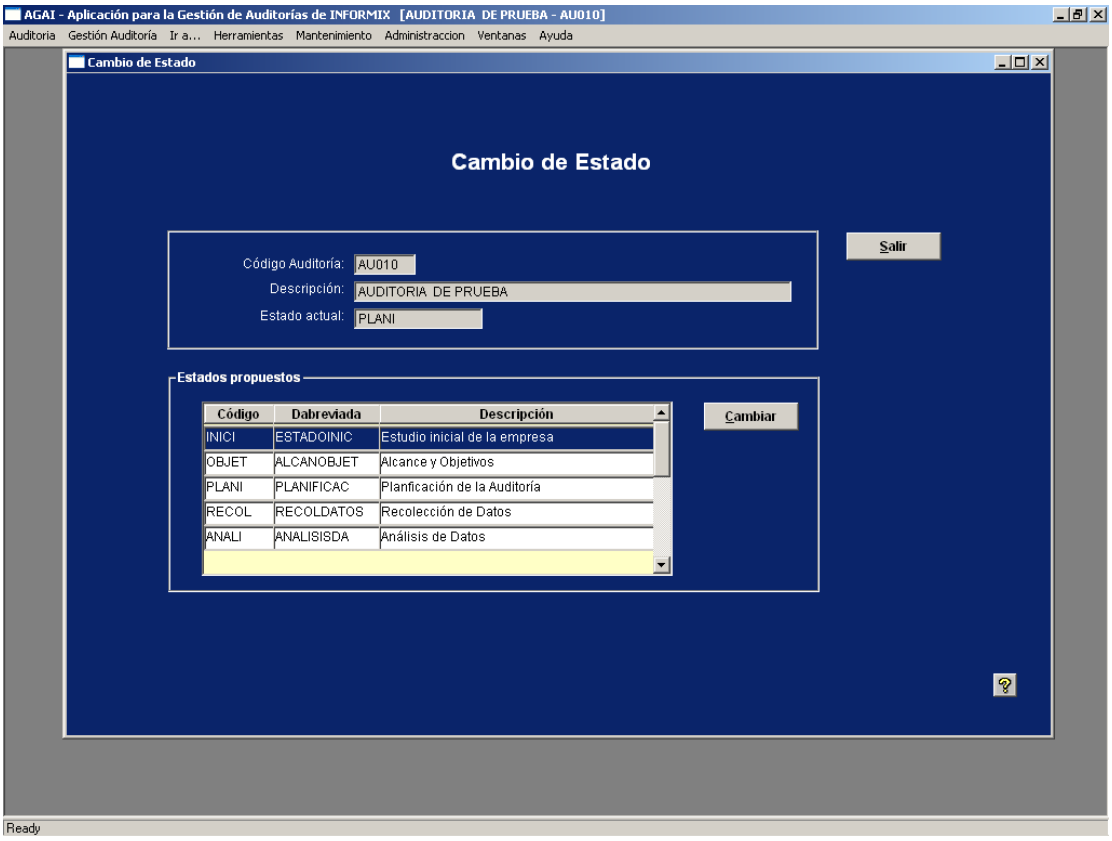
La siguiente pantalla permite modificar gran parte de los datos que identifican a la Auditoría, como son descripción, empresa auditada, fechas de inicio, modificación y fin, equipo de auditoría y estado en el que se encuentra la auditoría.

La forma de manejo de la ventana es similar a la ventana de *Nueva* auditoría. Existen varios botones que muestran en la parte inferior unas tablas donde se seleccionan la empresa auditada o el equipo de trabajo. También, se permite el cambio de estado de la auditoría a través del botón “Seleccionar” que existe junto a dicho campo.



- **Cambio de Estado**

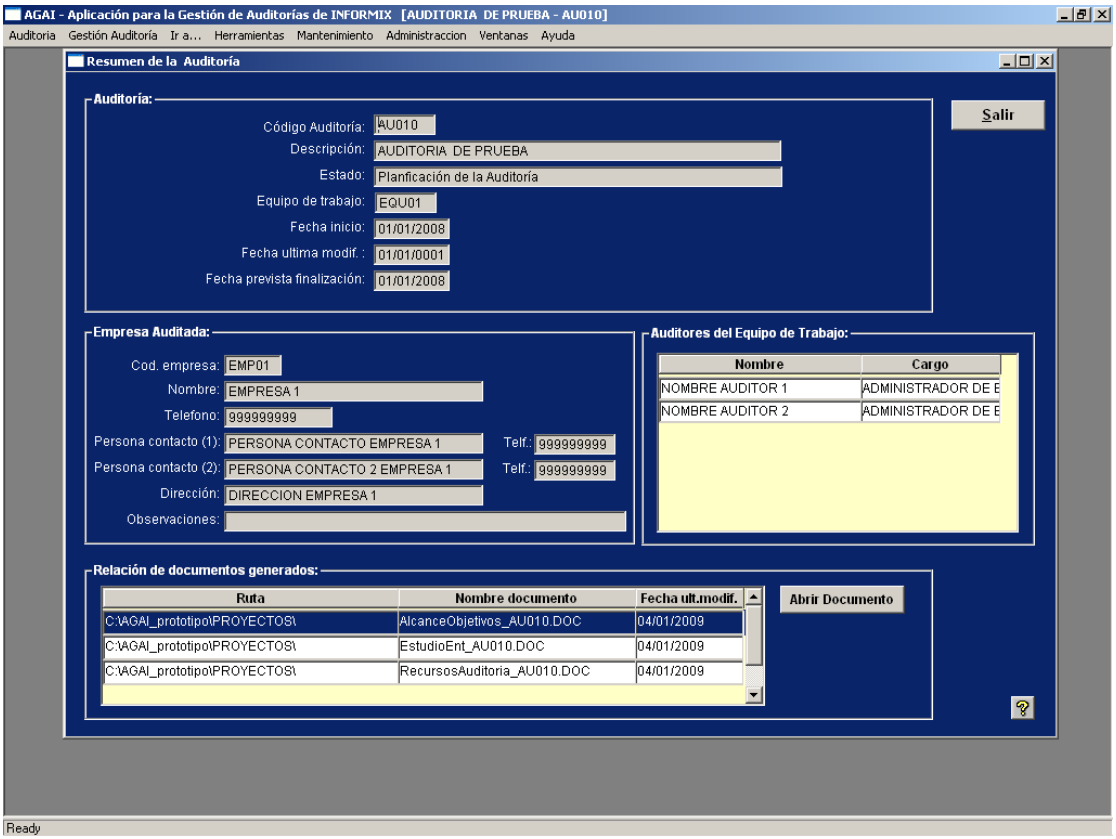
Esta ventana tiene como finalidad cambiar el estado de la Auditoría, campo muy importante a tener actualizado en todo momento, porque su correcto mantenimiento nos va proporcionar información sobre la fase en la que se encuentra la auditoría en cada momento. El estado también puede ser modificado desde la ventana Modificar, que se encuentra ubicada en este mismo submenú.



- **Resumen de la Auditoría**

En la siguiente pantalla se muestran los datos del Proyecto de Auditoría activo, se agrupan de la siguiente forma:

- Datos de la Auditoría, corresponde a datos genéricos como son nombre, estado, fechas de inicio, modificación y finalización.
- Datos de la Empresa Auditada.
- Equipo de trabajo asignado a la Auditoría.
- Relación de documentos generados.



8.1.4. Opciones del Menú Ir a...

Ir a: Donde se gestiona los documentos correspondientes a los informes y actividades relativas a la Auditoría. El submenú contiene las siguientes opciones:

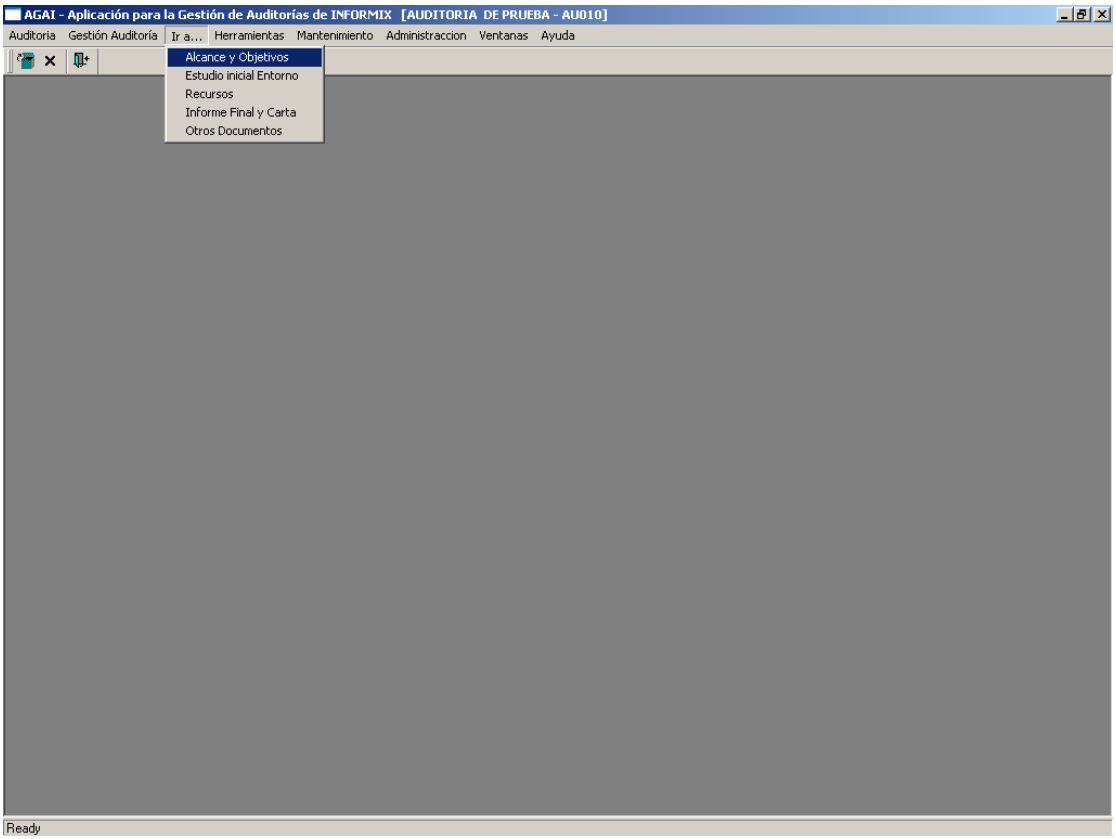
Alcance y Objetivos: Acceso o creación del documento que recoge el Alcance y Objetivos de la Auditoría.

Estudio Inicial del Entorno: Acceso o creación del documento que recoge la información referente al estudio inicial del entorno referente a la Auditoría.

Recursos: Acceso o creación del documento que recoge la relación de recursos necesarios.

Informe Final y Carta: Acceso o creación del documento correspondiente al Informe Final y Carta de la Auditoría.

Otros documentos: Relación de otros documentos que se han ido generando a lo largo del proceso de auditoría, así como la creación de los mismos.

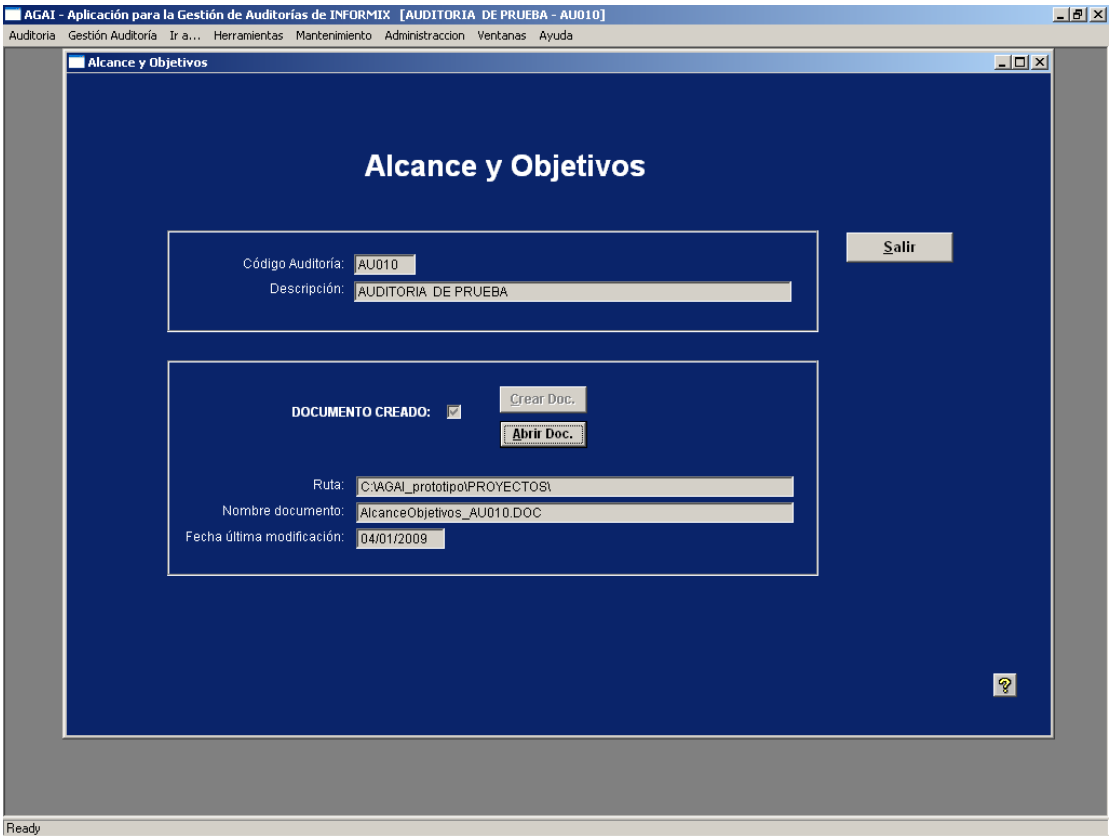


- **Alcance y Objetivos**

En la siguiente pantalla se acceder al documento que almacena el informe del Alcance y Objetivos de la Auditoría, si está creado o sino, se puede crear. En este último caso, se genera un documento con un formato determinado, el cual puede ser modificado. En el se almacenará toda la información referente a esta fase, quedará grabado y asignado a la auditoría en cuestión.

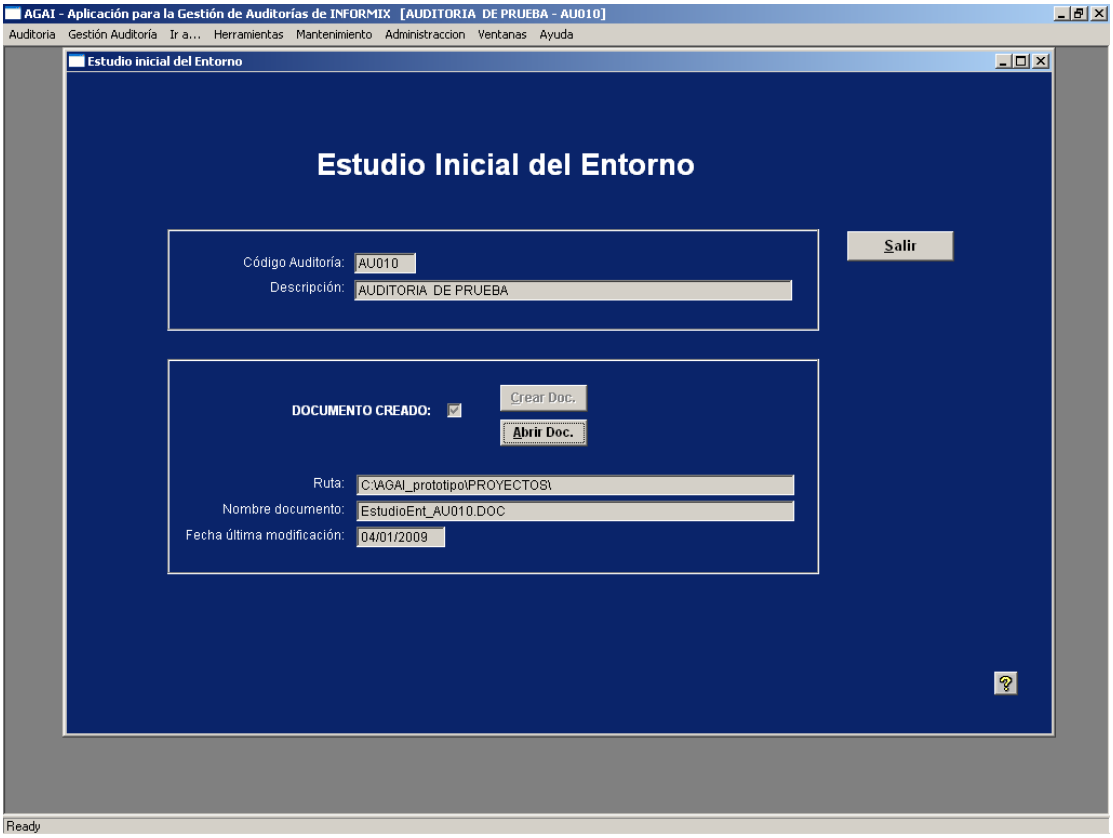
En la parte inferior de la ventana se muestra la ruta de almacenamiento, nombre y fecha de la última modificación. Este documento está almacenado en formato Word y se puede acceder directamente desde el explorador de Windows y ser modificado. La única restricción es que no puede ser cambiado el nombre ni el lugar de almacenamiento, porque dicha información está recogido en las tablas de la aplicación y variables de configuración de la aplicación.

También cabe destacar que en la opción e menú Administración se puede modificar las plantillas de estos documentos.



- **Estudio Inicial del entorno**

Esta opción de menú está estructurada de igual forma de la anterior, se muestra en la ventana los datos para acceder o crear un documento de Word que recoja dicha información de la auditoría seleccionada.

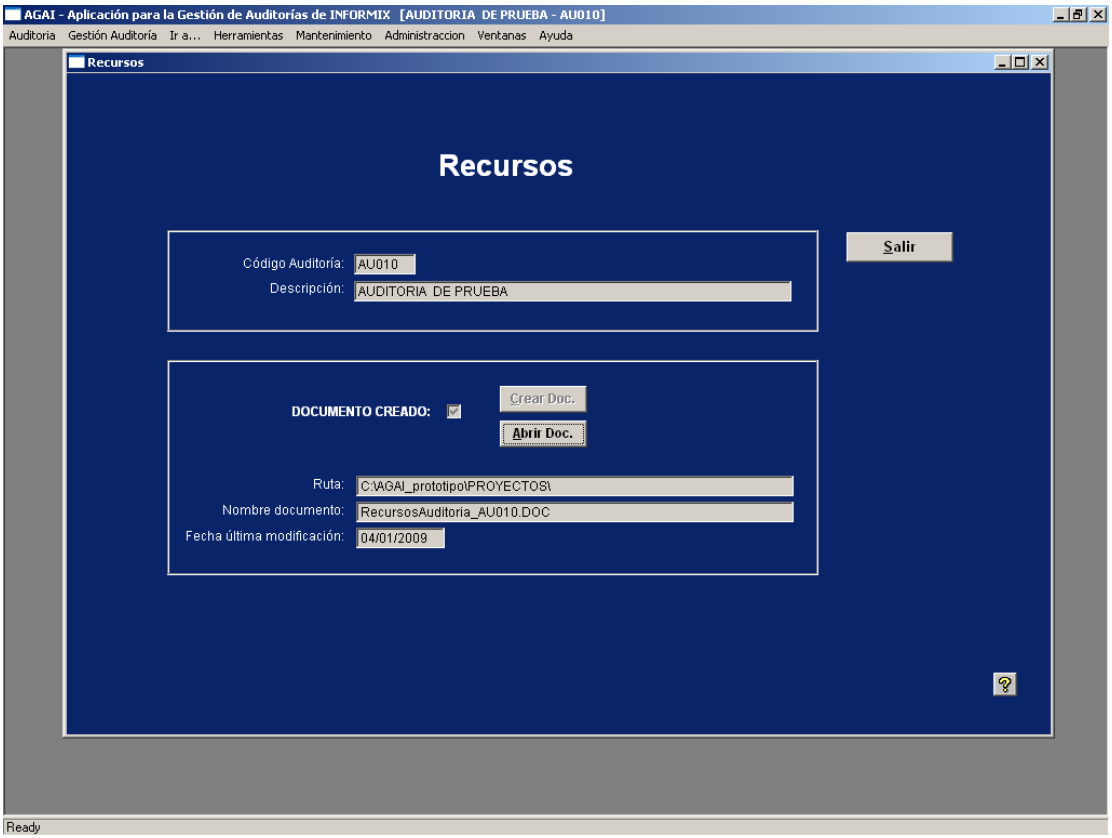


- **Recursos**

La opción de menú Recursos al igual que las anteriores, almacena la información de la Auditoría referente a los Recursos planificados y utilizados en la auditoría en cuestión.

En el documento de Word que se genera a través de esta opción, permite almacenar los recursos humanos y materiales que en gran medida se obtiene una vez realizado el estudio inicial del sistema.

Es importante identificarlos para posteriormente planificar su utilización, ya que es necesario establecer un calendario de trabajo donde se identifiquen las tareas y recursos que son necesarios.

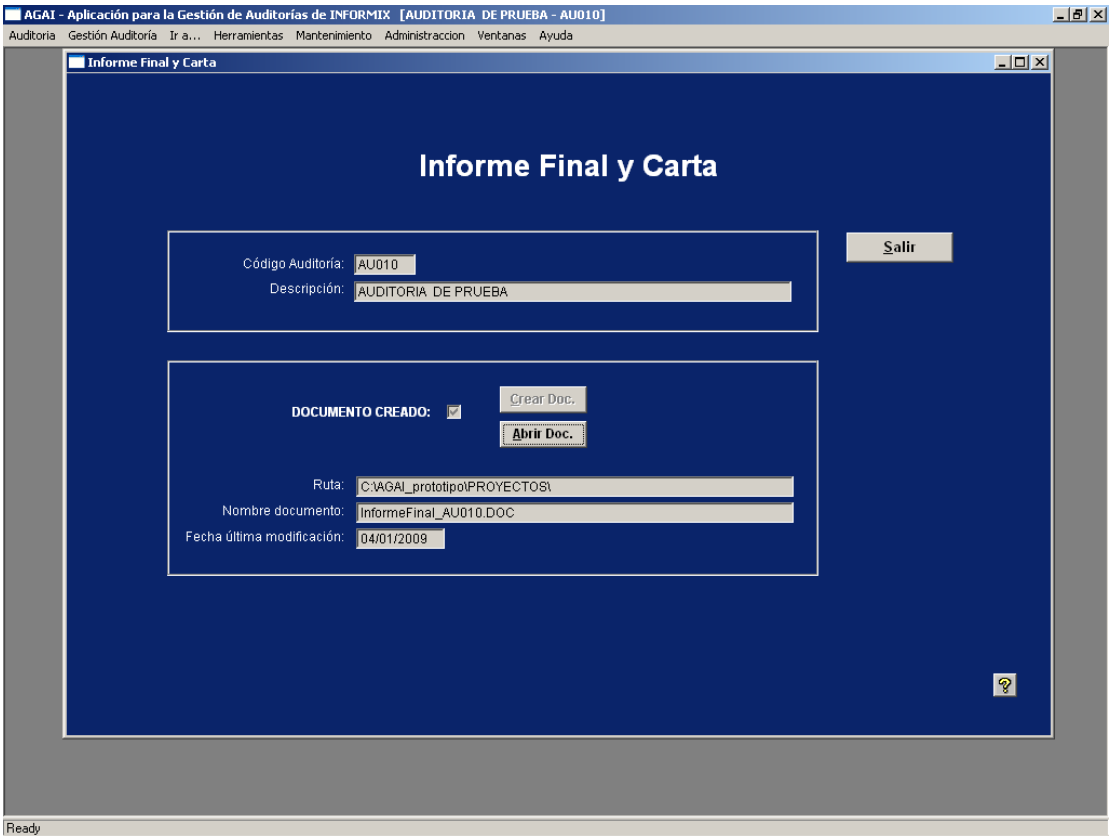


- **Informe final y Carta**

En toda Auditoría el documento principal y último del proceso de estudio es el Informe Final y Carta, donde se establecen las conclusiones obtenidas y directrices dadas, como conclusión obtenida del estudio realizado a través las diferentes etapas que conlleva una auditoría. Al igual que las opciones anteriores, en esta pantalla se muestra los datos relativos al documento Word que contiene el Informe Final y la Carta en caso que exista o sino nos permite generarlo, a partir de una plantilla.

Esta plantilla puede modificarse y adaptarse a las necesidades de los auditores. Para ello lo pueden realizar los propios usuarios de la aplicación accediendo al menú Mantenimiento y la opción Plantillas de Informes. Al entrar en esta pantalla aparece una tabla con todos las plantillas, cada fila tiene dos columnas. La platilla a la que hacemos referencia tiene en las columnas Fase y Nombre los valores “INFORME FINAL” e “InformeFinal.doc”, respectivamente.

Para poder acceder al documento se debe pulsar el botón *Abrir,* una vez seleccionada la plantilla, aparecerá un documento de Word, donde está almacenado un modelo de Informe Final y Carta. A partir de este momento se pueden realizarse los cambios que se deseen y cuando se haya terminado es importante salir de Word grabando. Es necesario indicar que los cambios que se realicen no afectarán a los documentos ya generados con anterioridad con esta plantilla.



- **Otros documentos**

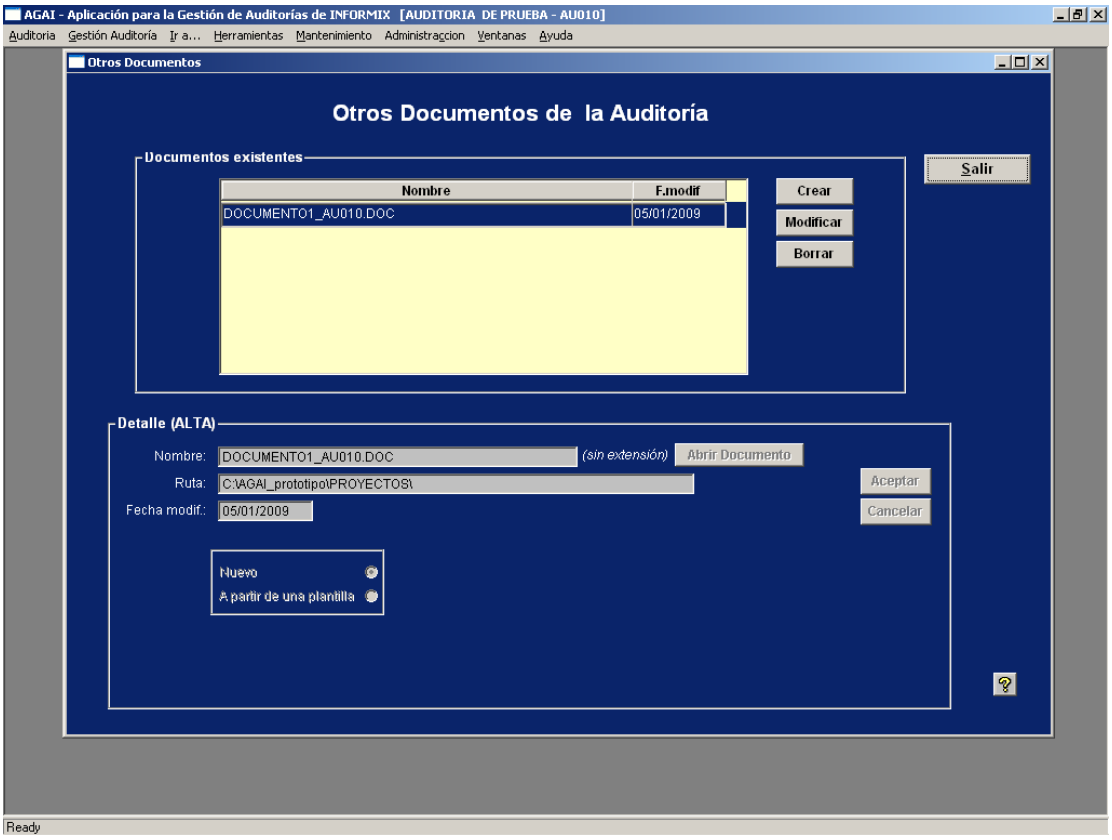
Y como todo proceso de auditoría, se lleva a cabo según una metodología, pero el equipo de trabajo la adapta a sus necesidades y experiencia, utilizando sus herramientas para obtener la información deseada. Todo esto genera un conjunto de documentos que se almacenan en esta opción de menú. Un ejemplo de informes que se podrían generar y almacenar serían : entrevistas, resultados de pruebas sobre los sistemas, etc.

La pantalla queda estructurada en dos partes, la zona superior muestra una tabla con los documentos ya existentes para el proyecto de auditoría activo, permitiendo abrirlos y borrarlos. En la parte inferior se da la opción de crear nuevos informes, estos pueden ser

nuevos, es decir no parte de ningún de documento existente, o pueden generarse a partir de una plantilla existente. Esta segunda forma de crear el documento, se activa al pinchar sobre la opción "*A partir de una plantilla*", donde se muestran una tabla con las existentes hasta el momento.

Una vez creado el documento, al pulsar el botón *Aceptar* se actualiza la tabla superior.

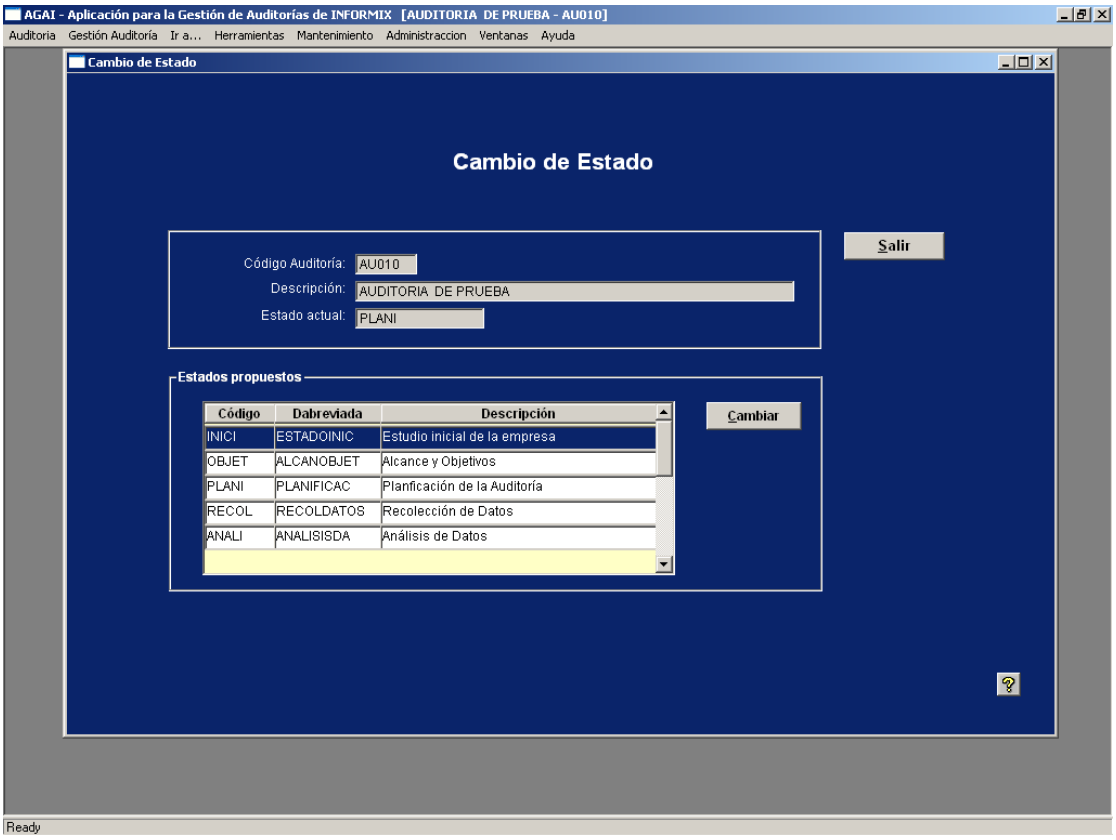
Esta pantalla gestiona el conjunto de documentos no asociados directamente a una fase de la auditoría, pero que recogen la información obtenida a través de la utilidades y herramientas utilizadas por el auditor.



- **Cambio de Estado**

Esta pantalla realiza el cambio de estado de una Auditoría, es decir, a medida que se va avanzando en el desarrollo de la auditoría se debería ir actualizando este campo. Es aconsejable hacerlo, porque va a suponer conocer en todo momento la fase en la que se encuentra la auditoría.

Cabe destacar que los posibles estados por lo que pasa un estudio de Auditoría se han cargado con unos valores iniciales, si se desean cambiar para adaptar a las necesidades y metodología de trabajo de la empresa, se pueden realizar a través de ventana de mantenimientos de *Estados de una Auditoría*, ubicado en el menú de Mantenimiento.



8.1.5. Opciones del Menú Herramientas

Herramientas: Opción de menú que permite obtener una relación de listas de comprobación sobre diversos aspectos al sistema y su entorno. Además también se gestiona las entrevistas y se da ayuda sobre el entorno Informix.

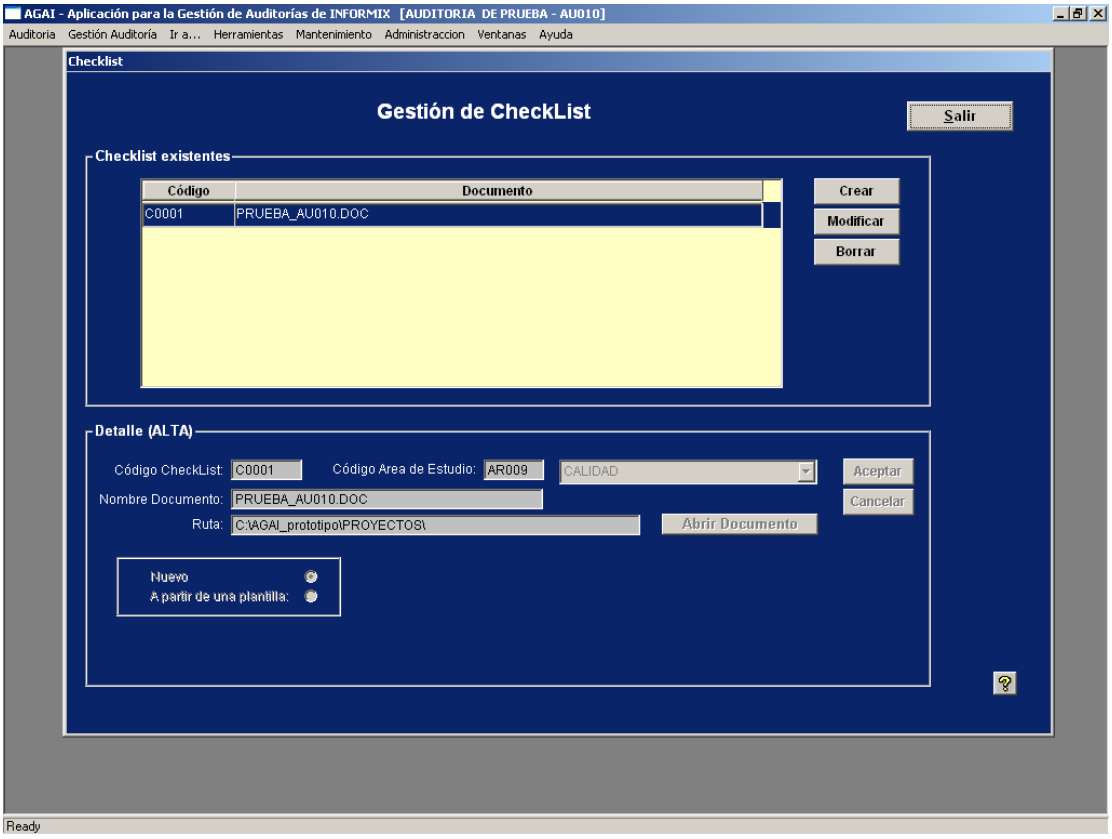
> **Lista de Comprobación**: Relación de listas de comprobación ya creadas y creación de nuevas.
>
> **Entrevistas**: Gestión y creación de informes correspondientes a entrevistas.
>
> **Informix**: Ayuda y pautas sobre Informix para poder obtener información del sistema.

- **Lista de Comprobación**

Pantalla que da acceso a una relación de Listas de Comprobación ya creadas, sobre diversos aspectos a estudiar en una auditoría, así como la posibilidad de crear uno nuevo o borrar una ya existente.

La aplicación proporciona una serie de Listas de Comprobación que pueden servir como base para la generación de las específicas a la auditoría que se está gestionando.

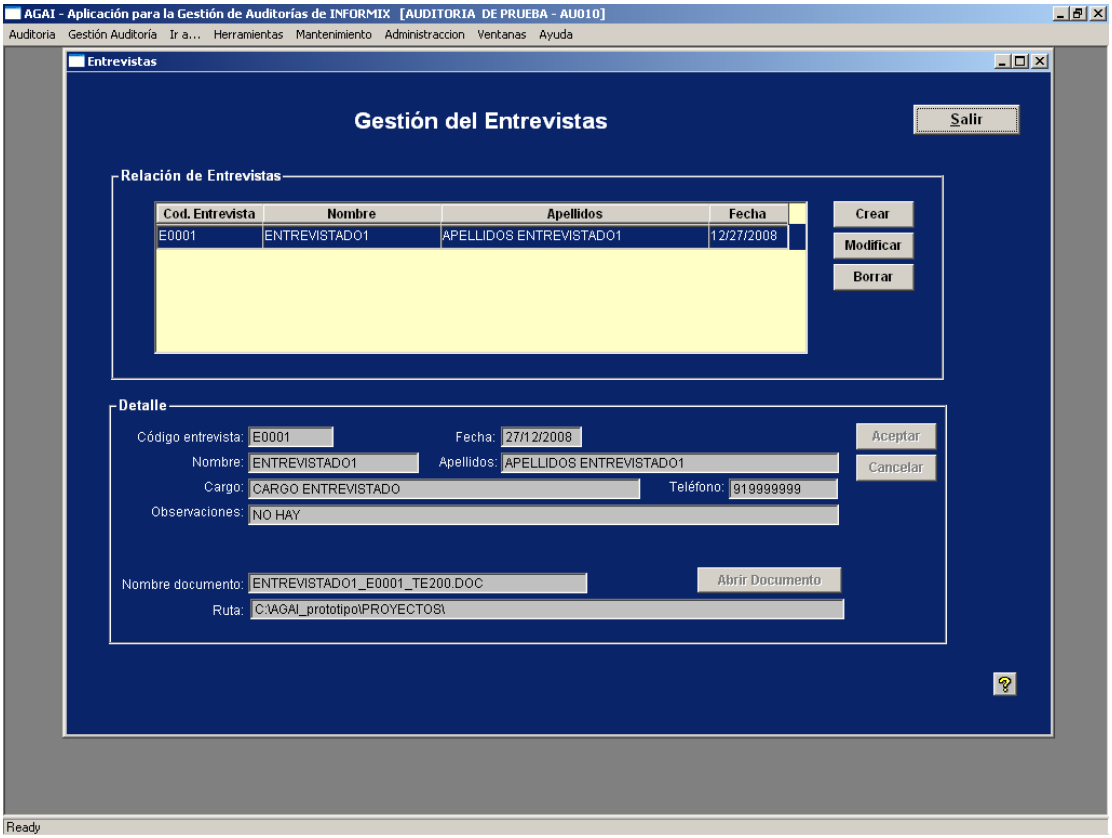
Cuando se pulsa el botón *Crear* se habilita el Detalle, donde es necesario completar los campos que aparecen. Entre la información a completar existe una agrupación donde se recogen dos controles: *Nuevo* y *A partir de una Plantilla*, esto permite generar una Lista de Comprobación con un documento en blanco o partir de una de las ya existentes, que aparecerán cuando se chequea la opción *A partir de una Plantilla.*



- **Entrevistas**

Esta opción de menú da paso a una ventana que nos ayuda a gestionar el almacenamiento de las entrevistas llevadas a cabo en el proceso de auditoría.

En la parte superior de la pantalla aparece una tabla donde se encuentran todas las entrevistas llevadas a cabo, también existen tres botones que nos permiten dar de *Alta* una entrevista, *Borrar o Modificar* una de las existentes en la tabla. Para poder acceder a estas dos últimas opciones es necesario antes de pulsar el botón correspondiente seleccionar en la tabla.

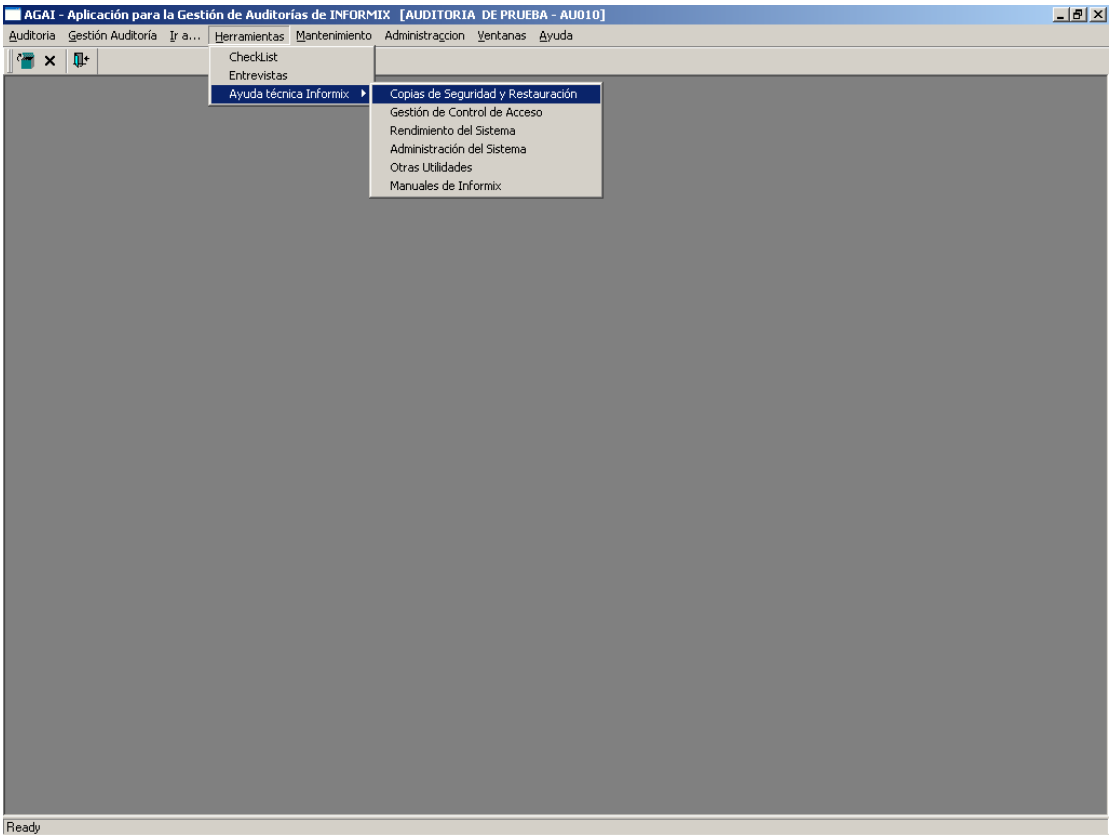


- **Ayuda Técnica Informix**

Esta opción de menú da acceso a un conjunto de documentos que van a ayudar al Auditor en los aspectos intrínsecos de Informix, es decir, indican como poder estudiar el sistema a través de sus utilidades y comandos. Además también dan enlace a documentación vía web proporcionada por Informix, para ampliar dicha información, cuando sea necesario.

Esta documentación en algunas ocasiones puede aportar nuevas formas de control a los sistemas e información de los mismos, que en algunas ocasiones pueden ser desconocidas por el Auditor.

Estas pantallas debe ser actualizada periódicamente, incluyendo información sobre las nuevas versiones y utilidades que aportan los productos ya existentes, así como los nuevos de Informix. Se encuentra estructurada en las siguientes opciones del submenu: Copias de Seguridad y Restauración, Gestión de Control de Acceso, Rendimiento del Sistema, Administración de sistemas, y Otras utilidades y Manuales de Informix.



8.1.6. Opciones del Menú Mantenimiento

Las opciones del menú Mantenimiento son las pantallas correspondientes a la gestión un conjunto de tablas genéricas a cualquier proyecto de Auditoría que deben ser cargadas inicialmente o cuando se detecte la falta de algún valor en un tipo de dato.

Además de mantener las tablas genéricas, también se puede acceder a las plantillas de los diferentes modelos de documentos que utiliza la aplicación, para configurar y formatearlos según sus necesidades y gustos.

El submenú contiene las siguientes opciones:

Empresas Auditadas: Alta, modificación y borrado de los datos de las empresas auditadas o a auditar.

Auditores: Alta, modificación y borrado de los datos de auditores.

Equipos de Trabajo: Alta, modificación y borrado de los equipos de auditores que llevan a cabo el estudio de un Proyecto de Auditoría.

Estados de Proyecto: Alta, modificación y borrado de los estados que puede estar un estudio de una auditoría.

Cargos: Alta, modificación y borrado de los cargos que pueden tener los auditores.

- **Empresas Auditadas**

La siguiente pantalla permite el mantenimiento de un tabla que almacena los datos de las empresas auditadas. A diferencia de otras tablas, esta se va manteniendo a medida que se van realizando nuevos proyectos de auditoría.

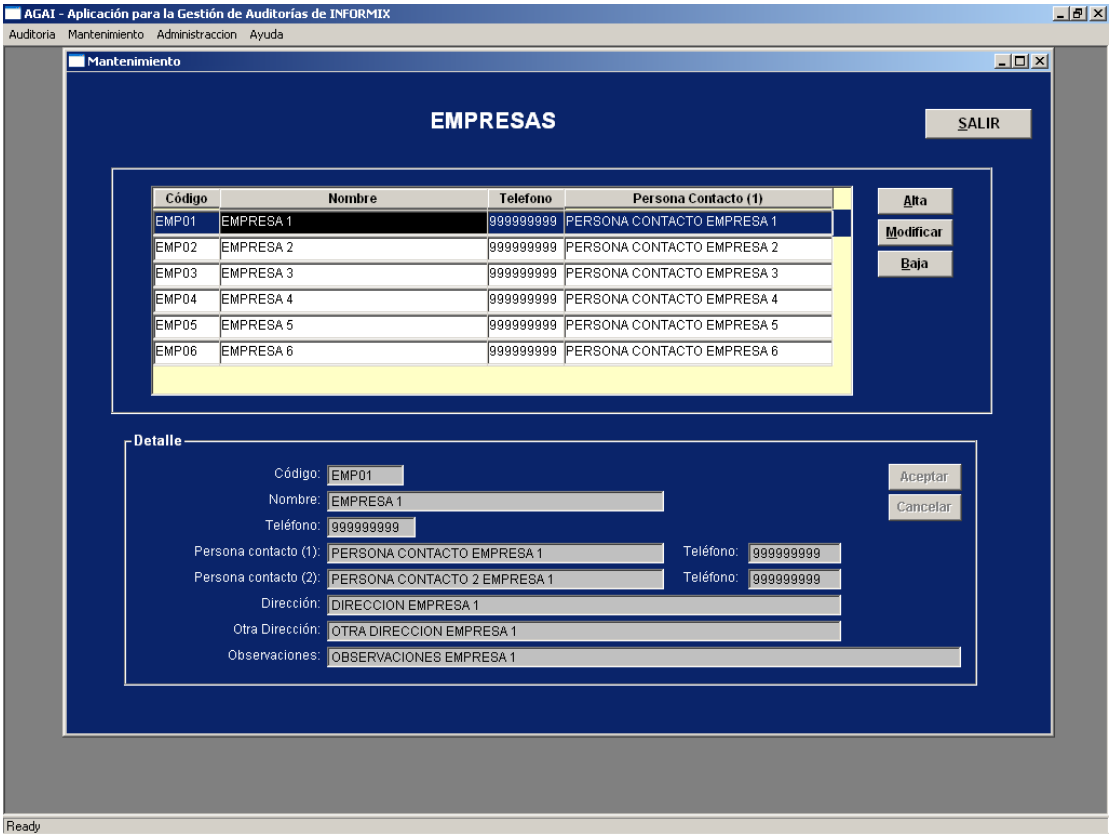
Es muy importante almacenar información, veraz y sin errores, debido a que a través de los datos almacenados en esta tabla se carga información en los Informes que se generan.

La ventana se estructura en dos zonas, en la parte superior aparecen las empresas auditadas que han sido grabadas, sobre estas pueden realizarse modificaciones o borrado.

Para poder modificar los datos de una empresa, se selecciona y se pulsa el botón Modificar, que habilita el detalle que se encuentra en la parte inferior, pueden modificarse todos los datos, excepto el Código de Auditoría, que es el campo clave. El cambio de este valor generará problemas de integridad de los datos en la base de datos. De igual forma ocurre con el borrado, hay que tener mucho cuidado que dicha información no se encuentre en otras tablas, ya que si se borra se produciría errores de integridad.

Una vez realizada la modificación o alta de los datos en la parte inferior de la ventana, estos no se materializarán en la base de datos hasta pulsar el botón aceptar. En caso de que no se quieran llevar a cabo se pulsa el botón cancelar.

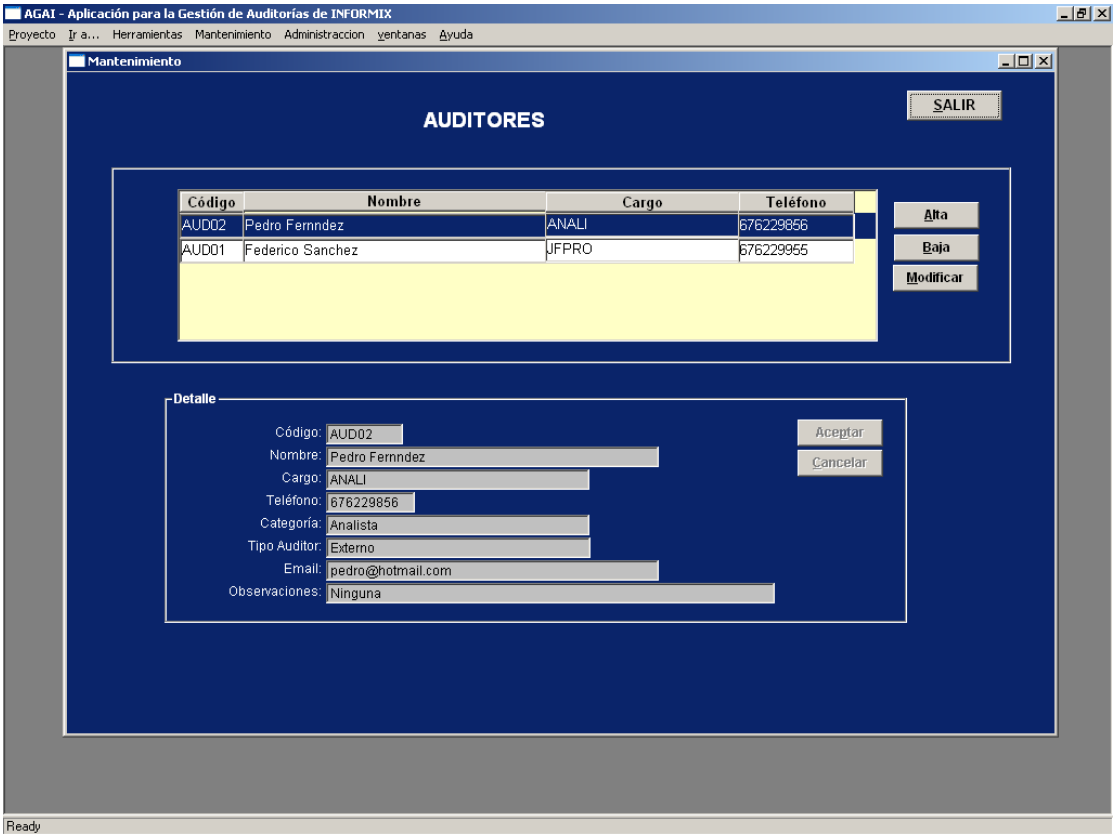
Tanto al pulsar el botón Aceptar como Cancelar, se deshabilita el detalle y se posiciona el cursor en la parte superior.



- **Auditores**

Este mantenimiento gestiona los datos de los Auditores. Cuando se realiza una auditoría, se asigna un grupo de trabajo que va a realizar el proyecto, dicho equipo se obtiene a partir de los auditores que aparecen en esta pantalla. Por ello toda persona que se incluya en equipo de trabajo debe ser dada de alta en esta ventana.

La información que aparece en esta ventana, debería tener un acceso restringido, debido a que aparecen datos que requieren una protección especial. Dicha información a lo mejor podría ser obtenida de la tablas o lugares de almacenamiento que utiliza el Dpto. de personal. Y sólo ciertos roles pueden tener acceso a esta.

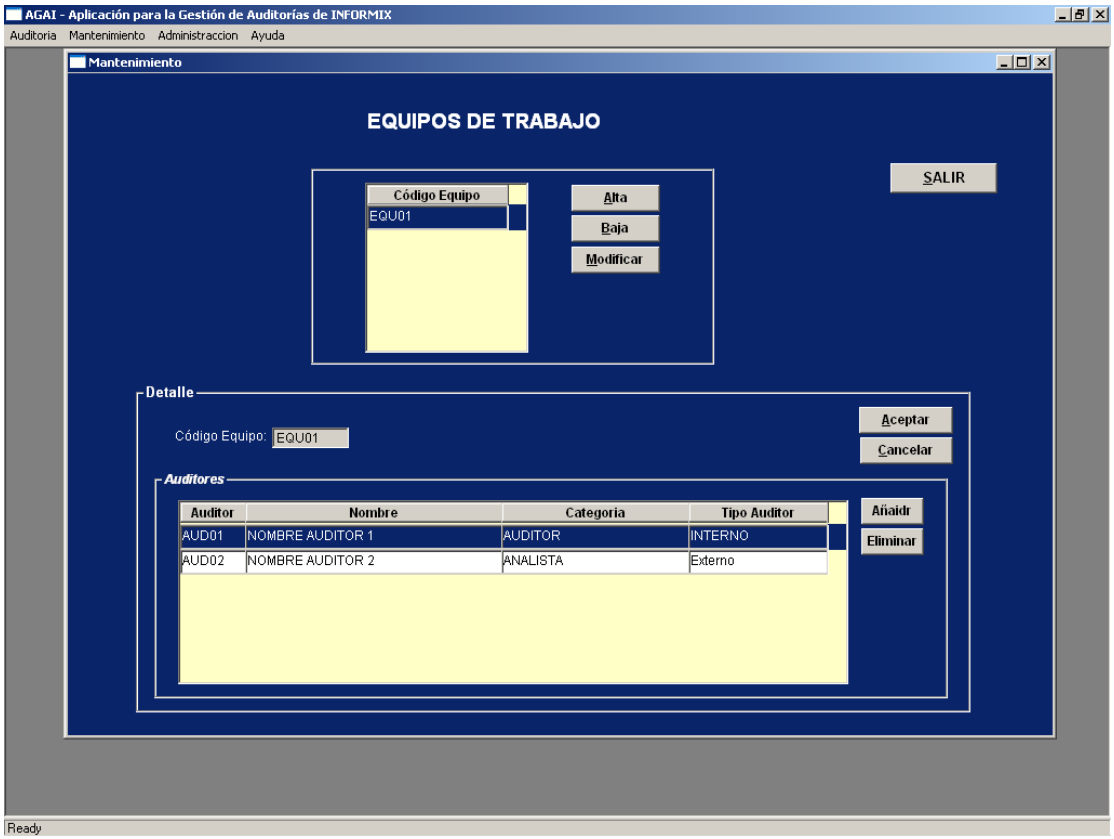


- **Equipos de trabajo**

Este mantenimiento permite gestionar los equipos de trabajo asignados a las auditorías. Un equipo está formado por un conjunto de auditores que son los que participan en el desarrollo de la auditoría.

La pantalla está dividida en dos zonas, en la parte superior aparecen los códigos de equipos existentes y en la parte inferior, los auditores pertenecientes al código de equipo seleccionado.

Como todo mantenimiento, se administra mediante las operaciones de alta, baja y modificación los equipos de trabajo de la aplicación



- **Estados de la Auditoría**

Un Proyecto de Auditoría pasa por diferentes estados, en este mantenimiento se graban dichos valores. En la aplicación a medida que se van completando fases, se permite modificar el estado del proyecto a través de unos indicadores, mostrarán un conjunto de valores y el usuario de la aplicación indicará que fase ha concluido o en la que está.

Si se gestiona correctamente esta información, cuando se acceda a la pantalla "*Resumen de la situación de la Auditoría*" se podrá conocer en el estado actual en que se encuentra el proyecto.

La aplicación tiene cargados unos valores por defecto, pero es importante realizar las actualizaciones que se crean necesarias y se adapten a la metodología de trabajo de la empresa.

Los valores cargados inicialmente son:

Sin Iniciar Auditoría
Estudio inicial de la empresa
Alcance y Objetivos
Planificación de la Auditoría
Recolección de Datos
Análisis de Datos
Evaluación de los Datos
Informe final y Carta
Implementación recomendaciones
Seguimiento
Finalizado y cerrado
Paralizado

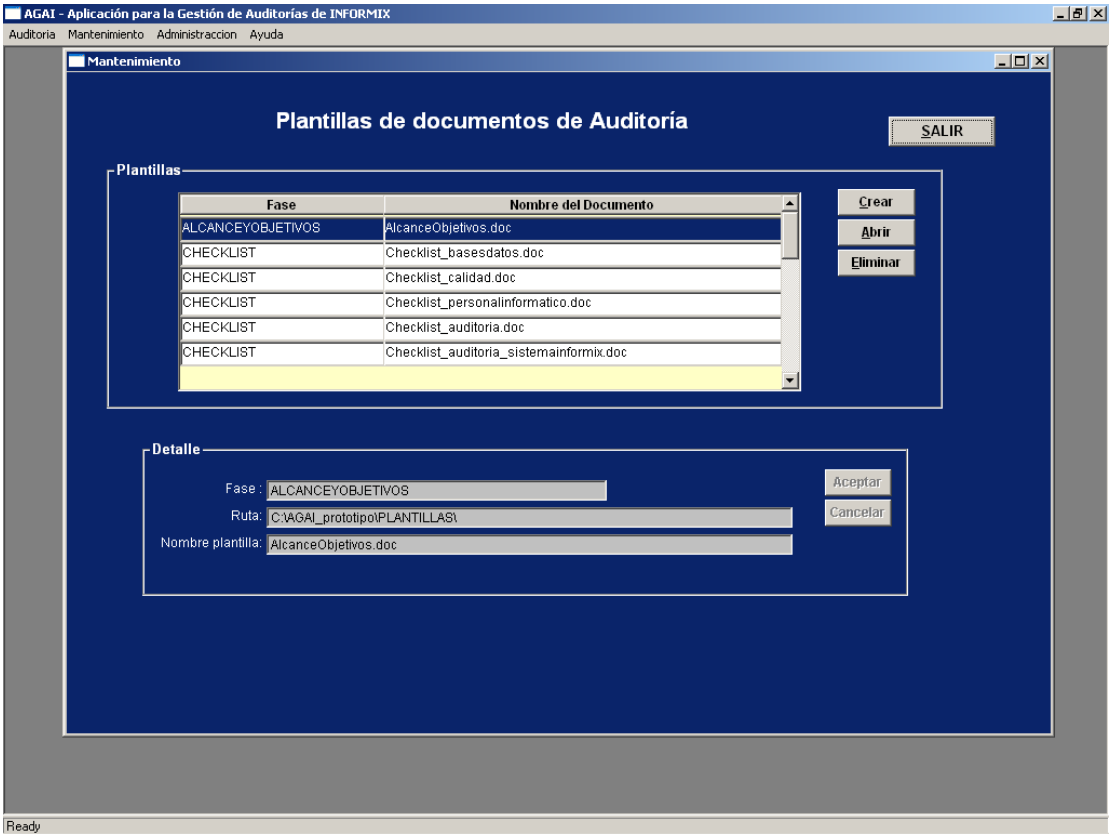
- **Plantillas de documentos de Auditoría**

Esta ventana corresponde al mantenimiento de los documentos que van a servir de plantilla para generar los informes de los estudios de Auditoría gestionados por la aplicación. De tal forma que todos los proyectos que se lleven a cabo puedan tener una misma presentación. Además ayudara.

Estos documentos cuando se crean, se hacen a través de Word, considerado como una de los procesadores de textos más potentes y con más posibilidades que existe en la actualidad.

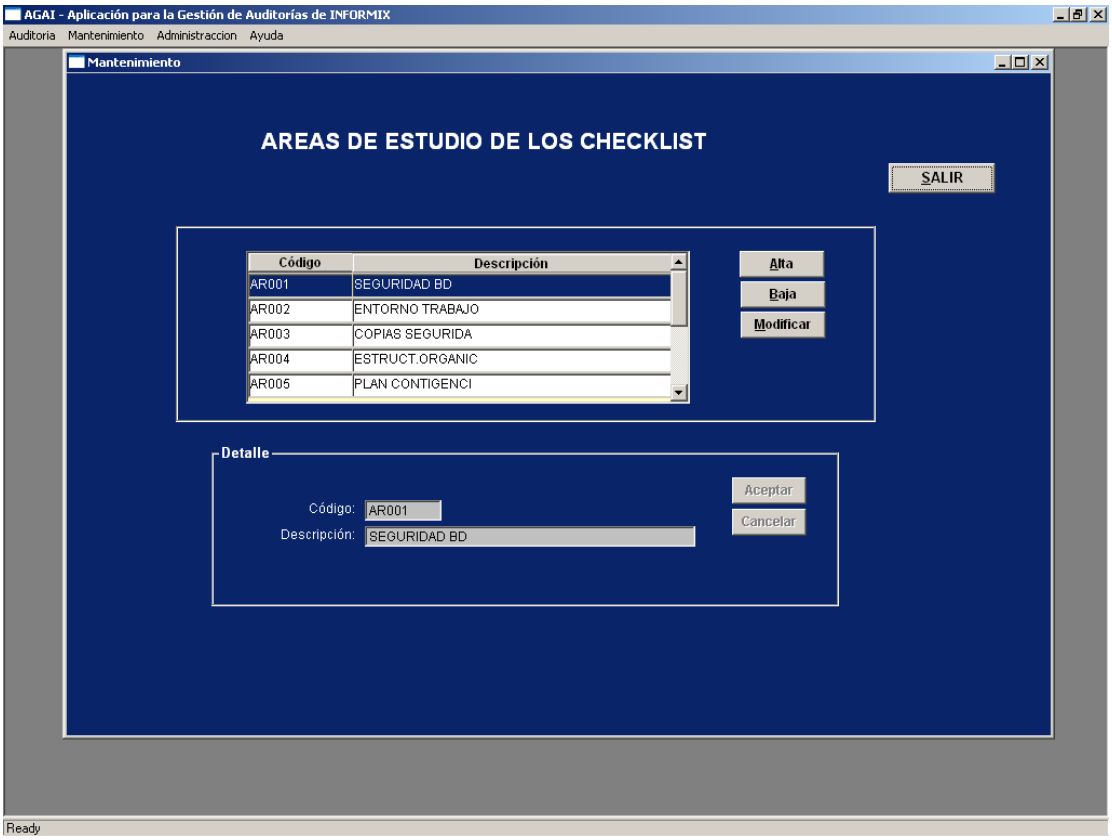
Como el resto de mantenimientos, en la parte superior se encuentran las plantillas existentes junto con tres botones que nos permite crear nuevas plantillas, modificar las existentes o eliminarlas.

Con la gestión de plantillas se permite ir mejorando los informes, de tal forma que cada vez se adapte mejor a las necesidades y facilite el trabajo,, mejorando el rendimiento y los resultados.



- **Áreas de estudio de las Listas Comprobación**

Esta ventana se encarga del mantenimiento de las áreas de las listas comprobación, es decir, los grupos en los que se puede organizar, de tal forma que queden estructurados los documentos y sea más fácil su acceso y organización.

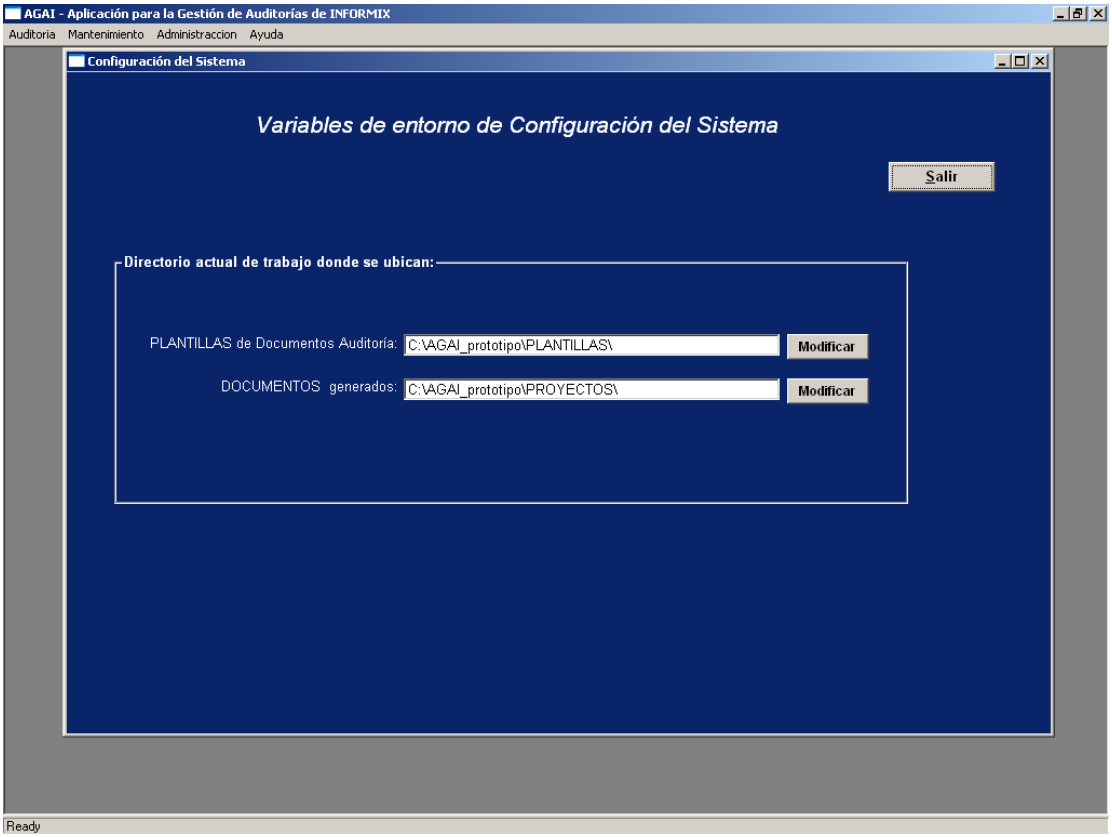


- **Variables de entorno de configuración**

En esta pantalla se mantiene las variables de configuración que permiten cambiar la ubicación de los documentos que se generan en la aplicación.

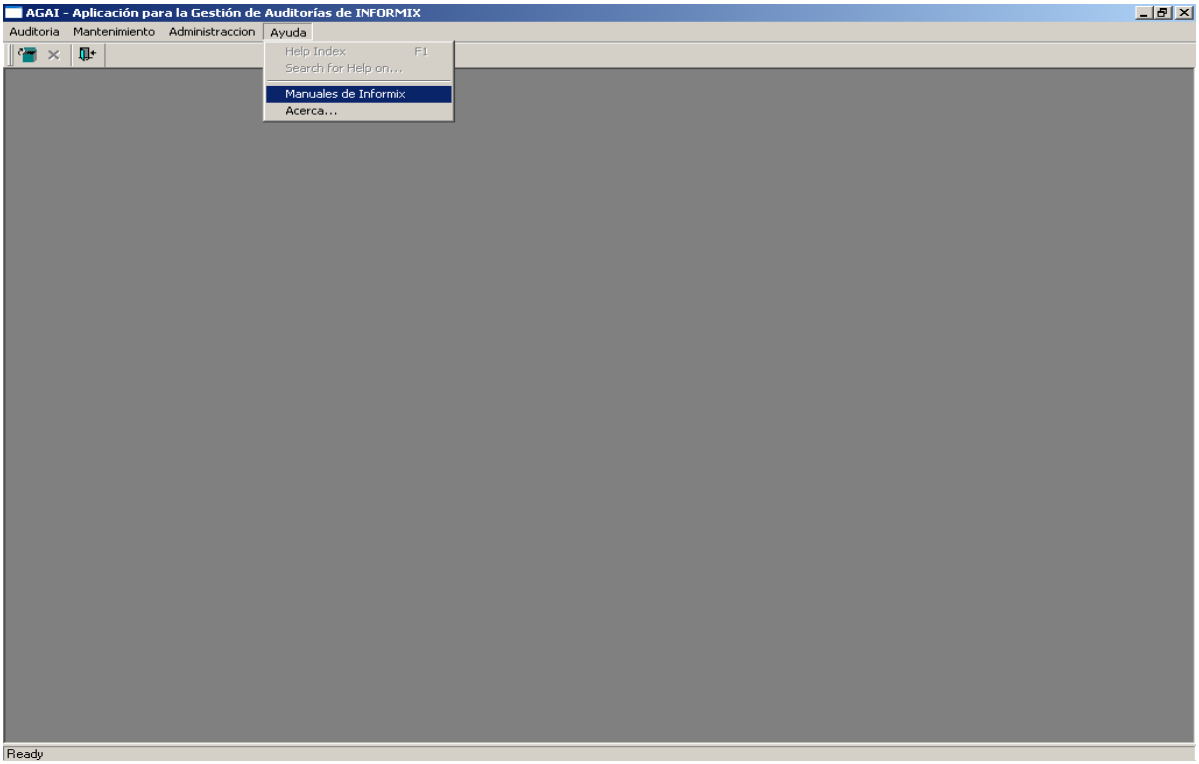
Es importante indicar que todos los archivos de Word generados por la aplicación pueden ser accedidos a través del explorador de Windows. Se encuentran almacenados en los directorios indicados en estas variables, aunque pueden existir en otros lugares, en el caso de que se haya modificado alguna vez estas variables.

Es importante hacer referencia a esta cuestión, ya que en caso de no poder acceder a la aplicación si se puede acceder a los documentos de word.



8.1.7. Opciones del Menú Ayuda

Esta opción de menú recoge una serie de opciones de ayuda e información acerca de la versión de la aplicación. La opción de Manuales de Informix da acceso a un documento word, donde están los manuales más importantes y referentes a las áreas tratadas



8.2. Posibles líneas de desarrollo

Podemos ampliar la aplicación mediante la implementación de la funcionalidad de importar los datos e informes de una auditoría ya existente en el momento de la creación de un nuevo proyecto de auditoría. Este hecho se puede producir con cierta frecuencia en auditoría que se realizan de forma periódica a una misma empresa, donde la estructura básica no varía aunque los resultados del estudio y análisis pueden ser muy diferentes a lo largo de los años.

Otra posible línea de desarrollo es el tratamiento de la información de forma impresa, es decir poder generar listados que nos aporten diferente tipo de información, muestren toda la información referente a una auditoría, resumen de la situación de las auditorías cargadas en el sistema, por diferentes parámetros, como pueden ser aquellas que estén en una determinada fase, las que estén más próxima su fecha de finalización, y muchos otros parámetros que aporte información importante para el usuario.

8.3. ANEXO APLICACIÓN

8.3.1. Menú Herramientas: Ayuda Técnica de Informix

En el menú de la aplicación *Herramientas*, submenú *Ayuda Técnica de Informix*, da acceso a un conjunto de documentos, que tienen una estructura de tabla donde se explican como realizar tareas a través del sistema Informix: línea comando o herramientas del propio gestor de base de datos. Además, también se Incluye acceso a los Manuales Oficiales de IBM que permite profundizar si se desease.

- Copias de Seguridad y Restauración
- Gestión de Control de Acceso
- Rendimiento del Sistema
- Administración del Sistema
- Otras utilidades
- Manuales de Informix

- **Copias de Seguridad y Restauración**

COPIAS DE SEGURIDAD Y RESTAURACIÓN

Tarea	Informix	Manual de consulta
Cómo se realizan las copias de seguridad y restauración.	ontape y ON-Bar	*IBM Informix: Guía de copia de seguridad y restauración (Versión 10.0/8.5)* http://publib.boulder.ibm.com/epubs/pdf/21001170.pdf
Copia de seguridad de las anotaciones lógicas	onbar –b –l	*IBM Informix: Guía de copia de seguridad y restauración.* http://publib.boulder.ibm.com/epubs/pdf/21001170.pdf
Descargar una base de datos en un fichero y más tarde cargarla. (copias de seguridad y restauración)	dbexport NOMBRE_BD tar (enviar a cinta) dbimport NOMBRE_BD	*IBM Informix: Dynamic Server Administrator's Reference* http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.adref.doc/adref202.htm
Carga y descargar de tablas enteras, en entornos idénticos	onload y onunload	*IBM Informix: Migration Guide* http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf
Cargar o descargar grandes cantidades de datos en o desde una base de datos Informix.	Ipload, onpload y onpladm	Programas de utilidad de High-Performance Loader. *IBM Informix: High-Performance Loader User's Guide* http://publib.boulder.ibm.com/epubs/pdf/25122860.pdf
Verificación de las copias de seguridad	archecker	*IBM Informix: Guía de copia de seguridad y restauración (Versión 10.0/8.5)* http://publib.boulder.ibm.com/epubs/pdf/21001170.pdf
Obtener información sobre la duplicación de las rutinas definidas por el usuario (UDR)	onstat –g dss UDR onstat –g dss UDRx onstat –g grp UDR onstat –g grp UDRx	Más información en el Apéndice sobre mandatos onstat del manual. *IBM Informix: Dynamic Server Guía Enterprise Replication.* http://publib.boulder.ibm.com/epubs/pdf/8334.pdf
Buscar un número de error específico de Enterprise Replication y visualizar el texto de error.	cdr finderr	*IBM Informix: Dynamic Server Guía de Enterprise Replication* http://publib.boulder.ibm.com/epubs/pdf/8334.pdf
Programa utilidad de línea de mandatos para crear, modificar, describir, listar, ejecutar, configurar y suprimir trabajos de carga y descarga de tablas o de toda una base de datos.	onpladm	Manual en onpladm.htm incluido con el servidor de bases e datos: *$INFORMIXDIR/release/en_us/0333/onpladm/index.htm.* (Misma funcionalidad que ipload)

- **Gestión de Control de Acceso**

CONTROL DE ACCESO AL SISTEMA

Tarea	Informix	Manual de consulta
Permisos a nivel de Base de Datos y tablas	GRANT y REVOKE	Para otorgar o denegar el acceso a una *base de datos* o a *tablas* específicas y para controlar las clases de usos de la base de datos, se denominan privilegios. Esta información queda almacenada en las tablas de catálogo del sistema: sysusers, systabauth y suscolauth A nivel de BD: Connect, Resource y Admon. BD A nivel de Tabla: SELECT, INSERT, UPDATE, DETETE, ALTER, ALL *IBM Informix: Dynamic Server Administrator's Guide.* http://publib.boulder.ibm.com/epubs/pdf/8324.pdf *IBM Informix;: Guía para el diseño e implantación de bases de datos.* *IBM Informix;: Guide to SQL Syntax.* http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf
Control acceso tablas	CREATE PROCEDURE	Para escribir y compilar un procedimiento almacenado que controle y supervise el acceso a las tablas. *IBM Informix: Dynamic Server Administrator's Guide.* http://publib.boulder.ibm.com/epubs/pdf/8324.pdf *IBM Informix;: Guía para el diseño e implantación de bases de datos.* *IBM Informix;: Guide to SQL Syntax* http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf
Restringir vistas de los datos	CREATE y REVOKE VIEW	Para preparar una vista restringida o modificada de datos. En las tablas de catálogo del sistema, sysviews y susdepend, se guarda las vistas existentes en la base de datos. *IBM Informix: Dynamic Server Administrator's Guide.* http://publib.boulder.ibm.com/epubs/pdf/8324.pdf *IBM Informix;: Guía para el diseño e implantación de bases de datos.* *IBM Informix;: Guide to SQL Syntax..* http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf
Otra forma de gestionar el perfil de uno o más usuarios	CREATE y REVOKE ROLES	Se crean ROLES para configurar clasificaciones con privilegios otorgados sobre objetos de base de datos en un rol específico. Estos roles se asignan a los usuarios que se desean que tengan dicho perfil. Es una forma de facilitar la

Tarea	Informix	Manual de consulta
		asignación de permisos. *IBM Informix: Dynamic Server Administrator's Guide* http://publib.boulder.ibm.com/epubs/pdf/8324.pdf *IBM Informix: Guía para el diseño e implantación de bases de datos.* *IBM Informix: Guide to SQL Syntax* http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf
Detectar acciones inhabituales de los usuarios y actividades no deseadas e identificar a los causantes.	onaudit, onshowaudit	Utilidades de auditoría para configurar, administrar e interpretar pistas de auditoría *IBM Informix: Trusted Facility Guide* http://publib.boulder.ibm.com/epubs/pdf/25123000.pdf
Cifrado de la password	SET ENCRYPTION PASSWORD	Para el cifrado de columna y mejorar la confidencialidad de los datos. El catálogo del sistema no identifica las columnas que contienen datos cifrados. La password no está almacenado como un texto plano en la Base de Datos y no es accesible por el Administrador de la Base de Datos. *IBM Informix: Guide to SQL: Syntax* http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf

- **Rendimiento del Sistema**

RENDIMIENTO DEL SISTEMA

Tarea	Informix	Manual de consulta
Mejora del rendimiento del sistema	Gestión de Memoria Fragmentación Paralelización Optimización consultas ONCONFIG UPDATE STATISTICS	**Gestión memoria:** *IBM Informix: Performance Guide (Apdo. Mejoras en SQL-pag 2-52)* http://publib.boulder.ibm.com/epubs/pdf/8344.pdf **Fragmentación***: IBM Informix: Guía para el diseño e implementación BD y IBM I. Performance Guide.* http://publib.boulder.ibm.com/epubs/pdf/8344.pdf **Consulta de BD en paralelo**: *IBM Informix: Performance Guide y IBM Informix: Guide to SQL Reference (ver variable de entorno PDQPRIORITY)* http://publib.boulder.ibm.com/epubs/pdf/8344.pdf **Optimizador de consultas***: IBM Informix: Performance Guide*
Mejorar y gestionar rendimiento a través de parámetros de configuración del sistema	onconfig	Ver Anexo, como configurar los parámetros.
Mejorar rendimiento tablas	update statistics	Ver Anexo, que tabla actualiza.
Supervisar el rendimiento del servidor de BD y poder diagnosticar y recoger información sobre problemas habidos	onstat –g onstat -l	*IBM Informix: Administrator's Referente* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Memoria que utilizan las sentencias SQL	onstat –g stm *id_sesion*	*IBM Informix: Performance Guide, IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf http://publib.boulder.ibm.com/epubs/pdf/8344.pdf
Visualizar el plan de consultas sin ejecutar la consultas	SET EXPLAIN ON AVOID_EXECUTE	Permite evaluar el plan de consulta que l optimizador ha grabado en el archive sqexplain.out. *IBM Informix: Performance Guide* (mejorar rendimiento consultas y utilizar directivas de optimizador) *IBM Informix Guide to SQL Syntax* (Utilizar SET EXPLAIN y directivas de optimizador) http://publib.boulder.ibm.com/epubs/pdf/8344.pdf http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Establecer la modalidad de bloqueo por omisión en página o fila para las nuevas tablas	LOCK MODE	Hay que realizar las siguientes tareas, la cláusula LOCK MODE de la sentencia ALTAR TABLE o CREATE TABLE , configurar la variable de entorno

Tarea	Informix	Manual de consulta
		IFX_DEF_TABLE_LOCKMODE y el parámetro de configuración DEF_TABLE_LOCKMODE. *IBM Informix: Performance Guide,* *IBM Informix: Administrator's Reference,* *IBM Informix: Guide to SQL Syntax.* http://publib.boulder.ibm.com/epubs/pdf/8344.pdf http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Visualización anotaciones lógicas temporales	onstat –l	*IBM Informix: Administrator's Guide,* *IBM Informix Administrator's Reference.* http://publib.boulder.ibm.com/epubs/pdf/ct1ucna.pdf http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Supervisar el Servidor de base de datos	Tablas de la BD sysmaster	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Funciones para controlar y obtener información sobre el entorno de procesadores virtuales		*IBM Informix:DataBlade API Programmer's Guide* http://publib.boulder.ibm.com/epubs/pdf/25122731.pdf

ONCONFIG

El rendimiento de la base de datos puede mejorar mediante la realización de cambios en los parámetros del archivo de configuración *onconfig.*

Opción de configuración	Descripción
SHMADD	Especifica tamaño del segmento de memoria que debe agregarse dinámicamente a la parte virtual de la memoria compartida del servidor Universal de Informix. Valores recomendados: Memoria física — Valor < 256 MB — 8192 KB > 256 MB y < 512 MB — 16384 KB > 512 MB — 32768 KB
SHMTOTAL	Especifica el tamaño máximo de memoria compartida para el servidor de BD Informix. Un valor cero permite que la memoria compartida pueda seguir tomando segmentos del sistema operativo en función de las necesidades. El valor debe establecerse en cero a menos que sea necesario restringir el acceso del servidor de BD a toda la memoria debido a que existen otras

Opción de configuración	Descripción
	aplicaciones que se ejecutan en el mismo sistema. *Valor recomendado: 0*
SHMVIRTSIZE	Especifica el tamaño inicial de la parte virtual de la memoria compartida del servidor de BD Informix. Puede hacerse que a la memoria compartida se agreguen dinámicamente segmentos de memoria pero, si el tamaño no es el tamaño necesario para los requisitos operativos diarios, puede que los procesos tarden más en completarse mientras esperan a que se agreguen los segmentos de memoria. De los siguientes, utilice el valor más grande: 8000 KB o el número de todos los tipos de conexión de red especificados en el archivo sqlhosts de Informix multiplicado por 350. *Valor recomendado para el archivo onconfig: SHMVIRTSIZE 8000*
RESIDENT	Especifica que el sistema operativo no puede intercambiar la parte residente de la memoria compartida de Informix si el sistema operativo da soporte a la residencia forzada de los segmentos de memoria. Al no estar permitido el intercambio de la parte residente, los datos contenidos en la BD permanecen en la memoria en lugar de intercambiarse con el disco, y el rendimiento se beneficia de ello. Si el sistema operativo no tiene la opción de residencia forzada, el servidor universal de Informix emite un mensaje de error y, a continuación, pasa por alto el parámetro. El valor RESIDENT debe establecerse en 1. *Valor recomendado para el archivo onconfig: RESIDENT 1*
DBSPACETEMP	Especifica una lista de nombres de espacio de BD que se utilizan para el área de trabajo temporal del servidor de base de datos de eventos. *Valor recomendado para el archivo onconfig: DBSPACETEMP*
MAX_PDQPRIORITY	Especifica el porcentaje de recursos de BD que un proceso que realiza consultas de base de datos en paralelo podrá tomar del porcentaje cuya utilización ha solicitado. Los recursos de BD que se utilizan en paralelo son la memoria, la E/S de disco y los threads de exploración que exploran las tablas en busca de las filas solicitadas. *Valor recomendado para el archivo onconfig: MAX_PDQPRIORITY 50*
DS_MAX_QUERIES	Especifica el número de consultas de tipo de soporte de decisiones que pueden ejecutarse simultáneamente. Las consultas de soporte de decisiones son consultas grandes, complejas, que exploran las tablas de la base de datos de eventos y que necesitan gran cantidad de recursos de base de datos. *Valor recomendado para el archivo onconfig: DS_MAX_QUERIES 10*
DS_MAX_ SCANS	Especifica el límite para el número de threads de exploración de consulta de BD en paralelo que una consulta de soporte de decisiones puede ejecutar concurrentemente. Las consultas de soporte de decisiones con consultas grandes, complejas, que exploran las tablas de la base de datos de eventos y que necesitan gran cantidad de recursos de base de datos. *Valor recomendado para el archivo onconfig: DS_MAX_ SCANS 20*
DS_ TOTAL_MEMORY	Especifica el porcentaje total de memoria del servidor universal de Informix que debe utilizarse para las consultas de base de datos en paralelo. Establezca este valor entre un 50% y un 80% para las aplicaciones que tienen gran número de consultas de tipo de soporte de decisiones.

Opción de configuración	Descripción
	Valor recomendado para el archivo onconfig: DS_ TOTAL_MEMORY 50
OPTCOMPIND	Ayuda al optimizador de BD Informix a elegir el mejor método de acceso a los datos. *Valor recomendado para el archivo onconfig: OPTCOMPIND 1*
LOGFILES	Especifica el número de registros lógicos. *Valor recomendado para el archivo onconfig: LOGFILES 5*
LOGSIZE	Especifica el tamaño del registro lógico. *Valor recomendado para el archivo onconfig: LOGSIZE 10000*
LOGSMAX	Especifica el número máximo de registros de transacciones. *Valor recomendado para el archivo onconfig: LOGSMAX 7*
PHYSDBS	Es el nombre del espacio de base de datos del registro físico. *Valor recomendado para el archivo onconfig: PHYSDBS espaciobd_registro_físico*
PHYSDBS	Especifica la ubicación del registro físico. Para minimizar la contención con el espacio de base de datos raíz, saque los registros físicos del espacio de base de datos raíz, donde se crean de forma predeterminada. Debido al valor de los datos de gran importancia que contiene, cree el registro físico en su propio dispositivo de E/S y duplíquelo. Cambie estas variables de configuración especificando sus nuevos valores y, a continuación, cambie el servidor universal de Informix al modo silencioso con el comando onmode -ky de Informix y, seguidamente, ejecute el comando onparams para establecer el nuevo registro físico. *Valor recomendado para el archivo onconfig: PHYSDBS espaciobd_registro_físico*
LOCKS	Establece el número de bloqueos disponibles en el servidor de la BD para todos los usuarios. Cada bloqueo utiliza hasta 44 bytes de memoria residente. *Valor recomendado para el archivo onconfig: LOCKS 10000*
DEADLOCK_TIMEOUT	Especifica el número de segundos que un thread espera para adquirir un bloqueo. Este parámetro lo utilizan las consultas distribuidas que acceden a un servidor remoto. *Valor recomendado para el archivo onconfig: DEADLOCK_TIMEOUT 60*
BUFFERS	Especifica la cantidad de memoria física que se ha asignado a los búffers. Calcule todos los demás parámetros de la memoria compartida después de haber determinado el espacio necesario para el parámetro de búffer. Si después de establecer los valores para los demás parámetros de la memoria compartida existe memoria por asignar, asigne más memoria a los búfers utilizando un máximo del 25%. Puede averiguar el número de búfers que deben asignarse tomando el 25% de la memoria física disponible y dividiendo el número por el valor del tamaño de página de Informix para el sistema operativo. También puede ejecutar el comando oncheck -pr para obtener el número de búffers que deben establecerse. *Valor recomendado para el archivo onconfig: BUFFERS 200*
LOGBUFF	Define el tamaño de los búfers de registro lógico en la memoria compartida.

Opción de configuración	Descripción
	Valor recomendado para el archivo onconfig: LOGBUFF 64
PHYSBUFF	Define el tamaño de los dos búfers de registro físico en la memoria compartida. Elija un tamaño que pueda dividirse, de forma equitativa, por el tamaño de página. Puede ejecutar el comando oncheck -pr para obtener el tamaño de página. *Valor recomendado para el archivo onconfig: PHYSBUFF 16*
CKPTINTVL	Define la frecuencia, expresada en número de segundos, con la que el servidor de base de datos de eventos comprueba si debe tomarse un punto de control. *Valor recomendado para el archivo onconfig: CKPTINTVL 120*
CLEANERS	Especifica el número de limpiadores de página que deben asignarse. Debe utilizar un limpiador de página por cada unidad de disco que se haya asignado al servidor de base de datos de eventos. Los limpiadores graban en el disco las páginas cambiadas. La especificación de limpiadores adicionales no tiene ningún efecto en los valores de la memoria compartida. *Valor recomendado para el archivo onconfig: CLEANERS 7*
LRUS	Define el número de colas que se han utilizado menos recientemente (LRU) en la memoria compartida que la agrupación de almacenamiento en búfer ha utilizado para realizar el seguimiento de las páginas más antiguas. A continuación, pueden sustituirse, dejando las páginas que se han utilizado más recientemente en la memoria. Establezca este valor en 4 para un sistema con un único procesador. En la documentación de la base de datos de Informix se proporciona una fórmula para calcular los valores para los sistemas multiprocesador. Supervise las colas LRU con el comando onstat-R y realice los ajustes que sean necesarios. *Valor recomendado para el archivo onconfig: LRUS 4*
LRU_MAX_DIRTY	Especifica que, cuando se haya modificado el porcentaje especificado de los búfers de página de una cola LRU, los limpiadores deben grabar los cambios en el disco para garantizar que la cola no se llenará. *Valor recomendado para el archivo onconfig: LRU_MAX_DIRTY 70*
NOAGE	Parámetro informativo que evita que un sistema operativo reduzca la prioridad de ejecución de un proceso cuando éste se ejecuta durante períodos de tiempo prolongados. Puede comprobar si el sistema operativo reduce la prioridad de los procesos a medida que éstos acumulan tiempo de proceso y, en caso afirmativo, establecer este parámetro en 1. *Valor recomendado para el archivo onconfig: NOAGE 1*
RA_PAGES	Define el número de páginas de disco cuya lectura anticipada debe intentarse durante las exploraciones secuenciales de datos o de tablas de índice. Esta característica puede acelerar considerablemente el proceso de la base de datos por haberse colocado ya en la memoria los datos necesarios antes de que la aplicación los necesite. *Valor recomendado para el archivo onconfig: RA_PAGES 10*
RA_ THRESHOLD	Define el número de páginas de disco que quedan sin procesar en la memoria antes de que el servidor de base de datos de eventos reciba la señal para leer más páginas en la memoria. *Valor recomendado para el archivo onconfig: RA_ THRESHOLD 5*

Opción de configuración	Descripción
SINGLE_CPU_VP	Define el número de procesadores virtuales en los que se ejecuta el servidor de base de datos de eventos. Establezca el valor en 1 si el servidor de base de datos de eventos se ejecuta en un procesador virtual, pues las distintas rutas de código van seguidas de este valor, que evita los cambios que se establecen cuando la ejecución tiene lugar en un sistema multiprocesador. *Valor recomendado para el archivo onconfig: SINGLE_CPU_VP 1*

UPDATE STATISTICS

Con UPDATE STATISTICS permite que la base de datos este sincronizada todas sus tablas. Este comando básicamente recorre la tabla especificada y actualiza los siguientes campos del catálogo, que son utilizados por el optimizador de la base de datos para elegir el mejor plan a la hora de ejecutar las queries.

systables.nrows	número de filas
systables.npused	número de páginas para almacenar los datos
yscolumns.colmax	segundo valor más grande para una columna
syscolumns.colmin	segundo valor más pequeño para una columna
sysindexes.nunique	número del único valor para la clave
sysindexes.clustered	cluster o no (-:normal, C: agrupado)

- **Administración del Sistema**

ADMINISTRACCIÓN DEL SISTEMA

Manual de Informix "***Performance Guide for IBM Informix Dynamic Server***", donde se recoge la configuración y funcionamiento de IBM Informix Dynamic Server para lograr un rendimiento óptimo. El enlace al documento: http://publib.boulder.ibm.com/epubs/pdf/8344.pdf.

Tarea	Informix	Manual de consulta
Programas de utilidad de Administración del Servidor de Base de Datos (Windows)	ixpasswd.exe ixsu.exe ntchname.exe	**ixpasswd.exe** – cambia la contraseña de inicio de sesión para todos los servicios que inicien la sesión como usuario informix. **ixsu.exe** – inicia una ventana de línea de mandatos que se ejecuta como el usuario especificado. **ntchname.exe** – Cambia las entradas del registro de Dynamic Server referentes al nombre de sistema principal antiguo por el nombre de sistema principal nuevo.
Ayuda INFORMIX DYNAMIC SERVER	Web IBM ayuda	Material de consulta *para Informix Dynamic Server Administrator's Reference.* http://publib.boulder.ibm.com/infocenter/idshelp/v10/index.jsp?topic=/com.ibm.adref.doc/adref202.htm
Programas de utilidad de INFORMIX DYNAMIC SERVER		
Controlar operaciones de Enterprise Replication	cdr	*IBM Informix: Dynamic Server Guia de Enterprise Replication* http://publib.boulder.ibm.com/epubs/pdf/ct1t2na.pdf
Descargar una base de datos en archivos de texto a fin de importarla más adelante a otra base de datos y crear un archivo de esquema.	dbexport	*IBM Informix: Migration Guide* http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf
Crear y llenar una base de datos a partir de archivos de texto. Utilizar el archivo de esquema con dbimport para volver a crear el esquema de base de datos.	dbimport	*IBM Informix: Migration Guide* http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf
Cargar datos en bases de datos o tablas.	dbload	*IBM Informix: Migration Guide* http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf
Crear un archive que contenga las sentencias de SQL necesarias para duplicar una tabla, vista o base de datos especificada o visualizar el	dbschema	*IBM Informix: Migration Guide* http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf

Tarea	Informix	Manual de consulta
esquema informativo.		
Iniciar o detener MaxConnect o para recopilar estadísticas sobre MaxConnect.	imcadmin	*IBM Informix: MaxConnect User's*
Realizar diversas tareas administrativas utilizando IBM Informix Server Administrator (ISA)	ISA	*Ayuda en línea de ISA*
Gestionar IBM Informix Storage Manager, dispositivo de almacenamiento y volúmenes de soportes de almacenamiento.	ism	*IBM Informix: Storage Manager Guía del Administrator* http://publib.boulder.ibm.com/epubs/pdf/25122990.pdf
Gestionar máscaras de auditoría y configuraciones de auditoría.	onaudit	*IBM Informix: Trusted Facility Guide* http://publib.boulder.ibm.com/epubs/pdf/25123000.pdf
Realizar copias de seguridad y restauraciones de los espacios de almacenamiento y las anotaciones lógicas.	onbar	*IBM Informix: Guía de copia de seguridad y restauración* http://publib.boulder.ibm.com/epubs/pdf/25122690.pdf
Comprobar si existen incoherencias en las estructuras de disco especificadas, reparar las estructuras de índice incoherentes y visualizar información sobre las estructuras de disco.	oncheck	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Cambiar la modalidad de anotaciones cronológicas.	ondblog	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Hacer que el servidor de bases de datos se coloque en línea.	oninit	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Cargar datos creados con onunload en el servidor de base de datos.	onload	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Visualizar el contenido de los archivos de anotaciones lógicas.	onlog	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Realizar las tareas administrativas utilizando los menús de ON-Monitor.	ON-Monitor	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Modificar la configuración de las anotaciones	onparams	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Supervisor el rendimiento del servidor de base de datos (crear gráficos, consultar árboles, mostrar estados y métricas).	onperf	*IBM Informix Performance Guide* http://publib.boulder.ibm.com/epubs/pdf/8344.pdf

Tarea	Informix	Manual de consulta
Para escribir scripts y crear archivos que automaticen los trabajos de carga y descarga de datos.	onpladm	*IBM Informix High-Perormance Loader User's Guide* http://publib.boulder.ibm.com/epubs/pdf/25122860.pdf
Extraer información de una pista de auditoría	onshowaudit	*IBM Informix: Trusted Facility Guide* http://publib.boulder.ibm.com/epubs/pdf/25123000.pdf
Modificar espacios de db, espacios de blob, espacios de sb o espacios ext.	onspaces	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Supervisor el funcionamiento del servidor de bases de datos	onstat	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Supervisar y depurar el servidor de bases de datos	onstat-g	*IBM Informix: Administrator's Reference* http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Anotar, copiar y restaurar datos	ontape	*IBM Informix: Guía de copia de seguridad y restauración* http://publib.boulder.ibm.com/epubs/pdf/25122690.pdf
Descargar datos del servidor de bases e datos	onunload	*IBM Informix: Migration Guide* http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf
Configurar el servidor de bases de datos, los espacios de almacenamiento, la conectividad de la red y J/Foundation.	Server Setup	*Ayuda en líena de ISA*
Explorar servidores de bases de datos, ejecutar sentencias de SQL y procedimientos almacenados (SPL) y visualizar los resultados.	Server Studio Java Edition 2.30 by AGS	*Ayuda en línea de Server Studio*

- **Otras Utilidades**

OTRAS UTILIDADES

Tarea	Informix	Manual de consulta
Utilidad que entre otras funcionalidades permite probar las aplicaciones de base de datos, para su posterior utilización en el entorno de producción.	DB-Access	*IBM Informix: Guía del usuario de DB-Access* http://publib.boulder.ibm.com/epubs/pdf/ct1skna.pdf
Para poder intercalar sentencias SQL directamente en programas de C.	Información en el manual	*IBM Informix: ESQL/C Programmer's Manual* http://publib.boulder.ibm.com/epubs/pdf/ct1uhna.pdf

- **Manuales de Informix**

MANUALES INFORMIX

Enlace a los manuales online http://www-01.ibm.com/software/data/informix/pubs/library/

Manual	Contenido
Administrator's Guide	Compresión, configuración y administración del servidor de base de datos http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Administrator's Reference	Material de consulta para Informix Dynamic Server, como por ejemplo los programas de utilidad onmode y onstat del servidor de base de datos, así como las descripciones de los parámetros de configuración, las tablas sysmasters y los registros de anotaciones cronológicas lógicas. http://publib.boulder.ibm.com/epubs/pdf/ct1syna.pdf
Guía de copia de seguridad y restauración	Los conceptos y métodos que tiene que comprender cuando utilice los programas de utilidad ON-Bar y ontape para realizar copias de seguridad y restauración de los datos. http://publib.boulder.ibm.com/epubs/pdf/25122690.pdf
Guía del usuario de DB-Access	Utilización del programa de utilidad DB-Access para acceder, modificar y recuperar datos de las bases de datos de Informix. http://publib.boulder.ibm.com/epubs/pdf/ct1skna.pdf
Datablade API Function Reference	Las funciones de la API de DataBlade, y el subconjunto de funciones ESQL/C que la API de DataBlade soporta. Puede utilizar la API DataBlade para desarrollar aplicaciones LIBMI clientes y rutinas C definidas por el usuario para acceder a los datos en las bases de datos de Informix. http://publib.boulder.ibm.com/epubs/pdf/25122721.pdf
DataBlade API Programmer's Guide	API de DataBlade, que es el interfaz de programación de aplicaciones en lenguaje C que se proporciona con Dynamic Server. Utilice la API de DataBlade para desarrollar aplicaciones cliente y servidor que acceden a los datos almacenados en bases de datos de Informix. http://publib.boulder.ibm.com/epubs/pdf/25122731.pdf
Guía para el diseño e implementación de bases de datos.	Diseño, implantación y gestión de las bases de datos de Informix.
Guía de Enterprise Replication	Cómo diseñar, implantar y gestionar un sistema Enterprise Replication para duplicar datos entre varios servidores de bases de datos. http://publib.boulder.ibm.com/epubs/pdf/ct1t2na.pdf
Archivo Mensajes de error	Causas y soluciones para mensajes de error numerados que podría recibir al trabajar con productos IBM Informix. http://publib.boulder.ibm.com/epubs/html/29920180.html

Manual	Contenido
Guía de iniciación	Describe los productos empaquetados con IBM Informix Dynamic Sever y la interoperabilidad con otros productos de IBM. Resume funciones importantes de Dynamic Server y las nuevas funciones para cada versión.
Guide to SQL: Reference	Información sobre bases de datos, tipos de datos, tablas del catálogo del sistema, variables de entorno y las bases de datos de demostración stores_demo de Informix. http://publib.boulder.ibm.com/epubs/pdf/ct1spna.pdf
Guide to SQL:Syntax	Descripciones detalladas de la sintaxis de todas las sentencias sQL y SPL de Informix. http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf
Guide to SQL: Tutorial	Guía de aprendizaje sobre SQL, implementada por los productos Informix. http://publib.boulder.ibm.com/epubs/pdf/25122842.pdf
High-Performance Loader User's Guide	Acceso y utilización de High-Performance Loader (HPL), para cargar y descargar grandes cantidades de datos hacia y desde bases de datos Informix. http://publib.boulder.ibm.com/epubs/pdf/25122860.pdf
Guía de instalación para Microsoft Windows	Instrucciones para instalar IBM Informix Dynamic Server en Windows. http://publib.boulder.ibm.com/epubs/pdf/8322.pdf
Guía de instalación para UNIX y Linux.	Instrucciones para instalar IBM Informix Dynamic Server en Unix y Linux. http://publib.boulder.ibm.com/epubs/pdf/8321.pdf
J/Foundation Developer's Guide	Escritura de rutinas definidas por el usuario (UDR) en el lenguajes de programación Java para Informix Dynamic Server con J/Foundation. http://publib.boulder.ibm.com/epubs/pdf/25122910.pdf
Large Object Locator DataBlade Module User's Guide	Utilización de Large Object Locator, un módulo de base de DabaBlade que pueden utilizar otros módulos que crean o almacenan datos de objetos grandes. Large Object Locator permite crear una única interfaz coherente para objetos grandes y amplía el concepto de objetos granes para incluir los datos almacenados fuera de la base de datos. http://publib.boulder.ibm.com/epubs/pdf/ct1v0na.pdf
Migration Guide	Conversión e inversión desde las últimas versiones de servidores de bases de datos Informix. Migración entre diferentes servidores de bases de datos Informix. http://publib.boulder.ibm.com/epubs/pdf/25122930.pdf
Optical Subsystem Guide	Optical Subsystem, un programa de utilidad que soporta el almacenamiento de datos BYTE y TEXTO en disco óptico.
Performance Guide	Configuración y funcionamiento de IBM Informix Dynamic Server para lograr un rendimiento óptimo. http://publib.boulder.ibm.com/epubs/pdf/8344.pdf

Manual	Contenido
R-Tree Index User's Guide	Creación de índices R-tree en tipos de datos adecuados, creando nuevas clases del operador que utilizan el método de acceso R-tree, y gestión de bases de datos que utilizan el método de acceso secundario R-tree. http://publib.boulder.ibm.com/epubs/pdf/8342.pdf
SNMP Subagent Guide	Subagente de IBM Informix que permite que un gestor de red SNMP (Protocolo simple de gestión de red) supervise el estado de los servidores Informix.
Storage Manager Guía del administrator	Informix Storage Manager (ISM), que gestiona dispositivos e almacenamiento y soportes de almacenamiento para el servidor de bases de datos Informix. http://publib.boulder.ibm.com/epubs/pdf/25122990.pdf
Trusted Facility Guide	Posibilidades de auditoría segura de Dynamic Server, entre las que se incluyen la creación y mantenimiento de registros de auditoría. http://publib.boulder.ibm.com/epubs/pdf/25123000.pdf
Guía del desarrollo de rutinas definidas por el usuario y tipos de datos	Cómo definir nuevos tipos de datos y habilitar rutinas definidas por el usuario (URD) para ampliar IBM Informix Dynamic Server.
Virtual-Index Interface Programmer's Guide	Creación de un método de acceso secundario (índice) con Virtual-Index Interface (VII) para ampliar los esquemas de creación e índices incorporados de IBM Informix Dynamic Server. Normalmente, se utiliza con un módulo Datablade. http://publib.boulder.ibm.com/epubs/pdf/25123020.pdf
Virtual-Table Interface Programmer's Guide	Creación deun método de acceso principal con Virtual –Table Interface (VTI) para que los usuarios tengan una única interfaz SQL con las tablas Informix y con los datos que no siguen el esquema de almacenamiento de Informix Dynamic Server. http://publib.boulder.ibm.com/epubs/pdf/25123020.pdf

CAPITULO 9

CONCLUSIONES

9. CONCLUSIONES

Con la realización de este PFC, una de las principales conclusiones a la que he llegado es que toda empresa que posea un Sistema de Información medianamente complejo debe de someterse a un control estricto de evaluación de eficacia y eficiencia. Casi todas las empresas tienen su información estructurada en sistemas informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente, además de que el éxito de una empresa depende de la eficiencia de sus sistemas.

La Auditoría, en particular la de sistemas de información, es la revisión, evaluación de los controles, sistemas y procedimientos informáticos, de su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información que servirá para una adecuada toma de decisiones.

Con la realización de una Auditoría se genera mayor confianza en el sistema, se identifican los aspectos positivos y los negativos, los cuales deberán ser reforzados con una gestión de calidad.

Es necesario mejorar la posición de la Auditoría dentro de las organizaciones, convirtiéndola en un apoyo a la alta dirección para mejorar la gestión y garantizar la existencia de un entorno e control adecuado.

En el campo de las bases de datos, el SGBD debe garantizar que la base de datos sea segura, entendiendo por seguridad a la protección frente a accesos no autorizados, ya sean intencionados o accidentales.

Podemos remarcar que en el trabajo de la auditoría se precisa de gran conocimiento de la Informática, seriedad, capacidad, minuciosidad y responsabilidad; por ello una auditoría debe realizarse con gente altamente capacitada, una auditoría mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.

Es importante destacar lo que aporta este Proyecto Fin de Carrera, el objetivo ha sido proporcionar un lugar de referencia y ayuda a la gestión de los sistemas Informix, debido a la poca existencia de documentos y libros que versen sobre este sistema. Podemos decir que prácticamente solo existen los manuales y documentación proporcionada por

IBM, casi todos en Inglés, y trabajos realizados por personas u organizaciones que han tenido que llevar a cabo un estudio sobre sistemas Informix por algún motivo profesional. Todo esto hace que considere alcanzados los objetivos que me había propuesto al inicio de este Proyecto de Fin de Carrera. Además de haber obtenido un enriquecimiento tanto a nivel técnico como a nivel personal.

Por ello, poder tener un lugar donde te permita obtener una respuesta rápida a problemas, formas de cómo realizar los controles, obtener información del sistema y en el caso de querer ampliar dicha información, tener un enlace a la propia documentación que proporciona IBM, es muy valioso, tanto en el tiempo necesario para la localización de la información, como la ayuda que proporciona obtener otros métodos que nos ayuden y no sabíamos de su existencia.

Otros Sistemas Gestores de Bases de Datos, como Oracle, MySql, etc que han originado en el mercado comercial gran cantidad de libros que permite un lugar de referencia, esto no se ha producido en Informix, apenas hay documentación diferente a la proporcionada por IBM.

Esto se ve reflejado en la información que existe en Internet, Oracle y otros SGBD, tienen una gran cantidad de documentación y versiones del producto que nos permiten instalarlos y poder conocerlo más ampliamente. Pero de Informix de IBM no hay apenas nada, está muy controlado y existen muy pocas versiones de demostración que permitan su instalación.

CAPITULO 10

LINEAS FUTURAS DE DESARROLLO

10. LÍNEAS FUTURAS DE DESARROLLO

Como todo trabajo de desarrollo, a medida que se va avanzando se abren nuevos caminos a desarrollar y se observa la posibilidad de profundidad más en otros. En mi estudio creo que una posible línea futura de desarrollo es la incorporación de más utilidades y herramientas en la aplicación. Existen aspectos que sólo un Auditor, con años de experiencia detecta que necesita y le supondría un gran avance en el estudio y desarrollo de una auditoría. De tal forma, que ayude a obtener más información y reducir tiempos de estudio, variables esenciales que afectan directamente en el éxito de la Auditoría y rentabilidad del trabajo.

El mundo de la informática y en concreto la aparición de nuevas tecnologías se llevan a cabo de una forma muy rápida en el tiempo, lo que supone una necesidad constante de actualizaciones. Por ello esta aplicación requeriría actualizaciones de forma constante, así como las mejoras que vayan sugiriendo por la experiencia y necesidades que puedan ir aportando los auditores, verdaderos usuarios de la aplicación.

Aunque ya hemos comentado en este Proyecto de Fin de Carrera la idea de realizar programas, codificados en Informix 4GL, que ataquen la base de datos y el sistema, hemos indicado la alta probabilidad que el cliente no nos permita ejecutarlos en sus sistemas. Sin embargo si podríamos crear programas que actuaran de forma independiente al sistema de base de datos y en un entorno aparte, con la entrada de un fichero de pistas de auditoría o cualquier otra información que nos proporcionasen los administradores del sistema, y tratarla de forma exhaustiva.. De tal manera que se pudiera ver de forma tangible como se comporta el sistema y si se observan irregularidades hasta ahora no detectadas. Todas estas funcionalidades podrían integrarse en la aplicación de forma que todo quede centralizado.

No obstante es necesario establecer unos objetivos y un alcance, como en toda auditoría. En este Proyecto de Fin de Carrera se ha analizado la Auditoría e Informix y con dichos estudios se ha llevado a cabo la Aplicación que versa sobre la gestión de una Auditoría en Informix, que en definitiva son los temas claves del proyecto.

CAPITULO 11

GLOSARIO

11. GLOSARIO

Este glosario contiene términos y definiciones que se encuentran en el presente manual, algunos son acrónimos. Muchos son términos específicos de IBM Informix.

Access. Acceder

AEPD. Agencia Española de Protección de Datos.

ANSI. American National Standards Institute.

API. Application Programming Interface – Interfaz de programación de aplicaciones.

Application. Aplicación, programa informático que permite a un usuario utilizar un ordenador con un fin específico. Las aplicaciones son parte del software de una computadora y suelen ejecutarse sobre el sistema operativo.

Backup. Copia de seguridad.

Buffer. Memoria intermedia.

Checklist. Lista de comprobación.

Checkpoint. Punto de recuperación.

Clonación. Proceso mediante el cual ISM crea una copia exacta de datos guardados (conjuntos guardados). ISM puede clonar conjuntos guardados individualmente o todo el contenido de un volumen de almacenamiento.

COBIT. Control Objectives for Information and related Technology – Objetivos de Control para la información y Tecnologías relacionadas

CODASYL. Conference on data System Languages

Commit. Confirmación de una transacción.

Chunk. Unidad mínima de disco que el sistema operativo puede asignar.

DAC. Control de acceso discrecional.

DBA. Administrador de Base de Datos.

DBSPACE. Unidad de asignación de espacio de Informix.

Dispositivo de tipo archivo. Sistema de archivos del servidor ISM que se utiliza como dispositivo de almacenamiento.

ER. Entidad /Relación

Host. Computadora principal de una instalación..

IBM. Internacional Business Machines.

IBM Informix Server Administrator. Herramienta basada en un navegador que proporciona la administración del sistema basada en la Web para los servidores de base de datos Informix.

IBM Informix Storage Manager. Recibe peticiones de copia de seguridad y de restauración desde ON-Bar y dirige los datos a y desde los volúmenes de almacenamiento que están montados en dispositivos de almacenamiento.

IBM Informix Storage Manager. Recibe peticiones de copia de seguridad y de restauración desde ON-Bar y dirige los datos a y desde los volúmenes de almacenamiento que están montados en dispositivos de almacenamiento.

IDS. Informix Dynamic Server.

ISA. Vease IBM Informix Server Administrator.

ISACA. Asociación de Auditoría y Control de Sistemas de Información.

ISM. Véase IBM Informix Storage Manager.

ISO. International Standard Operation- Organización Internacional para la estandarización.

Log. Registro cronológico de anotaciones.

LOPD. Ley Orgánica de Protección de Datos de Carácter Personal.

Metadatos. Información de los datos.

OLTP. Online Transaction Processing – Procesamiento de Transacciones En Línea. Es un tipo de sistemas que facilitan y administran aplicaciones transaccionales, usualmente para entrada de datos y recuperación y procesamiento de transacciones (gestor transaccional).

ON-Bar. Herramienta que utiliza Informix para la realización de copias de seguridad y restauración.

Ontape. Herramienta que utiliza Informix para la realización de copias de seguridad y restauración.

OODBMS. Sistema Gestor de Bases de Datos Orientados Objetos.

ORDBMS. Sistema Gestor de Bases de Datos objeto relacionales.

PC. Personal Computer.

RDBMS. Relational Database Management System.

Servidor ISM. Sistema UNIX o Windows que ejecuta el software de servidor ISM.

SGBD. Sistema de Gestión de Bases de Datos.

SPL . Stored Procedure Language – Lenguaje de procedimiento almacenado.

SQL. Lenguaje de Consulta Estructurado.

TI. Tecnología de la Información.

UDR. Rutinas externas escritas en los lenguajes C y Java.

Volumen. Soporte para realizar copias de seguridad, como una cinta magnética, una partición de unidad de disco o un disco óptico.

XBSA. X/Open Backup Services Application Programming Interface. Proporciona una interfaz de programas y funciones que gestionan operaciones de copia de seguridad y restauración. XBSA conecta ISM con el servidor de bases de datos.

CAPÍTULO 12

BIBLIOGRAFÍA

12. BIBLIOGRAFÍA

Alonso Rivas, Gonzalo. “Auditoría Informática”. 1989. Editorial: Díaz de Santos.

Alonso , A.J. “Auditoría Informática”. 1987. Editorial Paraninfo.

COBIT 4.0. “*Control Objectives*”. Publicado por IT Governance Institute (ITGI) Noviembre 2005.

COBIT actualización 4.1, “*Control Objectives for Information and related Technology”*. Publicado por IT Governance Institute (ITGI). Mayo 2007.

De Miguel, A. Y Piattini, M “*Fundamentos y modelos de bases de datos”* (Segunda edición,, Editoria Ra-ma, 1999).

IBM Informix Dynamic Server Administrator’s Reference (Version 9.4).

IBM Informix Guide to SQL, Reference (Version 9.4).

IBM Informix Guide to SQL: Syntax (Version 10.0).

IBM Informix Dynamic Server Performance Guide (Versión 9.4)

IBM Informix Backup and Restore Guide (Version 10.0).

IBM Informix Storage Manager Guía del administrador (DB2 IBM Informix Versión 2.2)

IBM Informix – Guía de copia de seguridad y restauración (Versión 10.0/8.5)

IBM Informix Trusted Facility Guide (Version 10.0).

IBM Informix Dynamic Server Enterprise Replication Guide (Version 9.4).

Mills David, *“Manual de Auditoría de la Calidad”*, Gestión 2000. 1997

Piattini Velthuis, Mario G., Emilio de Peso "*Auditoría Informática – Un enfoque práctico",* Editorial Ra-ma, 1996

Piattini Velthuis, Mario G. "*Auditoría de tecnologías y sistemas de información".* 2008. Editorial:RA-MA.

Piattini Velthuis, Mario G. "*Mantenimiento del Software: Modelos, técnicas y métodos para la gestión del cambio."* Diciembre 2000. Editorial Ra-Ma.

Ron Weber. *"Information Systems control audit.".* 1999 Editorial Prentice Hall.

Silberschatz, Korth, Sudarshan *"Fundamentos de Bases de Datos".* Quinta edición, 2006. McGrawHill

Thomas M.Connolly, Carolyn E. Begg, "*Sistemas de bases de datos: Un enfoque práctico para diseño, implementación y gestión"*. Cuarta edición, 2005. Editorial: Addison Wesley

Valle, Julián del. "Auditoría informática: glosario de términos" . 2002. Editorial: Fundación DINTEL.