UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

TRABAJO DE DIPLOMA PARA OPTAR POR EL TÍTULO DE INGENIERO EN CIENCIAS INFORMÁTICAS

TÍTULO: GUÍA PARA GARANTIZAR SEGURIDAD EN BASES DE DATOS ORACLE DURANTE EL PROCESO DE DESARROLLO DE APLICACIONES INFORMÁTICAS.

CLASIFICACIÓN: INVESTIGACIÓN

AUTOR:

ANAIVYS VÁZQUEZ ABASCAL

TUTORES:

ING. YUSLEYDI FERNÁNDEZ DEL MONTE

ING. SONIA GUERRERO LAMBERT

ING. YANDRY ALBERTO TERRY

CUIDAD DE LA HABANA

JUNIO 2010

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

_____	_____	_____	_____
Firma del Autor	Firma del Tutor	Firma del Tutor	Firma del Tutor

Ser lo que soy, no ha sido nada sin la seguridad.

William Shakespeare (1594)

DEDICATORIA

Quiero dedicarles esta tesis a aquellas personas que nunca están lejos porque siempre están pensando en mí, que jamás me han dado la espalda, que por sobre todas las cosas nunca me van a dejar de querer.

A esas personas que me aceptan con mis virtudes y mis defectos, que no cesan hasta verme feliz, que cada obstáculo de mi vida se convierte en nada ante ellos, que me perdonan por mis errores, que me ayudan en mis dificultades, que no vacilan en darme lo que tienen sin esperar nada a cambio y que por sobre todas las cosas de este mundo, yo siempre para ellos voy a seguir siendo una buena hija y una buena hermana.

Les dedico todo mi esfuerzo a mis padres y a mi hermana.

También dedicarle este trabajo a mi novio Ernesto que siempre me apoyó espiritualmente dándome mucho apoyo cuando me quedé sola con este trabajo, demostrándome que sí podía hacerlo y levantándome siempre el ánimo. No me dejó caer ante los desencantos a lo largo del camino para llegar hasta aquí. Además por saber comprender mis estados de ánimo y soportarme cuando más estresada estuve y nunca se rindió, luchó a mi lado para que alcanzara este sueño.

RESUMEN

El trabajo de diploma muestra una investigación sobre la seguridad en bases de datos (BD) teniendo en cuenta sus principales componentes: integridad, confidencialidad, disponibilidad y el no repudio, aspectos importantes que ayudan a determinar cuán seguro o fiable pueden ser las aplicaciones informáticas que se desarrollan en cualquier entorno de trabajo. Teniendo en cuenta los problemas que presenta el cliente, Centro de Tecnologías de Gestión de Datos (DATEC), al no contar con un modelo o pautas para garantizar seguridad en la base de datos desde el comienzo del proceso de desarrollo de software, es que se realiza un estudio minucioso sobre las bases de datos realizadas en Oracle para lograr asegurarla y para ello se crea una guía que garantice la seguridad de las bases de datos Oracle desde el proceso de desarrollo de software orientada por la metodología RUP, utilizada por el cliente. Una vez confeccionada la propuesta, se somete a una evaluación basada en la opinión de un grupo de especialistas en el tema. El método aplicado para evaluar la solución ha sido Delphi, mediante el cual se demuestra que la propuesta de solución es efectiva y resuelve el problema que da origen a la investigación, obteniendo un coeficiente de concordancia entre especialistas de un 0.877.

INDICE

INTRODUCCIÓN

Siempre, a lo largo de la historia de la humanidad, está latente la necesidad de conservar la información que posteriormente va a ser utilizada. Con el desarrollo de la ciencia surgen dispositivos de almacenamiento y programas que son capaces de organizar y guardar datos en estructuras llamadas bases de datos. Una base de datos o banco de datos es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. En la actualidad, debido al desarrollo tecnológico, la mayoría de las bases de datos están en formato digital, lo que ofrece un amplio rango de soluciones al problema de almacenar datos. Debido a la necesidad de almacenar grandes volúmenes de información de forma organizada, accesible y segura se crean los Sistemas Gestores de Bases de Datos (SGBD). En el mundo existen un gran número de gestores de bases de datos con diferentes características, los más utilizados son PostgreSQL, MySQL y Oracle.

A la hora de desarrollar un sistema es preciso darle gran importancia a la seguridad; las bases de datos no quedan exentas de esto, pues pequeños errores u omisiones, tanto en el desarrollo como en la administración de las mismas abren las puertas al atacante. La seguridad es una característica de cualquier sistema que nos indica que está libre de todo peligro, daño o riesgo, y en cierta manera, infalible. Se entiende que mantener un sistema fiable consiste básicamente en garantizar tres aspectos: **confidencialidad**, **integridad** y **disponibilidad**.

Actualmente en la Universidad de las Ciencias Informáticas (UCI) existe una red de centros de desarrollo de aplicaciones informativas; el centro de DATEC es el encargado de realizar los desarrollos relacionados con el tema de base de datos e inteligencia de negocio; el mismo ha decidido utilizar Oracle Business Intelligence Tools & Technology para realizar las aplicaciones informáticas. Esta suite de Oracle viene diseñada para utilizar Oracle Database como SGBD, por este motivo se hace obligatorio el estudio y comprensión de esta tecnología.

Oracle Database es el principal gestor de bases de datos de la compañía Oracle, la cual cuenta además con soluciones de código abierto como Oracle Berkeley, Oracle Express y MySQL, Oracle Database es una solución de bases de datos propietaria destinada a las soluciones empresariales que necesiten una alta demanda de almacenamiento por lo cual se considera como una de las soluciones más completas, seguras, configurables y de mayor cantidad de aplicaciones asociadas que existe hoy en el mundo.

Toda base de datos tiene que lograr asegurar los datos que contiene, por tal motivo la seguridad en Oracle Database es uno de los puntos claves, lo cual representa también uno de los aspectos por los cuales han ganado gran parte del mercado de las bases de datos. El proceso de desarrollo de software tiene en cuenta la base de datos en todas las etapas, realizar una administración eficiente de la base de datos presupone que la misma tenga un alto nivel de seguridad y por ende la aplicación informática también. La seguridad de los servicios y de los datos garantiza y complementa la eficiencia de desempeño de la solución informática a desarrollar, es por ello que contar con una buena gestión de la misma es una fortaleza en el proceso.

Hoy DATEC tiene planificado el desarrollo de varias aplicaciones informáticas en el área de las bases de datos, para la realización de estos desarrollos en muchas ocasiones no se garantiza la seguridad en las bases de datos desde el inicio del proceso de desarrollo, esta situación provoca que las pruebas realizadas a las aplicaciones informáticas desarrolladas no logren garantizar una correcta disponibilidad, confidencialidad e integridad de los datos que manejan. Además durante el desarrollo los roles que interactúan con la base de datos no tienen una correcta asignación de privilegios, los cambios realizados en la base de datos muchas veces se realizan y no se lleva un control de los mismos y no se cuenta con una política de seguridad para las bases de datos durante su ciclo de vida. A partir de lo antes expresado, el centro DATEC desea conocer cuáles son los elementos que permiten garantizar la seguridad desde el inicio de cada proyecto, con el objetivo de gestionar la seguridad de manera eficiente para lograr desarrollar aplicaciones informáticas más seguras y estables.

Teniendo en cuenta la problemática descrita anteriormente, se concibe la formulación del **problema científico** de la siguiente manera:

¿Cómo garantizar la seguridad en bases datos Oracle durante el proceso de desarrollo de aplicaciones informáticas?

El **objeto de estudio** está constituido por: Procesos de obtención de seguridad en bases de datos.

El **campo de acción** está centrado en: Procesos de obtención de seguridad en bases de datos realizadas en Oracle durante el proceso de desarrollo de aplicaciones informáticas.

La investigación tiene como **objetivo general**:

Desarrollar una guía para garantizar la seguridad en bases de datos Oracle durante el proceso de desarrollo de aplicaciones informáticas.

Para lograr un desempeño óptimo de la investigación se determinan los siguientes **objetivos específicos**:

- ✓ Investigar los aspectos relevantes relacionados con la seguridad en las bases de datos realizadas en Oracle profundizando en los principales aspectos del tema.
- ✓ Construir una guía para garantizar seguridad en las bases de datos realizadas en Oracle.
- ✓ Realizar un pronóstico del impacto de la propuesta de solución a través del método Delphi.

Para dar cumplimiento a los objetivos de la investigación se definieron como **tareas investigativas**:

- ✓ Estudio del proceso de desarrollo de software, para identificar las actividades y los roles interactúan con la base de datos.

- ✓ Estudio de la seguridad en Oracle Database, para conocer las tendencias existentes respecto al tema.
- ✓ Definición de las tareas por roles para garantizar la seguridad de la base de datos desde su creación en el proceso de desarrollo.
- ✓ Definición de la Guía de Seguridad de Oracle basándose en las tareas por roles definidas anteriormente para garantizar la seguridad de la base de datos.
- ✓ Evaluación de la Guía de Seguridad de Oracle para el proceso de desarrollo de aplicaciones informáticas a través de consulta a especialistas.

Se plantea la siguiente **Idea a defender**:
La realización de una guía para garantizar la seguridad en bases de datos Oracle durante el proceso de desarrollo de software puede mejorar la confidencialidad, integridad y disponibilidad de los datos de las aplicaciones informáticas.

Con el objetivo de desarrollar las tareas mencionadas anteriormente se trabaja con los siguientes **métodos de la investigación**:

Método Teórico Histórico Lógico:
Se logra una mayor comprensión del estado actual y las etapas por las que transitan las bases de datos. Muestra el desarrollo tecnológico y la evolución que tienen las principales compañías que reinan el mundo de los Sistemas Gestores de Bases de Datos como Oracle Database. Analizar las características comunes de las bases de datos, su funcionamiento, cómo se trata el tema de la seguridad de la información y especialmente enfocar este estudio a Oracle DataBase para lograr obtener una investigación fructífera y posteriormente realizar la guía que se desea proponer.

Método Teórico Analítico-Sintético:
Se utiliza este método para analizar los diferentes algoritmos de encriptación de datos, la estructura y almacenamiento de datos así como los servicios que propone Oracle. Además se realiza un estudio de la documentación que brindan en el sitio oficial acerca de cómo obtener

seguridad en esta base de datos y mediante ello se extraen los elementos fundamentales para darle solución al problema investigativo propuesto.

Método Empírico-Encuestas:
La encuesta permite a través de un conjunto de preguntas obtener información acerca de la validez de la guía que se confecciona para obtener seguridad. Esta encuesta se le aplica a un panel de especialistas en el tema permitiendo conocer que la propuesta de solución resuelve el problema existente.

Método Estadístico Descriptivo:
Se utiliza este tipo de métodos para evaluar la propuesta de solución, obteniendo información estadística sobre los resultados y beneficios de que se obtiene con la guía confeccionada. Muestra datos cuantitativos de las ventajas que ofrece cumplir con las actividades de la propuesta. Para obtener estos resultados se utiliza el método Delphi.

El trabajo de diploma viene estructurado por tres capítulos de la siguiente manera:

Capítulo 1 Fundamentación Teórica: Se realiza la fundamentación teórica de los principales elementos para alcanzar cierto nivel de conocimiento para luego desarrollar una excelente investigación. Se abordan los conceptos de seguridad informática, seguridad en bases de datos Oracle y se realiza un detallado estudio del Sistema Gestor de Bases de Datos Oracle. Además se refleja el estudio de las metodologías de desarrollo haciendo énfasis en RUP.

Capítulo 2 Propuesta de Solución: Muestra la propuesta de solución basada en el conocimiento adquirido en la investigación. Se presenta una guía para garantizar seguridad en las bases de datos Oracle durante las fases del proceso de desarrollo de software que propone la metodología RUP que ha sido definida por el cliente. Cada una de las fases que compone la guía cuenta con las actividades fundamentales que se deben llevar a cabo para asegurar la BD Oracle y cada una de ellas tiene un conjunto de buenas prácticas a tener en cuenta para ello así como los roles involucrados.

Capítulo 3 Evaluación de la propuesta: Se realiza un pronóstico de la propuesta determinando el impacto que va a tener una vez que se aplique. Para la evaluación se escoge el método Delphi, el cual propone que a través de la opinión de un panel de especialistas se pueda confirmar la validez de la guía y de esta manera ver la concordancia entre las respuestas de los especialistas, lo que demuestra si todos están de acuerdo con la veracidad de la propuesta de solución.

CAPÍTULO 1: FUNDAMENTACIÓN TEÓRICA

Introducción

En este capítulo se definen todos los conceptos teóricos necesarios para posteriormente realizar la guía que garantice seguridad en las bases de datos realizadas en Oracle. Se abordan los aspectos relacionados con la seguridad, y lo que ella implica, así como los términos relacionados con las BD realizadas en el SGBD Oracle. De igual manera se analizan cuáles son las estrategias actuales para asegurar los datos a nivel de las bases de datos en Oracle.

1.1. ¿Qué es seguridad?

Se puede entender como seguridad una característica de cualquier sistema (informático o no) que indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible. Como esta característica, particularizando para el caso de sistemas operativos o redes de computadoras, es muy difícil de conseguir (según la mayoría de expertos, imposible), se suaviza la definición de seguridad y se pasa a hablar de fiabilidad (probabilidad de que un sistema se comporte tal y como se espera de él) más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros. (1)

La seguridad informática se resume, por lo general, en cinco objetivos principales:

- ✓ **Integridad**: Garantizar que los datos sean los que se supone que son. Consiste en determinar si se han alterado los datos durante la transmisión (accidental o intencional).
- ✓ **Confidencialidad**: Asegurar que sólo los individuos autorizados tengan acceso a los recursos que se intercambian. Consiste en hacer que la información sea ininteligible para aquellos individuos que no han sido autorizados en la operación.
- ✓ **Disponibilidad**: Garantizar el correcto funcionamiento de los sistemas de información. Garantiza el acceso a un servicio o recurso.

- ✓ **Evitar el rechazo o no repudio**: Garantizar de que no pueda negar una operación realizada. Constituye la garantía de que ninguna de las partes involucradas pueda negar en el futuro una operación realizada.
- ✓ **Autenticación**: asegurar que sólo los individuos autorizados tengan acceso a los recursos. Garantiza que un usuario es quien dice ser permitiendo el control de acceso que permite el acceso solo a las personas autorizadas. (2)

La Norma de IRAM-ISO IEC 17799, en la implementación del sistema de administración de la seguridad de la información, orienta a preservar en un sistema informático los principios de **Confidencialidad, Integridad** y **Disponibilidad**. (1)

Por otro lado la ISO 27001 define la seguridad informática como la preservación de la disponibilidad, integridad y confidencialidad de la información, también se pueden involucrar otras propiedades como autenticidad, responsabilidad, confiabilidad y no repudio. Esta definición dada por la ISO 27001 es referenciada por Alan Calder, el experto en seguridad informática, actual director general de IT (Tecnologías de la Información) Governance, en los libros que ha publicado.

Por tanto los resultados arrojan que seguridad informática contiene cuatro aspectos fundamentales a tener en cuenta:

- ✓ La **Disponibilidad** de los sistemas de información: La información sólo debe ser legible para los autorizados.
- ✓ **Evitar el Repudio (No repudio)**: El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.
- ✓ La **Integridad** de la información: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- ✓ La **Confidencialidad** de la información: Dice que los objetos de un sistema han de ser accedidos únicamente por elementos autorizados a ello, y que esos elementos autorizados no van a convertir esa información en disponible para otras entidades.

1.2. Proceso de Desarrollo de Software. Proceso Unificado de Software (RUP).

El proceso de desarrollo de software es un conjunto de actividades que se relacionan entre sí, determinando quién debe hacer qué en un tiempo determinado y cómo hacerlo, las cuales tienen como propósito la producción eficaz y eficiente de una solución informática. Uno de los aspectos que caracteriza todo producto o solución informática es el nivel de seguridad de los datos que maneja, por tanto se considera de vital importancia lograr un alto nivel de seguridad en cada solución informática construida, lograrlo desde la fase de inicio del proceso de desarrollo de software debe ser considerado como estratégico e importante.

Todo proceso de desarrollo de software debe guiarse por una metodología la cual es la encargada de definir al detalle cada uno de los artefactos, roles, flujo de actividades, junto con prácticas y técnicas recomendadas. Las metodologías pueden dividirse en estructuradas y orientadas a objetos, estas últimas siendo las más conocida en la actualidad debido al desarrollo que ha tenido el paradigma Orientado a Objeto en los lenguajes de programación. Dentro de las metodologías orientadas a objetos se puede hacer una clasificación en ágiles y no ágiles o tradicionales. Entre las principales metodologías no ágiles se encuentra RUP. Las metodologías ágiles se pueden enmarcar en los procesos de desarrollo incrementales entre las mismas destacan:

- ✓ Extreme Programming
- ✓ Scrum
- ✓ Familia de Metodologías Crystal
- ✓ Feature Driven Development
- ✓ Proceso Unificado Rational, una versión ágil

En la realización de proyectos de software de alta complejidad técnica, es necesario basarse en una metodología de desarrollo de software que ayude a organizar y planificar todo el proceso para poder obtener un producto de óptima calidad y clientes satisfechos con el resultado. Debido a que RUP es una metodología de desarrollo de software robusta, altamente adaptable a cualquier proyecto que posee gran cantidad de documentación, muy organizada, planificada y que además es la metodología utilizada por el cliente, se utiliza RUP.

RUP contempla 4 fases: Inicio, Elaboración, Construcción, y Transición. A continuación se explica cada una de estas fases:

1.2.1. Fase de Inicio

El objetivo principal de la fase de inicio es alcanzar un acuerdo entre todos los interesados respecto a los objetivos del ciclo vital del proyecto. La fase de inicio es muy significativa fundamentalmente en los esfuerzos de desarrollo nuevos, pues son más arriesgados para los requisitos y para la actividad comercial y deben abordarse antes de que el proyecto pueda continuar. Para los proyectos que se centran en las mejoras de un sistema existente, la fase de incorporación es más breve, pero sigue centrándose en garantizar que el proyecto vale la pena y es posible de realizar.

Los **principales objetivos** de la fase de inicio son:

- ✓ Establecer el ámbito de software y las condiciones de los límites del proyecto, incluida una visión operativa, criterios de aceptación y lo que debe contener el producto y lo que no.
- ✓ Exhibir y demostrar al menos una arquitectura posible contra alguno de los principales casos de ejemplo.
- ✓ Estimar el coste global y la planificación de todo el proyecto (y estimaciones más detalladas para la fase de elaboración).
- ✓ Estimar los riesgos potenciales (las causas de incertidumbre).
- ✓ Preparar el entorno de soporte para el proyecto.

Las **actividades esenciales** de la fase de inicio son:

- ✓ Formular el ámbito del proyecto.
- ✓ Planificar y preparar un caso de negocio.
- ✓ Sintetizar una arquitectura posible, evaluar las concesiones de diseño y de fabricación, compra, y reutilización para poder estimar los costes, la planificación y los recursos. La intención es demostrar la viabilidad mediante alguna forma de prueba de concepto. Los

trabajos de prototipo durante la fase inicial deben limitarse a crear confianza en una solución posible, la solución se realiza durante la elaboración y la construcción.

- ✓ Preparar el entorno del proyecto, valorar el proyecto y la empresa, seleccionar herramientas, decidir las partes del proceso que deben mejorar.

Los **Roles en la fase de inicio** que están involucrados con la BD son:

- ✓ Especialista en herramientas: Encargado de realizar la selección, instalación, configuración y administración de las herramientas a utilizar.
- ✓ Integrador: Crea y planifica espacios de trabajo para la integración del sistema, donde se relaciona el Gestor de BD.

1.2.2. Fase de Elaboración

El propósito de la fase de elaboración es el establecimiento de una línea base para la arquitectura del sistema; lo que permite proporcionar una base estable para el grueso del diseño y del esfuerzo de implementación en la fase de construcción. La arquitectura evoluciona a partir de la consideración de los requisitos más significativos (los que tienen un gran impacto en la arquitectura del sistema) y una valoración de los riesgos. La estabilidad de la arquitectura se evalúa mediante uno o más prototipos arquitectónicos.

Los **principales objetivos** de la fase de elaboración son:

- ✓ Garantizar que la arquitectura, los requisitos y los planes son lo bastante estables, y que los riesgos están suficientemente mitigados para poder determinar con antelación el coste y la planificación de la finalización del desarrollo.
- ✓ Tratar todos los riesgos arquitectónicamente significativos del proyecto.
- ✓ Establecer una arquitectura de línea base derivada de abordar los casos de uso arquitectónicamente significativos, que suelen poner al descubierto los principales riesgos técnicos del proyecto.
- ✓ Producir un prototipo evolutivo de componentes de calidad de producción, así como posiblemente uno o más prototipos exploratorios desechables para mitigar riesgos específicos como:

- renuncias de diseño/requisitos.
- reutilización de componentes.
- viabilidad del producto o demostraciones para inversores, clientes y usuarios finales.

✓ Demostrar que la arquitectura de línea base brinda soporte a los requisitos del sistema a un coste razonable y en un plazo razonable.

✓ Establecer un entorno de soporte.

Para alcanzar estos objetivos principales, es igualmente importante configurar el entorno de soporte para el proyecto. Esto incluye la personalización del proceso del proyecto, la preparación de plantillas, las directrices y la configuración de herramientas.

Las **actividades esenciales** de la fase de elaboración son:

✓ Definir, validar y establecer la línea base de la arquitectura.

✓ Perfeccionar la visión, se basa en información nueva que se obtuvo durante la fase, establece un conocimiento sólido de los guiones de uso más importantes que dirigen las decisiones de planificación y arquitectónicas.

✓ Crear y establecer la línea base de los planes de iteración detallada de la fase de construcción.

✓ Perfeccionar el proceso de desarrollo y colocar el entorno de desarrollo en su lugar, incluido el proceso, las herramientas y el soporte a la automatización necesaria para dar soporte al equipo de construcción.

✓ Perfeccionar la arquitectura y seleccionar los componentes. Los componentes potenciales se han evaluado y las decisiones sobre el desarrollo del software se conocen lo suficiente como para determinar el coste y la planificación de la fase de construcción. Los componentes de la arquitectura seleccionados se han integrado y evaluado en comparación con los casos de ejemplo principales. Lo aprendido con estas actividades puede tener como resultado un rediseño de la arquitectura, que tenga en cuenta diseños alternativos o reconsidere los requisitos.

Los **Roles en la fase de elaboración** que están involucrados con la BD son:

- ✓ Diseñador de BD/Administrador BD: Realizan la especificación de servicios y definición de políticas de seguridad, además de instalar y configurar la BD Oracle con los requerimientos propuestos por el cliente.

1.2.3. Fase de Construcción

El **objetivo** de la fase de construcción es clarificar los requisitos restantes y completar el desarrollo del sistema basándose en la arquitectura de línea base. La fase de construcción es, de alguna manera, un proceso de fabricación, en el que se pone el énfasis en la gestión de los recursos y el control de las operaciones para optimizar los costes, la planificación y la calidad. En ese sentido, las intenciones de gestión sufren una transición del desarrollo de la propiedad intelectual durante la fase inicial y de elaboración, hasta el desarrollo de productos desplegables durante la construcción y la transición.

Los **principales objetivos** de la fase de construcción son:

- ✓ Minimizar los costes de desarrollo optimizando los recursos y evitando las reconstrucciones y los fragmentos innecesarios.
- ✓ Conseguir la calidad adecuada de forma rápida y práctica.
- ✓ Conseguir versiones útiles (alfa, beta y otros releases de prueba) de forma práctica.
- ✓ Completar el análisis, diseño, desarrollo y prueba de toda la funcionalidad necesaria.
- ✓ Desarrollar de forma iterativa e incremental un producto completo que esté preparado para la transición a su comunidad de usuarios.
- ✓ Decidir si el software, los sitios y los usuarios están listos para la aplicación que debe desplegarse.
- ✓ Alcanzar un cierto grado de paralelismo en el trabajo de los equipos de desarrollo. Una arquitectura sólida es esencial si debe alcanzarse alguna forma significativa de este paralelismo.

Las **actividades esenciales** de la fase de construcción son:

- ✓ Gestión de recurso, control y optimización de procesos.

- ✓ Completo desarrollo de componentes y pruebas contra los criterios de evaluación definidos.
- ✓ Valoración de los releases del producto contra los criterios de aceptación para la visión.

Los **Roles en la fase de construcción** que están involucrados con la BD son:

- ✓ Diseñador de BD: Realiza un ajuste bien riguroso sobre los requisitos y componentes para el diseño y pone a funcionar la BD oficial de la aplicación.
- ✓ Diseñador de BD/Arquitecto de Seguridad: Realizan un análisis exhaustivo de los activos existentes como el Modelo de Datos para implementarlo de la manera más satisfactoria posible y tratando de evitar errores.
- ✓ Administrador de Red: Define las políticas de seguridad de conexión a través de las redes.

1.2.4. Fase de Transición

El **objetivo** de la fase de transición es garantizar que el software esté disponible para los usuarios. La fase de transición puede acarrear varias iteraciones e incluye las pruebas del producto en preparación para el release, así como ajustes menores basados en la información de retorno de los usuarios. En este momento del ciclo vital, la información de retorno de los usuarios debe centrarse especialmente en el ajuste del producto, las cuestiones de configuración, instalación y utilización, todas las cuestiones estructurales principales deben haberse resuelto mucho antes en el ciclo vital del proyecto.

Los **principales objetivos** de la fase de transición son:

- ✓ Realizar pruebas de versión beta para validar el nuevo sistema contra las expectativas del usuario o para validar a un sistema heredado al que sustituye.
- ✓ Convertir las bases de datos en operativas.
- ✓ Capacitar a los usuarios y mantenedores.
- ✓ Despliegue de la fuerza de marketing, distribución y ventas.

- ✓ Ingeniería específica del despliegue como el traslado, el empaquetado y la producción comercial, el despliegue de ventas, la formación de personal de campo.
- ✓ Ajuste de actividades como la solución de defectos, la mejora del rendimiento y la utilización.
- ✓ Valoración de las líneas base de despliegue contra la visión completa y los criterios de aceptación del producto.
- ✓ Alcanzar la capacidad de soporte propio del usuario.
- ✓ Alcanzar la concurrencia de interesados en que las líneas base del despliegue sean completas.
- ✓ Alcanzar la concurrencia de interesados en que las líneas base del despliegue sean coherentes con los criterios de evaluación de la visión.

Las **actividades esenciales** de la fase de transición son las siguientes:

- ✓ Ejecutar los planes de despliegue.
- ✓ Finalizar el material de soporte para el usuario final.
- ✓ Probar el producto entregable en el sitio de desarrollo.
- ✓ Crear un release de producto.
- ✓ Obtener la información de retorno del usuario.
- ✓ Ajustar el producto a partir de la información de retorno.
- ✓ Poner el producto a disposición de los usuarios.

Los **Roles que intervienen en la BD** son:

- ✓ Administrador de BD: Desarrolla los componentes restantes del ámbito en que ya se encuentra el software, incluyendo la tarea de especificar la migración de los datos y la especificación de los servicios que está proporcionando el software o producto. (3)

1.3. Base de Datos.

¿Qué es una Base de Datos?

Base de Datos es un conjunto exhaustivo no redundante de datos estructurados, organizados independientemente de su utilización y su implementación en máquina accesibles en tiempo

real y compatibles con usuarios concurrentes con necesidad de información diferente y no predicable en tiempo. (4)

Una BD es la agrupación de los datos que son manejados por un sistema informático con el objetivo de organizar, evitar redundancias en los mismos, estructurado de una manera única y ubicado en un sólo lugar proporcionando acceso a datos por medio de lenguajes lo más naturales posibles. (5)

1.3.1. Componentes de una Base de Datos

Datos: Los datos son la base de datos propiamente dicha.

Hardware: Se refiere a los dispositivos de almacenamiento donde reside la base de datos, así como a los dispositivos periféricos (unidad de control, canales de comunicación, etc.) necesarios para su uso.

Software: Está constituido por un conjunto de programas que se conoce como Sistema manejador de Bases de datos (DMBS: Data Base Management System.). Este sistema maneja todas las solicitudes formuladas por los usuarios de la base de datos.

Usuarios: Se definen por aquellos que utilizan, gestionan e intervienen en la base de datos tanto en ambiente de desarrollo como en producción. (5)

Se necesita un software de gestión que facilite las operaciones y las interfaces con los usuarios. Este software es el que se conoce como SGBD.

1.4. Sistemas Gestores de Bases de Datos (SGBD).

Son programas que se ocupan de acceder y actualizar los Sistemas de Bases de Datos. Actúan como interface entre el programa de aplicación y la Base de Datos. Por ejemplo, cuando un programa debe actualizar una información en el Base de Datos, no lo hace directamente, sino que le pide al Sistema Gestor de Base de Datos para hacerlo, pues es quien conoce cómo es la Base de Datos por dentro. Un Sistema de Gestión de Base de Datos, es una forma de almacenar la información de tal manera que se eviten la duplicación de datos. (6)

Existen gran cantidad de sistemas gestores en el mercado, ya sean de código abierto, como MySQL hasta su versión 5.1 o PostgreSQL y otros propietarios como Oracle o SQL Server. El principal objetivo para un SGBD es que el usuario pueda acceder a los datos sin tener que saber cómo estos están estructurados y/o almacenados.

1.4.1. Las funciones de los S.G.B.D. son:

- ✓ Crear una base de datos y especificar su estructura usando para ello un lenguaje especializado llamado (lenguaje de definición de datos) DDL.
- ✓ Introducir, eliminar, consultar y modificar datos usando un lenguaje especializado llamado (lenguaje de manipulación de datos) DML.
- ✓ Permitir el almacenamiento de grandes cantidades de datos durante largos períodos de tiempo, manteniéndolos seguros de accidentes o uso no autorizado.
- ✓ Controlar el acceso a los datos de muchos usuarios a la vez, impidiendo que el acceso simultáneo introduzca incoherencia. (7)

1.5. Oracle DataBase.

En sus comienzos, Oracle era principalmente una empresa de bases de datos relacionales, las mismas eran una nueva forma de pensar sobre cómo deben estructurarse y almacenarse los datos; la clave de este nuevo pensamiento consiste en entender las relaciones existentes entre los datos y en estructurar la base de información para que refleje dichas relaciones. (8)

Oracle es un Sistema de Gestión de Bases de Datos Relacionales (SGBDR) que dispone de potentes herramientas para la gestión y seguridad de los datos. Debido a que cada versión o liberación es cada vez más eficiente y brida múltiples soluciones a los clientes además de mayor seguridad, se propone el uso de Oracle 11g liberación 2, su última versión. Algunas de las características que han hecho de Oracle el gestor más usado son las siguientes:

- ✓ **Amplía capacidades exclusivas**.

Oracle 11g amplía las capacidades exclusivas de clustering de base de datos, automatización de centro de datos y gestión de carga de trabajo. Con grids altamente disponibles y escalables

se mejora en el procesamiento de transacciones, almacenamiento de datos (data warehousing) y aplicaciones de gestión de contenido.

- ✓ **Real Application Testing.**

Forma parte de Oracle Database 11g y es la primera base de datos en realizar pruebas y gestionar cambios a su entorno de TI (Tecnologías de la Información) con rapidez, de manera controlada y económica. Se utiliza mucho cuando se deben realizar frecuentes actualizaciones de la base de datos y del sistema operativo, además de cambios en el hardware y en el sistema.

- ✓ **Aumento del retorno de la inversión.**

Dentro de Oracle Database 11g, Oracle Data Guard permite que los clientes utilicen el estado "stand by" para mejorar el desempeño de su entorno de producción y también para brindar protección contra las fallas del sistema y desastres en el sitio. Oracle Data Guard posibilita la lectura y recuperación simultánea de una sola base de datos en "stand by", lo que hace que esté disponible para la creación de informes, recuperación, pruebas y "ejecución" de actualizaciones a bases de datos de producción.

- ✓ **Gestión del ciclo de vida.**

Oracle Database 11g automatiza muchas operaciones manuales de partición de datos y amplía el rango existente, hash y partición de listas para incluir partición de intervalos, además de referencias y columnas virtuales. Brinda distintas opciones de partición, lo que permite la gestión de almacenamiento impulsadas por reglas de negocios.

- ✓ **Registro total de cambios de datos.**

Esta nueva versión también incluye "Oracle Total Recall" que permite a los administradores consultar datos en tablas designadas en fechas anteriores. Esta funcionalidad ofrece una manera fácil y práctica para agregar una dimensión de tiempo al rastreo de cambios, auditorías y cumplimiento de datos.

- ✓ **Máxima disponibilidad de la información.**

Oracle tiene nuevas características como son: Oracle Flashback Transaction que facilita volver atrás en una transacción realizada con errores, así como en cualquier transacción relacionada; Parallel Backupand Restore que ayudan a mejorar el desempeño de backup y de restauración de bases de datos muy grandes; y hotpatching que mejora la disponibilidad del sistema permitiendo aplicar los parches de base de datos sin que sea necesario cerrarlas. Además, un nuevo asesor, Data Recovery Advisor, que ayuda a los administradores a reducir considerablemente el tiempo de baja de recuperación, automatizando la investigación del problema determinando de manera inteligente el plan de recuperación y manejando varias situaciones de fallas.

- ✓ **Oracle Fast Files.**

La capacidad de última generación para almacenar objetos grandes (LOB's, por sus siglas en inglés) tales como imágenes, grandes objetos de texto, o tipos de datos avanzados, incluidos XML, imágenes médicas y objetos tridimensionales dentro de la base de datos. Oracle Fast Files ofrece desempeño de aplicaciones de base de datos totalmente comparables con los sistemas de archivos. Almacena una amplia variedad de información empresarial y recupera rápida y fácilmente.

- ✓ **XML, más rápido.**

Importantes mejoras en el desempeño para XML DB, una función de la base de datos de Oracle que permite a los clientes almacenar y manipular datos XML de forma nativa. Se ha incorporado soporte para XML binario, lo cual hace posible que los clientes puedan elegir opciones de almacenamiento XML para cumplir con los requerimientos específicos de desempeño y de aplicaciones. XML DB también permite la manipulación de datos XML utilizando interfaces estándares del sector con soporte a los estándares XQuery, Java Specification Requests (JSR)-170 y SQL/XML.

- ✓ **Encriptación transparente.**

La nueva versión incluye mejores capacidades de encriptación transparente de datos de Oracle más allá de la columna del nivel de encriptación. Oracle Database 11g brinda encriptación de espacio de tablas (tablespace) que pueden utilizarse para encriptar tablas e índices enteros y otros almacenamientos de datos. Además, también se ofrece encriptación para los LOBs almacenados en la base de datos.

- ✓ **Cubos OLAP incorporados.**

Ofrece innovaciones de data warehousing. Los cubos OLAP han sido mejorados para funcionar como visualizaciones materializadas en la base de datos. Esto permite a los desarrolladores utilizar SQL estándar para consulta de datos e incluso beneficiándose con el alto desempeño ofrecido por un cubo OLAP. Las nuevas funciones de Notificación de Consulta Continua permiten que las aplicaciones sean notificadas inmediatamente cuando se realizan cambios importantes a los datos de la base de datos sin que ésta sufra un sondeo constante.

- ✓ **Resultado de sondeo de conexión y de consulta.**

Oracle Database 11g presenta nuevas funciones, tales como Caches de Resultado de Consultas (Query Results Caches), las cuales mejoran el desempeño y la escalabilidad de la aplicación porque colocan en caché y reutilizan los resultados de las frecuentes consultas a las bases de datos. Database Resident Connection Pooling lo cual mejora la escalabilidad de los sistemas basados en la Web brindando un sondeo de conexión para aplicaciones no multi-threaded.

- ✓ **Mejora en el desarrollo de aplicaciones.**

Brinda a los desarrolladores la posibilidad de elegir herramientas de desarrollo, y un mejor proceso de desarrollo de aplicaciones que aprovecha al máximo las funciones clave de Oracle Database 11g. Estas incluyen nuevas funciones, tales como Caching del lado del cliente, XML binario para un desempeño de aplicaciones más rápido, procesamiento XML y el almacenamiento y recuperación de archivos. Además, Oracle Database 11g incluye un nuevo Compilador justo a tiempo (just-in-time) en Java para ejecutar más rápidamente

procedimientos java de base de datos sin necesidad de un compilador de terceros, integración nativa con Visual Studio 2005 para desarrollar aplicaciones .NET sobre Oracle; herramientas de migración de acceso con Oracle Application Express; y creación de consulta fácil SQL Developer para una codificación veloz de las rutinas SQL y PL/SQL.

- ✓ **Mejora en la autoadministración y automatización.**

Las nuevas capacidades de gestión de Oracle Database 11g incluyen SQL automático y afinación de memoria, un nuevo Asesor de Partición que guía automáticamente a los administradores sobre cómo particionar tablas e índices a fin de mejorar el desempeño y los diagnósticos de desempeño de los clusters de base de datos. Además, incluye un Support Work bench, soporte que brinda una interfaz fácil de usar y que le muestra a los administradores los incidentes relacionados con el estado de la base de datos junto con la información sobre cómo resolver rápidamente tales incidentes. (9)

1.5.1. Estructura de los Datos.

Desde el punto de los creadores de Oracle, una base de datos es una colección de datos tratados como una única unidad. Una BD Oracle contiene tres tipos de ficheros físicos:

- ✓ Archivos de Datos: Contiene los datos actuales de la BD así como el diccionario de datos.
- ✓ Archivos rehacer (Redo Logs): Almacenan datos recuperables en caso de error grave.
- ✓ Archivos de control: Necesarios para mantener la integridad de la base de datos.

Además se utilizan otros archivos de forma auxiliar.

- ✓ Archivos de parámetros: Definen algunas características de la instancia Oracle.
- ✓ Archivos de contraseñas: Sirven para autentificar a los usuarios.
- ✓ Copias de Archivos rehacer: Utilizadas para la recuperación de datos.

Cuenta además con 4 ficheros lógicos:

Bloques: Una base de datos se encuentra almacenada en bloques de datos que es el nivel más fino de unidades de almacenamiento. El tamaño de un bloque de datos siempre

corresponde a un múltiplo del tamaño de bloque manejado por el sistema de operación. El tamaño del bloque de datos es un valor configurable en el DBMS.

Extensiones: Las extensiones son las piezas utilizadas para constituir segmentos. Cada extensión se compone de una serie de bloques de datos. La razón principal de esta estructura es la de minimizar el espacio desperdiciado (vacío) de un tablespace. A medida que se insertan o eliminan filas de una tabla, las extensiones del tablespace asociado a la tabla pueden aumentar o disminuir de tamaño. De esta forma el espacio para el almacenamiento de los datos puede ser administrado dependiendo de cómo la tabla va sufriendo modificaciones en el número de filas.

Segmentos: Un segmento es un conjunto de extensiones que han sido asignados para el almacenamiento de un tipo de datos específico y todos ellos se encuentran ubicados dentro del mismo tablespace. Existen diferentes tipos de segmentos como lo son:

- ✓ Segmentos de datos: Cada segmento de datos almacena los datos correspondientes a una tabla.
- ✓ Segmentos de índice: Cada segmento de índice mantiene los datos para un índice definido dentro de la base de datos.
- ✓ Segmento de Rollback: un segmento de Rollback permite almacenar las acciones de una transacción que deben ser deshechas bajo ciertas circunstancias.
- ✓ Segmentos Temporales: Los segmentos temporales se crean cuando se requiere de un espacio temporal para procesar una instrucción de SQL, y son destruidos una vez que haya culminado el procesamiento de la instrucción.

Espacio de tablas: Formado por uno o más datafiles, cada uno solo puede pertenecer a un determinado tablespace. Al utilizar más de un datafile por tablespace puede distribuirse los datos sobre varios discos y balancear la carga de entradas y salidas (E/S), mejorando así el rendimiento del sistema. (10)

1.5.2. Encriptación de los Datos.

La información confidencial que se almacena en la base de datos o que viaja a través de las redes y el Internet puede ser protegida mediante algoritmos de encriptación. Un algoritmo de

cifrado transforma la información de una manera que no se puede descifrar sin un descifrado de la clave.

1.5.2.1. Algoritmos de Encriptación Soportados.

La Seguridad Avanzada de Oracle proporciona los siguientes algoritmos de encriptación para proteger la privacidad de las transmisiones de datos de red:

- ✓ Encriptación RC4
- ✓ Encriptación DES
- ✓ Encriptación Triple-DES
- ✓ Estándar de Encriptación Avanzada

La selección del algoritmo de encriptación de red es una opción de configuración de usuario, previendo niveles variantes de seguridad y rendimiento para los diferentes tipos de datos transferidos.

Encriptación RC4.

El módulo de encriptación RC4 usa el algoritmo de encriptación RC4 de seguridad. Usando una llave secreta, generada al azar y única a cada sesión, todo el tráfico de la red es totalmente resguardado incluyendo todos los valores de datos, declaraciones SQL y resultados de llamadas de procedimientos almacenados. El cliente, el servidor, o ambos, pueden pedir o requerir el uso del módulo de encriptación para garantizar que sus datos estén protegidos. La implementación optimizada de Oracle proporciona un alto grado de seguridad por un rendimiento mínimo. Para el algoritmo RC4, Oracle proporciona encriptación de llaves con longitudes de 40, 56, 128 y 256 bits.

Encriptación DES

La Seguridad Avanzada de Oracle implementa el algoritmo Estándar de Encriptación de Datos (DES) como una norma, este algoritmo de encriptación es optimizado a 56 bits y también proporciona DES40, una versión de 40 bits, para la compatibilidad de respaldo.

Encriptación Triple-DES

La Seguridad Avanzada de Oracle también soporta la encriptación Triple-DES (3DES) que encripta los datos del mensaje con tres pasadas del algoritmo DES. 3DES proporciona un alto grado de seguridad del mensaje, pero con una carga de rendimiento. La magnitud de carga depende de la velocidad del procesador que realiza la encriptación. 3DES toma típicamente el triple de tiempo de encriptar un bloque del que tomaría usando un algoritmo DES. Los algoritmos 3DES están disponibles en versiones de dos llaves y tres llaves, con longitudes eficaces de la llave de 112 y 168 bits, respectivamente. Ambas versiones están en distintos modos de Cadenas Bloque de Cifrado (CBC).

Estándar de Encriptación Avanzada

El Estándar de Encriptación Avanzada (AES) es un nuevo algoritmo criptográfico desarrollado para reemplazar DES. AES es un bloque de cifrado simétrico que puede procesar bloques de datos de 128 bits, usando llaves de cifrado de 128, 192 y 256 bits que son referidos como AES-128, AES-192 y AES-256 respectivamente. Todas las versiones operan en distintos modos de CBC.

Integridad de los Datos.

Para asegurar la integridad de paquetes de los datos durante la transmisión, la seguridad avanzada de Oracle puede generar un mensaje cristológicamente seguro utilizando un algoritmo hash (MD5 o SHA-1) y lo incluyen con cada mensaje enviado a través de la red. Los algoritmos hash son los que crean una clave única para cada palabra a cifrar.

Los algoritmos de integridad de datos protegen contra los siguientes ataques:

- ✓ Modificación de los datos.
- ✓ Eliminación de paquetes.
- ✓ Ataques de repetición.

(11)

La seguridad avanzada de Oracle permite seleccionar los algoritmos Message Digest 5(MD5) y Secure Hash Algorithm (SHA-1) que protegen la integridad de los datos ante ataques como Modificaciones de datos y Repetitivos ataques. Ambos algoritmos hash crean una suma de comprobación de los cambios si los datos se alteran de cualquier manera. Esta protección es

independiente del proceso de encriptación por lo que puede permitir la integridad de datos con o sin habilitar cifrado. (12)

En Oracle DataBase, el paquete DBMS_SQLHASH puede comprobar la integridad de datos mediante el uso de algoritmos hash. Proporciona un interfaz para generar el valor hash del conjunto de resultados devueltos por una consulta SQL. Los valores hash son similares a las huellas digitales de datos y se utilizan para garantizar la integridad de los datos. DBMS_SQLHASH proporciona soporte para varios algoritmos de hash estándar de la industria criptográfica hash, incluyendo MD4, MD5 y SHA-1. (13)

Encriptación Transparente de datos.

El Cifrado de datos transparente ayuda a proteger los datos almacenados en medios de comunicación en caso de que el soporte de almacenamiento o archivo de datos sea robado, ya que almacena las claves de cifrado en un módulo de seguridad (es decir, una billetera) externos a la base de datos. El beneficio de usar cifrado de datos transparente es que requiere poca codificación, rápido y fácil de implementar. Para cifrar los datos mediante el cifrado de datos transparente, crea los siguientes componentes:

- ✓ Una cartera para guardar la clave de cifrado: La billetera es un espacio de almacenamiento en forma de archivo binario. Este archivo se crea fuera de la base de datos y es accesible sólo para el administrador de seguridad. El Almacenamiento de la clave de cifrado maestra de esta manera impide el uso no autorizado. Para crear la carpeta, puede utilizar la instrucción ALTER SYSTEM, instrucción SQL, que permite especificar la contraseña de la cartera. El cifrado de clave para abrir la billetera tiene una contraseña asociada y el algoritmo de cifrado. Después de crear la cartera, tendrá que abrir la cartera, que se puede hacer en bases de datos de control o en SQL * Plus.
- ✓ Un lugar de la cartera: Usted puede especificar la ubicación de la cartera modificando el archivo SQLNET.ora.
- ✓ Un mecanismo para el cifrado de los datos: Puede utilizar SQL * Plus para designar una o más columnas o tablas a cifrar. Si decide que los datos no tienen por qué ser encriptados, puede descifrar en SQL * Plus. (11)

1.5.3. Protección de los datos del Diccionario de datos de Oracle.

El diccionario de datos de Oracle es un conjunto de tablas de la bases de datos de solo lectura que proporciona información de la base de datos. Un diccionario de datos tiene el siguiente contenido:

- ✓ Las definiciones de todos los objetos de esquema en la base de datos (tablas, vistas, índices, clusters, sinónimos, secuencias, procedimientos, funciones, paquetes, triggers, etc.).
- ✓ Valores por defecto para columnas.
- ✓ Integridad de la información de restricción.
- ✓ Los nombres de usuarios de Oracle de base de datos.
- ✓ Privilegios y las funciones otorgadas a cada usuario.
- ✓ Auditoría de la información, como quién ha tenido acceso o quién ha actualizado varios esquemas de objetos. (11)

1.5.4. Servicios que brinda Oracle.

Oracle Database ofrece múltiples servicios que ayudan en la administración, rendimiento, recuperación y seguridad de la base de datos haciéndola más potente y dinámica, éstos se dividen en Servicios de Administración, Red y Monitoreo.

.

1.5.4.1. Servicio de Administración.

Normalmente, el principal trabajo de un administrador de base de datos Oracle es realizar tareas de optimización de bases de datos tales como la instalación de actualizaciones, el seguimiento del estado de la base de datos y dar solución a los problemas que él encuentra. En una instalación predeterminada de Oracle de base de datos, los administradores de base de datos también tienen la capacidad de crear usuarios y los datos de acceso de los usuarios. Para mayor seguridad, debería restringir estas actividades sólo a aquellos usuarios que necesitan realizarlas. Esto se llama separación de servicio, y libera al administrador de base de datos para centrarse en las tareas ideales para su experiencia, como el ajuste de rendimiento. Al instalar Oracle Database, el proceso de instalación crea un conjunto de cuentas predefinidas. Estas cuentas se encuentran en las siguientes categorías:

Cuentas administrativas predefinidas: Estas son las cuentas que tienen privilegios especiales necesarios para administrar la base de datos, para proteger estas cuentas del acceso no autorizado, el proceso de instalación caduca y bloquea la mayor parte de estas cuentas. El responsable para el desbloqueo y restablecimiento de estas es el administrador de la base de datos.

Cuentas de usuario predefinidas no administrativas: Poseen sólo los mínimos privilegios necesarios para realizar sus trabajos. El proceso de cerraduras y expira se pone en ejecución inmediatamente después de la instalación, protegiéndolas del acceso no autorizado, el responsable de restablecer y desbloquear éstas es el administrador de BD.

Muestra de un esquema cuentas de usuario predefinidas:

Un esquema de cuentas de usuario es donde se muestra todas las cuentas no administrativas, y su tablespace es USER. Para proteger estas cuentas del acceso no autorizado, inmediatamente después de la instalación se realiza la cerradura y expira de estas cuentas. Es el administrador de la base de datos el responsable para el desbloqueo y restablecimiento de estas cuentas. (11)

Las cuentas predefinidas traen consigo contraseñas del mismo modo por lo que es necesario cada vez que se instale la base de datos Oracle desactivar estas cuentas y activarlas con contraseñas privadas y con una correcta política de contraseña, que puede hacerse manualmente o a través de Database Control solución que propone Oracle Corporation. Se puede encontrar información acerca de cuentas de usuario mediante la consulta de la opinión de DBA_USERS. Esta vista contiene una columna para las contraseñas, pero para mayor seguridad, Oracle DataBase cifra los datos de esta columna. El punto de vista DBA_USERS proporciona información útil como el estado de cuenta de usuario, sea o no la cuenta que está bloqueada, y las versiones de contraseña que tiene.

Privilegios y Roles.

Un privilegio es el permiso para acceder a un objeto nombrado de una manera prescrita; por ejemplo, el permiso para consultar una tabla. Los mismos son concedidos a los usuarios a discreción de los administradores. Pueden concederse a determinado usuario para conectarse a la BD (creación de sesión); crear tablas en su propio esquema; seleccionar tablas de otros esquemas o ejecutar procedimientos almacenados de otros esquemas entre otras aplicaciones.

Existen dos categorías distintas de privilegios dentro de una BD:

- ✓ Privilegios del sistema
- ✓ Privilegios de Objeto de esquema

Privilegios del sistema

Los privilegios del sistema les permiten a los usuarios realizar una acción global del sistema o una acción particular en un tipo específico de objeto de esquema. Por ejemplo, los privilegios crear un tablespace o eliminar filas de cualquier tabla en la BD son privilegios del sistema. Muchos privilegios del sistema sólo son disponibles a administradores y a desarrolladores de aplicaciones porque constituyen armas muy poderosas en la BD.

Privilegios de Objeto de esquema

El acceso a los datos normalmente es mayormente controlado en el nivel de acceso a la BD misma, o a tablas específicas. Los privilegios de objeto de esquema les permiten a los usuarios realizar una acción particular en un objeto del esquema específico. Los privilegios de objeto de esquema para tablas permiten la seguridad de la tabla a nivel de operaciones de Lenguaje de manipulación datos (DML) y Lenguaje de definición de datos (DDL).

Como una regla general, los privilegios del objeto pueden ser concedidos sólo por el dueño del objeto. Sin embargo, un dueño también puede especificar que un usuario particular tiene el derecho para conceder un privilegio a otros. El rango completo de privilegios para cualquier acción en cualquier objeto en el esquema se concede típicamente por defecto al administrador. (14)

Roles

ORACLE provee los roles para una administración más fácil y controlada de los privilegios. Los roles son un grupo de privilegios que son asignados a usuarios o a otros roles. Las siguientes propiedades de los roles permiten administrar los privilegios de una manera más fácil:

- ✓ Reducida asignación de privilegios: En lugar de otorgar explícitamente el mismo conjunto de privilegios a muchos usuarios el administrador de la base de datos puede asignar los privilegios a un rol y éste a un grupo de usuarios.
- ✓ Administración dinámica de los privilegios: Cuando los privilegios de un grupo deben cambiar, sólo los privilegios del rol necesitan ser modificados. Los dominios de seguridad de todos los usuarios a los que asignó dicho rol, reflejarán automáticamente los cambios hechos en el rol.
- ✓ Selectiva disponibilidad de los privilegios: Los roles asignados a los usuarios pueden ser selectivamente activados o desactivados. Esto permite control específico de los privilegios de los usuarios en cualquier situación.
- ✓ Consciencia de aplicación: Una aplicación de la base de datos puede ser diseñada para habilitar o inhabilitar roles automáticamente cuando un usuario intenta usar la aplicación. (15)

1.5.4.2. Servicio de Red.

Oracle Net Manager es una herramienta de interfaz de usuario gráfica, utilizada principalmente para configurar Servicios de Red en Oracle tanto para un cliente local o el host servidor. Aunque puede utilizar el Administrador de Oracle Net para configurar Oracle Net Servicies, como los oyentes (listeners), y la configuración general de red, también permite configurar las siguientes funciones de seguridad avanzada de Oracle, que utilizan el protocolo de red de Oracle:

- ✓ Métodos de autenticación fuertes (Kerberos, RADIUS y Secure Sockets Layer)

Kerberos: Proporciona los beneficios de inicio de sesión único y la autenticación centralizada de usuarios de Oracle. Es un sistema de autenticación de terceros de confianza que se basa

en secretos compartidos. Se presume que el tercero es seguro y proporciona inicio de sesión único en esta capacidad, el almacenamiento centralizado de contraseñas, la autenticación a la base de datos y seguridad mejorada de la PC. Lo hace a través de un servidor de autenticación Kerberos.

RADIUS: RADIUS es un protocolo cliente/servidor de seguridad que permite autenticación y acceso a distancia. Oracle Advanced Security utiliza este estándar de la industria en un cliente/servidor de entorno de red. Puede habilitar la red para utilizar cualquier método de autenticación que admite el estándar de RADIUS, incluyendo tarjetas token y tarjetas inteligentes, mediante la instalación y configuración del protocolo RADIUS. Por otra parte, cuando se utiliza RADIUS, puede cambiar el método de autenticación sin modificar el cliente de Oracle o la base de datos del servidor Oracle. Desde la perspectiva del usuario, el proceso de autenticación completo es transparente. Cuando el usuario desea acceder a un servidor de base de datos Oracle, el servidor de base de datos Oracle, en calidad del cliente RADIUS, notifica al servidor RADIUS. El servidor realiza lo siguiente:

- Busca información de seguridad del usuario.
- Busca los pases de autenticación y autorización de información entre el caso autenticación del servidor o los servidores y el servidor de base de datos Oracle.
- Otorga el acceso del usuario al servidor de base de datos Oracle.
- Registra información de la sesión, incluso cuándo, con qué frecuencia y por cuánto tiempo el usuario se conecta al servidor de base de datos Oracle.

Secure Sockets Layer: (SSL) es un protocolo estándar de la industria diseñada originalmente por Netscape Communications Corporation para la seguridad de las conexiones de red. SSL utiliza la criptografía de clave pública RSA, en relación con la criptografía de clave simétrica para proporcionar autenticación, encriptación e integridad de datos. Al utilizar Oracle Advanced Security en la funcionalidad SSL para proteger las comunicaciones entre clientes y servidores, puede usar SSL para cifrar la conexión entre clientes y servidores y autenticar

cualquier cliente o servidor, como Oracle Application Server 10g, a cualquier Oracle servidor de base de datos que está configurado para comunicarse a través de SSL.

SSL soporta cualquiera de los modos de autenticación siguientes: (12)

- Sólo el servidor se autentica ante el cliente.
- El cliente y el servidor se autentiquen entre sí.
- Ni el cliente ni el servidor se autentica ante el otro, por lo tanto utilizan la función de cifrado SSL por sí mismo.

✓ Algoritmos de cifrado de datos por la Red (RC4, DES, Triple-DES y AES)[1]**.**

✓ Métodos de chequeo de integridad de los datos (MD5, SHA-1) [2]**.**

El **Listener** es el software de componente del servidor de bases de datos que gestiona el tráfico de red entre la base de datos Oracle y el cliente. Listener escucha en un puerto de red específico (por defecto 1521). Se compone de dos binarios: (1) tnslsnr que es la escucha de sí mismo y (2) la escucha de la Utilidad de control (lsnrctl) que se utiliza para administrar el servicio de escucha en el servidor o de forma remota.

La contraseña para el oyente se almacena en el archivo listener.ora. Si el parámetro <listener<nombre PASSWORDS_ se fija manualmente, entonces la contraseña se guarda en texto plano. Si se establece mediante lsnrctl y el comando change_password, entonces la contraseña estará codificada. Para configurar el listener de la base de datos Oracle es recomendable utilizar en Oracle Net Services pues realiza todas estas funciones de manera automática.

1.5.4.3. Servicio de Monitoreo.

ORACLE permite realizar un monitoreo selectivo de las acciones de los usuarios para ayudar en la investigación de usos maliciosos de la base de datos. El monitoreo puede realizarse a tres niveles distintos:

[1] ver 1.5.2.1
[2] ver 1.5.2.1

- ✓ Monitoreo de sentencias: Es el monitoreo de sentencias SQL específicas sin atender concretamente a los objetos. Este tipo de monitoreo puede hacerse para todos los usuarios del sistema o se puede enfocar sólo a algunos usuarios seleccionados.
- ✓ Monitoreo de privilegios: Es el monitoreo de los privilegios del sistema sin atender concretamente a los objetos. Este tipo de monitoreo puede hacerse para todos los usuarios del sistema o se puede enfocar sólo a algunos usuarios seleccionados.
- ✓ Monitoreo de objetos: Es el monitoreo de los accesos a esquemas específicos sin considerar el usuario. Monitorea las sentencias permitidas por los privilegios.

Para todos los tipos de monitoreo, ORACLE permite el monitoreo selectivo de sentencias ejecutadas con éxito, sentencias ejecutadas sin éxito o ambas. Los resultados del monitoreo son registrados en una tabla llamada “the audit trail” (la pista de auditoría). (15)

Oracle Corporation anunció el Oracle Enterprise Manager, que permite a los directores de TI asegurarse de que todos los componentes de su infraestructura funcionen a capacidad: bases de datos, servidores de red y de aplicaciones, aplicaciones empresariales, sistemas de operaciones, plataformas de hardware, dispositivos de almacenamiento y la red. Con una consola de manejo de HTML, el Oracle Enterprise Manager ofrece monitoreo y control del desempeño de aplicaciones de principio a fin, desde una perspectiva centrada en el usuario.

Ventajas de Oracle Enterprise Manager:

Permite saber exactamente cuál es el desempeño de las aplicaciones que experimentan sus usuarios en la red. Hace posible diagnosticar la causa de los retrasos en el desempeño y la implementación de soluciones. Monitorea el rendimiento y comportamiento de una infraestructura. Es capaz de proveer reportes a los directores de TI, lo que permite arreglar cualquier problema en la infraestructura de una red antes de que ésta llegue a suceder. Resuelve la complejidad del manejo de la heterogénea y multifacética atmósfera de las TIs, con una arquitectura basada en un repositorio. Permite manejar, monitorear y configurar con mayor eficiencia la infraestructura completa de una empresa, establecer controles que automáticamente implementen sistemas para mantener un nivel de apoyo predeterminado,

aumentar la calidad del servicio y sistema de inteligencia y reducir los costos generales de administración. Funciona con otras herramientas administrativas tales como HP Open View y otras aplicaciones diferentes, desplegadas en la infraestructura de Oracle.

El Oracle Enterprise Manager tiene una consola única para manejar y monitorear todos los aspectos de la nueva infraestructura Oracle: la base de datos, el Servidor de Aplicaciones Oracle y sus componentes, incluyendo su servidor J2EE, infraestructura de servicios, portal, cache e integración en la Red, así como sistemas operativos, plataformas para hardware y la red. En contraste con los marcos genéricos que requieren un extenso trabajo de adaptación, el Oracle Enterprise Manager ofrece poderosas y originales capacidades para simplificar la tarea de administrar los productos de la infraestructura de Oracle. (16)

1.6. Soluciones de Seguridad de Oracle Database.

Desde el principio, Oracle desarrolla la tecnología más avanzada de la industria para proteger los datos en la base de datos. Ofrece una completa cartera de soluciones de seguridad para garantizar la privacidad de los datos, proteger contra las amenazas internas y permitir el cumplimiento regulatorio. Con poderosos usuarios con privilegios de Oracle y factor múltiple de control de acceso, clasificación de datos, cifrado de datos transparente, auditoría, mantenimiento y los datos de enmascaramiento. Mediante estas opciones los clientes pueden implementar soluciones de seguridad de datos que no requiere ningún cambio a las aplicaciones existentes, ahorrando tiempo y dinero. Éstas son las soluciones que hasta ahora acompañan a Oracle DataBase:

Oracle Virtual Private Database (VPD)

VPD aplica la seguridad a un nivel adecuado de granularidad, directamente en las tablas de las bases de datos, vistas o sinónimos. No hay manera de eludir a la seguridad debido a que existe la posibilidad de fijar las políticas de seguridad directamente a estos objetos de la base de datos y además que las políticas se aplican automáticamente cuando un usuario accede a los datos. Cuando un usuario acceda directa o indirectamente a una tabla, vista o sinónimo que está protegido con una política de VPD, Oracle Database modifica dinámicamente la

instrucción SQL del usuario. Esta modificación genera una condición WHERE (llamado un predicado) devuelta por una función, determinada por la política de seguridad que le fue aplicada. Oracle Database modifica la declaración de forma dinámica, transparente para el usuario. Puedes utilizar políticas de VPD para SELECT, INSERT, UPDATE y DELET. (13)

Oracle Label Security (OLS)

Oracle Label Security permite opciones de aplicación de políticas de seguridad para ser manejable en entornos industriales específicos. Se utiliza para garantizar seguridad en las tablas de la base de datos a nivel de fila y asignar a éstas los distintos niveles de seguridad basadas en las necesidades de la aplicación. Por ejemplo, las filas que contienen datos de alta sensibilidad se les pueden asignar una etiqueta de derecho HIGHLY SENSITIVE; filas que son menos sensibles pueden ser etiquetadas como SENSITIVE, y así sucesivamente. Las filas que todos los usuarios pueden tener acceso puede ser etiquetadas con PUBLICA. Se puede crear tantas etiquetas como se necesite, logrando cubrir las necesidades de agrupar los datos según su importancia. Oracle Policy Manager es la herramienta GUI(Graphical User Interface) de administración para Oracle Label Security. Con base en el marco de Oracle Enterprise Manager, Oracle Policy Manager se puede utilizar para definir las etiquetas de sensibilidad, autorizar a determinados usuarios y proteger las tablas.

Oracle Database Vault.

Oracle Database Vault le permite restringir el acceso administrativo a una base de datos Oracle. Esto le ayuda a abordar los problemas más difíciles de seguridad actualmente: la protección contra las amenazas internas, cumplir con los requisitos de cumplimiento normativo y la aplicación de la separación del servicio. Regula fuertes controles internos sobre el acceso, la divulgación o modificación de información sensible que podría dar lugar a fraudes, robo de identidad y las irregularidades financieras. Además ofrece las siguientes maneras para poder restringir el acceso de administrador a una base de datos Oracle:

- ✓ Grupo de esquemas de bases de datos, objetos y roles que se desea proteger: Esta agrupación se llama un reino, y todos los componentes del reino están protegidos.

Después de crear un reino, debe designar a un usuario para administrar el acceso al reino.

- ✓ Crear expresiones PL / SQL para personalizar las restricciones a la base de datos: Se crea una expresión en una regla, múltiples reglas dentro de una categoría y asociar un conjunto de reglas con un reino, para personalizar aún más el tipo de protección que se desea para el reino.
- ✓ Designar a los usuarios, normas específicas de PL / SQL para que sean accesibles o no accesibles por ellos: Estos se llaman normas de comandos. Además se crea una regla para proteger los comandos SELECT, ALTER SYSTEM, el lenguaje de definición de datos (DDL), y el lenguaje de manipulación de datos (DML) que afectan a uno o más objetos de base de datos por lo que permite asociar un conjunto de reglas para personalizar aún más el estado de los comandos.
- ✓ Definir los atributos para registrar datos como los usuarios de sesión o de las direcciones IP que Oracle Database Vault puede reconocer y asegurar: Estos atributos se denominan factores y se pueden usar para actividades como la de autorizar cuentas para conectarse a la base de datos o la creación de la lógica de filtrado para restringir la visibilidad y capacidad de la gestión de datos.

Oracle Secure Backup.

Oracle Secure Backup ofrece una solución de recuperación integrada y fácil de usar que codifica los datos en las cintas para protegerlos ante la mala utilización de datos sensibles en caso de que las cintas de backup se pierdan o sean robadas. Brinda protección de datos para entornos heterogéneos UNIX, Linux y Windows. Ofrece capacidades locales y remotas para cumplir con los requisitos de restauración y backup, básicos o más avanzados para todo el entorno de Oracle. Además utiliza políticas de recuperación automáticas basadas en la gestión para consolidar alguna falla o robo de datos y cifra los datos antes de salir de la base de datos permitiendo elegir los destinos físicos y virtuales de las copias de seguridad. Aprovecha la tecnología a nivel de conexión segura (SSL) optimizando la confiabilidad. A partir de Oracle Database 10g versión 2, las recuperaciones de la base de datos pueden ser

encriptadas por la integración con Oracle Recovery Manager (RMAN) y escritas en cintas por Oracle Secure Backup en formato encriptado. (17)

Oracle Data Masking.

Oracle Data Masking, permite garantizar la información confidencial, como números de tarjeta de crédito o de seguridad social que pueden reemplazarse por valores reales, permitiendo que los datos de producción puedan usarse de manera segura en el desarrollo y las pruebas. Oracle Data Masking utiliza una biblioteca de plantillas y reglas de formato, que consiste en transformar los datos a fin de mantener la integridad referencial para las aplicaciones. Aplica políticas de enmascaramientos de datos que define el administrador de la base de datos y se aplican de manera automática a los datos especificados, ahorrando tiempo y aumentando seguridad en los datos sensibles.

Oracle Total Recall.

Aumenta la seguridad y reduce el costo de almacenar los datos históricos. Permite que las empresas mantengan disponibles los datos históricos durante largos períodos de tiempo. Oracle Total Recall forma parte de la cartera completa de soluciones de seguridad de la base de datos de Oracle y con Oracle Database 11*g* Enterprise Edition, ayuda a las organizaciones a almacenar la información en una base de datos segura a prueba de sabotajes que a la vez permanece accesible para las aplicaciones existentes. Esta herramienta no requiere cambios en las aplicaciones ni interfaces especiales, y proporciona el tamaño de almacenamiento óptimo. Además de administrar los datos históricos proporciona una solución segura, eficiente, fácil de usar y transparente a la aplicación para el almacenamiento y la auditoría de la información histórica a largo plazo. Permite almacenar los valores históricos de los registros de una tabla. La manera en que los almacena hace posible que se pueda consultar el valor de determinado registro en determinada fecha sin necesidad de acceder a un modelo de datos paralelo o a un data warehouse. También se puede acceder a las tablas donde se almacena esta información para poder hacer informes y consultas personalizadas. (18)

Oracle Advanced Security

Oracle Advanced Security, permite de forma transparente cifrar todos los datos específicos de la aplicación, espacios de tablas o columnas sensibles, como tarjetas de crédito, números de seguro social o información de identificación personal (PII). Cifra los datos en reposo de la base de datos, así como cada vez que sale de la base de datos por la red o a través de copias de seguridad, lo que proporciona una solución más rentable para la protección de datos de manera integral. Todo el tráfico de cifrado de los datos, tanto las copias de seguridad en discos como las exportaciones, lo realiza en completa transparencia sin realizar ningún cambio en la aplicación. (19)

Oracle Audit Vault.

Oracle Audit Vault, reduce la complejidad del cumplimiento y el riesgo de amenazas internas al automatizar la recolección y consolidación de los datos de auditoría. Proporciona un almacén de auditoría seguro y altamente escalable, lo que permite simplificar la presentación de informes, análisis y detección de amenazas en los datos de auditoría. Además, la configuración de la auditoría de la base de datos es administrada centralmente y puede vigilarse desde Audit Vault, lo que proporciona la reducción de costos de las tecnologías de seguridad. Con esta herramienta se puede hacer cumplir mucho mejor las políticas de privacidad y la protección contra las amenazas internas. Permite:

- ✓ Simplificar el cumplimiento de presentación de informes, analiza fácilmente los datos de auditoría y toma medidas en forma oportuna con los informes generados.
- ✓ Detecta las amenazas con rapidez y automáticamente detecta actividades no autorizadas que violen la seguridad y las políticas establecidas, frustra los autores de cubrir sus huellas. Reduce los costos con las políticas de auditoría y administrar de forma centralizada la configuración de auditoría en todas las bases de datos desde una única consola.
- ✓ Recopila y consolida de forma transparente los datos de auditoría.
- ✓ Proporciona una garantía líder en la tecnología de almacenamiento de datos y es un depósito de auditoría seguro y escalable. (20)

Oracle Configuration Management.

Oracle Configuración es un módulo de administración del Oracle Enterprise Manager, que integra además la cartera global de Oracle para soluciones de seguridad de la base de datos. Oracle Configuration Management combina la exploración de análisis de vulnerabilidades, la evaluación comparativa de cumplimiento y la dirección central de la configuración de la base de datos para detectar y prevenir cambios no autorizados de configuración. Además realiza críticas de gestión de configuración de los parches de actualización, como también realiza la función de asesoramiento de alerta a los clientes de los parches esenciales formulados por Oracle e inmediatamente identifica a los sistemas a través de la empresa para que se pueda exigir la revisión crítica. Opcionalmente invoca el asistente de parches para implementar de forma automática el parche, asegurando que las bases de datos de la aplicación siempre están actualizadas y protegidas.

Beneficios:

- ✓ Posee predefinidos y personalizables grupos políticos integrados en la colección de más de 250 mejores prácticas basadas en estándares de la industria de la seguridad y la gestión de configuración, que puede ser personalizado por el administrador del entorno de TI especificadas por los interesados.
- ✓ Cumplimiento de resultados de la evaluación continua, por lo que ofrece la posibilidad del desglose de los detalles y seguimiento de los progresos hacia el cumplimiento teniendo en cuenta el tiempo de duración.

1.7. Aplicaciones Informáticas.

En los inicios de la computación, sólo existían aplicaciones del tipo consola, posteriormente aparecieron las aplicaciones de escritorio basadas en GUI, y como toda evolución, en los años 90 con el nacimiento de Internet fueron surgiendo lo que hoy conocemos como aplicaciones web, que en ese entonces se limitaban a ser simples páginas de texto estático, pero que con el tiempo han ido tomando fuerza hasta llegar a lo que conocemos hoy en día…y lo que falta. (21)

Aplicación informática: Un programa de ordenador que se compra ya realizado y listo para usar. Las hay de muy diversos tipos, según para qué propósito se hayan diseñado: procesadores de texto, bases de datos, programas de contabilidad, de facturación, etc. (22)

1.7.1. Tipos de Aplicaciones Informáticas

Las aplicaciones informáticas se dividen en aplicaciones de escritorio y aplicaciones web. Algunos ejemplos de aplicaciones de escritorio son: Windows Live Messenger, iTunes, Adobe Photoshop, Microsoft Word, Excel, Limeware, Winamp, etc. Este tipo de aplicaciones tienen en común el hecho de que son ejecutadas directamente por el sistema operativo, ya sea Microsoft Windows, Mac OS X, Linux o Solaris, y su rendimiento depende de diversas configuraciones de hardware como memoria RAM, disco duro, memoria de video, etc. (21)

Por otro lado, como ejemplos de aplicaciones web, se tienen las conocidas redes sociales como Facebook y MySpace, tiendas virtuales como E-Bay y Amazon, la enciclopedia en línea Wikipedia, el buscador Google, etc. Dado estos ejemplos, cabe mencionar que la principal característica de las aplicaciones web es que son ejecutadas sobre aplicaciones de escritorio que son conocidas como navegadores web, de los cuales los más conocidos son Internet Explorer, Mozilla Firefox y Safari.

Una de las principales ventajas que presentan las aplicaciones web ante las aplicaciones de escritorio o consola es el hecho de que no dependen de ningún sistema operativo ni configuración de hardware específica; para su ejecución simplemente basta con teclear su dirección URL en cualquier navegador web. De igual manera sus actualizaciones se hacen manera muy sencilla, sin necesidad de hacer descargas, instalaciones o comprar físicamente el producto. (21)

1.7.2. Seguridad en las Aplicaciones Informáticas.

No solamente se logra una seguridad eficiente asegurando la base de datos, hoy las aplicaciones informáticas utilizan frameworks para desde la capa de la aplicación garantizar la seguridad de los datos que van hacer introducidos. Esto permite la confidencialidad e

integridad de los datos antes de ser almacenados en la base de datos. Cada uno de los lenguajes de programación actuales tiene un framewok que garantiza la seguridad a nivel de aplicación como por ejemplo:

Frameworks en PHP para asegurar las aplicaciones informáticas:

En la actualidad existen muchos frameworks implementados en el lenguaje PHP, como principales y más usados en el desarrollo de software se destacan Symfony, Zend Framework, CakePHPy CodeIgniter, entre otros..

Frameworks en Java para asegurar las aplicaciones informáticas:

Existen varios frameworks implementados en el lenguaje java entre los más usados en el desarrollo de software se destacan Acegi Security, JGuard y Jasypt, entre otros.

Estos presentan herramientas que le brindan seguridad al sistema que se está desarrollando pero no implementan la seguridad de forma centralizada en entornos de varias aplicaciones.

Conclusiones

En este capítulo se realiza una fundamentación teórica acerca de la seguridad en las bases de datos Oracle, determinando que seguridad es la unión de los conceptos integridad, confidencialidad, disponibilidad y no repudio de los datos o información a asegurar. Se realiza un estudio de la estructura y almacenamiento de los datos enfocando la investigación en Oracle DataBase. Se analiza las soluciones que tiene asociadas para asegurar la base de datos, así como la encriptación de los mismos y los servicios que brinda esta tecnología. Conservando un estado del arte de las bases de datos realizadas en Oracle, lo que permite una preparación suficiente para poder proponer una solución al problema planteado.

CAPITULO 2: PROPUESTA DE SOLUCIÓN

Introducción

En este capítulo se muestra cómo se puede garantizar seguridad en las Bases de Datos Oracle desde las fases del proceso de desarrollo de software que propone la metodología RUP: Inicio, Elaboración, Construcción y Transición, para asegurar todo lo posible desde las etapas tempranas del proyecto posibilitando que el sistema ya en su despliegue e instalación se encuentre lo más robusto y fiable posible.

Todo proyecto independientemente de cuál sea su aporte debe de realizase de forma correcta y entendible, además de tener como propósito la producción eficaz y eficiente de un producto software que reúna los requisitos del cliente y para lograr ello no se permite dejar a un lado la seguridad del mismo porque es quien brinda el grado de fortaleza del producto ante las amenazas que intervienen durante todo un proceso. Logrando garantizar la seguridad desde sus inicios en el ciclo de vida del proyecto, es una vía muy importante a seguir que erradica más dificultades una vez que esté en uso la base de datos.

En el desarrollo de la guía se determina a partir de una serie de pasos cómo asegurar la base de datos Oracle en cada una de las etapas que propone RUP durante proceso de desarrollo del software.

2.1. Estructura de la guía.

La guía para garantizar seguridad en las bases de datos Oracle que se propone a continuación debe ser utilizada desde el proceso de desarrollo de software. Consta de cuatro epígrafes, los cuales responden a las etapas que define la metodología RUP durante el proceso de desarrollo de software. Cada una de estas etapas cuenta con actividades, éstas con buenas prácticas que las definen y el rol que las realiza (Ver figura 1)**.**

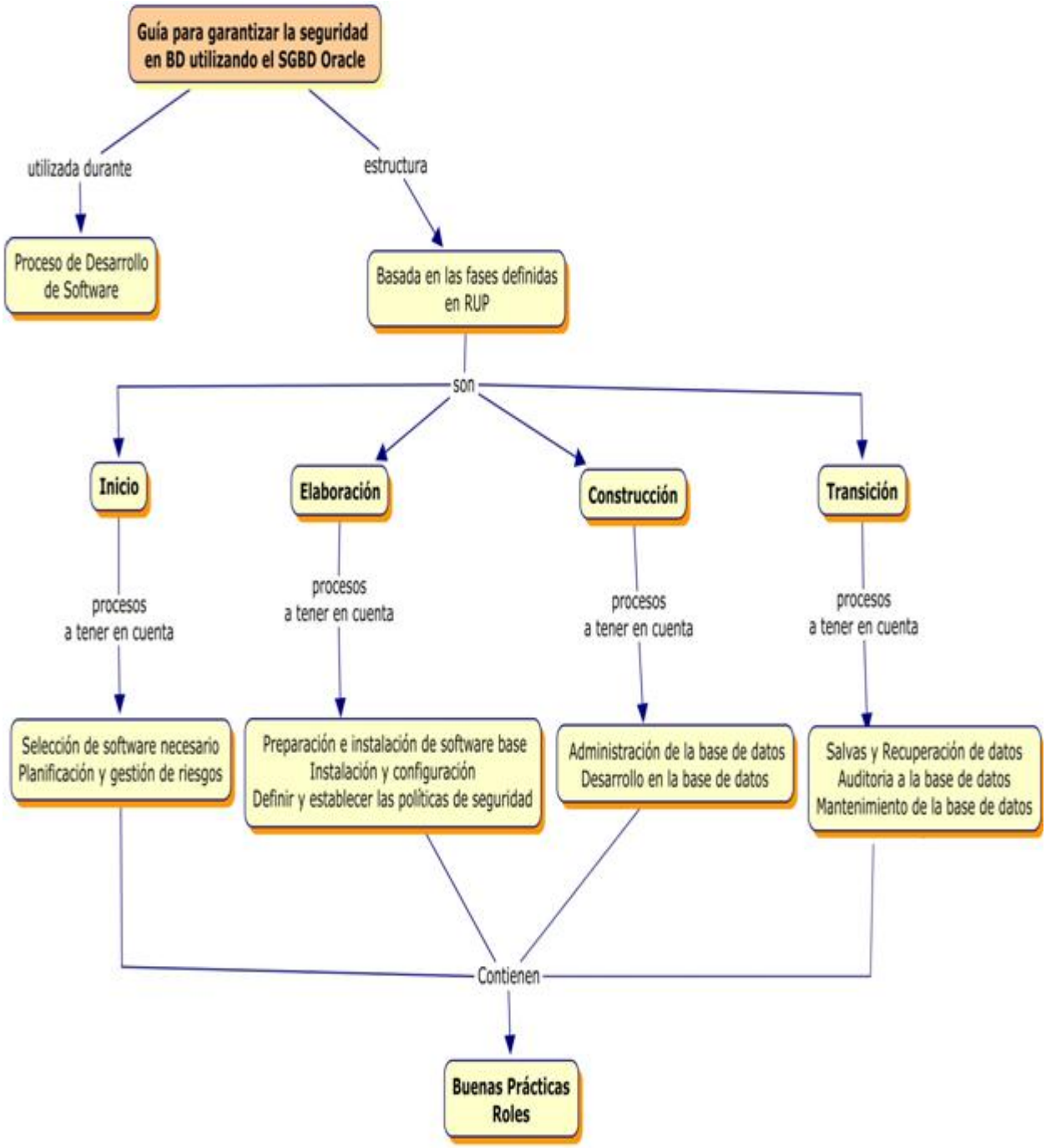

Fig1: Mapa Conceptual de la guía.

2.2. Fase de Inicio

En la fase de inicio se realiza la planificación de las tareas principales para el desarrollo de la base de datos. Por tanto se lleva a cabo la **planificación y gestión de riesgos** en la base de datos y **selección del software base** teniendo gran importancia creando cimientos fuertes para futuras fases. A continuación se muestra paso a paso lo que se propone hacer para cada una de estas actividades.

2.2.1. Planificación y gestión de riesgos

- ✓ Elaborar un cronograma de instalación y configuración de la base de datos. Rol: Diseñador BD.
- ✓ Prever una capacitación de los roles involucrados con la base de datos, en caso de que sea necesario. Rol: Jefe Proyecto
- ✓ Realizar un chequeo de los requerimientos de hardware necesarios para la instalación de la base de datos, tanto en el ambiente de desarrollo como en el ambiente real. Rol: Administrador BD.
- ✓ Establecer las políticas de seguridad que establece Oracle. Rol: Diseñador BD, Administrador.
- ✓ Definir los locales físicos donde se encontrará la base de datos, en ambiente de desarrollo y producción. Tener en cuenta el control de acceso a los servidores física e remotamente. Rol: Jefe de Proyecto, Diseñador BD.

2.2.2. Selección de software necesario.

- ✓ Identificar la versión de Oracle a instalar, seleccionar la última liberación de la versión escogida. Rol: especialista en herramientas de software.
- ✓ Revisar los requerimientos de software: Sistemas operativos que soporta la versión escogida y conocer arquitectura del sistema informático a desarrollar. Rol: Administrador del Sistema Operativo.
- ✓ Adquirir un usuario en My Oracle Support para realizar el mantenimiento de la base de datos, durante el proceso de desarrollo. Rol: Administrador de la BD.

- ✓ Seleccionar de las soluciones complementarias que brinda Oracle para garantizar la seguridad en la base de datos. Rol: Administrador de la BD
- ✓ Identificar los parches necesarios de la versión escogida. Remitirse a My Oracle Support para la instalación de los mismos. Rol: Administrador de la BD.
- ✓ Instalar solamente los módulos necesarios de la base de datos. Rol: Administrador de la BD.

2.3. Fase de Elaboración

En esta fase la base de datos tiene tres actividades fundamentales: **preparación e instalación del software base** fundamental para posteriormente **instalar y configurarla base de datos Oracle** y en último lugar **la definición y establecimiento de las políticas de seguridad para el acceso a la BD**, ofreciendo una base estable para el grueso del diseño y del esfuerzo de implementación en la fase de construcción.

2.3.1. Preparación e instalación del software base.

- ✓ Instalar y configurar el sistema operativo utilizando la guía de instalación de Oracle Database de la versión escogida en la fase de inicio. Rol: Administrador BD.
- ✓ Buscar historial de usuarios y contraseñas del sistema operativo en caso de estar ya instalado. Rol: Administrador BD.
- ✓ Revisar la seguridad en las conexiones de red en el sistema operativo. Revisar las interfaces de red del sistema operativo y los archivos de red. Rol: Administrador BD.
- ✓ Auditar las variables de entorno del sistema operativo. ORACLE_HOME, ORACLE_SID, ORACLE_TMP. Rol: Administrador BD.
- ✓ Revisar las tareas del cron para los sistemas operativos Linux. Rol: Administrador BD.

2.3.2. Instalación y configuración.

- ✓ Chequear los permisos de los controlfile. Rol: Administrador BD.
- ✓ Chequear que los usuarios del sistema no tengan permisos para realizar tareas de ALTER SESSION y ALTER SYSTEM. Rol: Administrador BD.

- ✓ Cambiar la contraseña de la base de datos luego de realizar una importación de la misma. Rol: Administrador BD.
- ✓ Colocar las contraseñas de SYS y SYSTEM diferentes cada una. Rol: Administrador BD.
- ✓ Chequear que ningún software diferente a Oracle tenga permisos de lectura sobre los archivelog. Rol: Administrador BD.
- ✓ Salvar los archivelog en un disco duro aparte y borrarlos periódicamente cada 6 meses.
- ✓ Realizar lista de usuarios por roles y permisos. Rol: Administrador BD.
- ✓ Chequear los permisos en los archivos de trazas de los procesos de background (trace files). Rol: Administrador BD.

2.3.3. Definir y establecer las políticas de seguridad.

- ✓ Establecer políticas de usuarios para que los mismos no puedan compartir sus identificadores. Rol: Administrador BD.
- ✓ Realizar auditorías quincenales sobre usuarios que utilicen como contraseña el nombre de usuario. Cambiar la misma. Rol: Administrador BD.
- ✓ Realizar auditorías quincenales sobre usuarios con contraseñas débiles. Cambiar las mismas. Rol: Administrador BD
- ✓ Auditar las tablas externas usadas en la base de datos una vez al mes. Rol: Administrador BD.

2.4. Fase de Construcción

La fase de construcción es, de alguna manera, un proceso de fabricación, en el que se pone el énfasis en la gestión de los recursos y el control de las operaciones para optimizar los costes, la planificación y la calidad. Las bases de datos no quedan exentas de este proceso y sus actividades en esta fase se definen en: **administración de la base de datos, desarrollo de la base de datos** y **administración de la red** la conexión segura**.**

2.4.1. Administración de la base de datos

- ✓ Bloquear las cuentas de usuario inactivas y remover después de un tiempo de retardo definido, se sugiere 3 meses. Rol: Administrador BD.
- ✓ Monitorear las cuentas para evitar sobre carga de memoria en las mismas utilizando Oracle Configuration Manager. Rol: Administrador BD.
- ✓ Usar convención de nombre ofuscados para cuentas de usuarios. Rol: Administrador BD.
- ✓ Revisar la lista de usuarios del negocio para comprobar los mismos en la base de datos. Rol: Administrador BD.
- ✓ Chequear los roles por jerarquía en profundidad trimestralmente. Rol: Administrador BD.
- ✓ Chequear que ningún usuario externo tenga permisos de los roles SYSDBA o SYSOPER. Rol: Administrador BD
- ✓ Adicionar contraseñas para roles administrativos. Rol: Administrador BD.
- ✓ Cambiar ciclo de vida de las contraseñas en profile a 60 días. Rol: Administrador BD.
- ✓ Cambiar grace time en las contraseñas a 3 meses. Rol: Administrador BD.
- ✓ Cambiar intentos fallidos de autenticación a 5 veces. Rol: Administrador BD.
- ✓ Cambiar parámetro _trace_files_public a falso. Rol: Administrador BD.
- ✓ Revisar parámetros ocultos de la instalación y removerlos. Rol: Administrador BD.
- ✓ Borrar los objetos que pertenecen a los tablespaces de la aplicación y que no son propietarios del esquema de la misma. Rol: Administrador BD.

2.4.2. Desarrollo en la base de datos

- ✓ Auditar todo el código PL/SQL para evitar ataques de inyección SQL. Rol: Desarrollador BD.
- ✓ Revisar cada procedimiento almacenado agregado automáticamente por aplicaciones. Rol: Desarrollador BD.
- ✓ Auditar permisos en los ficheros de las aplicaciones. Rol: Desarrollador BD.

- ✓ Restringir sentencias ad-hoc una vez que la base de datos está en producción. Rol: Administrador BD.
- ✓ Revisar los permisos de los usuarios desarrolladores realizando pruebas de acceso y ejecución. Rol: Administrador BD.
- ✓ No colocar la base de datos de desarrollo y de producción en el mismo servidor. Rol: Administrador BD.
- ✓ No dejar usuarios de desarrollo en la base de datos de producción. Rol: Administrador BD.
- ✓ Las salvas automáticas no deben contener las contraseñas de los usuarios desarrolladores. Rol: Administrador BD.
- ✓ No usar un usuario para autenticar a todos los roles de la base de datos. Rol: Administrador BD.
- ✓ No colocarle a los usuarios de desarrollo permisos de ejecución de tareas administrativas de la base de datos. Rol: Administrador BD.
- ✓ Asegurarse de que el esquema de los usuarios de desarrollo no tenga como propietario a dba. Rol: Administrador BD.
- ✓ Bloquear los esquemas administrativos a los usuarios desarrolladores. Rol: Administrador BD.
- ✓ Auditar los sinónimos de Oracle que sean públicos. Rol: Administrador BD.
- ✓ No permitir que las aplicaciones modifiquen los esquemas de la base de datos. Rol: Administrador BD.
- ✓ No usar usuarios externos para ejecutar procesos batch. Rol: Administrador BD.
- ✓ Auditar el uso de las colas avanzadas de Oracle. Rol: Desarrollador BD.
- ✓ Configurar el SQL*Plus y el iSQL*Plus a través de los esquemas de usuarios. Rol: Desarrollador BD.
- ✓ Deshabilitar el iSQL*Plus una vez que la base de datos está en producción. Rol: Desarrollador BD.
- ✓ Encriptar los datos sensibles utilizando la encriptación transparente de datos que ofrece Oracle Advance Security y Oracle Virtual Private DataBase.

2.4.3. Administración de Red.

- ✓ Prevenir los comandos establecido en el listener. Rol: Administrador de Red.
- ✓ Auditoría al archivo listener.ora. Rol: Administrador de Red.
- ✓ Habilitar tomas para compartir (shared sockets). Rol: Administrador de Red.
- ✓ No utilizar los puertos estándares de escuchas como 1521 y 1526, dejarlos solo para el listener. Rol: Administrador de Red.
- ✓ No utilice nombres de servicios, como el conocido SID y ORCL. Rol: Administrador de Red.
- ✓ En ambientes pequeños no utilizar nombres de host en listener.ora. Rol: Administrador de Red.
- ✓ Use un firewall personal en la computadora de administrador de base de datos. Rol: Administrador de Red.
- ✓ Asegure el archivo listener.ora en el nivel O / S. Rol: Administrador de Red.
- ✓ Asegurar que el registro de listener está habilitado. Rol: Administrador de Red.
- ✓ Restringir las fuentes de conexión a la base de datos. Rol: Administrador de Red.
- ✓ Administrar las conexiones a la BD a través de Oracle Net Manager. Rol: Administrador de Red.
- ✓ Establecer una contraseña para el listener. Rol: Administrador de Red.
- ✓ Usar un firewall para proteger el servidor de Oracle. Rol: Administrador de Red.
- ✓ Auditoría los archivos de permisos de los clientes y los lo que contienen los ficheros de configuración de los mismos. Rol: Administrador de Red.
- ✓ Auditoría para contraseñas difíciles de texto sin cifrar en vínculos a la base de datos. Rol: Administrador de Red.
- ✓ Crear una política para gestionar los links a la base de datos utilizando Oracle Net Services. Rol: Administrador de BD.
- ✓ Auditoría cuáles son los links que existen de entrada y salida a la base de datos. Rol: Administrador de BD.
- ✓ Confirmar los archivos de permisos en el directorio de administración de red. Rol: Administrador de Red.

- ✓ Añada sólo los archivos de configuración mínima para todos los clientes. Rol: Administrador de BD.
- ✓ Mantener al día las vulnerabilidades de listener de Oracle y los parches. Rol: Administrador de BD.
- ✓ Limitar toda la administración remota de listener, aunque por encima de la versión10.1, viene por defecto. Rol: Administrador de BD.
- ✓ Establecer servidor dedicado en el archivo tnsnames.ora. Rol: Administrador de BD.
- ✓ Deshabilitar los puertos de Oracle que no son necesarios.
- ✓ Usar Oracle Advanced Security para cifrar la transmisión de datos. Rol: Desarrollador de BD.
- ✓ Habilitar SSL para proteger la transmisión de cliente. Rol: Administrador de BD.

2.5. Fase de Transición

La fase de transición puede acarrear varias iteraciones e incluye las pruebas del producto en preparación para la versión entregable del mismo, así como ajustes menores basados en la información de retorno de los usuarios. En este momento del ciclo vital, la información de retorno de los usuarios debe centrarse especialmente en el ajuste del producto. Para garantizar la seguridad de la base de datos en esta fase es preciso definir tres actividades fundamentales**: salvas y recuperación de datos**, **auditorías a la base de datos** y **mantenimiento de la base de datos**.

2.5.1. Salvas y Recuperación de datos

- ✓ Revisar y documentar los procedimientos de salvas y restauraciones de la base de datos utilizando Oracle Backup Secure. Rol: Administrador BD.
- ✓ Revisar, probar y documentar los procedimientos de las recuperaciones de la base de datos. Rol: Administrador de BD.
- ✓ Colocar un espejo para los archivos redo logs en linea. Rol: Administrador BD.
- ✓ Asegurar siempre que la base de datos se encuentre en modo archivelog. Rol: Administrador BD.

- ✓ Asegurarse que el directorio de los archivos archivelogs exista y tenga protección se recomienda colocar en dispositivo externo. Rol: Administrador BD.
- ✓ Monitorear y definir la política de borrado de los archivos archivelogs utilizando Oracle Total Recall. Rol: Administrador BD.
- ✓ Separar en directorios diferentes los datos de la base de datos del software de Oracle. Rol: Administrador BD.
- ✓ Mantener los datos de la base de datos en un disco o partición aparte. Rol: Administrador BD.
- ✓ Usar OFA. Rol: Administrador BD.
- ✓ Usar siempre RAID 1 para todos los datos de la base de datos de Oracle. Rol: Administrador BD.

2.5.2. Auditoría a la base de datos

- ✓ Configurar la auditoría y el almacenamiento a través de Oracle Audit Vault. Rol: Administrador BD.
- ✓ Auditar intentos fallidos de inserción y objetos marcados como críticos en la base de datos. Rol: Administrador BD.
- ✓ Realizar triggers para capturar eventos de autenticación en la base de datos. Rol: Administrador BD.
- ✓ Usar Log Miner para auditar en casos de desastres. Rol: Administrador BD.
- ✓ Realizar auditoría de uso de los privilegios de administrativos a través de Oracle DataBase Vault. Rol: Administrador BD.
- ✓ Realizar auditorías sobre actividades de los usuarios a través del Oracle Enterprise Manager (OEM). Rol: Administrador BD.
- ✓ Realizar auditoría sobre la autenticación de la aplicación informática a la base de datos a través de OEM. Rol: Administrador BD.
- ✓ Usar Virtual Private Database, Row-Level Security con Label Security para la protección de los datos. Rol: Administrador BD.
- ✓ Realizar Enmascaramiento de datos a través de las políticas que ofrece Oracle Data Masking.

- ✓ Auditar las contraseñas de los usuarios mensualmente a través del Oracle Audit Vault. Rol: Administrador BD.
- ✓ Auditar el parámetro utl_file_dirse recomienda hacerlo trimestralmente. Rol: Administrador BD.
- ✓ Auditar permisos del paquete dbms_backup_restorese recomienda hacerlo trimestralmente. Rol: Administrador BD.

2.5.3. Mantenimiento de la base de datos.

- ✓ Asegurarse siempre que todos los servicios de la base de datos están funcionando correctamente 30 min antes de comenzar a ser consumidos. Rol: Administrador BD.
- ✓ Realizar pruebas de estrés a los servicios una vez concluida la jornada de trabajo. Rol: Administrador BD.
- ✓ Realizar ejecución de sentencias de forma automática para los casos en que se determine. Rol: Administrador BD.
- ✓ Realizar auditorías integrales a la base de datos cada 45 días. Rol: Administrador BD.
- ✓ Tener a un administrador de la base de datos monitoreando el consumo de recursos del servidor de Oracle. Rol: Administrador BD.

Conclusiones

La seguridad es la característica de cualquier sistema que permite descubrir cuan potente ante amenazas pueda estar el mismo. Se propuso entonces una guía que mida cada indicador de seguridad en las etapas por la que transcurre el proceso de crear una base de datos segura usando Oracle como sistema gestor de bases de datos y todas las facilidades que este posee en la protección de datos. Se espera que con la guía propuesta en este capítulo se garanticen de las bases de datos Oracle a lo largo del ciclo de vida de la misma, garantizando en el despliegue y mantenimiento, una base de datos robusta. Dando cumplimiento de al objetivo de este trabajo.

CAPÍTULO 3 EVALUACIÓN DE LA PROPUESTA

Introducción

En el presente capítulo se realiza la evaluación y aceptación de la guía propuesta. Para ello se utilizan métodos que permiten dar un pronóstico sobre la veracidad de la solución. Existen diferentes métodos para evaluar la propuesta, algunos son: el Test de Turing, el de Validación de comportamientos en casos extremos y el método Delphi. Teniendo en cuenta que el objetivo de este trabajo es realizar una guía para garantizar seguridad en las bases de datos Oracle durante el proceso de desarrollo, se hace necesaria la opinión de un grupo de especialistas que valoren y opinen sobre el trabajo realizado. Por tanto se toma como herramienta el uso del criterio de un panel de especialistas y el empleo de técnicas propuestas en el Método Delphi pues es quien define mejor cómo se debe evaluar el trabajo que se ha venido realizando. Se plantea una descripción de cómo fue ejecutado el método y los resultados que se obtienen.

3.1. Método de Evaluación.

El método de evaluación, Delphi, permite obtener las opiniones de un panel de especialistas. En esta técnica se interroga de forma individual. Se inicia enviando a los especialistas una encuesta evitando el encuentro y permitiendo que la realicen de manera anónima. Esta precaución permite que las respuestas de unos no influyan en las de otros. Después de esta primera ronda, se agrupan las respuestas y se vuelve a enviar la información al panel de especialistas. El número de rondas varía según el nivel de consenso deseado por el investigador. Este proceso se repite las veces que sean necesarias para lograr un determinado consenso. (28)

3.2. Características del Método Delphi.

Presenta tres características fundamentales:

- ✓ **Anonimato**: Ningún experto conoce la identidad de los otros que componen el grupo de debate. Esto tiene una serie de aspectos positivos, como son:
  - Impide la posibilidad de que un miembro del grupo sea influenciado por la reputación de otro de los miembros o por el peso que supone oponerse a la mayoría. La única influencia posible es la de la congruencia de los argumentos.
  - Permite que un miembro pueda cambiar sus opiniones sin que eso suponga una pérdida de imagen.
  - El experto puede defender sus argumentos con la tranquilidad que da saber que en caso de que sean erróneos, su equivocación no va a ser conocida por los otros expertos.
- ✓ **Iteración y realimentación controlada**: La iteración se consigue al presentar varias veces el mismo cuestionario. Como, además, se van presentando los resultados obtenidos con los cuestionarios anteriores, se consigue que los expertos vayan conociendo los distintos puntos de vista y puedan ir modificando su opinión si los argumentos presentados les parecen más apropiados que los suyos.
- ✓ **Respuesta del grupo en forma estadística**: La información que se presenta a los especialistas no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo que se ha obtenido. (29)

3.3. Evaluación de la Guía por los especialistas.

Para evaluar la solución se confecciona un cuestionario referente a la guía en el cual se les permite a los encuestados interactuar con el documento y ejercer sus criterios al respecto, además de permitir evaluar en una escala del 1 al 5 cada pregunta que se le realiza con respecto a la guía.

3.3.1. Selección de los especialistas.

Para la selección de los especialistas se han tomado en cuenta distintos aspectos que el autor considera importante. Uno de estos aspectos es la competencia de cada uno de los encuestados, este permite visualizar en una escala de 0 – 10 el nivel de conocimientos que considera que posee cada uno de los encuestados de acuerdo a los aspectos relacionados con el tema central en cuestión: Seguridad en Bases de datos y Desarrollo de bases de datos utilizando Oracle. Mientras más se acerque a 10, el nivel de conocimientos es más avanzado. En el **Anexo 1** se muestra el nivel de los especialistas escogidos.

Se selecciona para la evaluación, profesores que imparten asignaturas de Base de Datos con conocimientos sobre seguridad en los SGBD, profesionales de otras instituciones que laboran con el gestor Oracle, personal de la UCI dedicado a la producción con este SGBD y además que atiendan la seguridad del mismo. Elegir los especialistas con las características mencionadas propicia tener resultados gratificantes y de mayor calidad acerca de la solución propuesta al problema presentado.

El grupo de especialistas seleccionados funciona como un todo ya que sus conocimientos combinados formarían el especialista ideal para ejercer en cualquier esfera del tema central de este Trabajo de Diploma. De esta manera se pretende obtener distintos puntos de vistas en dependencia de la esfera en que se desempeñe cada uno de los especialistas para poder llegar a conclusiones favorables que permitan asegurar la guía.

3.3.2. Elaboración de la encuesta.

La encuesta consta de seis preguntas de enfoque investigativo sobre la validez de la solución propuesta al problema planteado, son de tipo contable, lo que permiten graficar el resultado de las mismas y abiertas para dar oportunidad a los encuestados de hacer una valoración crítica del tema. Estas preguntas le brindan la ventaja a los especialistas de proporcionar una mayor riqueza a las respuestas ofrecidas. También se brinda la posibilidad de presentar sus opiniones sobre la guía para que tengan la libertad de opinar para conocer sus criterios relativos sobre los diferentes temas tratados. A los especialistas se les puso a su disposición

la documentación de la guía y se les requirió un tiempo determinado para las respuestas o hacer las preguntar pertinentes que les hubiesen surgido al presentar el documento. Para conocer las preguntas en detalles que componen la encuesta, vea el **Anexo 2**.

3.3.3. Resultados de la evaluación a través del método Delphi

Los resultados de la validación se ven a través de las respuestas de cada especialista en las distintas preguntas que se realizaron.

Pregunta 1 Necesidad de Contar con una Guía.

Muchos proyectos realizan determinadas actividades que se exponen en la guía, otras ni las tienen en cuenta por desconocimiento. La seguridad de las bases de datos en los ambientes de desarrollo (al menos dentro de la Universidad de las Ciencias Informáticas) es un aspecto que no se le dedica toda la atención que requiere a diferencia de otros procesos en el desarrollo del software. Además de resultar interesante poder contar con un documento que refleje de manera oficial las actividades que debe realizar cada rol para asegurar la base de datos. Contar con una guía que permita ayudar a los administradores en este sentido es un gran paso de avance en este aspecto. Por lo antes mencionado el resultado arroja que solo un especialista cree que es **bastante necesaria (4)** la guía y demás opinan **muy necesaria (5)**, **Fig. 2**.

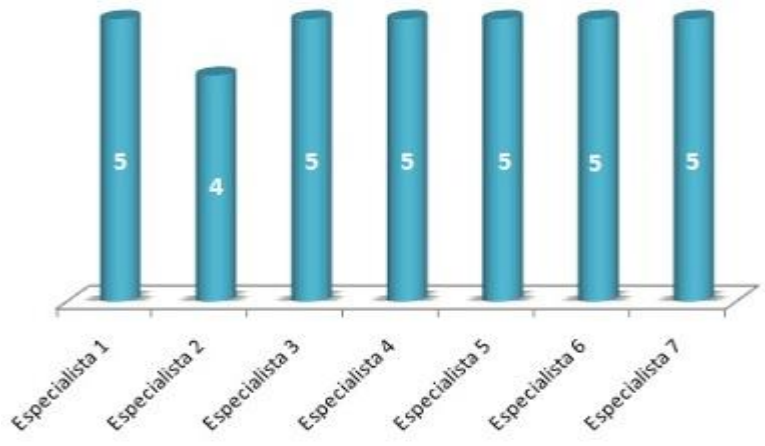

Fig.2 Necesidad de contar con una guía.

Pregunta 2 Garantía de seguridad que presenta la guía al ser ejecutada.

En la gráfica que se presenta a continuación muestra el nivel de garantía que según los especialistas tiene la propuesta de solución. La guía tiene muy buena calidad y propone aspectos muy importantes a tener en cuenta. Es meritorio destacar que abarca puntos muy vulnerables a la hora de instalar y configurar la base de datos en Oracle pues se manipulan detalles esenciales de este SGBD en cuanto a la seguridad. En la misma se registran una serie de pasos que cumpliendo cabalmente se obtendrán BD en Oracle robustas, potentes y seguras, una vez finalizado el proceso de desarrollo. Según lo antes mencionado tres especialistas expresaron **elevada garantía (5)**, tres que **garantiza bastante (4)** y el próximo calificó de que si garantiza la seguridad pero **no de forma absoluta (4.5)**, ver **Fig.3**.

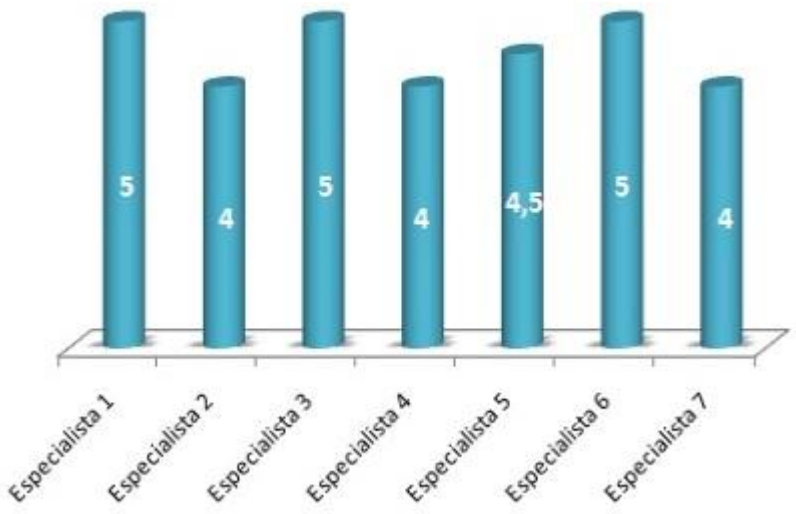

Fig. 3 Garantía de seguridad que presenta la guía.

Pregunta 3 Orden y estructura correcta de la guía.

Los especialistas determinan que la guía está bien estructurada de acuerdo a las fases del proceso de desarrollo de software. El gráfico nos muestra que un especialista la califica de **muy adecuada (5)**, cuatro de ellos como **bastante adecuada (4)** y los restantes la califican de **adecuada (3)**, ver **Fig.4**. Se determina que la guía recoge los principales e importantes

puntos a tener en cuenta en cada fase y se ajusta a la metodología seleccionada. Además se percibe que cada tarea propuesta se corresponde con la fase en la que interviene. La guía muestra los elementos esenciales a tener en cuenta para el aseguramiento de la base de datos, correctamente estructurados en cada fase y siguiendo un orden jerárquico.

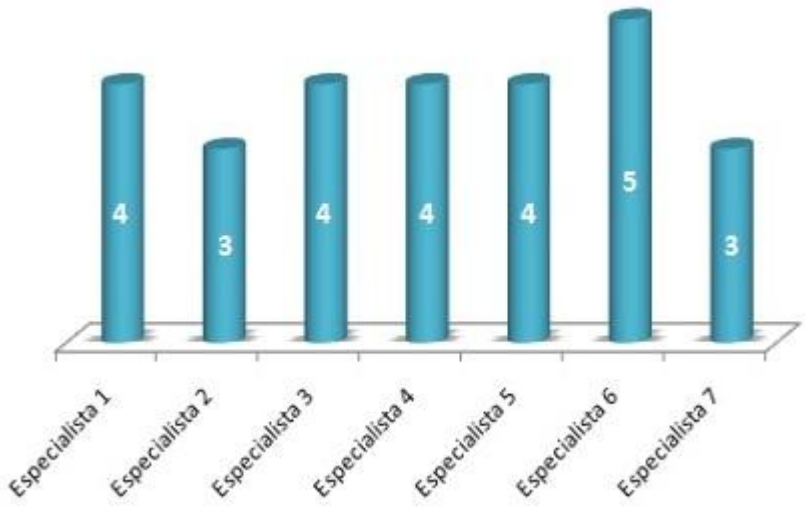

Fig. 4 Orden y estructura correcta de la guía.

Pregunta 4 Relación entre actividades y roles en la guía para cada fase.

El gráfico que a continuación se percibe muestra la opinión de los especialistas acerca de la relación entre las actividades y los roles que intervienen en la guía para cada fase. Muestra que seis especialistas determinan como **bastante correcta (4)** y el que sigue califica de **buena (3)**, la relación entre roles y actividades, descritas en cada fase, ver **Fig. 5**. En la guía se específica detalladamente y se ajusta correctamente cada actividad para un rol, lo que permite delimitar el espacio de cada involucrado. Se denota a simple vista las actividades y cada rol que debe ejecutarla, sin dejar de reconocer que otros roles que posean el conocimiento requerido pueden realizar las actividades de otro rol en una circunstancia dada.

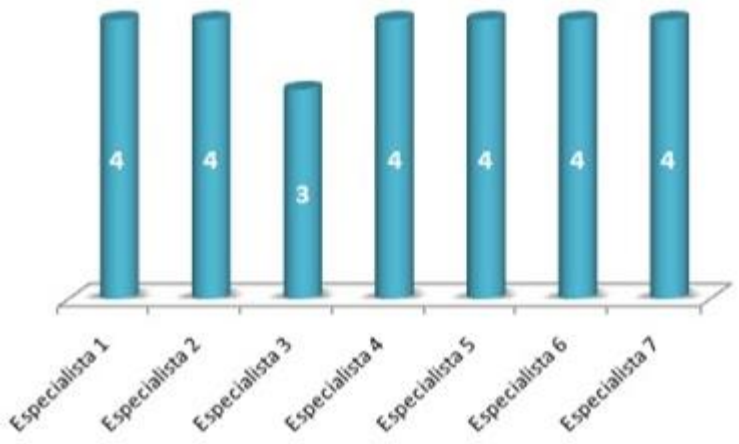

Fig. 5 Relación entre actividades y roles en la guía para cada fase.

Pregunta 5.1 Nivel de Satisfacción de la guía.

El nivel de satisfacción por parte de los especialistas ha sido elevado, demostrando que la guía satisface las necesidades por la que fue creada. La misma muestra los principales aspectos a medir para garantizar seguridad durante el proceso de desarrollo de software y las actividades con sus roles correspondientes, lo que hace que el nivel de satisfacción sea elevado ya que responde a las necesidades del cliente. Dos de los especialistas opinan como **muy satisfactoria (5)** y el resto de **bastante satisfactoria (4)**, ver **Fig. 6**.

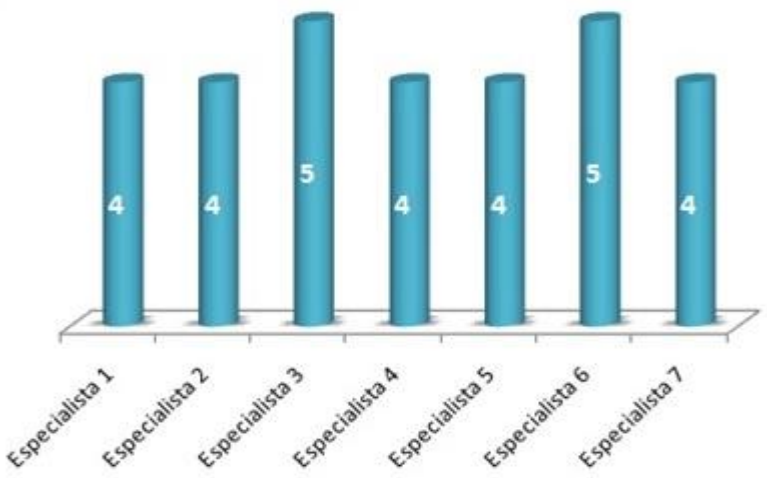

Fig. 6 Nivel de satisfacción.

Pregunta 5.2 Posibilidad de Aplicación de la guía.

La guía puede ser aplicada a todos los proyectos de la universidad que decidan escoger Oracle DataBase como SGBD que utilicen la metodología de desarrollo RUP en sus proyectos. Los especialistas otorgan la categoría de muy aplicable en los proyectos de la universidad que decidan trabajar con Oracle como SGBD utilizando la metodología RUP, preferiblemente en los proyectos que se inician ya que realizar paso a paso cada una de las actividades en el tiempo definido y la etapa requerida. Uno de los especialistas la califica de **bastante aplicable (4)** y los demás de **muy aplicable (5)**, ver **Fig. 7**.

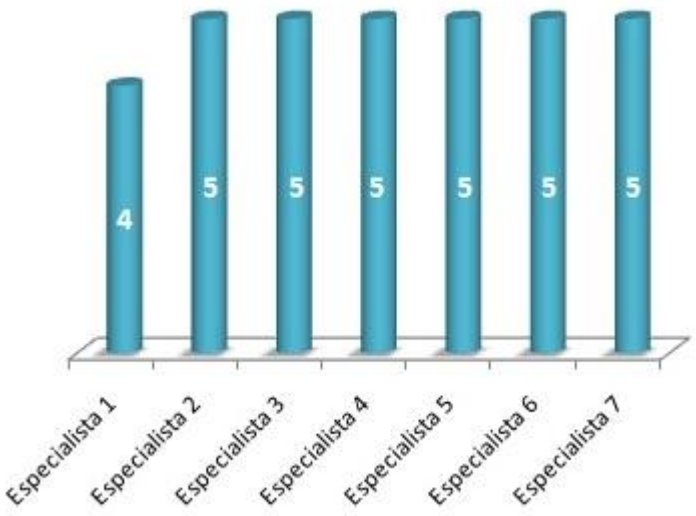

Fig. 7 Posibilidad de aplicación de la guía.

Pregunta 5.3 Nivel de Repercusión de la guía. La gráfica muestra el grado de repercusión como muy elevado, que según los especialistas tiene la solución una vez que se ponga en práctica. Plantean que no existe tal guía que proponga actividades a realizar desde el mismo proceso de desarrollo con el fin de asegurar las bases de datos. Sirve de apoyo tanto a los desarrolladores como los administradores para asegurar la base de datos, importante

elemento para la creación de robusta y potente de la misma. Cinco de los especialistas consideran que la guía tiene **elevada repercusión (5)** y el resto le confiere **bastante repercusión (4)**, ver **Fig. 8**.

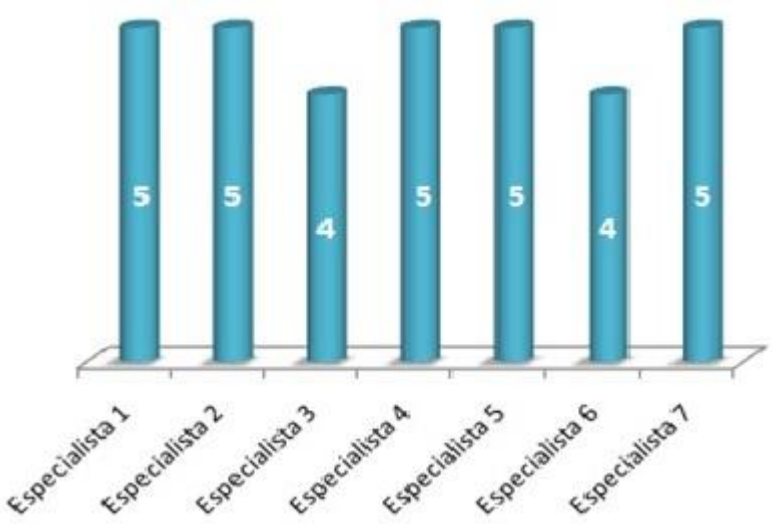

Fig. 8 Nivel de repercusión de la guía.

Pregunta 5.4 Nivel de cumplimiento en el área de proceso de la guía.

Se percibe en el gráfico que los especialistas califican como muy elevada la seguridad que se obtendrá si se le otorga cumplimiento estricto a las actividades que presenta la guía. Cumpliendo cabalmente los aspectos que se exponen en la misma los proyectos informáticos obtendrán un alto nivel de seguridad en sus bases de datos una vez concluido todo el proceso de desarrollo. Por tanto se obtiene como resultado de las opiniones de los especialistas que cuatro de ellos proponen **muy elevada (5)** si se cumple paso a paso lo que dicta la guía y el resto, **bastante elevada (4)**, ver **Fig. 9**.

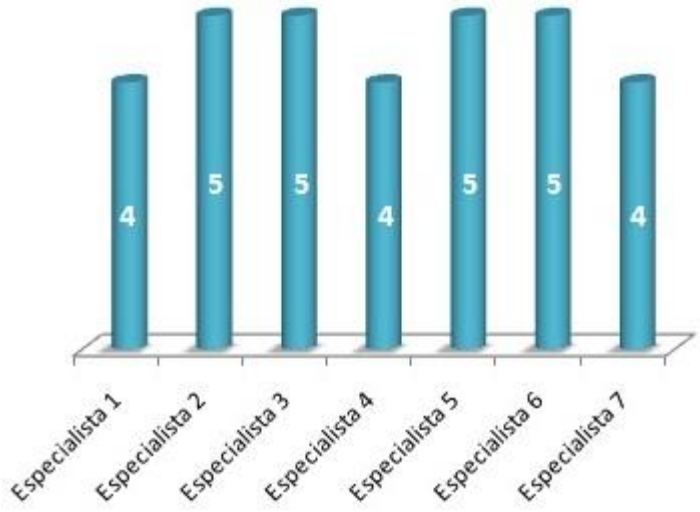

Fig. 9 Nivel de cumplimiento en el área de proceso de la guía.

Pregunta 5.5 Nivel de Seguridad de la guía.

La guía apoya y garantiza de manera muy elevada la seguridad. Los especialistas determinan que utilizando la guía se elimina de manera casi absoluta las amenazas y riesgos. Opinan que no existe algo completamente absoluto pero sí bastante cerca y en ese rango ubican la propuesta realizada. Cumple con los principales requisitos de seguridad en la BD, así como llegar a lo específico del gestor estudiado. Propone actividades concretas y el rol que debe hacerla, permitiendo que se realice una correcta asignación de privilegios lo que puede ser adaptado a las necesidades de cada proyecto que utilice RUP como metodología de desarrollo y la base de datos realizada en Oracle. Por lo que categorizan la guía, seis especialistas de **bastante segura (4)** y el restante de **muy segura (5)**, ver **Fig. 10.**

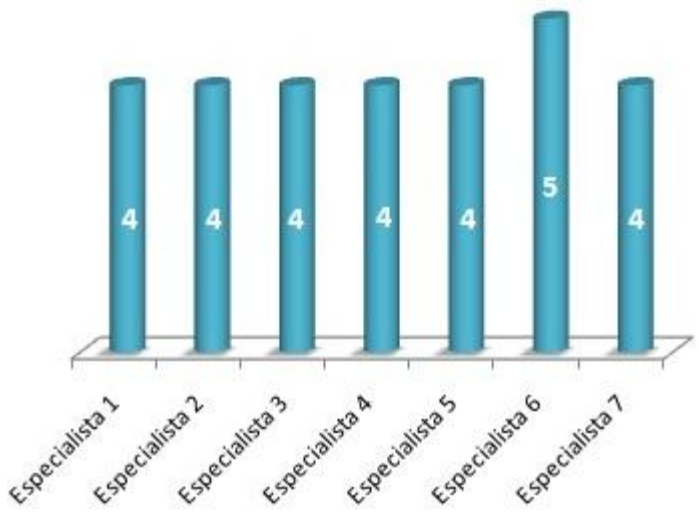

Fig. 10 Nivel de Seguridad de la guía.

Por ciento de aceptación de la guía por pregunta teniendo en cuenta las respuestas.

Al observar la siguiente gráfica se puede determinar claramente el elevado porciento de aceptación que presenta la guía para los especialistas; demostrando un alto porcentaje de certeza en cada pregunta de la encuesta realizada, lo que demuestra que la guía cumple con el propósito por la que fue creada. Se analiza con estos porcentajes que la propuesta de solución es **altamente aplicable**, **aseguradora** y **adaptable** por lo que satisface en un gran porciento a los desarrolladores y administradores de estas bases de datos. Además la misma brinda **garantía** de obtener una base de datos robusta y potente una vez concluido el proceso de desarrollo, la conciben **muy necesaria** en todos los proyectos que utilicen el SGBD Oracle y la metodología de desarrollo RUP. Ver **Fig. 11**.

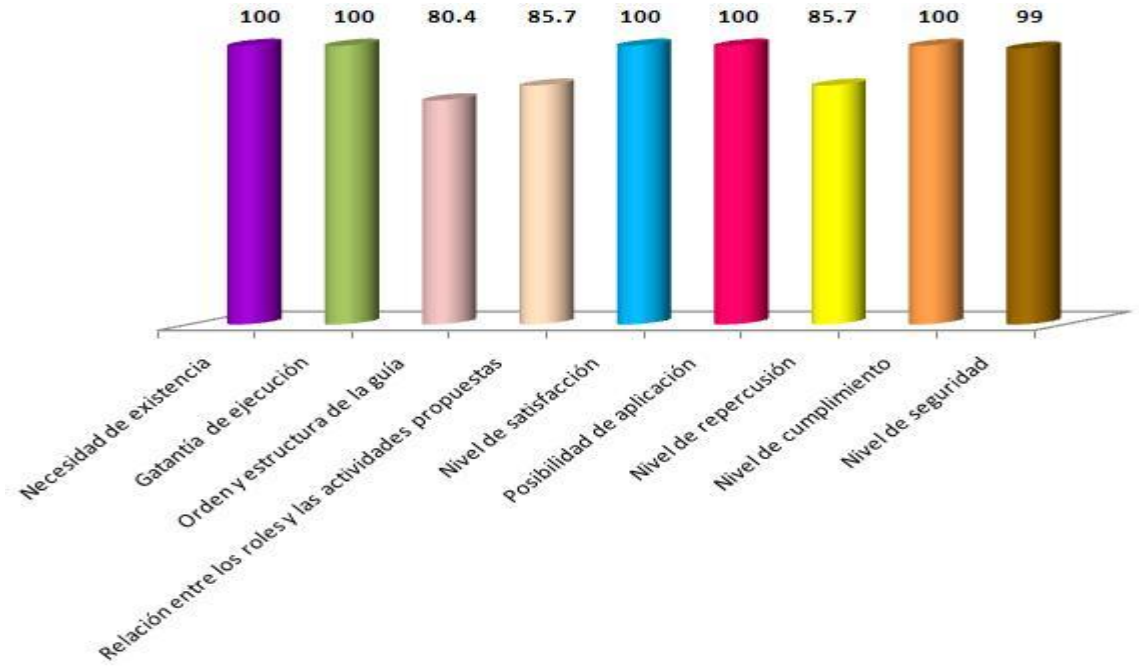

Fig. 11 Porciento de aceptación de la guía por pregunta teniendo en cuenta las respuestas.

Coeficiente de Kendall.

A través de la herramienta SPSS, versión 13.0, se calcula el coeficiente de Kendall que determina el grado de concordancia en las respuestas dadas por los especialistas. Se define que mientras más cerca se encuentre de 1.00 (uno) entonces existe un alto grado de concordancia entre las respuestas de los especialistas sobre la guía. Como resultado se obtuvo el coeficiente de **Kendall con un 0.877**, (Fig. 12); lo que determina que hubo un alto grado de concordancia por parte de los especialistas a la hora de opinar que la guía es factible y responde al problema por la que fue creada.

Test Statistics

N			7
Kendall's W[a]			,877
Chi-Square			61,400
df			10
Asymp. Sig.			,000
Monte Carlo Sig.	Sig.		,000[b]
	95% Confidence Interval	Lower Bound	,000
		Upper Bound	,000

a. Kendall's Coefficient of Concordance

b. Based on 10000 sampled tables with starting seed 2000000.

Fig.12 Coeficiente de Kendall.

Conclusiones

Se escoge un grupo de especialistas en el tema tratado: seguridad en bases de datos Oracle, que permiten certificar la guía confeccionada. Con la evaluación realizada se puede apreciar un resultado satisfactorio, obtenido de la opinión de los especialistas a través de las encuestas realizadas. Por lo que muestra la garantía de seguridad que tiene la guía propuesta.

CONCLUSIONES GENERALES

En el presente trabajo de diploma, con el objetivo de asegurar las bases de datos realizadas en Oracle desde el proceso de desarrollo de software en aras de solucionar los problemas existentes, se llevaron a cabo varias acciones:

- ✓ Se investigó cuáles son las actividades y los roles que intervienen en el proceso de desarrollo de software para la utilización correcta de estos aspectos en la guía.

- ✓ Se estudió la seguridad en las bases de datos Oracle y las aplicaciones complementarias de seguridad que propone Oracle Corporation adquiriendo mayor conocimiento, lo que permitirá obtener una solución eficiente al problema de la investigación.

- ✓ Se confeccionó la propuesta de solución que permitirá asegurar las bases de datos Oracle desde comienzo del proceso de desarrollo de software utilizando la metodología RUP.

- ✓ Se realizó un pronóstico de la propuesta por un grupo de especialistas determinando que la guía es factible y permitirá garantizar seguridad en las BD Oracle durante todo el proceso de desarrollo de software.

RECOMENDACIONES

Se recomienda:

- ✓ Poner en práctica la propuesta de solución en todos los proyectos de la UCI que elijan utilizar Oracle como SGBD para sus aplicaciones informáticas.
- ✓ Profundizar en el estudio de la seguridad en este sistema gestor de bases de datos pues se encuentra en constante actualización de sus productos.
- ✓ Estudiar el nuevo servicio de consultoría de Oracle, que realiza Diagnósticos de Seguridad a la base de datos realizadas en Oracle con el objetivo de integrar esta nueva estrategia a la guía elaborada, permitiendo asegurar aún más la base de datos.

BIBLIOGRAFÍA REFERENCIADA

1. **MARTINEZ, David Luis La Red.** Universidad Nacional del Nordeste. [En línea] noviembre de 2001. [Citado el: 17 de octubre deL 2009.] http://exa.unne.edu.ar/depar/areas/informatica/SistemasOperativos/MonogSO/SEGUNIX012.htm.

2. **Kioskea.** Kioskea.net. [En línea] 16 de octubre de 2008. [Citado el: 18 de octubre de 2009.] http://es.kioskea.net/contents/secu/secuintro.php3.

3. **UCI.** Entorno Virtual de Apendizaje. [En línea] 2009. [Citado el: 22 de noviembre de 2009.] http://eva.uci.cu/mod/resource/view.php?id=21621&subdir=/Ayuda_del_Rational_/Espanol.

4. **SOTO, Lauro.** Mi Tecnologico. [En línea] 2008. [Citado el: 26 de noviembre de 2009.] http://www.mitecnologico.com/Main/ConceptoSeguridadBaseDatos.

5. **RAMIREZ, Mercede.** Monografías.com. [En línea] 30 de julio de 2003. [Citado el: 25 de noviembre de 2009.] http://www.monografias.com/trabajos14/basededatos/basededatos.shtml.

6. **Mari_88_990.** Monografía. [En línea] 2008. [Citado el: 27 de noviembre de 2009.] http://www.monografias.com/trabajos26/seguridad-base-datos/seguridad-base-datos.shtml.

7. **FRANCO, Andrés Cordón.** Universidad de Sevilla,España. *Dpto de Ciencias de la Computación e Inteligencia Artificial.* [En línea] 2005-2006. [Citado el: 29 de noviembre de 2009.] http://www.cs.us.es/cursos/bd-2005/tema-BD-1.pdf.

8. **Free Encyclopedia of Ecommerce .** Free Encyclopedia of Ecommerce . *Oracle Corp - Early History.* [En línea] [Citado el: 22 de noviembre de 2009.] http://ecommerce.hostip.info/pages/815/Oracle-Corp-EARLY-HISTORY.html.

9. **LAFUENTE, Alvaro.** Portal Paraguayo de Noticias. [En línea] 8 de febrero de 2007. [Citado el: 24 de noviembre de 2009.] http://www.ppn.com.py/html/noticias/noticia-ver.asp?id=30426&desc=Oracle-Database-11g-la-nueva-solucion-tecnologica-para-las-empresas.

10. **VALDÉS, Luis Manuel.** Institut Montilivi. [En línea] 22 de septiembre de 2009. [Citado el: 30 de noviembre de 2009.] http://www.iesmontilivi.net/Departaments%5CInformatica%5CDAI%5CC3-ABD%5Cdocs%5Capunts/oracleadm.pdf.

11. **HUEY, Patricia.** *Oracle Database 2 Day + Security Guide, 11g Release 1 (11.1).* s.l. : Oracle USA, 2007.

12. **JELOKA, Sumit.** *Oracle® Database Advanced Security Administrator's Guide.* s.l. : Oracle USA, septiembre,2007.

13. **HUEY, Patricia.** *Oracle Database Security Guide 11g Release 1 (11.1).* s.l. : Oracle USA, febrero,2008.

14. **Arena, Osvaldo José Sanchéz.** *Propuesta de un esquema de seguridad para las Bases de Datos Oracle del MININT.* Cuba : Tesis,UCI, julio,2008.

15. **Conocimientoweb.** Red del Conocimiento. [En línea] 28 de enero de 2009. [Citado el: 15 de enero de 2010.] http://www.reddelconocimiento.org/profiles/blogs/seguridad-del-sistema-oracle.

16. **GARCÍA, Angélica.** ChannelPlanet. [En línea] 17 de enero de 2002. [Citado el: 18 de enero de 2010.] http://www.channelplanet.com/?idcategoria=10511.

17. **Oracle Corporation.** Oracle,Documentacion de orade. *Oracle Secure Backup:Optimizado para los Entornos de Oracle.* [En línea] abril de 2006. [Citado el: 3 de febrero de 2010.] http://www.oracle.com/technology/global/lad-es/documentation/collaterals/optimized_oracle_osb_cast.pdf.

18. —. Oracle.com. [En línea] [Citado el: 20 de febrero de 2010.] http://www.oracle.com/us/products/database/options/total-recall/index.html.
19. —. Oracle.com. *Advance Security.* [En línea] [Citado el: 26 de febrero de 2010.] http://www.oracle.com/database/audit-vault.html?origref=http://www.oracle.com/us/products/database/advanced-security-066516.html.
20. —. Oracle.com. *Audit Vault.* [En línea] [Citado el: 3 de marzo de 2010.] http://www.oracle.com/database/audit-vault.html.
21. **Amed.** Develoft. [En línea] 16 de marzo de 2009. [Citado el: 12 de marzo de 2010.] http://blog.develoft.com/?p=18.
22. **CABANES, José Ignacio.** Diccionario Básico de Informática. [En línea] [Citado el: 12 de marzo de 2010.] http://usuarios.multimania.es/resve/diccioninform.htm#A.
23. **POTENCIER, Francois Zaninotto y Fabien.** Google Libros. [En línea] 2007. [Citado el: 8 de marzo de 2010.] http://books.google.com.cu/books?id=2eS5oTEYk8QC&printsec=frontcover&dq=The+Definitive+Guide+to+Symfony&source=bl&ots=zia9JDUXtV&sig=4m-v--8JPhgglMo6vxmT2U4B-6g&hl=es&ei=twzyS8upKIaBlAf8prn3DA&sa=X&oi=book_result&ct=result&resnum=4&ved=0CCsQ6AEwAw#v=onepa.
24. **RIGAZZI, Pablo.** Zend Framework. [En línea] 9 de septiembre de 2008. [Citado el: 11 de marzo de 2010.] http://spanish.zendfw.com/.
25. **EllisLab, Inc.** CodeIgniter. [En línea] 2009. [Citado el: 13 de marzo de 2010.] http://www.codeigniter.com.
26. **CakePHP Development.** CakeCD. [En línea] 3 de febrero de 2008. [Citado el: 4 de diciembre de 2009.] http://www.cakedc.com.
27. **Open web application security project.** Java Security Frameworks. [En línea] 20 de abril de 2009. [Citado el: 17 de marzo de 2010.] http://www.owasp.org/index.php/Java_Security_Frameworks.
28. **12Manager.** 12Manager. *Método Delphi(Gordon, Helmer, Dalkey).* [En línea] [Citado el: 22 de marzo de 2010.] http://www.12manage.com/methods_helmer_delphi_method_es.html.
29. **Grupo de Tecnologías de la Información y las Comunicaciones.** El Metodo Delphi. [En línea] [Citado el: 23 de marzo de 2010.] http://www.gtic.ssr.upm.es/encuestas/delphi.htm.
30. **TEJADA, Luis.** Babo´S Blog. [En línea] 16 de junio de 2007. [Citado el: 14 de noviembre de 2009.] http://babotejada.wordpress.com/2007/06/16/proceso-unificado-de-rational/.
31. **RIOS, Alexander.** Desarrollo de Aplicaciones. [En línea] 4 de agosto de 2006. [Citado el: 5 de marzo de 2010.] http://alxplus.blogspot.com/2006/08/aplicaciones-web-vs.html.

BIBLIOGRAFÍA CONSULTADA

1. **SESESMA, Majo.** Todo Expertos. [En línea] 17 de marzo de 2003. [Citado el: 4 de diciembre de 2009.] http://www.todoexpertos.com/categorias/tecnologia-e-internet/bases-de-datos/oracle/respuestas/403836/listar-las-tablas-de-una-base-de-datos-de-oracle.

2. **Evidiala.** Tutoriales en la Red. [En línea] 2009. [Citado el: 20 de enero de 2010.] http://www.tutorialesenlared.com/index.php?&t=sub_pages&link_order_c=link_date&link_sort_c=desc&cat=22&start=10&sid=517434025&.

3. **Oracle Corporation.** Oracle. [En línea] [Citado el: 22 de enero de 2010.] http://www.oracle.com/technology/global/lad-es/documentation/database.html.

4. **Soporte Microsoft.** Soporte Microsoft. [En línea] 5 de septiembre de 2007. [Citado el: 4 de febrero de 2010.] http://support.microsoft.com/kb/841180/es.

5. **Kanter, Stephen Kost and Jack.** Integrigy. [En línea] abril de 2007. [Citado el: 15 de febrero de 2010.] http://www.integrigy.com/securityresources/whitepapers/Integrigy_Oracle_Listener_TNS_Security.pdf.

6. **SoftwareONE.** SoftwareONE Provides Solutions Worldwide. [En línea] julio de 2006. [Citado el: 13 de febrero de 2010.] http://www.softwareone.com/files/Oracle_Audit_Vault.pdf.

7. **CGISecurity.** Web Application Security Services. [En línea] febrero de 2001. [Citado el: 26 de febrero de 2010.] http://www.cgisecurity.com/database/oracle/pdf/f5crypt.pdf .

8. **Pontecorvo, Bruno.** Departamento de Informatica: universidad de Pisa,Italia. [En línea] 2005. [Citado el: 2 de marzo de 2010.] http://www.di.unipi.it/~ghelli/didattica/bdldoc/B19306_01/network.102/b14266/checklis.htm.

9. **ZARAGOZA, Mtra. María de Lourdes Santiago.** Programa Educativo de Tecnologías de la Información y Comunicación. [En línea] julio de 2007. [Citado el: 12 de marzo de 2010.] http://www.utvm.edu.mx/OrganoInformativo/orgJul07/INDICE.htm.

10. **INFOFIA.** Universidad de San Martín de Porres, Lima, Perú. [En línea] noviembre de 2002. [Citado el: 15 de marzo de 2010.] http://www.usmp.edu.pe/publicaciones/boletin/fia/info49/articulos/RUP%20vs.%20XP.pdf.

11. **NECHES, Luix Rodríguez.** La Red para los profesionales IT. [En línea] 2009. [Citado el: 2 de noviembre de 2009.] http://es.debugmodeon.com/articulo/scrum-una-metodologia-agil-ii.

12. **MORALES, Andrea.** Ideas.3p. [En línea] 14 de febrero de 2007. [Citado el: 5 de noviemvre de 2009.] http://blog.tercerplaneta.com/2007/02/ms-all-de-las-capacidades-tcnicas-que.html.

13. **Ecomba.** Agile Spain. [En línea] 13 de enero de 2003. [Citado el: 13 de novienbre de 2009.] http://www.agile-spain.com/feature_driven_development.

14. **TEJADA, Luis.** Babo´S Blog. [En línea] 16 de junio de 2007. [Citado el: 14 de noviembre de 2009.] http://babotejada.wordpress.com/2007/06/16/proceso-unificado-de-rational/.

15. **GONZÁLEZ, Jorge Fernández.** Sistemas Decisionales, algo mas que Business Intelligence. [En línea] 1 de febrero de 2007. [Citado el: 15 de noviembre de 2009.] http://sistemasdecisionales.blogspot.com/2007/02/dynamic-systems-development-method.html.
16. **Aidanamax.** Adaptive Software Development. [En línea] 28 de mayo de 2008. [Citado el: 16 de noviembre de 2009.] http://aidanamx.blogspot.com/.
17. **ACUÑA, César javier.** Open Source Software y Metodologías ágiles ¿Qué tanto se parecen? [En línea] 2002-2003. [Citado el: 20 de noviembre de 2009.] http://curso-sobre.berlios.de/curso/trab/cjacuna/Open_Source_y_Met_Agiles.pdf.

GLOSARIO DE TÉRMINOS

[C]

Clustering: El término se aplica a los conjuntos o conglomerados de computadoras construidos mediante la utilización de componentes de hardware comunes y que se comportan como si fuesen una única computadora.

[D]

Data warehousing: Almacenamiento de datos. De almacén de datos (data warehouse): colección de datos orientada a un determinado ámbito, integrado, no volátil y variable en el tiempo, que ayuda a la toma de decisiones

[F]

Frameworks: Es una estructura conceptual y tecnológica de soporte definida, normalmente con artefactos o módulos de software concretos, con base en la cual otro proyecto de software puede ser organizado y desarrollado.

[I]

ISO: International Organization for Standardization.

[J]

J2EE (Java Platform, Enterprise Edition): Es una plataforma de programación para desarrollar y ejecutar software de aplicaciones en el lenguaje de programación Java con arquitectura de N niveles distribuidos, basándose ampliamente en componentes de software modulares ejecutándose sobre un servidor de aplicaciones.

[P]

Plugin: es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy especifica.

[S]

Spring: es un framework de código abierto de desarrollo de aplicaciones para la plataforma Java.

ANEXOS

Anexo 1. Nivel de conocimiento de los encuestados.

No. Experto	0	1	2	3	4	5	6	7	8	9	10
1											X
2											X
3											X
4										X	
5										X	
6								X			
7									X		

Anexo 2. Encuesta para evaluar la guía.

Encuesta para la evaluación de la Guía.

Rol en que se desempeña: _____

Categoría Docente: _____

Cuestionario

1. ¿Considera necesario la definición de una guía para obtener seguridad en bases de datos realizadas en Oracle en los proyectos que la utilicen en la Universidad?

   __Muy necesaria (5) __Bastante necesaria (4) __ Necesaria (3) __Poco necesaria (2) __Innecesaria (1).

   ¿Por qué?_____

2. ¿Qué valor usted considera que presenta la Guía para incidir en la mejora gradual de la seguridad en los proyectos que decidan usarla?

   __ Elevada garantía (5) __Garantiza bastante (4) ___Garantiza (3)__ Poca garantía (2) __No garantiza (1).

   ¿Por qué?_____

3. ¿Considera que la estructura y el orden de la Guía son adecuados?

   __Muy adecuada (5) __Bastante adecuada (4) __ Adecuada (3) __Poco adecuada (2) __Inadecuada (1).

   ¿Por qué?_____

   _____

4. ¿Existe una correcta relación entre las actividades y roles propuestos en la Guía que permitirá garantizar seguridad en BD Oracle?

   __Muy correcta (5) __Bastante correcta (4) __ correcta (3) __poco correcta (2) __Incorrecta (1).

   ¿Por qué?_____

   _____

   _____

5. En una escala del 1 al 5 confiera una evaluación a la propuesta según los siguientes criterios:

   __Satisfacción a las necesidades de los proyectos que decidan usar el SGBD Oracle.

   __Posibilidad de aplicación en los proyectos que decidan usar el SGBD Oracle.

   __Repercusión a los proyectos que decidan usar el SGBD Oracle.

   __Cumplimiento de lo establecido en el área de proceso que va a ser implantada la guía.

   __Mejora de la Seguridad para los proyectos que decidan usar el SGBD Oracle.