UNIVERSIDAD NACIONAL DE INGENIERÍA

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS

APLICACIÓN DE INTELIGENCIA DE NEGOCIOS A LOS ESTUDIOS DE AUDITORIA DE TIENDA (RETAIL AUDIT)

INFORME DE SUFICIENCIA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

HUGO CARLOS VALER ROJAS

LIMA - PERÚ

2005

DEDICATORIA

Dedico este trabajo a todas aquellas personas que me han apoyado en la vida, a mi padre, Félix, a mi madre, María, y a mis hermanos Jaime y Roger; a ellos gracias por todo.

ÍNDICE DE CONTENIDOS

DESCRIPTORES TEMÁTICOS

- ✓ Retail Audit.
- ✓ Auditoría de Negocios (Tienda)
- ✓ Inteligencia de Negocios
- ✓ DataWarehouse
- ✓ OLAP
- ✓ Herramientas OLAP
- ✓ Seguridad Web
- ✓ E-Business
- ✓ Arquitectura Aplicaciones Web

RESUMEN EJECUTIVO

La inteligencia de Negocios apoya a los tomadores de decisiones con la información correcta, en el momento y lugar correcto, lo que les permite tomar mejores decisiones de negocios. La información adecuada en el lugar y momento adecuado incrementa la efectividad de cualquier empresa.

Este informe trata de la manera como la empresa XYZ Audit apoya a tomar decisiones oportunas y certeras de los clientes en función de las Auditorias de Producto, con la ayuda de la tecnología y al menor costo posible.

Como se verá más adelante, la materia prima usada por XYZ Audit son datos, y el producto final pasa por obtener información hasta generar conocimiento, la cual es entregada a sus clientes. El hacer uso de Inteligencia de negocios para estos procesos genera una gran ventaja competitiva.

Dentro de los procesos tradicionales, especificados en la Cadena de valor de la empresa, se encuentran varias problemáticas que van desde el seguimiento del estado del requerimiento del cliente, la toma manual de datos, demora de lectura, supervisión costosa, sustentación de resultados, etc.

Aplicando Inteligencia de Negocios y tecnología de punta se busca

resolver estas problemáticas, para satisfacción del cliente, optimización de recursos, reducción de costos, generación de ventaja competitiva, etc.

En este contexto, los clientes de XYZ Audit no cuentan con herramientas de análisis para los estudios de auditoria de Negocios, que le permitan analizar el resultado de estos estudios en tiempo real y en cualquier lugar sin depender de alguna herramienta propietaria.

Para resolver este problema se desarrolló un sistema que permite hacer análisis de auditoria de Negocios a través de Internet, el cual no requiere de licencia alguna en el cliente y con funcionalidades similares a cualquier herramienta propietaria de análisis de datos (Bussines Object, Power Play, Oracle Sales Analyser, etc.)

En conclusión, esta herramienta no solo permite analizar información, sino que además es un portal que permitirá a la empresa XYZ mantener informado, en tiempo real del avance de sus estudios de auditoria, además de contar con información sobre tendencias del mercados, alertas, noticias, reportes predefinidos, además de poder hacer operaciones sobre las mismas, como compartir información con otros ejecutivos. Es decir se brindara información personalizada a cada uno de sus clientes lográndose fidelidad de los mismos.

Finalmente, uno de los requerimientos no funcionales del sistema estuvo enfocado al tema de seguridad. Entre las estrategias adoptadas para atacar este punto se tomo en cuenta subsanar y evitar las diez vulnerabilidades más críticas en aplicaciones Web (Anexo 3). Este punto es crucial por el tipo de información confidencial que es manejada por cada uno de los clientes de XYZ Audit.

INTRODUCCIÓN

Lo que antes generaba una ventaja competitiva, tales como precio, producto, posicionamiento, promoción, etc. ya no representan ventajas competitivas. Debido a esto, ahora, las empresas se preocupan de cómo desarrollar una lealtad duradera, de cómo apoyar cada vez más en el posicionamiento de su marca.

Cada vez mas las interacciones con los clientes es el núcleo del negocio, es la clave para generar y mantener lealtad de sus clientes, Pero esta interacción debe ser de alta calidad y de constancia a través del tiempo.

Ante las nuevas tendencias tecnológicas, es responsabilidad de las empresas usarlas adecuadamente para ofrecer a sus clientes herramientas y soluciones que satisfagan las necesidades cada vez más crecientes en este mundo competitivo.

Internet y las Nuevas Tecnologías, la gestión de recursos humanos y del conocimiento, la globalización, el mayor poder en el cliente, el cambio constante, la gestión de la innovación, etc., son nuevos conceptos que las empresas deben incorporar en su gestión.

Mediante una gestión eficiente de la tecnología, XYZ Audit busca generar una ventaja competitiva sobre sus competidores. Entre estas tecnologías emergentes están Internet, los sistemas de Información, el

comercio electrónico, Inteligencia de Negocios, Gestión del conocimiento DataWarehouse, OLAP, etc.

Las tecnologías sobre las cuales se sustenta el presente Informe son la Inteligencia de Negocios y la tecnología de Internet. Pero se debe tener en cuenta que para tener éxito en un proyecto de Inteligencia de Negocios se debe focalizar en obtener el conocimiento para la toma de decisiones en las áreas claves de la empresa, es decir, donde se obtiene el valor agregado.

La ventaja que nos ofrece la tecnología Internet es que permite a las personas poder acceder a todo tipo de información, desde cualquier lugar, en cualquier momento.

Juntos, la tecnología de Internet y la Inteligencia de Negocios (Business Intelligence), usadas adecuadamente, podrían generar una gran ventaja competitiva para la empresa.

CAPITULO I
ANTECEDENTES

1. DIAGNÓSTICO ESTRATÉGICO

1.1. VISIÓN

La Visión Corporativa definida por XYZ AUDIT es la siguiente:

"Mantener el Liderazgo en el mercado, proporcionando información veraz y oportuna, para la satisfacción de las necesidades de nuestros clientes."

1.2. MISIÓN

La misión corporativa de XYZ AUDIT, es la siguiente:

"Proporcionar a nuestros clientes, estudios de mercado que ayuden a minimizar el riesgo en la toma de decisiones."

1.3. OBJETIVOS ORGANIZACIONALES

A fin de alcanzar la visión y cumplir la misión, XYZ AUDIT ha establecido los siguientes objetivos organizacionales:

- ✓ Cubrir las necesidades de información que satisfagan los intereses de nuestros clientes en cada investigación en particular.
- ✓ Proporcionar información veraz y oportuna (velocidad de respuesta) a través del desarrollo de los sistemas de Información, con el uso de tecnología de punta.
- ✓ Cultivar relaciones perdurables que permitan obtener lealtad y reconocimiento de nuestros clientes.
- ✓ Capacitar a nuestro personal, manteniéndolo comprometido y motivado con la empresa.

1.4. ANÁLISIS FODA

1.4.1. FORTALEZAS:

- ✓ Conocimiento de mercado
- ✓ Liderazgo
- ✓ Personal con alta experiencia
- ✓ Tecnología de punta
- ✓ Alcance Nacional y algunos países de la región
- ✓ Alianza estratégica con Empresas de nivel Mundial
- ✓ Certificación ISO 9000

1.4.2. OPORTUNIDADES

- ✓ Realización de Venta cruzada
- ✓ Desarrollo de nuevas líneas de negocios
- ✓ Ingreso de nuevos productores de artículos de consumo masivo

1.4.3. DEBILIDADES

- ✓ Insatisfacción de los clientes

- ✓ Precios demasiado altos
- ✓ Tiempos de entrega de informes

1.4.4. AMENAZAS

- ✓ Ingreso de nuevos competidores pequeños
- ✓ Ingreso de nuevos productos sustitutos
- ✓ Fusión de empresas de producción. De consumo Masivo
- ✓ Creación de empresa de estudios de mercado por los principales clientes

2. DIAGNÓSTICO FUNCIONAL

2.1. PRODUCTOS

XYZ Audit tiene dos divisiones dedicadas a brindar estudios específicos, estas son:

2.1.1. DIVISIÓN DE AUDITORIA: Realiza una variada gama de investigaciones de orden cuantitativo, ofreciendo los siguientes estudios:

- ✓ Auditoria de Producto: estudios sistemáticos y estandarizados.
- ✓ Auditoria de Merchandising: Evaluación del comportamiento de los autoservicios
- ✓ Mercado de Prueba: Es una mini auditoria enfocada a un segmento específico del mercado definido por el cliente.
- ✓ Category Trends:
- ✓ Auditoria Express: Estudios puntuales.
- ✓ Recolección de Muestras: Identificación de centros de negocios
- ✓ Chequeo de Distribución: Evalúa la presencia del producto en el mercado.

- ✓ Chequeo de Precios: Mide la evolución de los precios.
- ✓ Panel de Ambulantes: estudios de auditoria dirigido al segmento informal.
- ✓ Exhibición de Góndolas: porcentaje de exhibición de los productos en autoservicios.
- ✓ Space Manager: estudio permite administrar óptimamente los espacios en autoservicios:
- ✓ Price Manager:
- ✓ Índice de Distribución Nacional "Indis": Chequeo de distribución productos de los negocios a nivel nacional.

2.1.2. DIVISIÓN DE ESTUDIOS ESPECIALES: Esta división se encarga de brindar información específica para una problemática en particular, generalmente confidencial, tanto de carácter puntual como sistemática, ofrece estudios sobre:

- ✓ Productos / Servicios
- ✓ Comportamiento del Consumidor
- ✓ Comunicación
- ✓ Empresas y Negocios
- ✓ Fuerza de Venta
- ✓ Calidad del Servicio

2.2. CLIENTES

- ✓ Alicorp
- ✓ British American Tobacco
- ✓ Kola Real
- ✓ Johnson's
- ✓ Kraft
- ✓ Nestle
- ✓ Unilever

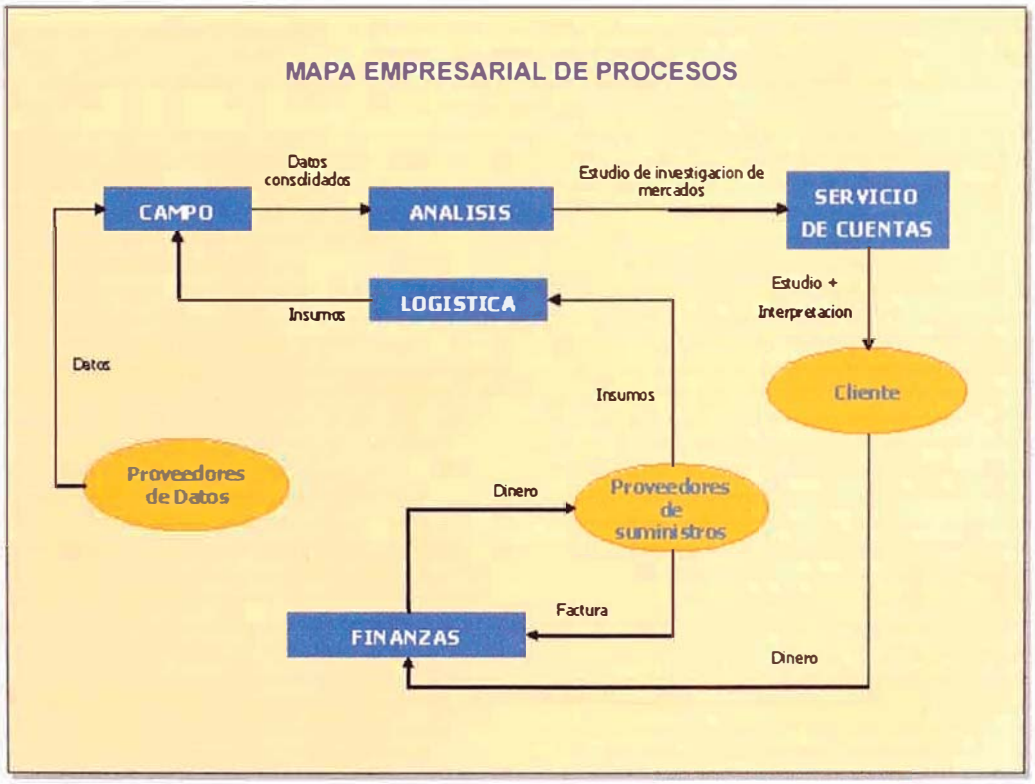
- ✓ Procter&Gamble
- ✓ Química Suiza

2.3. PROVEEDORES

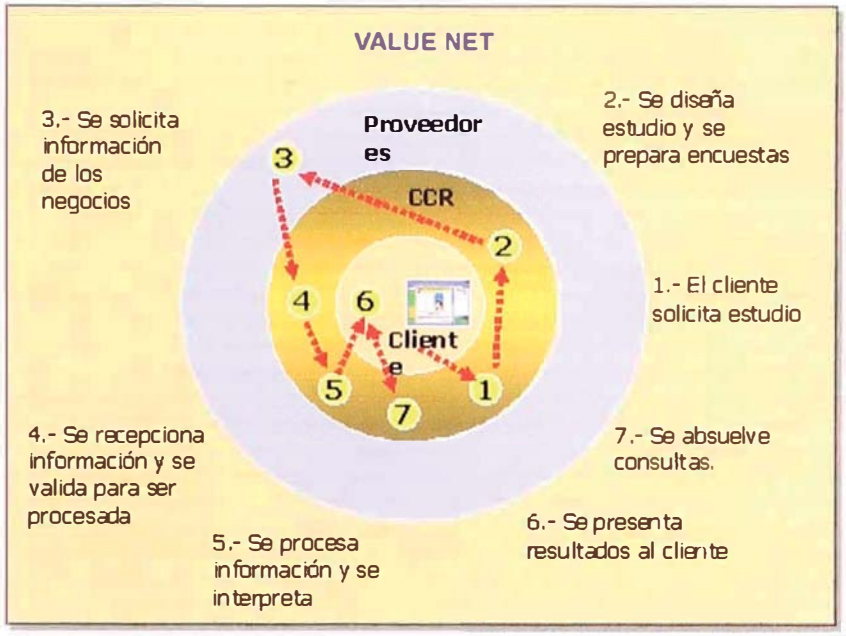
- ✓ Bodegas, kioscos , ambulantes
- ✓ Farmacias
- ✓ Metro, Wong , Santa Isabel , Plaza Vea

2.4. PROCESOS

El gráfico siguiente muestra la interrelación de los procesos y funciones a través de un Mapa de Procesos.



2.4.1. VALUE NET: Las interacciones de XYZ Audit. con sus clientes y proveedores se basa básicamente en el flujo y procesamiento de información:



2.4.2. LA CADENA DE VALOR: la figura nos muestra las actividades primarias que conforman la cadena de valor de XYZ Audit así como las actividades que dan soporte a las mismas.

- **Contrato Y Diseño:** Abarca desde el inicio de las negociaciones con el Cliente hasta la aceptación de la propuesta por el mismo.

El diseño comprende elaborar la encuesta en base los requerimientos del estudio solicitado por el cliente como son evolución de ventas, precios, canales de distribución, etc.

El diseño es preparada por el departamento de Área Técnica en base a técnicas estadísticas, Ej.: Dalenius que permite estratificar o segmentar en función al comportamiento de ventas los negocios.

Una vez dada la aprobación por parte del cliente del contrato y/o diseño, se inicia el proceso de levantamiento de información.

- **Levantamiento De Información:** Abarca todo el proceso de recojo de la información en el campo, supervisión y edición de la misma; pasando después de esta etapa al procesamiento de la información. El levantamiento de información es a través de encuestas preparadas en la etapa de diseño y abarca un conjunto de negocios en función ala muestra definida en el diseño.

  Actualmente estas encuestas se realizan en formatos OMR.

- **Procesamiento, Análisis y Presentación de Resultados**

  Es el proceso donde se realiza la elaboración del producto final, que es el informe o resultado de consolidados de las encuestas realizadas en campo, clasificados jerarquizados, por ciudad, tipo de negocio, año, mes, etc. Estos resultados en cuadros estadísticos presentados en diversos medios (impresos, hojas de calculo y en formato multidimensional- cubos).

La información obtenida en las encuestas es introducida a una base de datos OLTP y luego procesada y cargada a la Base de datos OLAP, generando cubos de información lo desde la cual se genera los informes que serán entregadas al cliente en los diversos formatos.

En el proceso de análisis se verifica la consistencia entre las variables de venta, inventarios y distribución

- **Servicio Post-Venta:** a solicitud del cliente ese presenta una sustentación y análisis de los datos de resultados de l estudio de auditoria.

2.4.3. DESCRIPCION DE ACTIVIDADES POR PROCESOS

PROCESO: CONTRATOS Y DISEÑO

Objetivo

Asegurar que los requisitos establecidos por el cliente se encuentren definidos y XYZ AUDIT tenga la capacidad para satisfacerlos.

Descripción de la Revisión de Contratos

La Gerencia de Auditoria y la Presidencia Ejecutiva son responsables de la revisión de las Cotizaciones, Contratos y Cartas Compromiso antes de su firma para asegurar que:

- ✓ Los requisitos estén definidos y documentados adecuadamente
- ✓ Las diferencias entre los requisitos solicitados por el cliente y lo ofrecido por XYZ AUDIT estén resueltas.

- ✓ XYZ AUDIT tiene la capacidad para satisfacer los requisitos establecidos.

Si durante el periodo de vigencia del servicio de Auditoria de Producto el cliente solicita la modificación de algún requisito establecido, la Gerencia de Auditoria analiza la factibilidad de dicha solicitud, comunicándola de ser aprobada a todas las áreas involucradas.

Se conservan registros de las revisiones y modificaciones de las Cotizaciones, Contratos o Cartas Compromisos.

Procedimiento

Consta de las siguientes actividades principales:

- ✓ Recepción de los requerimientos del cliente
- ✓ Revisión y aprobación de la cotización en XYZ AUDIT
- ✓ Aprobación y/o modificación de la cotización por parte del cliente
- ✓ Elaboración del contrato o carta de compromiso
- ✓ Elaboración del requerimiento del servicio.

Entradas

Requerimiento de servicio realizado por el cliente en forma escrita u oral

Salidas

- ✓ Formato de Requerimiento de Servicio aprobado por el Gerente de División o por el Presidente Ejecutivo, o el Director de Auditoria.
- ✓ Cotización Aprobada

A continuación detallamos cada una de las actividades.

Recepción de los Requerimientos del Cliente

El Ejecutivo de Cuentas, el Director de Auditoría, el Gerente de División o el Presidente Ejecutivo, recepcionan los requerimientos del Cliente en forma escrita u oral:

- ✓ En forma escrita, a través de un documento propio del Cliente enviado vía fax, por mensajería externa o por correo electrónico.

- ✓ En forma oral, ya sea a través de una reunión previamente concertada o a través de una llamada telefónica.

En el caso de que el requerimiento sea solicitado por un Cliente nuevo y recepcionado por el Director de Auditoría, el Gerente de División o por el Presidente Ejecutivo, éste designa al Ejecutivo de Cuentas responsable de elaborar la Cotización.

El Ejecutivo de Cuentas inicia la elaboración de la cotización, haciéndose responsable del envío de la misma al cliente, definición de contrato y memorando de facturación.

Revisión y Aprobación de la Cotización en XYZ AUDIT

Luego de elaborar la Cotización, el Ejecutivo de Cuentas entrega la misma al Gerente de División o al Presidente Ejecutivo o al Director de Auditoría para su revisión. y/o aprobación. Una vez aprobada la Cotización, el Ejecutivo de Cuentas se encarga de enviarla al Cliente.

Aprobación o Modificación de la Cotización por parte del Cliente

El Cliente puede aprobar la Cotización en cualquiera de las siguientes formas:

- ✓ Enviando una Orden de Compra.
- ✓ Enviando una Carta o correo electrónico, donde aprueba a la Cotización de XYZ AUDIT.
- ✓ Enviando la Cotización de XYZ AUDIT firmada, en señal de aprobación.
- ✓ Verbalmente, en cuyo caso el Ejecutivo de Cuentas o el Gerente de División o el Presidente Ejecutivo, señala dicha aprobación firmando y colocando el nombre del representante del Cliente que realizó la aprobación verbal en la copia de XYZ AUDIT.

Si el Cliente no aprueba la Cotización y solicita una revisión de la misma; el Ejecutivo de Cuentas procede a la re-elaboración de la misma y se repiten los pasos anteriores.

Elaboración del Contrato o Carta de Compromiso

El Ejecutivo de Cuentas prepara el Contrato de Suscripción o si el Cliente lo solicita una Carta Compromiso que es firmada por el Representante Legal de XYZ AUDIT.

El Contrato de Suscripción o la Carta Compromiso, es enviado al cliente acompañados de una Carta de Entrega en donde se indica la entrega de dichos documentos, y de ser el caso, se indica también cuáles son los Estudios que se van a

entregar al Cliente a manera de Bonificación, los cuales no figuran en el Contrato de Suscripción o en la Carta Compromiso.

El Ejecutivo de Cuentas es responsable de realizar las modificaciones solicitadas por el cliente en el Contrato de Suscripción o la Carta Compromiso.

Elaboración del Requerimiento de Servicio

Luego de la aprobación de la Cotización por parte del cliente Gerente de División o el Presidente Ejecutivo designa o confirma al Ejecutivo de Cuentas que será responsable del Cliente.

El Ejecutivo de Cuentas elabora rellena el formato de Requerimiento de Servicio, en donde se registra todo lo solicitado por el Cliente.

El Director de Auditoría, Gerente de División o el Presidente Ejecutivo envía al Gerente Administrativo Financiero con copia a la Secretaria de División por correo electrónico el Requerimiento de Servicio aprobado, la Cotización aprobada por el Cliente y el Contrato de Suscripción o Carta Compromiso si el cliente los hubiera firmado para que autorice se proceda a la facturación del Estudio.

Luego el Gerente de División, el Director de Auditoría envía por correo electrónico el Requerimiento de Servicio aprobado, al Gerente de Operaciones, Ejecutivo de Cuentas, y todas áreas involucradas en proceso operativo.

Estudios entregados a manera de Bonificación

Los Estudios que se entreguen al Cliente a manera de Bonificación tienen el mismo tratamiento de un Estudio

comprado por el Cliente, es decir que el Ejecutivo de Cuentas asignado al Cliente, seguirá los pasos descritos en los puntos anteriores, para informar al resto de áreas involucradas para la realización del servicio.

Modificación del Servicio

En el caso de que el Cliente solicite una modificación de las características del servicio, el Ejecutivo de Cuentas, consulta al Gerente de Operaciones, sobre la viabilidad operativa de la modificación solicitada, el Gerente de Operaciones evalúa la misma, y los cambios que signifiquen en la toma de información, proceso o creación de módulos de software, que satisfagan dichas necesidades, comunicando al Ejecutivo de Cuentas el tiempo que se requerirá para desarrollar las actividades necesarias, así mismo comunica al Director de Auditoría, el Gerente de División o al Presidente Ejecutivo, si los cambios solicitados implican aumento de costos solicitando la aprobación de los nuevos requerimientos del cliente.

Si el Gerente de División o el Presidente Ejecutivo aprueban los nuevos requerimientos el Ejecutivo de Cuentas comunica este hecho al Cliente.

Anulación del Servicio

Si por acuerdo con el Cliente se anula el servicio solicitado, el Ejecutivo de Cuentas informa del hecho a través de un correo electrónico al Gerente de División o al Presidente Ejecutivo, quien aprueba dicha comunicación y la envía vía correo electrónico al Director de Auditoría, Gerente de Operaciones y otras áreas involucradas, incluye al Gerente Administrativo Financiero.

Renovación del Servicio

En el transcurso del último mes previo a la culminación del servicio, el Ejecutivo de Cuentas se comunica con el Cliente, ya sea por vía telefónica o mediante una reunión previamente acordada, para negociar la renovación del servicio y las condiciones del mismo. Se elabora una nueva Cotización de acuerdo a lo conversado y acordado con el Cliente.

Una vez finalizada la negociación y aprobado el servicio por parte del Cliente, el Ejecutivo de Cuentas procede registrando los detalles en el formato de Requerimiento de Servicio y comunicando a todas áreas involucradas para el cumplimiento del servicio.

PROCESO: LEVANTAMIENTO DE INFORMACIÓN

Objetivo

Asegurar que la información levantada en campo sea confiable.

Alcance

Levantamiento de información y supervisión de Auditoria y Merchandising de Producto.

Descripción

La medición de campo corresponde a un mes calendario, donde se inicia la primera semana del mes, culminándose durante cualquier día de la última semana del mes. Tanto en Lima como en Provincias.

A diferencia de Lima los Volcados de Provincias se imprimen directamente en la ciudad, dado que reciben de Lima los archivos en formatos de impresión, los siguientes

procedimientos son similares al descrito en este documento. Al culminar la lectura de los volcados se procede a preparar los datos de provincia a archivos compactos que contiene la información digitada para su envío a través de correo electrónico a Lima.

El Jefe de campo es responsable de los Jefes de Zona y Auditores de Mercado de Lima y Provincias.

Procedimiento

Consta de las siguientes actividades principales:

- ✓ Planificación del levantamiento de información
- ✓ Levantamiento de información
- ✓ Supervisión
- ✓ Apertura de variedades
- ✓ Transferencia de la data y corrección de errores
- ✓ Cierre de medición
- ✓ Y las siguientes actividades secundarias
- ✓ Selección de postulantes para auditores de mercado
- ✓ Capacitación

Entradas

Requerimiento de servicio realizado por el cliente en forma escrita u oral, las Especificaciones de producto y la relación de negocios a auditar.

Salidas

Información validada registrada en el sistema para su procesamiento.

Informe por Categoría de la medición.

Planificación del Levantamiento de Información

El Cronograma de Levantamiento de Datos correspondiente a la medición siguiente, se elabora la última semana de cada mes

El Jefe de Campo verifica los requerimientos nuevos y modificados a través del Requerimiento de Servicio que debe estar acompañado de las Especificaciones de Producto y la relación de los negocios a auditar en caso de que sea nuevo.

Estos documentos son entregados por el Área Técnica.

Estas muestra ideales son distribuidos a los Jefes de zona, quienes a su vez distribuyen dichos negocios entre los Auditores de Mercado, indicando las especificaciones a tener en cuenta para el levantamiento de información.

Asimismo, para los productos que no son nuevos los Auditores de Mercado reciben los Volcados, previa revisión:

- ✓ De la impresión de los códigos de: negocio, producto variedad y medición que estén centrados en los casilleros correspondientes. De no estarlo los devuelve al Editor para su reimpresión.
- ✓ Del Volcado, que no presente roturas ni enmendaduras (la lectora óptica puede atracarse). De encontrarse alguna hoja de la volcada rota, el Auditor de Mercado deberá pasar la información a un volcado nuevo.
- ✓ De la impresión, que sea nítida. En caso que la impresión no sea nítida o que tenga demasiada tinta entonces se comunicará al Jefe de Campo para el ajuste del software de la lectora óptica en

Edición y los volcados sean leídos sin ningún problema.

El Auditor de Mercado desglosa el Volcado por distrito y agrupa las hojas desglosadas por código de negocio, adjuntándole los detalles del negocio con la Tarjeta de Identificación del negocio.

El Auditor de Mercado revisa los volcados con la Tarjeta de Identificación.

El Auditor de Mercado verifica que los productos por negocio que están registrados en el formato de Productos Auditados por Negocio estén impresos en los volcados.

El Auditor de Mercado llena el formato Hoja de Salida y Retorno por distrito.

El Jefe de Zona utilizando el formato Productos Auditados por Negocio compara la muestra real levantada en campo con la muestra ideal indicada por el Encargado del Área Técnica y elabora una lista con la cantidad de productos que faltan para completar las cuotas. Asimismo imparte instrucciones verbales a los Auditores de Mercado sobre el levantamiento de información de los productos nuevos y/o modificados.

El Auditor de Mercado confecciona la ruta para el día siguiente teniendo en cuenta:

- ✓ Dirección (sí lo requiere usa el plano de Lima o la guía de calles)
- ✓ Fecha de visita anterior
- ✓ Horario de atención

El Auditor de Mercado procede a llenar el formato Hoja

de Ruta en el orden en que ha de visitar los negocios al día siguiente. La ruta no puede ser alterada en campo a menos que se haya consultado con el Jefe de Zona o el Jefe de Campo previamente. Este orden es importante para el seguimiento o supervisión, en caso de ser necesario.

El Jefe de Zona llena el formato Control de Negocios por Canal de Venta.

El Jefe de Zona recibe las hojas de ruta y selecciona la ruta a supervisar al día siguiente de acuerdo al tipo de supervisión indicado por el Jefe de Campo. Existen 4 tipos de supervisión:

- ✓ Supervisión Coincidental, consiste en dar el encuentro al Auditor de Mercado en el primer negocio señalado en su hoja de ruta. El Jefe de Zona evalúa el desempeño del Auditor de Mercado en campo, corrige errores que haya detectado en la información tomada por el Auditor de Mercado y enseña la mejor forma de obtener los datos requeridos. La selección del Auditor de Mercado a supervisar se realiza a criterio del Jefe de Zona, de acuerdo con el desenvolvimiento del Auditor de Mercado, observado durante la medición
- ✓ Supervisión aleatoria, consiste en verificar en campo los datos levantados en los volcados ya realizados por el Auditor de Mercado. La selección de los volcados es aleatoria. La selección de los volcados a supervisar la realiza el Jefe de Zona abarcando durante el mes a todos los Auditores de Mercado a su cargo. Para ello se guía del Registro de Supervisiones.

- ✓ Supervisión por Edición, consiste en supervisar aquellos volcados que durante la primera revisión realizada por los Jefes de Zona le son detectadas incoherencias o anomalías en la toma de información. También se considera dentro de este tipo de supervisión, las que se realizan a los negocios que contienen datos atípicos mostrados en los listados de Control de Errores y Atípicos por Encuestas-SIA.
- ✓ Supervisión por Análisis.-Consiste en efectuar la supervisión de acuerdo a los requerimientos señalados por los Analistas de acuerdo a la Solicitud de Supervisión por Análisis.

Levantamiento de Información

El Auditor de Mercado sale a campo en la mañana y recorre los negocios de acuerdo a la ruta diseñada sin alterarla. Toma la información en los volcados (siguiendo los pasos especificados en las instrucciones de Toma de Información en el Volcado).

El Jefe de Zona realiza la supervisión coincidental a los Auditores de Mercado seleccionados previamente. Si el Jefe de Zona tuviera otro tipo de supervisión adicional a la coincidental, acompaña al Auditor de Mercado hasta una hora predeterminada y luego procede a empezar la siguiente supervisión.

El Auditor de Mercado se presenta a la oficina de XYZ AUDIT en la tarde y marca en los casilleros correspondientes del Volcado donde se indica el tipo de supervisión realizado y el código del supervisor. Actualiza el formato Productos

Auditados por Negocio con la debida autorización del Jefe de Zona:

- ✓ Agrega los negocios contratados durante el día.
- ✓ Borra los negocios anulados durante el día.
- ✓ Agrega los productos incluidos a negocios durante el día.
- ✓ Elimina los productos que ya no se debe auditar en los negocios.

Supervisión

El Jefe de Zona se presenta a la oficina de XYZ AUDIT en la tarde y llena el Informe Diario acerca de lo acontecido en campo durante el día.

El Jefe de Campo recibe diariamente el Informe Diario, y si considera conveniente conversa con el Auditor de Mercado. Es responsable de evaluar el porcentaje de supervisión alcanzado durante el mes y el cumplimiento de los objetivos de supervisión mensual.

Para la obtención del porcentaje de supervisión se utiliza el formato Registro de Supervisiones, lo cual es llenado por los Jefes de Zona diariamente y el total de negocios auditados que se obtiene a través del formato de Salida y Retorno

El Jefe de Zona recibe los volcados de los negocios auditados durante el día, los revisa y anota en el formato de Salida y Retorno.

El Jefe de Zona recibe también los Volcados de los negocios muertos o dejaron de atender definitivamente a XYZ AUDIT, los negocios que cambiaron de rubro, los que no quisieron o pudieron atender temporalmente por diferentes

motivos, lo cual debe ser registrado en el formato de Salida y Retorno.

El Jefe de Zona revisa el Volcado marcado en su totalidad, de la siguiente forma:

- ✓ Revisa que el código del negocio esté marcado en el volcado.
- ✓ Si no estuviera marcado, verifica si se trata de un "Contrato de Negocio".
- ✓ Si no es un "Contrato de Negocio", devuelve el volcado al Auditor de Mercado para que lo marque.
- ✓ Si es un "Contrato de Negocio", el Jefe de Zona procede a ingresar los datos al sistema como se especifican en las instrucciones de registro de Contratación de Negocios.
- ✓ Revisa el contenido del volcado: compras, inventario, precios.
- ✓ Si detecta alguna incoherencia o anomalía en el contenido del volcado, separa los volcados en el fólder de supervisiones y verifica al día siguiente en campo los datos tomados por el Auditor de Mercado, con una supervisión por edición.
- ✓ Revisa que el volcado esté totalmente codificado: código de producto y código de variedad.
- ✓ Si hay variedades en el volcado que no están codificadas entonces revisa el Directorio de Variedades nacional de la fecha y verifica si tiene código dicha variedad.
- ✓ Si tiene código, se lo devuelve al Auditor de Mercado para que lo codifique. Si no tiene código se hace la apertura de la nueva variedad nueva

de acuerdo al procedimiento de Apertura de Variedades.

Mensualmente los Jefes de Zona elaboran un Informe por Categoría en que se refleja las promociones nuevas, variedades que se hayan percibido más en el período de levantamiento de información, este informe es remitido a los Analistas.

Apertura de Variedades

Se hace cuando se encuentran Volcados que no tiene codificado el código de Variedad. Lo cual es separado por los Jefes de zona.

Se hace la Verificación o confirmación de estas variedades en el mismo negocio donde se encontraron las nuevas variedades.

Si la variedad no existe, el Jefe de Zona determina a que variedad pertenece realmente los datos tomados y se le devuelve al Auditor de Mercado para que corrija el marcado.

Si la variedad existe, el Jefe de Zona llena el formato de Apertura de Variedades y se lo entrega al Editor.

El Editor recibe el formato Apertura de Variedades y consulta con el Ejecutivo de Cuentas o el Analista encargado del producto si es que tuviera dudas sobre alguno de los datos de la apertura.

El Editor asigna códigos a las aperturas de variedades, para ser ingresados al sistema de acuerdo a los atributos indicados al inicio del proceso.

Luego el Editor entrega los códigos de las aperturas a

los Jefes de Zona para que procedan al marcado del volcado.

Finalmente el Jefe de Zona coloca todos los volcados que incluyen Contratos, aperturas, etc. previamente codificado y revisado en la lectora óptica para su lectura.

Transferencia de la Data y Corrección de Errores

Los datos leídos en bloques de 200 hojas de volcado se almacenan en un archivo tipo texto (formato de salida de la Lectora Óptica), lo cual es transferido a una base de datos DBF para que posteriormente se efectúe el procesamiento de la data.

Luego de la transferencia, el Jefe de Zona imprime el listado de Control de Errores y Atípicos por Encuestas-SIA. Detectados por el Sistema de Auditoria.

Con el Control de Errores y Atípicos por Encuestas-SIA, el Jefe de Zona, separa el Volcado de la siguiente forma:

- ✓ De Acuerdo al listado se separa los volcados con errores EC y ATIP (EC: Errores de consistencia y ATIP: Errores por Atípico).
- ✓ En los volcados que tienen errores de Atípicos el Jefe de Zona las líneas con dichos datos y los circula con un lapicero rojo.
- ✓ Si indica error de consistencia y atípico al mismo tiempo significa que existen errores de consistencia y atípicos simultáneamente, por lo que el Jefe de Zona separa el Volcado y circula con lapicero rojo los productos y líneas señaladas con datos atípicos.
- ✓ Los volcados con EC. Se corrigen en el sistema y separa los Volcados con datos atípicos ATIP para

ser supervisados en campo de acuerdo al tipo de supervisión preestablecido.

Cierre de Medición

El Jefe de Campo comunica al Jefe de Operaciones y Jefe de Análisis que la lectura, correcciones y supervisiones de la medición fueron terminadas.

Luego del cierre el Editor procede a imprimir los Volcados para la siguiente medición, tomando como base la medición acabado de cerrar.

Selección de Postulantes para Auditores de Mercado

El Jefe de Campo solicita al Jefe de Operaciones convocar personal para Auditores de Mercado, quien a su vez comunica al Gerente de División.

El Jefe de Campo entrega la Ficha de Datos Personales a los postulantes para que llenen sus datos. Realiza una charla con todos los postulantes, después solicita: que los que están de acuerdo con las condiciones de trabajo continúen en la selección. Siendo este el primer filtro.

Los interesados entregan al Jefe de Campo la Ficha de Datos Personales debidamente llenado y su currículum vitae para luego citarlos a la entrevista personal.

El Jefe de Campo revisa los curriculums, los selecciona, luego convoca a una entrevista personal. El jefe de Campo de acuerdo a la entrevista elige un grupo de personas para su posterior capacitación.

Capacitación

El Jefe de Campo o el Jefe de Zona designado por el Jefe de campo, se encarga de realizar la capacitación de los postulantes durante cuatro días. En la tarde del cuarto día los postulantes realizan una prueba piloto.

El quinto día el Jefe de Campo o el Jefe de Zona designado por el Jefe de campo toma un examen teórico de todo lo enseñado durante la capacitación en el Examen.

El Jefe de Campo califica el examen, siendo contratados aquellos que alcancen las mayores calificaciones.

Luego el Jefe de Campo envía el formato Ficha de Datos Personales de los seleccionados al Jefe de Recursos Humanos, previa probación del Jefe de Operaciones.

Todos los contratados son asignados por el Jefe de Campo a una zona determinada a cargo de un Jefe de Zona, quien se hace responsable del aprendizaje en campo del Auditor de Mercado y de levantar la información acompañado del nuevo a fin de reforzar su aprendizaje.

Si el Jefe de Zona determina que el Auditor de Mercado nuevo está apto para realizar las entrevistas sólo, éste empieza a realizar las encuestas a los negocios diariamente. De lo contrario continúa saliendo a campo con un Auditor antiguo por aproximadamente 3 días más, después de los cuales se vuelve a evaluar al Auditor.

El Auditor de Mercado nuevo es supervisado constantemente por el Jefe de Zona para asegurarse el buen levantamiento de información.

El Jefe de Campo sale a campo para supervisar a los

Jefes de Zona y Auditores de Mercado en cualquier momento durante la medición.

PROCESO: PROCESAMIENTO, ANÁLISIS E INFORME FINAL

Objetivo

Generar y emitir los Informes de Auditoria de Producto, de acuerdo a los requerimientos de los clientes, transformando la información de campo en cuadros estadísticos.

Verificar que la Información sea de buena calidad y culminada oportunamente.

Procedimiento

Consta de las siguientes actividades principales:

- ✓ Procesamiento de la información
- ✓ Validación de los cuadros estadísticos
- ✓ Revisión del informe final
- ✓ Envío del informe final al cliente
- ✓ Y las siguientes actividades secundarias
- ✓ Presentación y sustento oral del informe final
- ✓ Solicitud de fax y/o información de la data de XYZ AUDIT

Entradas

- ✓ Información validada registrada en el sistema para su procesamiento
- ✓ Requerimiento de Servicio
- ✓ Especificaciones del Producto

Salidas

- ✓ Informe final escrito o en medio magnético

- ✓ Sustento de resultados con documentos y gráficos

Procesamiento de la Información

Cada inicio de medición, con la información de los Requerimientos de Servicio, el Jefe de Análisis comunica al Jefe de Operaciones y Logística la Relación de Despacho de Informes Finales.

El Jefe de revisa y actualiza el cronograma de actividades distribuyendo las categorías de productos, de acuerdo a la complejidad de la Categoría y los requerimientos del Cliente.

De acuerdo a la asignación de las Categorías de Producto, el Analista Encargado procede a realizar el procesamiento de la Información utilizando el Sistema de Auditoria, generando de esta manera los Cuadros Estadísticos.

En el caso de nuevos productos se procede a verificar si los procesos concuerdan con lo especificado en los Requerimiento de Servicio y las Especificaciones del Producto entregado por Área Técnica.

Si algún requerimiento no se ajusta a los estándares de cuadros estadísticos que contempla el sistema de auditoria, se procede a realizar un requerimiento de desarrollo y al Área de Desarrollo de Sistemas, para que se realice el ajuste del Sistema de Auditoria, siempre en cuando sea conveniente.

Validación de los Cuadros Estadísticos

El procedimiento de validación de la información de los cuadros estadísticos, consiste en verificar:

- ✓ Para productos nuevos: Verificar Universos, Estratos, muestra real de procesamiento debe ser aproximado al Ideal. De encontrarse diferencias con la hoja de Especificaciones de producto, se procede a informar a Área Técnica o Jefe de Campo según corresponda, para que éste realice las correcciones pertinentes.
- ✓ En los productos ya existentes: Que los universos de producto sean iguales a los utilizados en procesos anteriores y que haya coherencia en la estratificación de la muestra por canal de venta con relación a la estratificación histórica. Si hubiera cambios, este debe estar sustentado en los documentos de especificaciones de producto o requerimiento de servicio.

La correlación entre las variables de ventas, inventarios y distribución; de encontrarse incoherencias se procede a ubicar los datos de cada uno de los negocios que genera la incoherencia, de ser necesario se ubican los volcados para poder determinar la causa del problema, que podría ser:

- ✓ Mal sombreado del Volcado.
- ✓ Sobrepasar el recuadro que se debe de marcar.
- ✓ Calibración de la Lectora óptica.
- ✓ Verificación de Atributos de las Variedades
- ✓ Verificación de los factores de conversión
- ✓ Verificación de las unidades de procesamiento.

Si no se ubica el origen del problema, se procede a solicitar a Campo una Supervisión por Análisis.

Una vez finalizada la supervisión por análisis, el Jefe de

Campo entrega al Analista Senior, vía correo electrónico, el Informe de Resultados de la Supervisión por Análisis.

El Analista Encargado, con el resultado de la supervisión por análisis corrige la información y la reprocesa con los datos correctos

Revisión del Informe Final

El Jefe de Análisis revisa los Informes Finales elaborados por cada Analista asegurándose de que:

- ✓ Exista coherencia en la información.
- ✓ Se cumpla con Requerimiento de Servicio.
- ✓ En el caso de haber errores se procede a ubicar al Analista Encargado de la categoría para su respectiva revisión.

De ser necesario, el Analista Encargado reprocesa la información, y emite un nuevo Informe Final, el cual es sometido a una nueva revisión por parte del Jefe de Análisis.

Si esta Conforme, el Analista Encargado procede a imprimir el Informe Final.

El Jefe de Operaciones es responsable de controlar el avance de los Informes Finales a fin de asegurar que se cumpla con las fechas de entrega pactadas con el Cliente.

Envío del Informe Final al Cliente

Envío del Informe Final Impreso o en Medio Magnético:

- ✓ Se entrega los informes Finales impresos al Editor para que lo anille.
- ✓ Luego el Editor entrega los informes anillados al Ejecutivo de Cuentas del cliente para su revisión.

- ✓ En caso de estar conforme, el Editor confecciona la Carta de Cargo hace firmar al Ejecutivo de Cuentas responsable del Cliente, o en su ausencia, el Jefe de Operaciones o el Gerente de División
- ✓ El editor prepara un sobre conteniendo la Carta de Cargo, el Informe Final y en caso de que el cliente haya solicitado también la entrega del informe por medio magnético, se acompaña el Disquete correspondiente.
- ✓ Luego el editor procede a entregar el sobre a Logística previo registro de su entrega.
- ✓ El Jefe de Logística designa un mensajero para que la entrega del sobre llegue en óptimas condiciones al Cliente.
- ✓ Una vez realizado la entrega al cliente, el Jefe de Logística actualiza su registro de Relación de Despacho de Informes Finales, el cual también esta compartido por los Ejecutivos de Cuenta, y el Jefe de Operaciones para que puedan acceder al mismo e informarse sobre el estado de entrega de los "Informes Finales".

Envío del "Informe Final" en Medio Magnético:

- ✓ Si el Requerimiento de Servicio, solicita se entregue la información del "Informe Final" en medio magnético a través de Disquete o correo electrónico, el Ejecutivo de Cuentas ubica el archivo que dio origen a la impresión del Informe Final, a fin de copiar a un disquete o él envió por correo
- ✓ Envío por Disquete; En este caso, el Ejecutivo de

Cuentas graba el archivo en un disquete y lo entrega al Editor, para que éste sea enviado junto con el "Informe Final" impreso.

- ✓ Envió por Correo Electrónico; En este caso el Ejecutivo de Cuentas envía el "Informe Final" al Cliente directamente con copia a la Secretaria de Gerencia, a fin de que mensualmente se imprima el listado de los Informes Finales enviados por Correo Electrónico al Cliente.

Presentación y Sustento oral del "Informe Final"

La presentación y sustento oral del Informe Final, es responsabilidad de los ejecutivos de Cuentas responsables por cada cliente, es necesario antes de ello se revisen los Informes por Categoría de Producto del último periodo, elaborados por los Jefes de Zona, así mismo la elaboración de los gráficos o presentaciones en Power Point a fin de que el sustento sea claro y quede constancia del mismo.

La presentación puede realizarse en las instalaciones de XYZ AUDIT o de la empresa del cliente, previa coordinación y programación del mismo.

Finalizada la presentación del "Informe Final", el Ejecutivo de Cuentas hace entrega al Cliente de una copia impresa o en medio magnético de la presentación realizada.

Solicitud de Fax y / o información de la data de XYZ AUDIT

Además, de los informes Finales estipulados en el contrato, XYZ AUDIT también puede proveer información adicional o parcial de la Auditoria de Producto:

- ✓ De la información contratada, si el cliente solicita

algún o algunos cuadros específicos ya sea como informe o gráficos, el ejecutivo de cuentas tiene la responsabilidad de extraerlos o elaborarlos para su envió vía fax o correo electrónico.

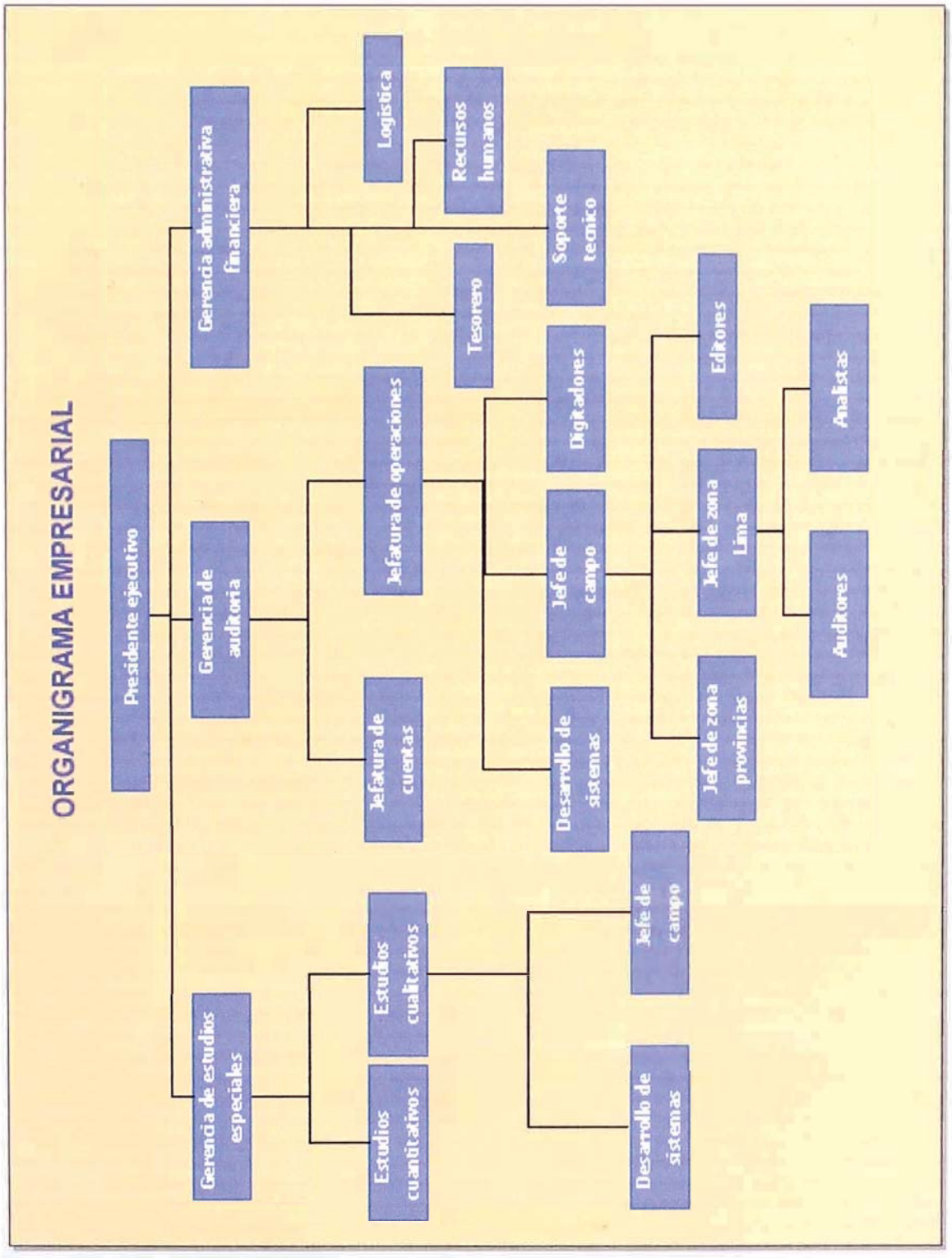
- ✓ Información solicitada por un No Cliente, previa aprobación al Gerente de División o al Presidente Ejecutivo, el Ejecutivo de cuentas extrae o elabora a partir del Banco de datos de XYZ AUDIT para ser enviado por fax o por correo electrónico
- ✓ Avance de Venta:
- ✓ Si el pedido del cliente es un "Avance de Ventas", este debe ser elaborado o preparado por el Ejecutivo de Cuentas en coordinación con el Analista del Producto y el Jefe de Análisis. Luego, previa aprobación del Gerente de División o al Presidente Ejecutivo, la Secretaria de Gerencia prepara el envío por fax del Avance de ventas, el cual es firmado por el Gerente de División o por el Presidente Ejecutivo.

2.5. ORGANIZACIÓN DE LA EMPRESA

El organigrama de XYZ AUDIT IR, nos muestra a la cabeza de la compañía al Presidente Ejecutivo, quien es el principal accionista de la empresa. Debajo de él se encuentran tres gerencias Estudios Especiales, Auditoria y Administrativa Financiera.

La Gerencia Administrativa Financiera, es una gerencia de apoyo de las otras dos, las cuales funcionan como negocios independientes y en cierta medida replican funciones. En la, se muestra el organigrama actual de XYZ AUDIT IR. No existe un área

de sistemas corporativo, las gerencias de Estudios Especiales y de Auditoria, cada una de ellas tiene su propia área de sistemas, las cuales efectúan los requerimientos propios de la gerencia.



CAPITULO II
MARCO TEORICO

1. RETAIL AUDIT.

El Retail Audit es una herramienta de información de mercados que ha demostrado ser eficaz en el seguimiento y control de las estrategias de comercio al por menor o retail de las compañías.

El Retail Audit es útil para establecer:

- ✓ Tamaño del mercado, segmentación y evolución
- ✓ Fortalezas y debilidades en distribución por área y tipo del punto de venta
- ✓ Posicionamiento y valuación de marcas
- ✓ Market share
- ✓ Oportunidades de precio
- ✓ Ventas y Compras (volumen y valor)
- ✓ Inventarios en poder de los detallistas (bodega y área de venta)
- ✓ Abastecimiento (Rotación)
- ✓ Precio promedio de venta al consumidor
- ✓ Distribución numérica y ponderada
- ✓ Agotamiento numérico y ponderado.
- ✓ Promedio de ventas e inventario por tiendas
- ✓ Distribución de ofertas de material publicitario y exhibidores preferenciales

En otras palabras, es una buena forma para evaluar las tendencias del mercado haciendo una comparación producto a producto y marca a marca en los puntos de venta.

Las principales características del Retail Audit son:

- ✓ Acompañamiento minucioso del desempeño de las ventas de un producto dentro de la categoría del producto estudiado en un punto de venta.
- ✓ Posibilita la selección de lugares representativos, en términos de uso del producto y perfil poblacional dentro del punto de venta.
- ✓ Permite la determinación de costos, tamaños de los diferentes espacios de un punto de venta para la ubicación de productos y líneas de producto.

En términos generales, la auditoria de Retail ofrece resultados con altas dosis de precisión y comparabilidad para la toma de decisiones específicas en los ámbitos de: producto (características, diseño, empaque), comunicación (merchandising, publicidad, promoción), precio y distribución o un agregado de los cuatro.

El primer paso del Retail Audit consiste en analizar el flujo de distribución del producto, analizando toda la cadena desde el productor hasta el consumidor final, las preguntas que se deben realizar quiénes pretendan hacer una auditoria de este tipo son: ¿Dónde se vende el producto? se tienen puntos de venta propios, se trabaja mediante minoristas, se comercializa en las grandes cadenas de almacenes. ¿Qué es lo que se vende del producto? se vende su marca, sus características, su tecnología, su diseño. ¿Por cuánto se vende el producto? Cuál es el precio de venta al por menor en el punto de venta, cuánto es el margen del productor, cuál el margen del minorista.

Las desventajas más reconocidas son:

- ✓ Altos costos de realización
- ✓ Consume mucho tiempo
- ✓ La dirección puede no acatar sus resultados con lo cual quedaría sin piso
- ✓ La información recolectada puede ser inapropiada

Retail Audit es un servicio diseñado para ayudar a las compañías a administrar sus canales de distribución más efectivamente con información con alto nivel de profundidad y precisión acerca de sus productos y los productos de sus competidores. Provee datos críticos y ayuda hacia las respuestas correctas de las siguientes preguntas:

- ✓ ¿Porque los usuarios finales de sus productos pagan diferentes precios?
- ✓ ¿Pueden disparase los precios si afectar la demanda?
- ✓ ¿Cuál es el impacto de las estrategias de promoción y publicidad?

Consideremos el escenario del gráfico que se encuentra debajo, con un revendedor y tres tiendas para cuatro usuarios finales y tiendas, esta compañía tiene un limitado conocimiento de cómo su productos es distribuido. Mas importante, la estructura de precios dentro de la red de distribución son dispares, y el real impacto de los recursos de marketing, como son promoción y publicidad, son desconocidos.

Retail Audit provee a las compañías con un continuo flujo de información acerca de los movimientos de sus productos en el mercado. Con tales conocimientos, usted puede:

- ✓ Seguir las ventas totales mas exactamente.
- ✓ Corregir las insuficiencias en la estructura de precios a través de su cadena de distribución.
- ✓ Evaluar y ajustar estrategias de ventas y marketing.

2. INTELIGENCIA DE NEGOCIOS

Algo peor que no tener información disponible es tener mucha información y no saber qué hacer con ella. La Inteligencia de Negocios o Business Intelligence (BI) es la solución a ese problema, pues por medio de dicha información puede generar escenarios, pronósticos y reportes que apoyen a la toma de decisiones, lo que se traduce en una ventaja competitiva. La clave para BI es la información y uno de sus mayores beneficios es la posibilidad de utilizarla en la toma de decisiones. En la actualidad hay una gran variedad de software de BI con aplicaciones similares que pueden ser utilizados en las diferentes áreas de la empresa, tales como, ventas, marketing, finanzas, etc. Son muchas las

empresas que se han beneficiado por la implementación de una sistema de BI, además se pronostica que con el tiempo se convertirá en una necesidad de toda empresa.

La Inteligencia de Negocios se puede definir como el proceso de analizar los bienes o datos acumulados en la empresa y extraer una cierta inteligencia o conocimiento de ellos. Dentro de la categoría de bienes se incluyen las bases de datos de clientes, información de la cadena de suministro, ventas personales y cualquier actividad de marketing o fuente de información relevante para la empresa.

BI apoya a los tomadores de decisiones con la información correcta, en el momento y lugar correcto, lo que les permite tomar mejores decisiones de negocios. La información adecuada en el lugar y momento adecuado incrementa efectividad de cualquier empresa.

Inteligencia de Negocios es una manera de manejar la información histórica de una empresa a través de la construcción de Bodegas de Datos o Data Warehouses y explotarla con fines de análisis y para la mejor toma de decisiones. A través de la creación de modelos de información multidimensionales una organización puede beneficiarse al conocer de mejor manera cómo su negocio se ha comportado a lo largo del tiempo, cómo se comporta en el presente y cómo se estima se comportará en el futuro.

Con BI se puede:

- ✓ Generar reportes globales o por secciones
- ✓ Crear una base de datos de clientes
- ✓ Crear escenarios con respecto a una decisión
- ✓ Hacer pronósticos de ventas y devoluciones
- ✓ Compartir información entre departamentos

- ✓ Análisis multidimensionales
- ✓ Generar y procesar datos
- ✓ Cambiar la estructura de toma de decisiones
- ✓ Mejorar el servicio al cliente

3. DATA WAREHOUSE

Es el proceso de organizar la información en una forma que crea conocimiento basado en datos. Los productos de software que presentan este conocimiento a los usuarios se llaman a veces Herramientas de Inteligencia de Negocios (Business Intelligence Tools).

Un data warehouse es una herramienta para almacenar y analizar información numérica.

A continuación listamos seis requerimientos críticos para un almacén de Datos (Datawarehouse):

- ✓ La recuperación del almacén debe ser rápida.
- ✓ Los valores almacenados deben ser internamente consistentes
- ✓ Los usuarios deben poder rebanar y cortar en cubitos - Esto es, extraer un solo articulo(rebanar) y comparar artículos en una tabla cruzada-tabulada(cortar en cubitos)
- ✓ Un Almacén debe incluir herramientas de navegación fáciles para usar.
- ✓ El Almacén de datos debe ser completo y confiable
- ✓ Calidad de datos almacenados requiere calidad de procesos de recolección de datos.

3.1. Propósito.- Un Data Warehouse almacena valores de datos estables y verificados. Es muy útil comparar una base de datos warehouse

con una transaccional:

- ✓ Una Base de transaccional ayuda a las persona realizar actividades, y un datawarehouse ayuda a la gente tomar decisiones.
- ✓ Un Base de datos transaccional es volátil, su información cambia constantemente; Un datawarehouse es estable, la información es actualizada a intervalos estándares.
- ✓ Una Base de transaccional se centra sobre los detalles, un Data Warehouse se centra sobre agregaciones de alto nivel.
- ✓ Una Base de datos transaccional típicamente provee de valores de datos que son luego almacenados en un datawarehouse.

CAPITULO III
PROCESO DE TOMA DE DECISIONES

1. SITUACION ACTUAL:

Este año se termino la migración del sistema de procesamiento de datos para los estudios de Auditoria de Sistema.

El producto final de los estudios de auditoria es el informe o resultado estadísticos consolidados presentados al cliente en diversos formatos:

- ✓ **Impreso:** Son informes impreso entregados a los clientes como resultado de los estudios de Auditoria, estos reportes son tediosos de analizar por los ejecutivos de las empresas cliente.

- ✓ **Hojas de Calculo:** Los reportes en hojas de calculo son preferentemente hechos en Microsoft Excel, aquí hay que diferenciar los informes entregados en versiones de Excel 97 y anteriores y en versiones del Excel 2000 y XP. El uso de uno u otra versión del Excel dependen de las licencias respectivas que tenga el cliente.

- ✓ **Cubos:** Se entrega a los clientes cubos de datos para que lo carguen en sus sistemas de gestión de base de

datos y lo puedan analizar a través de algún programa de análisis instalada en sus empresas.

2. PLANTEAMIENTO DEL PROBLEMA:

Si analizamos la visión podemos encontrar que para mantener el liderazgo de mercado, es necesario cumplir con los siguientes 2 grandes objetivos:

- ✓ Información veraz y oportuna.
- ✓ Satisfacción de las necesidades de los clientes de XYZ Audit.

El 90% de clientes de XYZ Audit reciben los resultados de sus estudios de Auditoria en formato impreso y en Excel 97, ya que no cuentan con licencias de herramientas de análisis mas avanzadas.

Cada formato en la que los clientes reciben sus estudios de auditoria presenta diversas deficiencias.

En cualquier de estos formatos en que se entregan los informes de Auditoria de negocios el cliente no cuenta con información en actualizada en tiempo real, solo recibiendo información en intervalos periódicos, sin poder hacer seguimiento diarios a sus estudios de auditoria.

Además de no contar con una herramienta en la que pueda analizar esta información desde cualquier lugar, en cualquier momento y sin tener licencias de alguna herramienta propietaria.

A continuación presentamos algunos problemas a las que los de las empresas clientes se enfrentan al recibir los informes de auditoria de negocios en los diversos formatos:

✓ **Impresos:**

- Análisis tedioso
- Demasiado uso de papel

✓ **Informes en Excel 97:**

- La información esta presentada en forma estática.
- Los usuarios no pueden realizar análisis multidimensional con las opciones de corte y rotación (slice and dice) y exploración en cualquier dimensión (drill- anywhere).

✓ **Informes en Excel 2000-XP:**

- Permite análisis multidimensional, pero los principales clientes no disponen de las licencias respectivas.
- No permite guardar las iteraciones realizadas por los clientes en los informes.
- No permite compartir información con otros usuarios fácilmente.

✓ **Cubos:**

- Involucra licencia para el servidor OLAP en el servidor del cliente
- Requiere de una herramienta de acceso a la información residente en el servidor OLAP

3. ALTERNATIVAS DE SOLUCIÓN:

Para lo solución a esta problemática se planteo el uso de una herramienta Web basada en tecnología Web.

Hacer que un almacén de datos sea accesible desde el Web entraña varios beneficios. Por ejemplo, las interfaces Web constan de clientes livianos, poco exigentes en cuanto a los requerimientos de hardware, frecuentemente menores a. los de sistemas de escritorio comunes.

El uso de una herramienta Web OLAP reduce significativamente el esfuerzo que implica la instalación y el mantenimiento de software cliente, tal como en el caso de las herramientas DSS y el software intermedio para bases de datos.

XYX Audit evaluó la compra de una herramienta Web OLAP suministrada por algún fabricante de software o desarrollar una herramienta personalizada.

El mercado ofrece una amplia gama de herramientas que soportan la ejecución y envío de resultados de lotes hacia el ambiente Web. Estos productos incluyen a Business Objects Document, Agent Server, Brio Enterprise Server, Information Builder WebFocus, IQ Soft ware IQ/LiveWeb, Oracle Reports y Sea gate Crystal Reports y Crystal Info. Otros dos productos nuevos para envío de da tos sobre el Web dignos de mención son MicroStrategy DSSBroadcaster y VIT de liveryManager.

En el cuadro hacemos una breve descripción de algunas de estas herramientas.

Empresa	Herramienta OLAP Web	Descripción
Business Objetcs	Web Intelligence	Solución para entornos Web que permite a los usuarios acceder, analizar y compartir los datos corporativos a través de un navegador. Gracias a esta herramienta se elimina la necesidad de instalar el software en el puesto del cliente y el mantenimiento del mismo
BG&S	Panorama Nova View e-B I	Tercera generación de la solución Nova View, un front-end diseñado para aprovechar las funciones de SQL Server 2000 y Analysis Services de Microsoft. Dado que es un producto de usuario final, éste puede acceder directamente a la información crítica de la empresa desde entornos Web o redes de área local.
Cognos	Cognos Series 7	Software analítico que ofrece un amplio abanico de funciones BI, desde la capacidad para confeccionar informes avanzados hasta la elaboración de consultas o la creación de data marts. Asimismo incluye un entorno Web único y permite gestionar el rendimiento corporativo desde un

		portal central.
Information Builders	WebFocus Reporting Server	Aplicación que permite realizar informes y análisis a partir de cualquier dato y sobre cualquier plataforma o estructura de ficheros generando contenidos en HTML, DHTML, XML, Excel y PDF, tanto para navegadores web como dispositivos inalámbricos. También incorpora un lenguaje específico para aplicaciones financieras que posibilita la creación y cálculo de datos relacionados.

Una evaluación mas detallada sobre estas herramientas OLAP se vera en el Anexo 1(Evaluación herramientas OLAP).

Esta evaluación se hace evaluando las siguientes características:

- ✓ Funcionalidad usuario final
- ✓ Construcción del modelo del negocio
- ✓ Poder analítico avanzado
- ✓ Soporte Web
- ✓ Administración
- ✓ Adaptabilidad
- ✓ Ejecución afinada
- ✓ Personalización

4. METODOLOGÍA DE LA SOLUCIÓN

El uso de una metodología de gestión de proyectos nos ayudó a

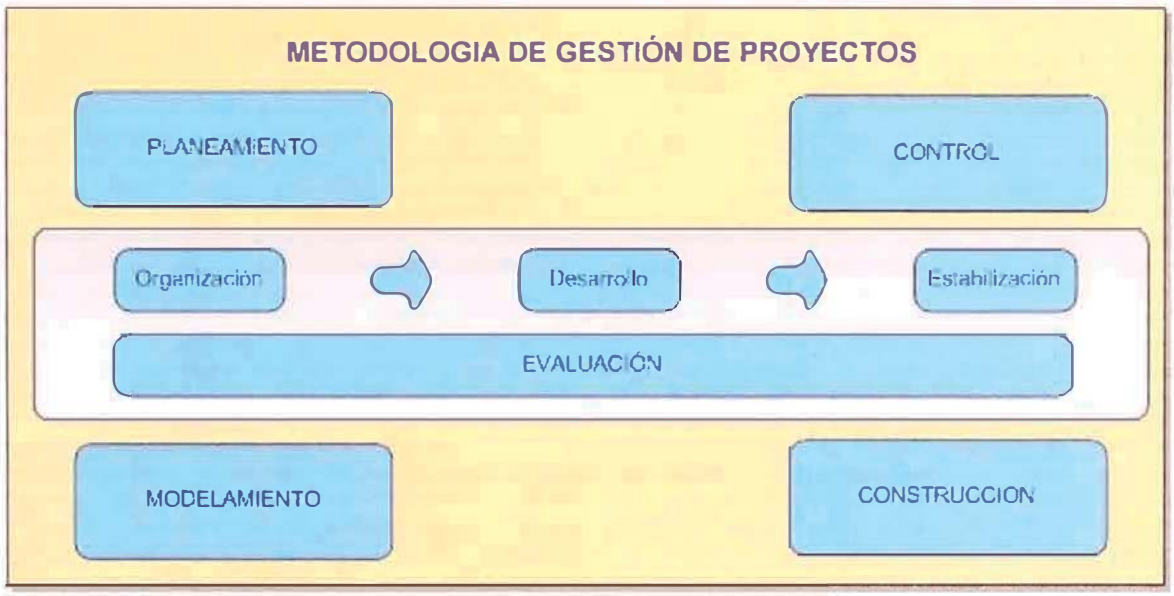
obtener un buen resultado del mismo. En este proyecto se uso una metodología resultado de la combinación de otras. Esta metodología constaba de 4 fases para la gestión del proyecto:

- ✓ **Organización**. Representa todo aquello que hay que hacer antes de iniciar el proyecto.
- ✓ **Desarrollo.** Representa la ejecución del proyecto, desde el inicio del desarrollo hasta la puesta en producción.
- ✓ **Estabilización.** En esta fase se efectúan las mejoras al proyecto que se ha puesto en producción.
- ✓ **Evaluación.** Representa la fase en que se determina si se están cubriendo todos los elementos necesarios para iniciar, continuar, y/o culminar el desarrollo. No se da exactamente después de la estabilización, sino que se dio a lo largo del desarrollo.

A su vez cada una de estas fases contiene cuatro dimensiones, que son:

- ✓ **Planeamiento,** por ejemplo: elaboración del cronograma de trabajo.
- ✓ **Control, por ejemplo:** aprobación del plan de proyecto.
- ✓ **Modelamiento**
- ✓ **Construcción**

Las dos primeras dimensiones implican la gestión y las dos últimas la ejecución.



A continuación mostramos el modelo integral que se uso para el desarrollo de la solución Web.

Como podemos observar existen 7 fases que se llevaron a acabo para el desarrollo del Sistema:

F1: Análisis Preliminar / Determinación de Requerimientos.

- ✓ Levantamiento de Información Inicial.
- ✓ Establecer la Problemática Existente.
- ✓ Determinar las Necesidades de Información.
- ✓ Alcance del Sistema Propuesto(Definición / Objetivo, Funciones, Desempeño, Estructura de Funcionamiento)

F2: Análisis / Diseño General.

- ✓ Modelo Funcional del Sistema Propuesto.

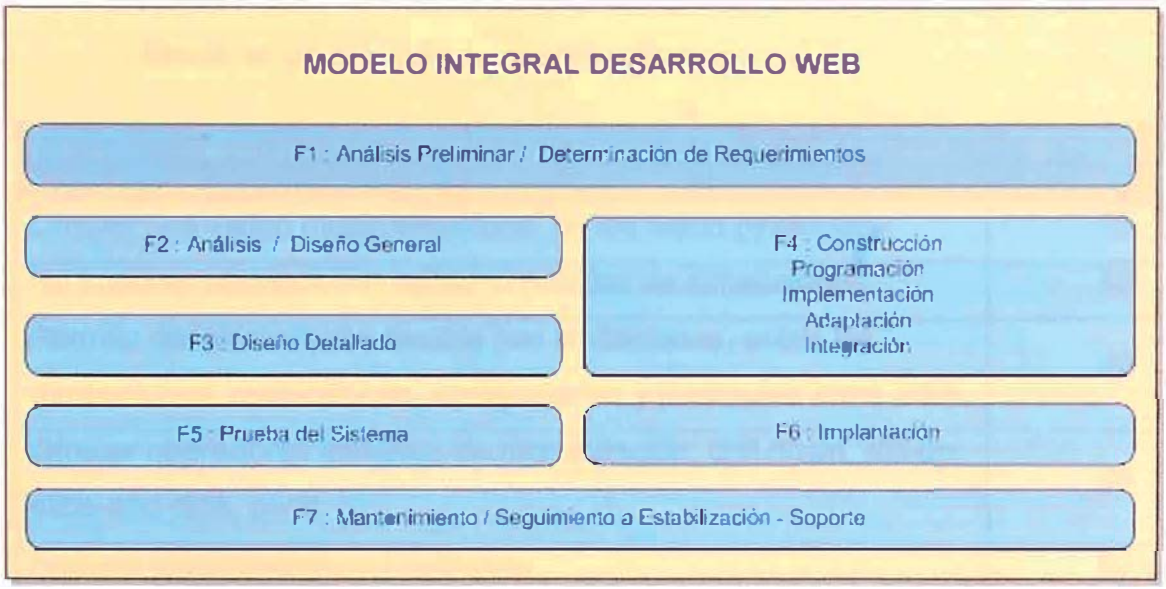
- ✓ Estructura Funcional Preliminar
- ✓ Diseño de Interfases de Usuario
- ✓ Elaboración del Prototipo
- ✓ Revisión - Ajustes del Prototipo

F3: Diseño Detallado.

- ✓ Modelo Físico de Datos (Diseño de la Base de Datos
- ✓ Diseño Detallado de Componentes
- ✓ Afinar Estructura Funcional.

F4: Construcción.

- ✓ Programación/Implementación/Adaptación/Integración de Componentes.
- ✓ Prueba Individual de Componentes.
- ✓ Prueba de Integración.



5. TOMA DE DECISIONES

5.1. ELECCIÓN DE ALTERNATIVAS

Para evaluar la compra de una herramienta Web OLAP suministrada por algún fabricante de software o desarrollar una herramienta personalizada, XYX Audit considero factores técnicos y de costo.

5.1.1. CRITERIOS TÉCNICOS

E. F. Codd, creador del Modelo Relacional, publica en 1993 un artículo técnico realizado para la empresa Arbor Software en donde propone doce reglas que debe seguir una aplicación para ser considerada OLAP.

En base a estas reglas se elaboro una lista de consideraciones técnicas para la evaluación de las principales herramientas OLAP, obteniéndose el siguiente cuadro resumen:

Característica	%*
Ofrecer una visión multidimensional de los datos (matricial).	95
No imponer restricciones sobre el número de dimensiones	82
Permitir definir de forma flexible (sin limitaciones) sobre las dimensiones: restricciones, agregaciones y jerarquías entre ellas.	92
Ofrecer operadores intuitivos de manipulación: drill-down, roll-up, slice-and-dice, pívot.	85
Análisis Multidimensional Gráficos	82
Base de Conocimiento y Noticias	0
Personalización de Carpetas	0
Portafolio Virtual	0

*Representa el porcentaje de las herramientas OLAP analizadas que disponen la característica mencionada

En las características que se refiere al manejo ya análisis de los datos en los cubos la mayoría de las herramientas cumple con las especificaciones requeridas. El factor que ninguna de las herramientas OLAP propietarias no dispone están en las que dan un valor agregado al cliente de XYZ.

5.1.2. CRITERIOS DE COSTO:

Todas las herramientas OLAP que cumplían con las principales características técnicas involucran altos costos de licencias:

- ✓ Licencia por servidor Web
- ✓ Licencia por servidores OLAP
- ✓ Licencias por conexión

Lo cual involucraba un promedio de inversión entre $ 60000 a $70000, solo el costo de la herramientas, sin considerar los gastos de Implementación que involucrarían estas soluciones.

En base a los 2 criterios, técnicos y costos, la gerencia decidió por la opción de desarrollo de una herramienta personalizada.

5.2. ESTIMACIÓN DE COSTOS

La estimación de tiempos y costos nos va a permite identificar nuestras necesidades de recursos humanos, financieros y de tiempo para el desarrollo del Proyecto.

Identificamos primero nuestros recursos disponibles, sus habilidades y conocimientos respecto a los requerimientos del proyecto. En base a este conocimiento definimos si se trabajara con nuestros recursos y/o recursos externos.

De acuerdo a los requerimientos definimos el tiempo y el recurso necesario para el desarrollo del proyecto.

Para la estimación de tiempos se considero que el mes se trabajan 20 días y por día 8 horas.

5.2.1. COSTOS DE DESARROLLO

Sobre la base de los criterios considerados anteriormente, se determino los costos estimados del desarrollo, para lo cual se estimo que los costos generales fueron el 30% del costo de personal.

El desarrollo de la solución estuvo a cargo de un consultor externo, por lo que los costos de licenciamiento de software de desarrollo, así como el hardware empleado no se toman en cuenta en el análisis.

A continuación mostramos el cuadro resumen de la estimación de costos y tiempos del desarrollo del proyecto:

Costos y Tiempos estimados para el desarrollo del Sistema RAI	
Organización	25
Desarrollo	80
Estabilización	15
TOTAL DIAS UTILES	120
TOTAL MESES	6

Recursos	CU/Mensual(US$)	Cantidad	Total(US$)
Analista CCR	1000	1	1000
Analista Outsourcing	1500	1	1500
Programador Outsourcing	1000	1	1000
TOTAL MES			3500
COSTO PERSONAL(US$)			21000
COSTOS GENERALES(US$)	30%		6300
COSTO DESARROLLO DEL PROYECTO(US$)			27300

5.2.2. COSTOS DE IMPLEMENTACIÓN

Para los costos de implementación se tuvo en cuenta los costos tanto nivel de hardware como de software (licencias), así como los costos de conectividad a Internet.

La tabla siguiente muestra los costos estimados para la implementación del sistema desarrollado.

COSTOS ESTIMADOS PARA LA IMPLEMENTACION DEL RAI	
INVERSION POR UNICA VEZ	**$9 550.00**
HARDWARE Y SOFTWARE	**$5 100.00**
Windows 2000 STD (sin licencias cliente)	*
Office XP (solo word, excel, outlook)	$350.00
SQL 2000 STD (sin licencias cliente)	
Swicht 3COM de 8 puertos	$250.00
PC para Servidor WEB	$4 500.00
LICENCIAS POR ACCESO CONCURRENTE (10 Licencias)	**$2 250.00**
Licencia de Windows por Usuario Concurrente de Internet($80 CAL Windows)	**$800.00**
Licencia de BD SQL por Usuario Concurrente de Internet ($145 CAL SQL)	**$1 450.00**
HARDWARE Y SOFTWARE DE SEGURIDAD	**$2 200.00**
PC PENTIUM IV: controlador DMZ (Zona desmilitarizada)	$700.00
Software DMZ (Zona desmilitarizada)	$1 500.00
INVERSION MENSUAL	**$857.00**
Ampliación de Ancho de Banda: de 128 kb a 512 Kb ($1450-$593)	$857.00
INVERSION ANUAL	**$3,363.33**
Nombre de Dominio	$30.00
Certificado Digital de 128 bits	$1,000.00
Seguridad de acceso mediante clave aleatoria	$2,333.33

(*El costo es CERO porque ya se tienen esas licencias)

Se ha considerado como inversión por única vez los conceptos de hardware y Software, tanto lo necesario para el funcionamiento del aplicativo como lo concerniente a la seguridad.

5.2.3. COSTOS DE OPERACIÓN

La siguiente lista muestra un aproximado de los costos de operación del sistema desarrollado:

COSTOS ESTIMADOS PARA LA OPERACIÓN DEL RAI	
INVERSION POR RECURSOS HUMANOS	**$ 400.00**
1 Operador del Sistema RAI a tiempo Parcial	**$ 400**
INVERSION POR MANTENIMIENTO	**$ 350.00**
Mantenimiento de Servidores Web y Archivos	$ 250
Mantenimiento Servidores OLAP	$ 150
INVERSION MENSUAL	**$ 750.00**

5.3. ORGANIGRAMA DEL PROYECTO

El organigrama del proyecto fue desarrollado a fin organizar los equipos de trabajo que participaran en la ejecución del proyecto.

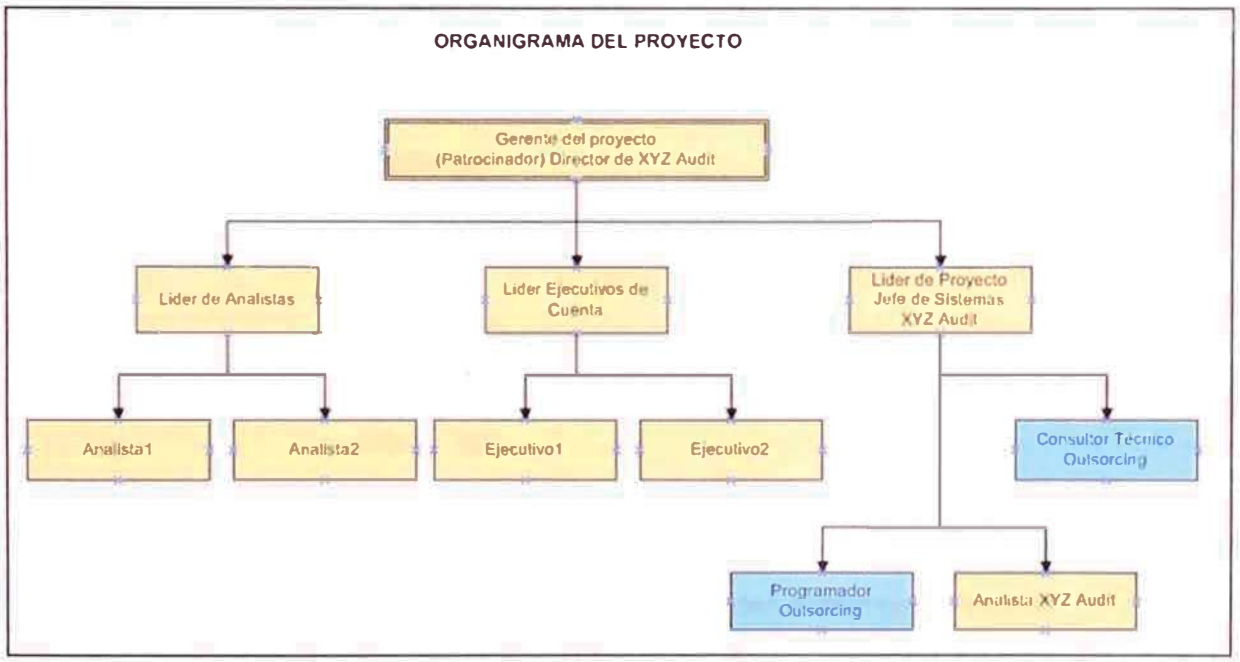
En el se observa que 3 equipos de trabajo, 2 orientados a evaluar el avance del mismo desde el punto funcional, así como el de proveer toda la información necesaria para hacer y el otro orientado al desarrollo.

El equipo del área de análisis básicamente estaba orientado a

revisar la consistencia de datos, tiempos de respuestas, manejo de errores, entre otros aspectos del aplicativo.

El equipo de los ejecutivos de cuenta estaba orientado a hacer una retroalimentación así como capturar los requerimientos y necesidades de los clientes, para que dichas características sean consideradas en el proyecto.

El equipo de desarrollo estuvo conformado por un consultor técnico y un programador outsourcing especializado en el desarrollo de soluciones Web, y por el líder de proyecto y un analista los cuales eran los encargados del intercambio de información, requerimientos, etc. entre el personal outsourcing y el personal interno de XYZ Audit.



6. ESTRATEGIAS ADOPTADAS

6.1. DIAGRAMAS CASOS DE USO

6.1.1. ACTORES:

Los actores del Sistema RAI, básicamente son 2:

- ✓ **Administrador RAI**

Es la entidad que encargada de la configuración inicial del sistema, así como labores de mantenimiento, seguimiento de todo el sistema.

Entre los labores de mantenimiento están la carga de la información de valor agregado, asignaciones de perfiles y opciones, asignación de cubos por producto, por cliente, etc.

- ✓ **Analistas**

Es la entidad que va analizar la información presentada por la aplicación, realiza acciones como compartir información, subir archivos a su portafolio virtual, etc.

Estos Analistas comprendían tanto los analistas internos (CCR) o los analistas externos (clientes).

6.1.2. INVENTARIO DE CASOS DE USO:

Presentaremos los casos de Uso agrupados por Actores, haremos un resumen de los principales casos de uso:

ADMINISTRADOR:

A continuación damos una breve descripción de cada caso de uso:

- ✓ **Administrar Empresas:** Crear, modificar, eliminar los diverso datos asociados a las empresas clientes, como son Usuarios, lista de productos, etc.

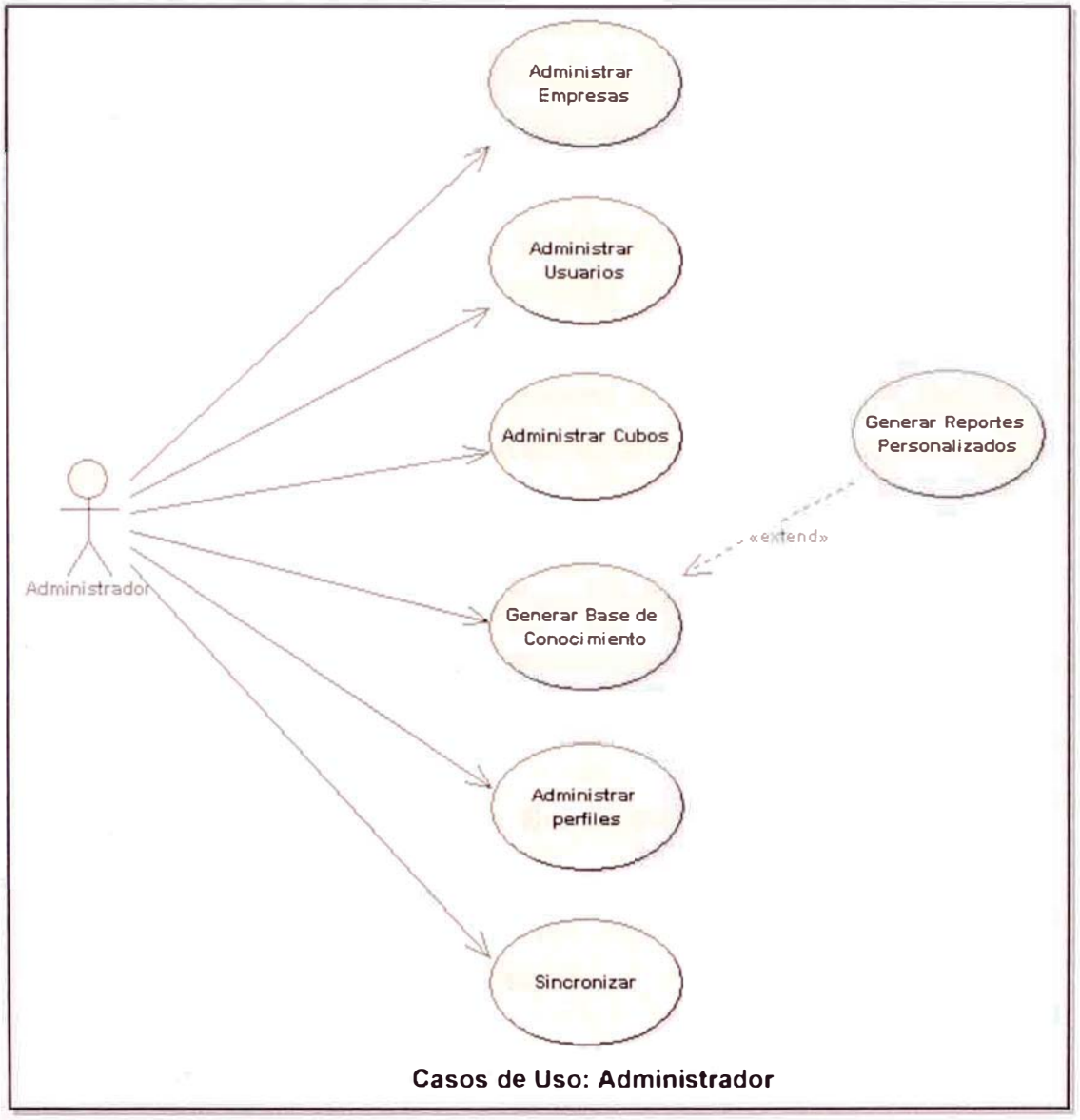
- ✓ **Administrar Usuarios:** Administrar los diversos usuarios que accederán al sistema, sus perfiles, roles, opciones, etc.

- ✓ **Administra Cubos:** Administrar toda la información referente a los cubos, reportes autogenerador, métricas predefinidas, asociarlo a las diversas empresas y /o usuarios, etc.

- ✓ **Generar base de Conocimiento:** Involucra la carga de información adicional, que se le brindara a los clientes: alertas, noticias, etc.

- ✓ **Generar Reportes Personalizados:** Involucra la elaboración de reportes personalizados, tanto reportes clásicos como gráficos, de acuerdo al estudio solicitado por el cliente.

- ✓ **Sincronizar:** Involucra sincronizar la información para que todos los usuarios tenga información concordante, en tiempo real



Casos de Uso: Administrador

ANALISTA

A continuación damos una breve descripción de cada caso de uso:

- ✓ **Portafolio Virtual:** El analista podrá navegar a través de un portafolio virtual, similar al explorador de Windows donde podrá acceder a documentos que

han sido guardado por él, compartidos por potros usuarios y/o aprovisionados por XYZ audit.

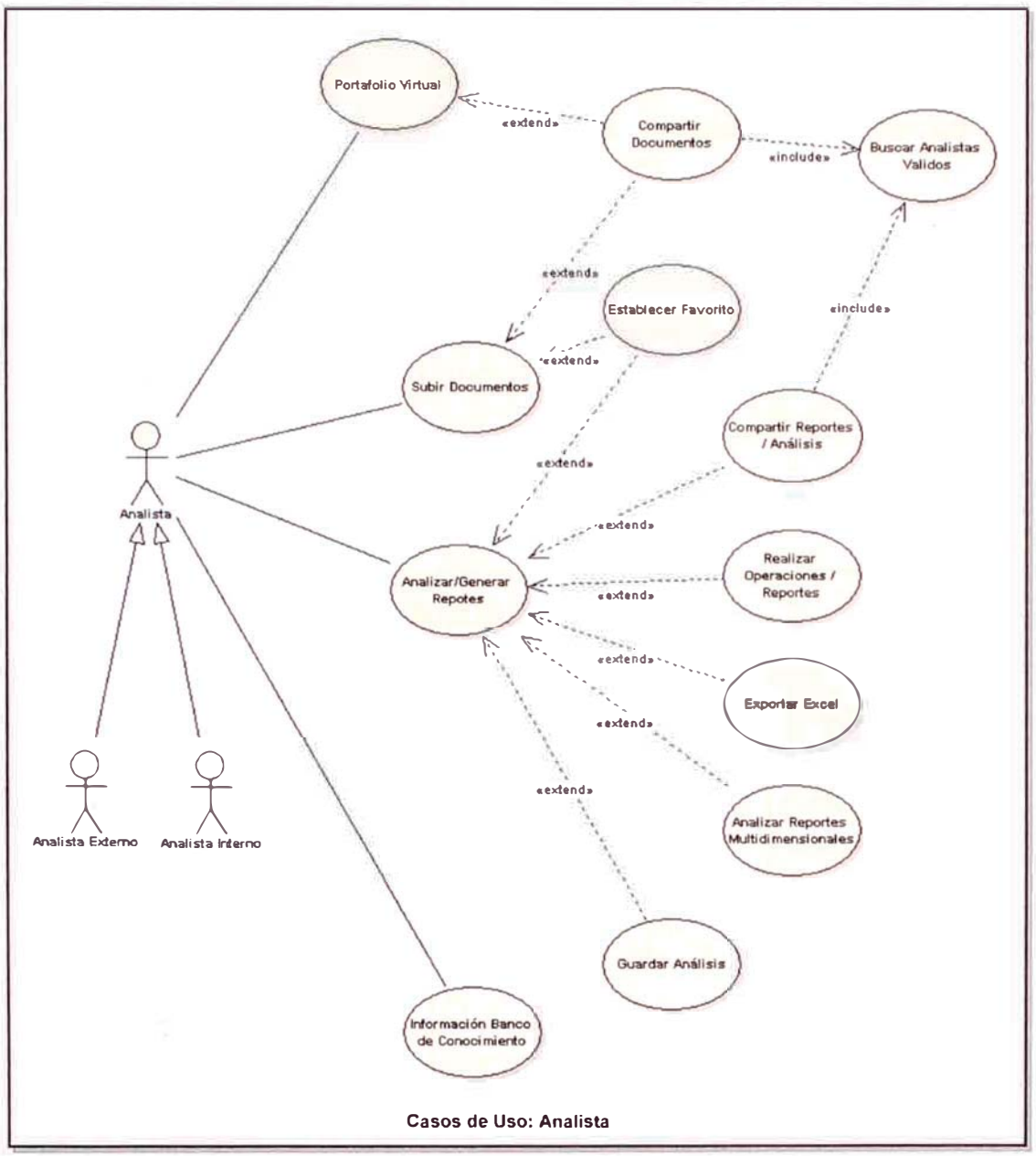
- ✓ **Subir Documentos:** El analista podrá subir cualquier tipo de documento a un servidor de archivos, desde donde podrá acceder a ellos desde cualquier lugar y a cualquier momento.

- ✓ **Analizar Reportes:** El analista podrá analizar y generar reportes dinámicamente con la información de los cubos.

- ✓ **Guardar Análisis:** Todos los reportes que genere el usuario podrán ser guardados en el portafolio virtual, para un rápido acceso posterior.

- ✓ **Información Banco de Conocimiento:** El analista podrá acceder aun conjunto de información aprovisionada por XYZ Audit que le ayudara en la toma de decisiones.

- ✓ **Compartir Documentos:** El Analista podrá compartir documento y reportes generados dinámicamente a otros Analistas de su empresa.



Casos de Uso: Analista

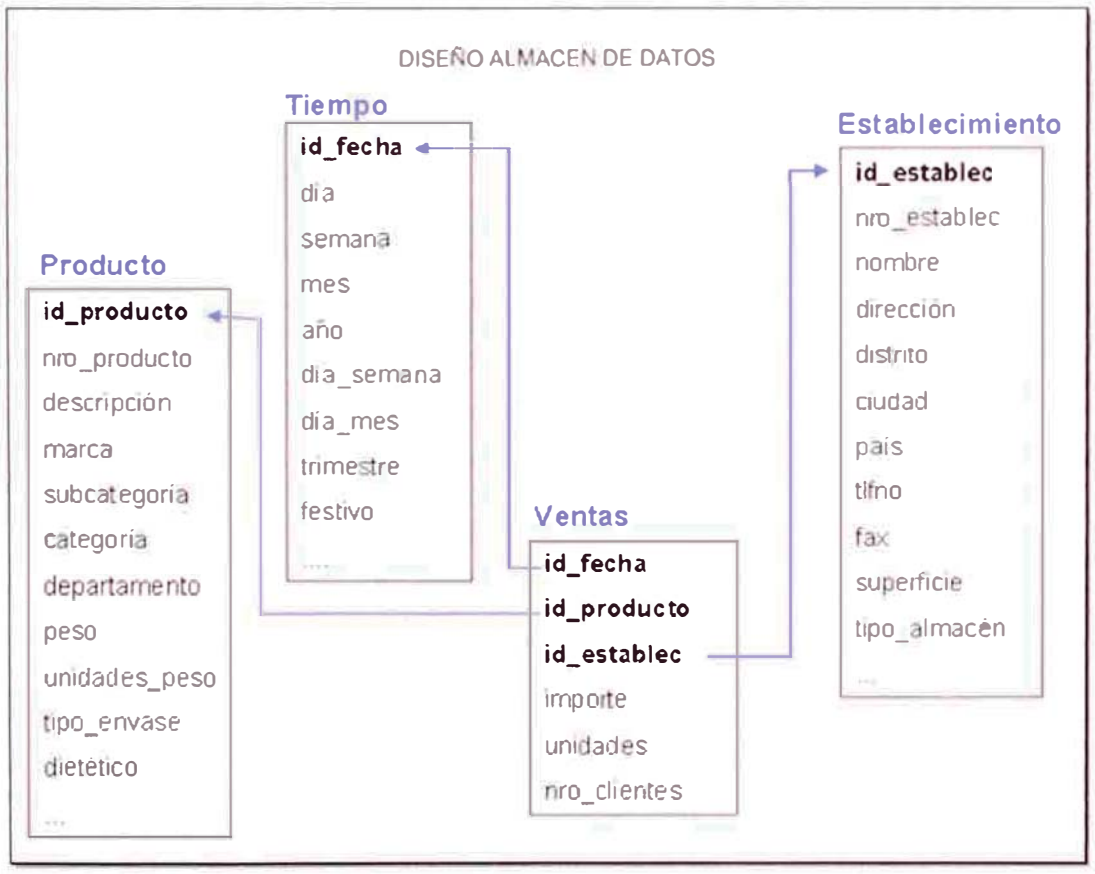
6.2. MODELO DE DATOS DEL SISTEMA RAI

El sistema RAI recupera información de los Cubos almacenados en el Servidor de Cubo, estos cubos tienen estructuras diferentes y variantes de acuerdo a los requerimientos del Cliente. El sistema RAI no realiza ningún proceso de transformación sobre la información almacenada en los cubos.

El modelo de datos del sistema RAI básicamente esta estructurado para la administración y control de los usuarios, empresa cliente, productos, nombre de cubos, información de conexión, documentos, etc.

En los gráficos siguientes mostraremos el modelo de datos usado por el sistema RAI, así como un diseño básico de un almacén de datos usado en XYZ AUDIT.

DISEÑO ALMACEN DE DATOS



Como podemos ver este diseño consta de 3 dimensiones: Producto, tiempo y establecimientos, y como medida: Venta.

En los estudios que realiza XYZ Audit se tienen básicamente

definidos varias dimensiones y medidas estándares, las cuales pueden variar de acuerdo al cliente y al tipo de estudio solicitado por el mismo.

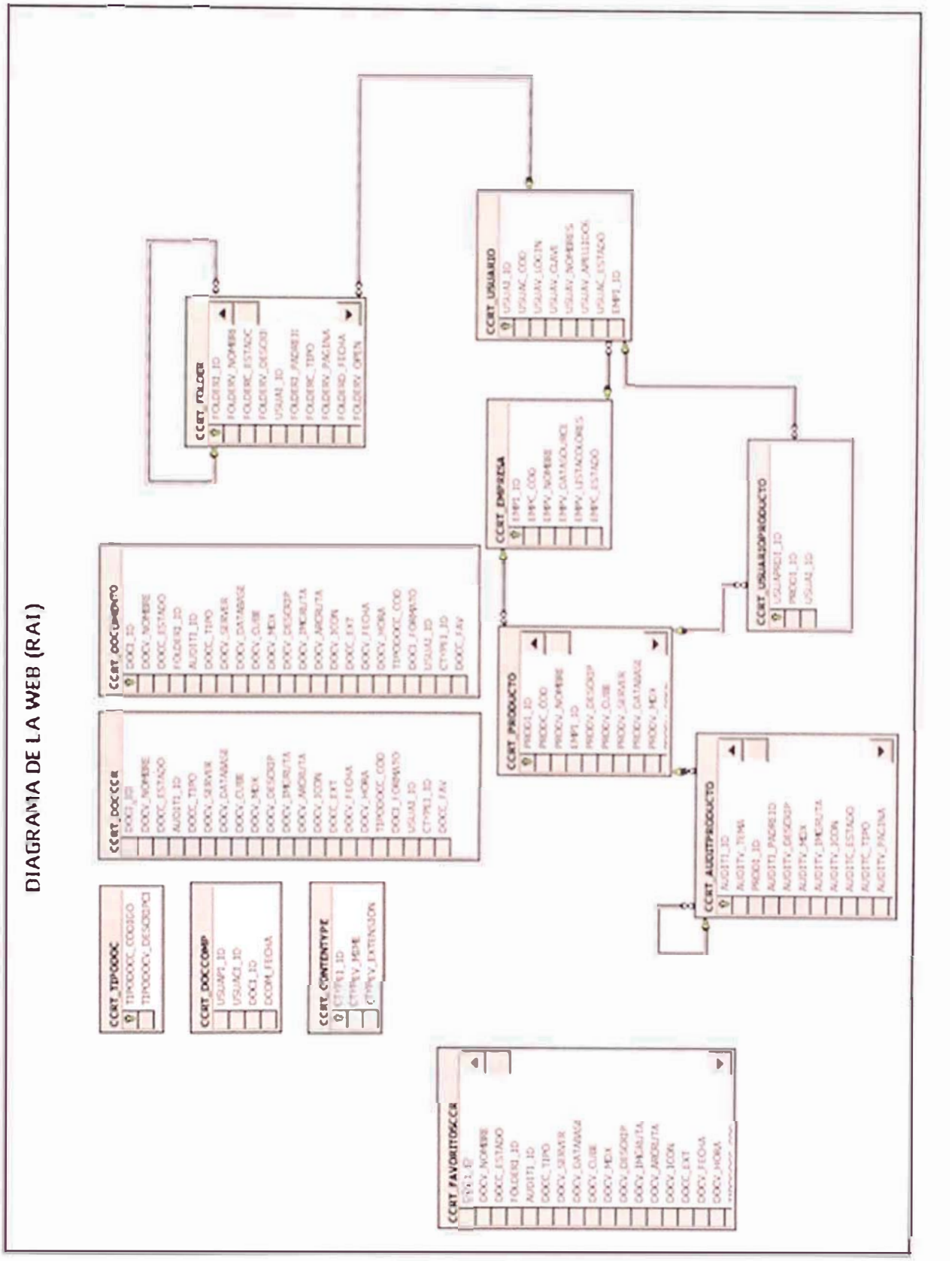
Dimensiones:

- ✓ Canal de venta
- ✓ Ciudad, Zona
- ✓ Descripción
- ✓ Fecha(Año, mes, día)
- ✓ Frecuencia
- ✓ Jerarquía
- ✓ Producto
- ✓ Segmento

Medidas:

- ✓ Ventas
- ✓ Chequeo de distribución
- ✓ distribución por tipo
- ✓ Mínimo y máximo
- ✓ Moda
- ✓ Promedios
- ✓ Mercado Valorizado
- ✓ Exhibición
- ✓ Perfil
- ✓ Compras
- ✓ Stock Ponderado
- ✓ Días Stock
- ✓ Inventario

D AGRAMA DE LA WEB

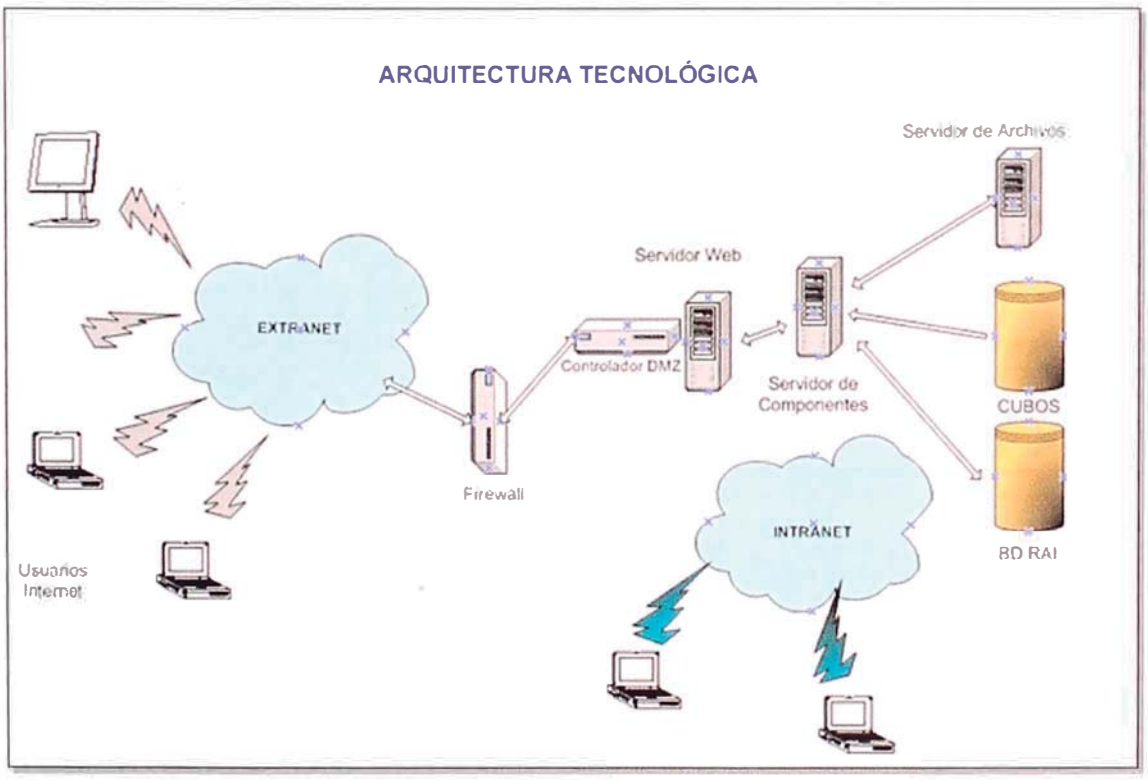


6.3. ARQUITECTURA TECNOLÓGICA

La definición de la arquitectura tecnológica es un proceso de decisión importante pues define los recursos de hardware y software que soportaran los procesos de la organización.

Básicamente la arquitectura tecnológica esta compuesta por:

- ✓ 1 Servidor de Archivos
- ✓ Servidor de Componentes
- ✓ Servidores de Cubos
- ✓ Servidor de la Base de Datos RAI
- ✓ Servidor Web
- ✓ Firewall
- ✓ Controlador DMZ



6.4. NIVELES DE SEGURIDAD

- ✓ Identificación, Autentificación y Autorización
- ✓ Seguridad a nivel de Aplicación a 3 capas
- ✓ Seguridad a través de FireWall
- ✓ Seguridad a través de Certificado Digital
- ✓ Eventos y acciones auditados
- ✓ Codificación Segura

Los detalles de las políticas de seguridad tomadas en cuenta para el desarrollo e implementación del sistema estaban orientados a cubrir las vulnerabilidades de seguridad mas criticas detalladas en el Anexo 3.

6.5. SEGURIDAD Y AUDITORÍA DEL APLICATIVO WEB

El grafico siguiente muestra el esquema de seguridad y auditoria usada en el aplicativo.

Aquí va se administra los archivos y valores de Registry que contiene la información de la cadena de conexión a la Base de datos.

También se administra a los usuarios, verificando si es usuario, los perfiles que le corresponde, las opciones de página y las opciones de Menú.

OBJETOS PRINCIPALES:

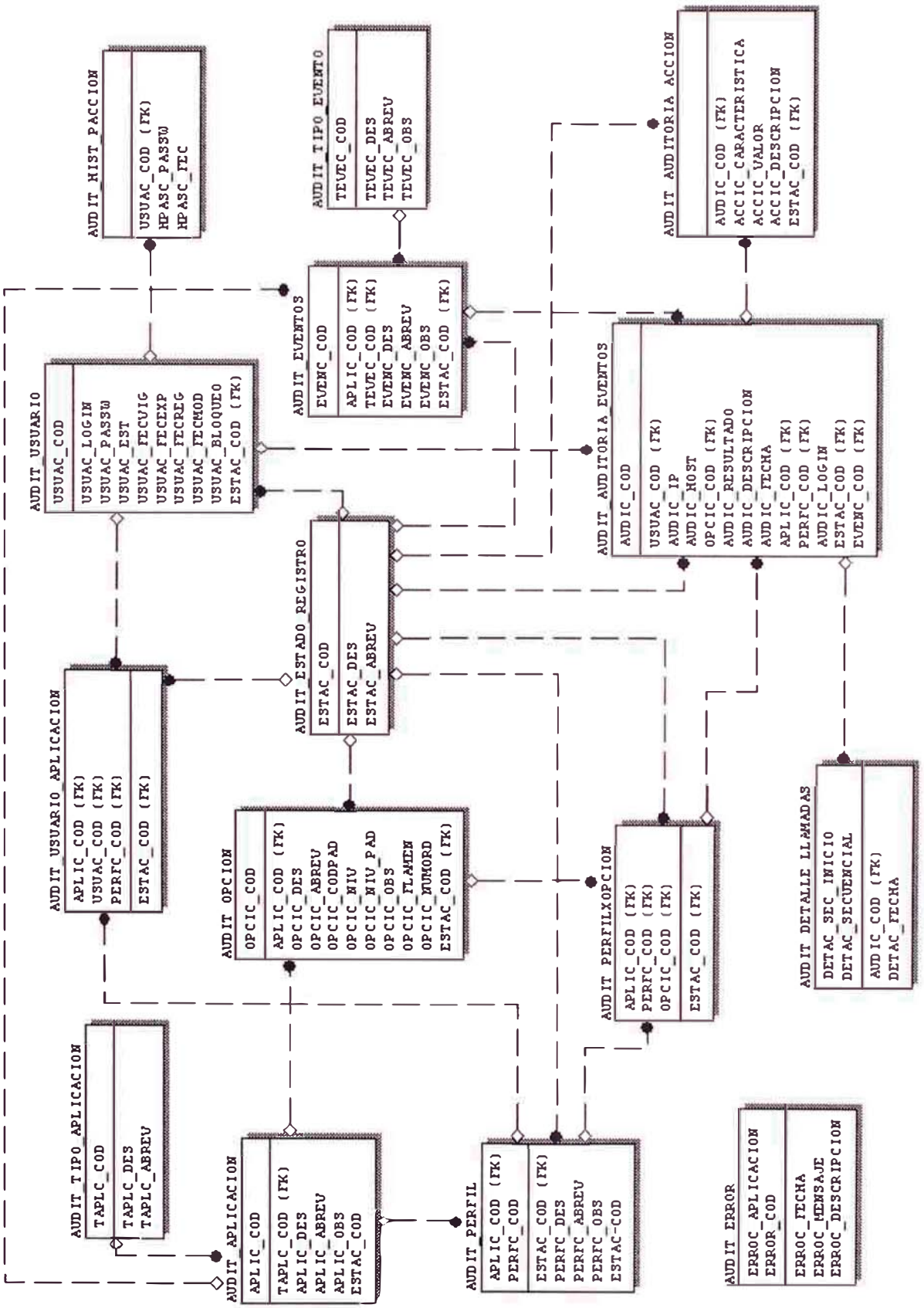
Objeto	Descripción
Usuario	Son todos los usuarios del aplicativo, tanto internos como externos
Usuarios Aplicativo	Son los usuarios por Aplicativo, aquí se almacenan los usuarios del sistema RAI, cada uno tiene características de acuerdo al Perfil que ha sido asignado y cada perfil tiene grupo de opciones definidas para el Aplicativo.
Perfil	Es un grupo de opciones definidas para el aplicativo. Los nombres de los perfiles tienen que ser representativos del grupo de opciones que pertenecen a él.
Opciones	Las opciones definen el tipo de acceso para el aplicativo
Aplicación	Es el aplicativo WEB, para el cual se va definir los perfiles, opciones y usuarios.
PerfilxOpcion	Representa las opciones que existen en la aplicación entre perfil – Opción.
Eventos	Son los eventos del aplicativo como pueden ser Buscar, registrar, Actualizar, enviar correo, etc.

REGISTRO DE AUDITORIA:

Todas las acciones (eventos) realizados por los usuarios a través de las opciones del aplicativo son registradas, así como los resultados de sus acciones.

Existiendo estándares para dicho registro especificado en el documento de Estándares de Seguridad y Auditoria de los aplicativos Web.

MODELO DE DATOS SEGURIDAD Y AUDITORIA



6.6. ARQUITECTURA DEL APLICATIVO:

La elección y diseño de la arquitectura del aplicativo encerró decisiones importante sobre:

- ✓ Organización del Sistema del Aplicativo
- ✓ Selección de elementos que constituyen el sistema (estructura) y sus interfaces así como la colaboración entre elementos (comportamientos).
- ✓ Estilo arquitectural que guía la organización, elementos y sus interfaces, sus colaboraciones y su composición.

También tuvo que ver con el contexto: uso, funcionalidad, rendimiento, flexibilidad, reutilización, inteligibilidad, restricciones económicas y tecnológicas, apariencia, etc.

Esta arquitectura también debe ser capaz de cumplir los requisitos del sistema.

Para la elección y diseño de la Arquitectura Web del aplicativo se siguió una plantilla que cubría los siguientes puntos:

1. **Aplicabilidad**

   - ✓ Útil para aplicaciones Web
   - ✓ Mínimo control de la configuración del cliente
   - ✓ El cliente solo debe necesitar un Navegador Web para hacer peticiones de páginas.
   - ✓ Lógica de negocio ejecutada en el servidor

2. **Usos Conocidos**

   - ✓ Aplicaciones de Comercio Electrónico

3. Estructura

- ✓ Mínima arquitectura para una aplicación Web
- ✓ Sus principales componentes están en el servidor
- ✓ Componentes:
- ✓ Navegador del Cliente
- ✓ Servidor Web
- ✓ Conexión HTTP
- ✓ Páginas HTML
- ✓ Archivos de configuración
- ✓ Páginas del servidor
- ✓ Servidor de aplicaciones

4. Dinámica

- ✓ Comportamiento de aplicaciones construidas con ese patrón de arquitectura
- ✓ La lógica del negocio solo se ejecuta durante el procesamiento de las peticiones de Paginas Web por el cliente
- ✓ Una vez hecha la petición, se devuelve una pagina HTML al cliente y finaliza la conexión entre cliente y servidor

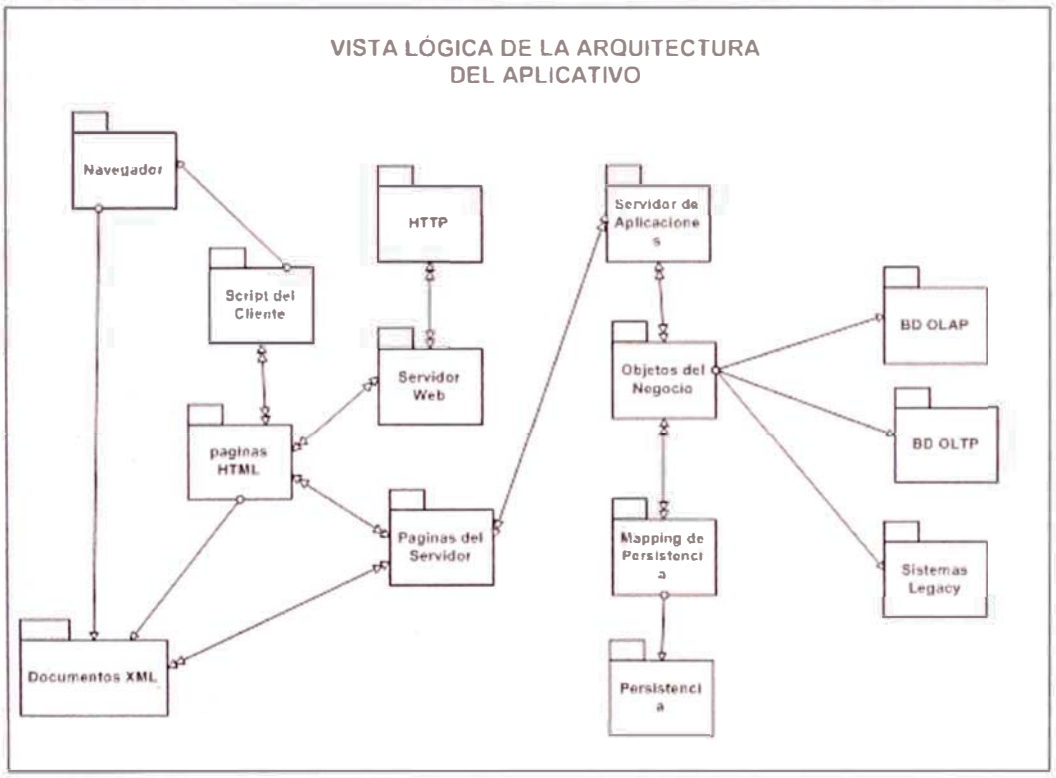
5. Consecuencias

- ✓ Tiempo de Respuesta:
  - Adecuada para aplicaciones cuyas respuestas del servidor pueda ser completada dentro del tiempo de respuesta aceptable esperado por el usuario y del valor time out permitido por el navegador del cliente.
  - Tiene que ser adecuad para permitir al usuario iniciar

y controlar un proceso de negocio duradero.

- ✓ Pruebas: Comprobar el comportamiento correcto de los scripts para cada navegador y configuración del cliente que deba ser soportada.

En base a estos criterios se diseño la siguiente Arquitectura del Aplicativo:



CAPITULO IV
EVALUACIÓN DE RESULTADOS.

XYZ Audit al impulsar este el desarrollo de este proyecto buscaba alcanzar con los siguientes 2 grandes objetivos:

- ✓ Brindar información veraz y oportuna tanto a sus clientes internos (Analistas de XYZ Audit) como a los externos (Analistas y ejecutivos de las empresas clientes).
- ✓ Cultivar relaciones perdurables que permitan obtener lealtad y reconocimiento de nuestros clientes.

1. Debemos tomar en cuenta que la gerencia de XYZ Audit al evaluar la factibilidad este proyecto, tomo como puntos de partida los 2 objetivos anteriormente mencionados.

2. También se tuvo en cuenta que este sistema no iba cambiar ningún proceso existente en XYZ Audit, si no que involucraba un nuevo servicio o producto que se le brindaba a los clientes, tanto externos como internos. Servicio que se les va entregar como valor agregado, incluido en los reportes tradicionales.

3. Como podemos observar en el organigrama del proyecto, los analistas de XYZ tomaron un importante rol en el desarrollo del mismo. Esto favoreció que los requerimientos y características que esperaban del

sistema le hayan sido satisfechos.

4. Si bien se tuvo la participación de los ejecutivos de cuentas, que son los encargados de obtener las necesidades de los clientes, la no participación de los clientes externos, al menos de un subgrupo que represente a los principales clientes, en forma directa en el proyecto podría con llevar a que sus necesidades no sean satisfechas y aun podría darse el caso de que el sistema no sea usado por algunos clientes.

5. Cabe hacer notar que el desarrollo del proyecto involucro más tiempo del estimado y por ende de un mayor costo, esto se debió principalmente a que no se identifico inicialmente los riesgos inherentes en el desarrollo del proyecto. Así como no se tuvo con una adecuada administración de cambios.

6. Entre los riesgos no identificados el principal que se dio, fue en la etapa de pruebas al subir archivos infectados con virus al servidor de archivos, que en esta etapa era el mismo que el servidor Web, provocando infección en archivos de programación.

   Este punto fue contemplado e implementado mediante un componente que analizar y filtrara que los archivos subidos estén libres de virus, troyanos, o algún software malicioso.

1. IMPACTO DE LA SOLUCIÓN

A continuación mostraremos tablas y gráficos donde se hace un análisis del impacto de la solución en los procesos contemplados en la cadena de Valor de XYZ Audit.

Cadena de Valor	Procesos Tradicionales	Nuevos Procesos: SIA
Contrato y Diseño	• Definición del servicio • Seguimiento del estado de requerimiento	• Seguimiento en línea del estado de requerimiento
Levantamiento de Información	• Toma Manual de datos • Supervisión costosa • Demoras de lectura o transferencia de datos • Corrección de datos	• Captura de datos informatizada. • Supervisión informatizada • Transferencia de información al sistema
Proceso y Análisis	• Demoras en corrección y reproceso de información • Alto índice de supervisión • Control de calidad exhaustivo	• Corrección y reproceso se reduce hasta en un 80% • Control de calidad solo por muestreo.
Servicio Post - Venta	• Envió de información • Sustentación de resultados	• Análisis en línea • Informes disponibles 24X7 • Artículos y mas

Cada proceso de la cadena de valor es contemplado por los siguientes sistemas:

Cadena de Valor	Sistemas
Contrato y Diseño	*SIA Clientes*
Levantamiento de Información	*SIA FFA (Field Force Automation)*
Proceso y Análisis	*SIA Administración, Procesos e Informes*
Servicio Post - Venta	*SIA RAI (Retail Audit Intelligence)*

El esquema de trabajo en XYZ Audit sufre un gran cambio, especialmente para los analistas tanto externos como internos.

Las principales características de la solución RAI son:

- ✓ Análisis en Línea
  - Reportes y Gráficos dinámicos:
- ✓ Indicadores de Performance por:
  - Marca
  - Variedad, etc.
- ✓ Semáforos o Alertas
- ✓ Personalización de Reportes y Gráficos
- ✓ Personalización de Carpetas
- ✓ Banco de Conocimiento
- ✓ Portafolio Virtual
- ✓ Noticias y enlaces de interés
- ✓ Seguridad

El cliente podrá acceder desde cualquier lugar del mundo una base de conocimiento, noticias, etc. Mediante Herramientas de análisis en Línea. Agregando Valor al análisis, mediante el uso Reportes Multidimensionales, indicadores, alertas, semáforos, presentaciones, etc.

Este cambio se ve reflejado en el siguiente gráfico.

CAPITULO V
CONCLUSIONES Y RECOMENDACIONES

1. CONCLUSIONES

- ✓ Información es poder, pero la información no son solamente datos, mas bien son datos organizados que pueden ser útiles en el momento oportuno para la toma de decisiones estratégicas

- ✓ La información reduce nuestra incertidumbre (sobre algún aspecto de la realidad) y, por tanto, nos permite tomar mejores decisiones

- ✓ Entender las prioridades del cliente y que sus expectativas son cambiantes y cada vez más altas.

- ✓ Un diseño efectivo de negocio y su ejecución depende de la forma en que la administración utiliza la tecnología para entregar más rápidamente los servicios, de una manera más barata, y con mejor calidad que la de sus competidores

- ✓ Actualmente los mercados son muy dinámicos y exigen una continua toma de decisiones importantes y además con

pocas posibilidades de errores si no se quiere poner en peligro la viabilidad de una organización.

- ✓ En la empresa actual se da cada vez más importancia al control de gestión. Los recursos son escasos, los procesos son complejos, y cada vez es más crítica la información que se requiere para una correcta toma de decisiones. Por ello, son primordiales las herramientas de apoyo a la toma de decisiones, entre los que se encuentra el Inteligencia de Negocios y el cuadro de mando (tanto por áreas como integral) que ayude a los directivos en este sentido.

2. RECOMENDACIONES

- ✓ Para llevar al éxito un proyecto de Inteligencia de Negocios se necesita personas tanto con visión de tecnología como de negocio definiendo la herramienta más adaptada a sus necesidades, que asegure el éxito. para que no le confundan las luces de colores

- ✓ Para alcanzar el éxito en un proyecto de Inteligencia de Negocios se debe centralizar en obtener el conocimiento para la toma de decisiones en las áreas clave de la empresa, es decir, donde se obtiene valor añadido

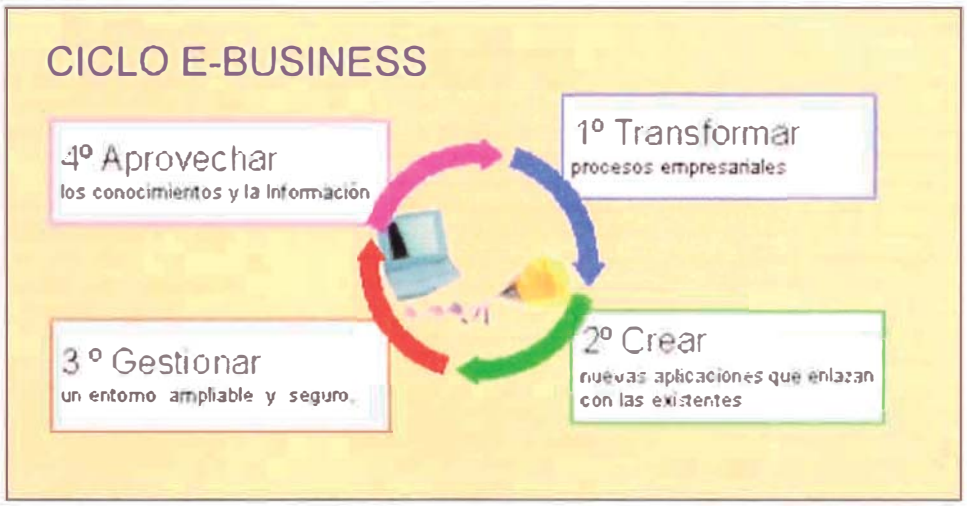
- ✓ Construir un diseño eficiente que supere a la competencia

- ✓ Obtener y mantener la información actualizada, donde, cuando y donde se necesite

- ✓ Enfocarse en el consumidor.

- ✓ Transformar los procesos del negocio en formato digital.

- ✓ Finalmente recomendamos poner en practica la estrategia del ciclo de ebusiness:



GLOSARIO DE TÉRMINOS

1. **Cadena de Valor:** La cadena de valor es la forma de análisis de la actividad empresarial mediante la cual descomponemos una empresa en sus procesos que crean valor, buscando identificar fuentes de ventaja competitiva en aquellas actividades generadoras de valor. Esta ventaja competitiva se logra cuando la empresa desarrolla e integra las actividades de su cadena de valor de forma menos costosa y mejor diferenciada que sus rivales. La cadena de valor de una empresa esta conformada por todas sus actividades generadoras de valor agregado y por los márgenes que estas ofrecen.

2. **Value NET:** Es el análisis de un modelo de cinco fuerzas considerando beneficios de cooperación. Una empresa puede cooperar con :

   Competidores estableciendo estándares para la tecnología del sector. Proveedores y clientes para lograr un diseño convenido de procesos e incrementar la eficiencia de la logística. La relación con los competidores no solo tiene que ser de competencia si no también de coordinación pues juntos podrían hacer crecer el tamaño del mercado.

   Es un diseño de negocio que usa conceptos avanzados de Supply Chain a fin de lograr una satisfacción mayor de llos clientes e incrementar los ingresos de la compañía.

DATOS: Describen la realidad o percepción de la existencia humana, corporativa institucional, comunitaria, etc. Las computadoras almacenan y procesan datos. Al nivel más bajo los datos no tienen significado alguno.

3. **INFORMACIÓN:** Es lo que una persona es capaz de entender sobre la realidad. Los sistemas de información en la actualidad utilizan computadoras para procesar y presentar los datos en un formato comprensible para el ser humano.

4. **CONOCIMIENTO:** Es el acervo de información utilizado en el proceso de la toma de decisiones.

5. **GESTIÓN DE CONOCIMIENTO: (**Knowledge Management) Es la disciplina que busca enfocar el uso de las Tecnologías de Información en las personas, con el fin de que estas y sus organizaciones aprendan a utilizar los recursos y fuentes de información para el logro de objetivos estratégicos.

BIBLIOGRAFÍA

1. Step by Step Microsoft SQL Server 2000 Analyses Services
   OLAP Train Reed Jacobson
   Microsoft Press

2. MDX Solutions With Microsoft SQL Server Analysis Services
   George Spofford
   Editorial Wiley

3. Olap Solutions Building Multidimensional Information Systems
   Erik Thomsen
   John Wiley & Sons, Inc.

4. Distributed Data Warehousing Using Web Technology
   R.A. Moeller
   AMACOM © 2001

5. Building the DataWarehouse
   V. H Inmon
   Editorial Wiley

6. OWASP Top Ten Most Critical Web Application Security Vulnerabilities – 2004 Update
OWASP: The Open Web Aplication Security Project
http://www.owasp.org

7. Ovum Evaluates
OLAP
Software Testing Tools

8. Enlaces Internet
http://www.graliteo.si/eng/2_8_retail.php
http://www.marketoption.com/marketing-retail-audit.asp

ANEXO 1: EVALUACIÓN DE HERRAMIENTAS OLAP

Online application processing (OLAP) es el interactivo análisis de la información del negocio. Los usuarios finales pueden explorar medidas importantes del negocio (tales como utilidades, ventas y costos) a lo largo de muchas diferentes 'dimensiones'. Con una herramienta OLAP, el usuario se mueve fácilmente de una perspectiva del negocio ("ventas anuales de todas las tiendas") a otra ("la tiendas mas rentables sobre los ultimas tres meses") y profundizar a diferentes niveles de detalle (ventas por día, semana o meses). Esta exploración interactiva de información es conocida como análisis multidimensional. El factor común que enmarca a todas las herramientas OLAP es un motor analítico que pone datos corporativos dentro de datos multidimensionales para análisis online.

PLATAFORMA DE EVALUACIÓN OLAP

La meta de la plataforma de evaluación es suministrar una comprensiva manera de describir herramientas OLAP. La plataforma cubre la totalidad de funcionalidades OLAP.

Funcionalidad Usuario Final

¿Qué tan fácil es para usuarios casuales encontrar y usar un modelo creado previamente?

Se ha considerado soporte para distribución y suscripción de reportes.

Construcción del Modelo del Negocio

¿La herramienta facilita el constructor de modelos para construir un modelo complejo modelo multidimensional del negocio?

Poder Analítico Avanzado

Que soporte provee la herramienta para análisis complejo.

Soporte Web

¿La herramienta puede ser usada para acceder y crear modelos vía Web?

Administración

¿Cuán fácil es administrar los modelos, datos persistentes y usuarios.

Adaptabilidad

Como la herramienta asegura que las fuentes de datos, modelos, reportes derivados de estos y meta datos estén todos sincronizados.

Ejecución Afinada

¿Cuáles son las herramientas de afinación?

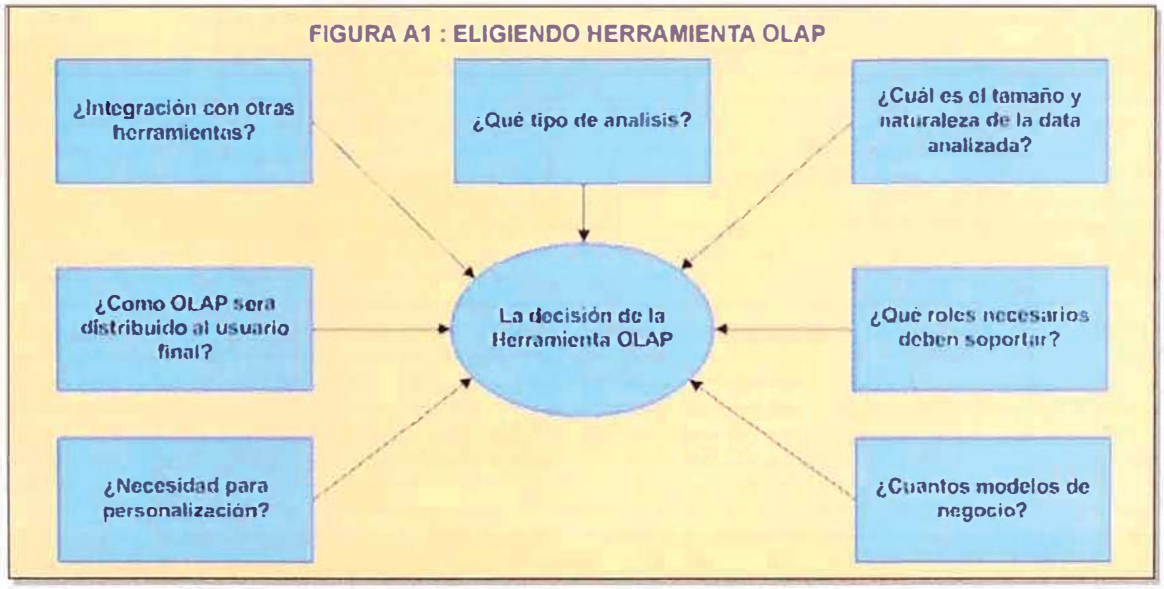
Personalización

¿Qué soporte esta disponible para personalizar y desarrollar aplicaciones?

IMPORTANTES CONSIDERACIONES CUANDO SE CONSTRUYE UN PERFIL DE REQUERIMIENTOS OLAP

En la figura A1 se muestra las principales preguntas que necesitan ser considerados para decidir los requerimientos organizacionales para OLAP.

FIGURA A1 : ELIGIENDO HERRAMIENTA OLAP



Como debe ser usada esta Evaluación

Cuando se ha decidió cuáles consideraciones descritas son importantes en el escenario organizacional, se puede usar esta información cuando se lea esta evaluaciones. La Figura A2 da una indicación de cómo esto puede ser hecho, la figura muestra cuales aspectos de esta plataforma de evaluación son importantes en evaluar la herramienta para estos requerimientos de negocio. Estos son los aspectos que son necesarios prestar particular atención para cuando se lea las evaluaciones.

Comparando su perfil de necesidades con los puntajes es el primer paso para escoger una herramienta que satisfaga sus necesidades. Los detalles en la evaluación lo habilitaran refinar sus decisiones.

FIGURA A2 . EMPLEO DE EVALUACIONES

	Funcionalidad Usuario Final	Construcción del modelo del Negocio	Poder Analítico Avanzado	Soporte Web	Administración	Adaptabilidad	Ejecución Alineada	Personalización
Análisis complejo y especializado	–	●	●	–	–	–	–	–
Soporte a los usuarios Avanzados	○	●	●	–	–	–	–	–
Soporte a los usuarios casuales	●	–	–	○	–	–	–	●
Soporte para diseñadores	–	●	○	–	–	●	–	○
Soporte para el administrador	–	–	–	–	●	●	●	–
Soporte par el desarrollador de aplicaciones	–	○	○	–	–	–	–	●
Administrar un gran número de modelos volátiles	–	–	–	–	●	●	○	–
Soporte para personalización	–	○	○	–	–	–	–	●
Acceso Web para explorar modelos /reportes	–	–	–	●	–	–	–	○
Acceso Web para crear modelos	–	–	–	●	–	–	–	–
Uso de Internet/Web para distribuir reportes OLAP	●	–	–	●	–	–	–	–
Una arquitectura apropiada a la naturaleza de los fuentes de datos y modelos	Ver descripción de configuración de la arquitectura en las evaluaciones							
Integración con otras herramientas	Información es dada en Adaptabilidad y despliegue							

METODOLOGÍA DE EVALUACIÓN

Las Herramientas bajo evaluación provienen de diferentes entornos y han sido desarrollados para satisfacer diferentes necesidades. Este no es un conjunto homogéneo de productos, no hay una aplicación OLAP estándar. Las fortalezas y debilidades reflejan la causalidad del producto y la base de clientes de los proveedores.

Se debe decidir:

- ✓ Cual perspectiva es el 'mínimo' y 'mas' importante.
- ✓ Que funcionalita es critica dentro de estas perspectivas.

Describiremos cada uno de las ocho perspectivas usadas para evaluar los productos y dar los argumentos para su inclusión. No todos de estos serán de igual importancia en cada configuración. Indicaremos las características que diferencian productos, incluyendo por que y cuando ellos son importantes.

1. FUNCIONALIDAD USUARIO FINAL

Fácil de usar es un tema particularmente importante en OLAP por que:

- ✓ Los usuarios principales son trabajadores del negocio, no el staff IT.
- ✓ En comparación con la serie de sistemas de entrada, donde no hay otra posibilidad, el uso de herramientas OLAP puede ser opcional, por que hay muchas caminaos para tomar decisiones de negocio.
- ✓ La herramienta frontal es la parte mas visible de un

almacén de datos, y la elección de la herramienta se vera incrementado por la utilidad percibida del almacén de datos.

2. CONSTRUCCIÓN DEL MODELO DEL NEGOCIO

Los diseñadores de modelos de negocios multidimensionales necesitan herramientas que ofrezcan suficiente flexibilidad por que el modelo a ser construido debe satisfacer las necesidades del negocio,

Una alta puntuación aquí es importante si se quiere sintonizar un modelo de negocios complejo usando la Herramienta OLAP. Una alta puntuación indica que la herramienta ofrece mas soporte para ajustar dimensiones y medidas, Una baja puntuación no será de preocupación si el modelo de datos pretendido es simple y mayormente un reflejo de la estructura de datos en el almacén de datos u orígenes de datos.

Cuando se construye el modelo de negocio haya requerimientos para la definición de dimensiones y medidas.

3. PODER ANALITICO AVANZADO

Usuarios especializados necesita una selección 'fácil de usar' de funciones estadísticas, financieras y de pronósticos, así como también la habilidad para escribir funciones adicionales.

Un alto puntaje es esencial si los usuarios tienen la intención de usar la herramienta OLAP para trabajos analíticos complejos, modelar o pronosticar negocios, probablemente como un analista de negocios o usuario avanzado. Una baja puntuación será aceptable si el análisis consiste de manipulación y presentación de datos históricos, mas bien que la aplicación de formulas o algoritmos a los datos.

4. SOPORTE WEB

Para una total explotación de la Web, las herramientas deben

soportar publicaciones Web y la explotación y creación de modelos a través de navegadores Web.

Un alto puntaje es crucial si la intención es facultar a un gran número de usuarios con OLAP a un costo mínimo, o los usuarios requieren 'acceder desde cualquier ordenador de escritorio', pero será menos importante si la intención es forzar el uso a un pequeño grupo de usuarios avanzados equipados con computadoras de escritorios estándares.

Hay muchos factores que han contribuido al crecimiento de la importancia del acceso Web a OLAP, incluyendo:

- ✓ El costo beneficio de usar de navegadores requiere un mantenimiento mínimo.
- ✓ La facilidad de aprovisionar funcionalidad OLAP a un gran numero de usuarios a través de la Web.
- ✓ El incremento de las expectativas que las intranets así como la Internet serán usadas para la diseminación de la información.

Aprovisionar OLAP a través de la Web es ahora un requerimiento intrínseco. Sin embargo, mientras todos os proveedores ofrecen acceso Web, hay importantes diferencias en las soluciones Web.

Un importante aspecto es la comparación de la funcionalidad de usuario final a través de interfaces Web y de ordenador de escritorios. El acceso Web debe ser entregado con la misma funcionalidad al usuario tanto como acceso de escritorio.

5. ADMINISTRACIÓN

Herramientas deben ofrecer soporte para la administración de modelos, datos y usuarios que es fácil para usar y reducir la carga de trabajo del administrador.

Un alto puntaje es esencial si la administración del sistema OLAP es emprendido por un administrador general antes que especialista DBA. La importancia del puntaje aquí también esta en función del numero de usuarios y la complejidad de modelos que son mantenidos. Un bajo puntaje no ser causa de demasiada preocupación si hay pequeños datos para administrar y la seguridad nos es un tema importante.

Administración de Modelos: el tema principal en administrar modelos es la seguridad y el monitoreo de consultas.

La información sobre el monitoreo del uso de modelos habilita al administrador a responder a cambios de demandas, y soportar los procesos de afinamientos de los modelos y los orígenes de datos que los alimenta.

Administración de Datos: la administración de datos persistentes es más complicado, en MOLAP, por definición, los datos usados en el modelo de datos multidimensionales es almacenado en base de datos multidimensionales. En ROLAP, mientras el origen de datos principal es una base de datos relacional.

Las tareas de administración detallada asociadas con MOLAP; ROLAP Y HOLAP son diferentes, pero el tema principal en todos los caso es la calidad de soporte que la herramienta da para la fácil administración.

Administración de Usuarios: la Herramienta debe permitir al administrador definir políticas de seguridad individual y grupal.

6. ADAPTABILIDAD

Las herramientas necesitan proveer soporte para mantener los orígenes de datos, modelos de negocios multidimensionales (y los reportes derivados de ellos) y los meta datos acerca de todos estos sincronizados.

Un alto puntaje es importante si los orígenes de datos o requerimientos de usuarios son probables a ser volátiles y la

implementación es medio a largo. Un bajo puntaje será aceptable en la improbable situación que los requerimientos de usuarios y orígenes de datos son considerados a ser comprensible y estable.

7. EJECUCIÓN AFINADA

El administrador necesita que la herramienta soporte el incremento del desempeño por afinación de la extracción de datos y el proceso de manipulación de datos.

Un alto puntaje es esencial cualquiera sea el alcance o naturaleza de la operación OLAP.

Hay algunos aspectos de la ejecución afinada que son aplicables independientemente de la arquitectura, pero algunos son particulares a MOLA y ROLAP.

Requerimientos compartidos, independientemente de la arquitectura, es la necesidad a:

- ✓ Extraer datos lo mas rápidamente posible desde orígenes relaciónales.
- ✓ Distribuir el procesamientote las consultas de los usuarios
- ✓ Incrementar la velocidad de procesamiento para tomar ventajas de multiprocesamiento simétrico (SMP).

Herramientas con diferentes arquitecturas ofrecen diferentes cambios a la ejecución, y diferentes opciones de sintonización:

- ✓ ***MOLAP***

  Como cambiar el tamaño y el tiempo de carga contra la velocidad de repuesta y el soporte de múltiples de usuarios.

- ✓ ***ROLAP***

  Tiempo de respuesta de consultas es el principal tema de ejecución.

8. PERSONALIZACIÓN

Consideramos el soporte que la herramienta proporciona para desarrollar aplicaciones que incluye data multidimensional en tabular y formato grafico que el usuario puede explorar interactivamente.

Un alto puntaje es esencial si la organización quiere desarrollar aplicaciones dentro de la organización para OLAP si la herramienta será usada como la base de aplicaciones soporte de decisiones por un ISV o un VAR.

El soporte más fuerte es proporcionado por herramientas con una ambiente de desarrollo completo, el cual incluye la provisión de componentes y un 4GL que pueden directamente ayudar construir aplicaciones multidimensionales. Aunque este requiere desarrolladores para dominar un nuevo entorno, reduce el tiempo de desarrollo.

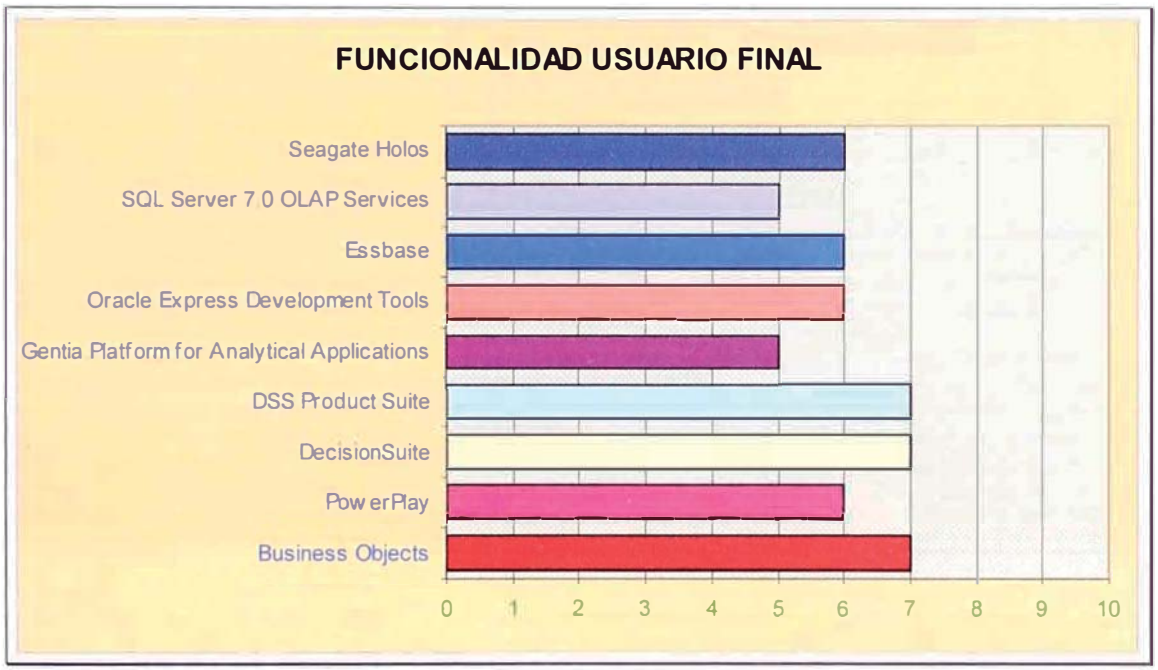
En contraste a esto, hay herramientas que proporciona un API abierto a través del cual los datos pueden ser extraídos de modelos y luego manipulados en aplicaciones construidos usando entornos de desarrollo de aplicaciones familiares (como son C++ o Visual Basic). Sin embargo, con estas herramientas mas trabajo es requerido para dar al usuario las mismas facilidades para explorar dinámicamente los datos. Algunos, pero el menor, créditos es dado a herramientas que ofrecen esta facilidad.

Análisis multidimensional puede ser el punto focal de la aplicación, o puede ser incrustado parte de un paquete cuyo principal enfoque es la administración de ventas, financieros u otros tipos de información. En este

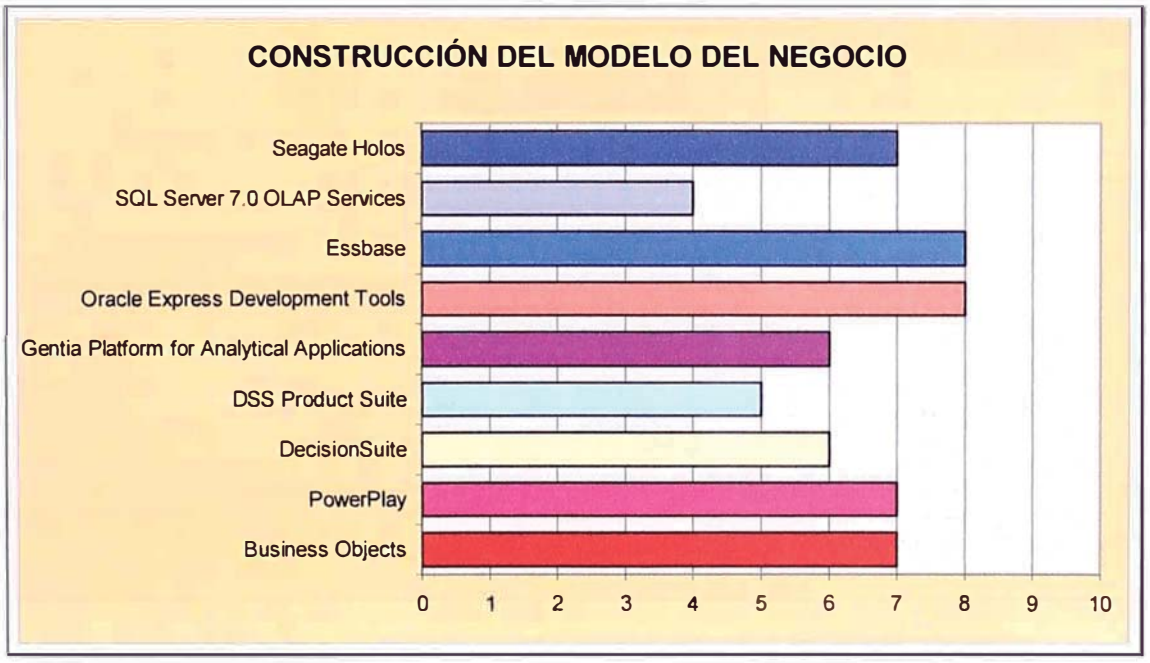
caso, las características OLAP son suplementarias. En ambos casos, la ventaja de construir tales aplicaciones OLAP internamente incluye el ajuste con requerimientos, la gran complejidad soportada y una reducción potencial en costo.

RESUMEN DE LAS EVALUACIONES

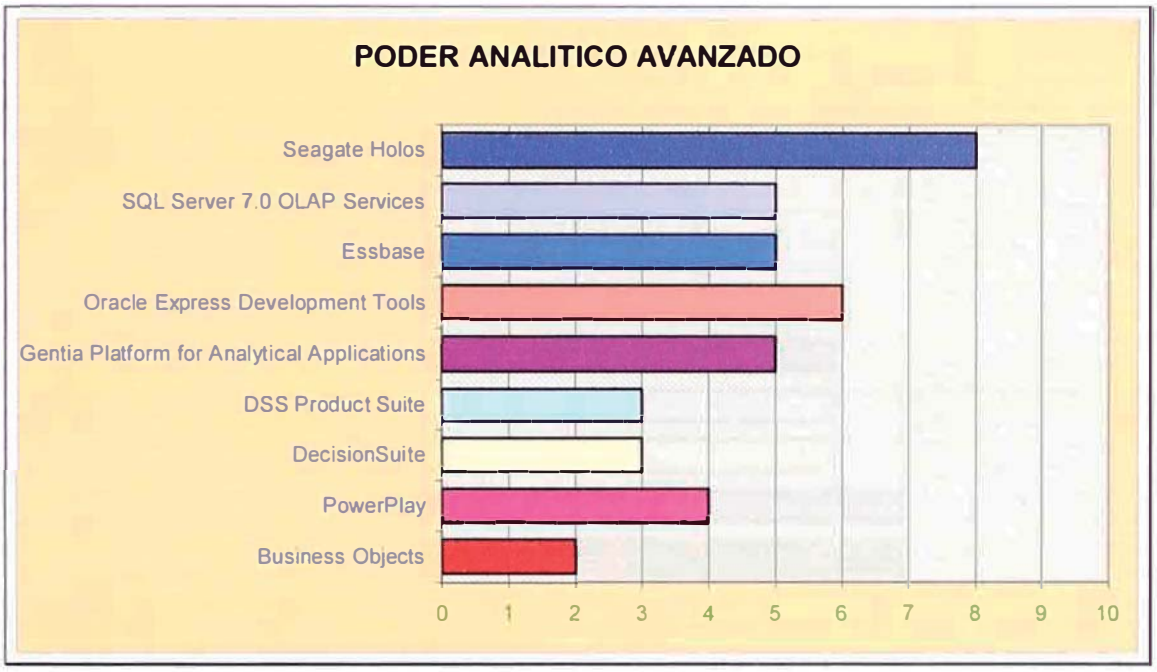
1. FUNCIONALIDAD USUARIO FINAL



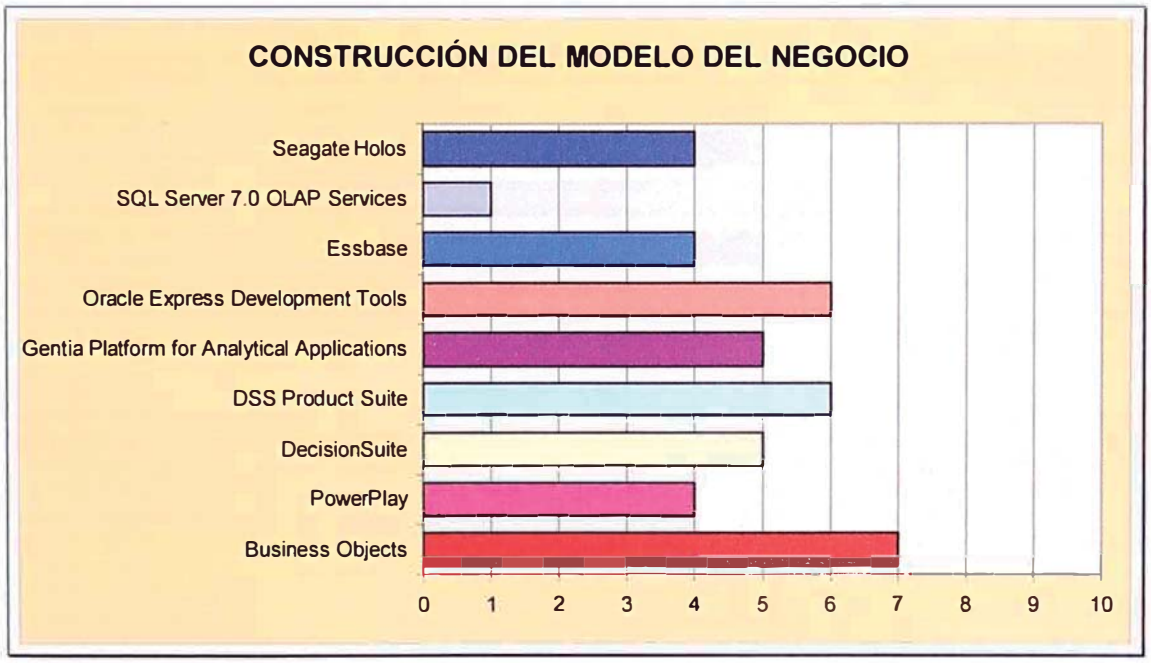
2. CONSTRUCCIÓN DEL MODELO DEL NEGOCIO



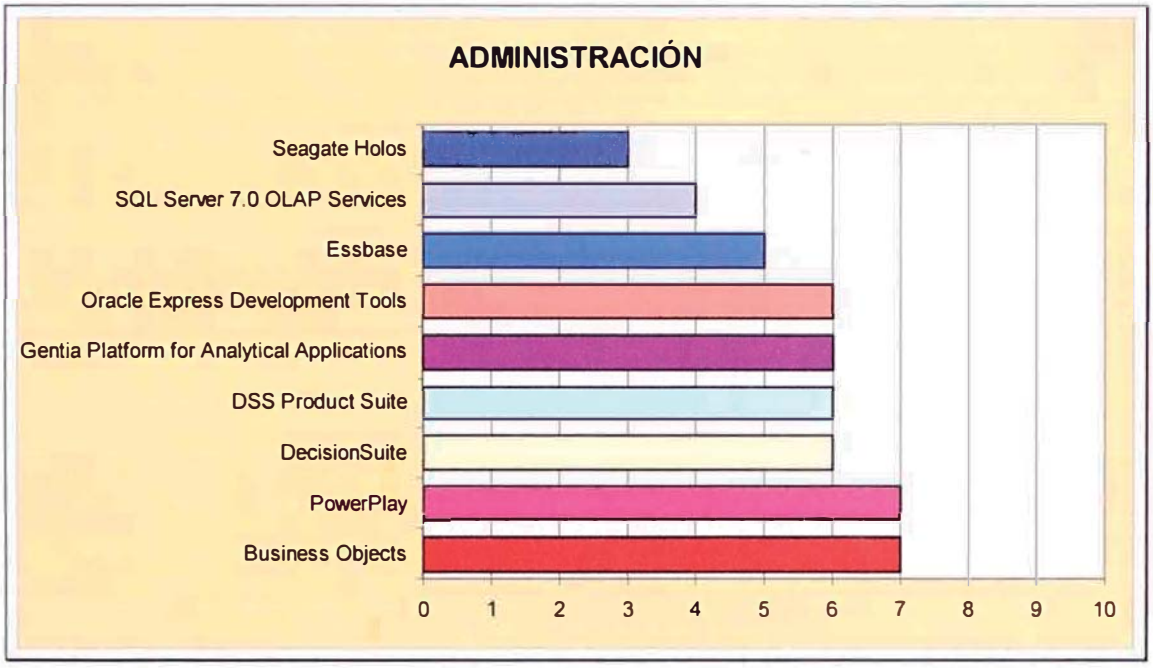
3. PODER ANALITICO AVANZADO



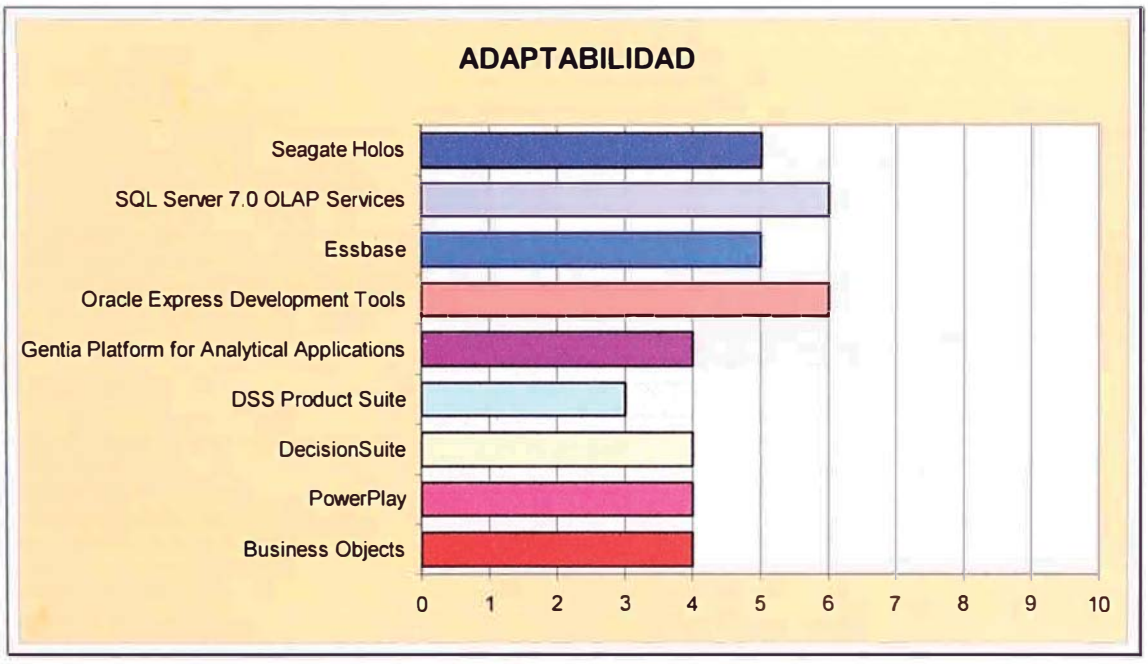
4. SOPORTE WEB



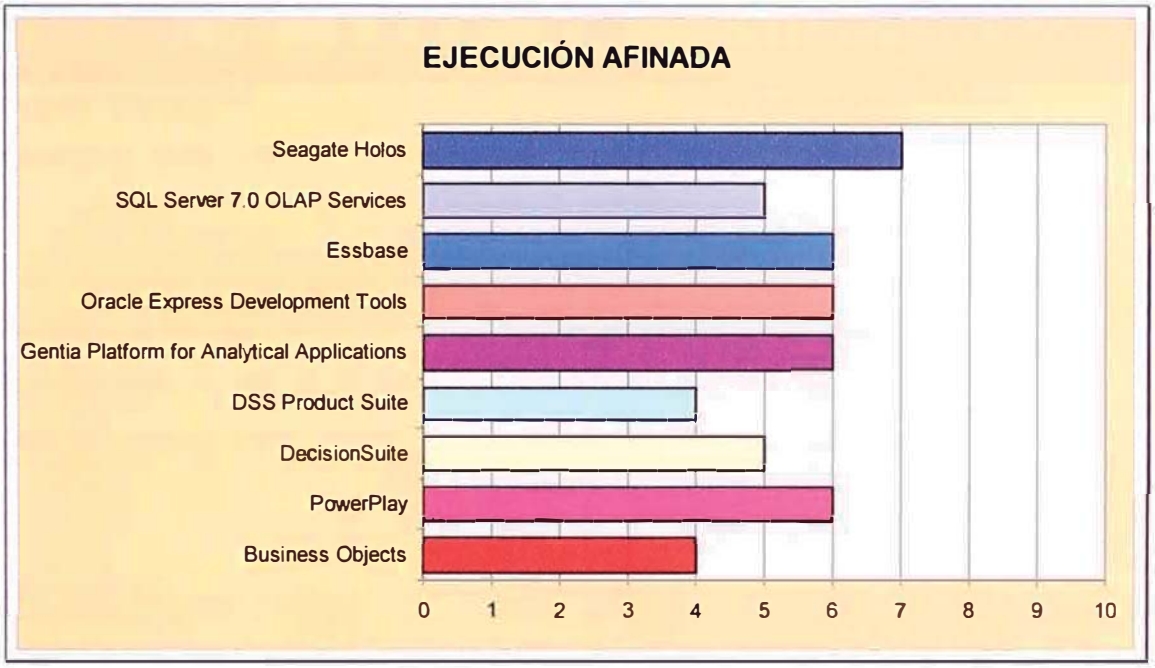
5. ADMINISTRACIÓN



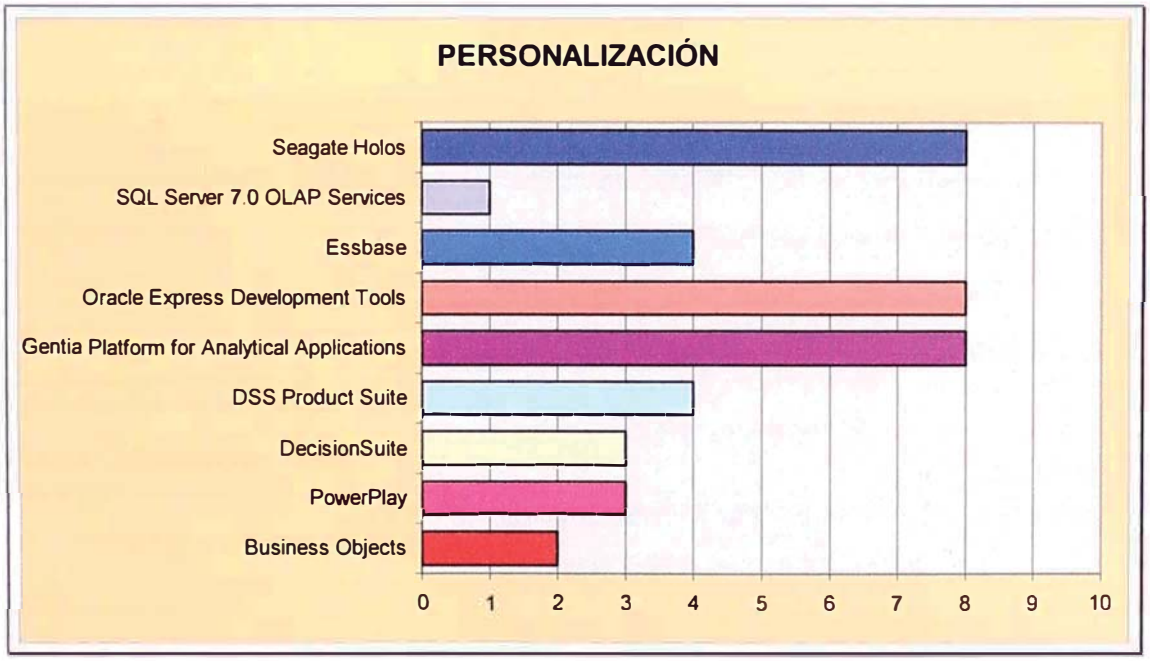
6. ADAPTABILIDAD



7. EJECUCIÓN AFINADA



8. PERSONALIZACIÓN



Las evaluaciones han sido hechas sobre las siguientes plataformas y herramientas:

Empresa	Herramienta / Versión
Applix, Westboro, Massachusetts, USA	Applix TM1 version 7.1
Business Objects, twin headquarters in Paris, France and San Jose, USA	BusinessObjects version 4.0, comprising of the BusinessObjects user module, BusinessObjects Designer, BusinessObjects Supervisor, Document Agent Server, BusinessQuery and BusinessMiner; and WebIntelligence II version 2.0
Cognos, Ottawa, Canada	PowerPlay and PowerPlay Web version 6
Gentia Software, London (UK)	Gentia Millennium Applications Platform (G-MAP), version 5.0.2
Hummingbird Communications, North York, Ontario, Canada	BI/Suite version 5.1, comprising BI/Query version 5.0.2, BI/Analyze version 5.1, BI/Web version 2.0 and BI/Broker version 2.0.
Hyperion Solutions, Sunnyvale, California, USA	Hyperion Essbase Server version 6.0; Wired for OLAP version 4.1; Hyperion Integration Server version 1.1; Hyperion Essbase Web Gateway version 2.1; Hyperion Essbase Objects version 1.1
Information Advantage, Eden Prairie, Minnesota, USA	DecisionSuite version 5.7
Microstrategy, Vienna, Virginia, USA	DSS Product Suite version 5.5, consisting of: DSS Architect, DSS Agent, DSS Server, DSS Administrator, DSS Web, DSS Broadcaster, DSS Executive and

	DSS Objects
Microsoft, Redmond WA, USA	Microsoft SQL Server 7.0 OLAP Services (Beta 3 and Final Feature Editions)
Oracle, Redwood Shores, CA, USA	Oracle Express Server, version 6.2; Oracle Objects and Express Analyzer, version 2.2; Oracle Web Publisher, version 2.0
Pilot Software, Cambridge, Massachusetts, USA	Pilot Decision Support Suite version 6.1
SAP AG, Walldorf, Germany	SAP Business Information Warehouse (BW), version 1.2A
Seagate Software Information Management Group, Scotts Valley, CA, USA	Seagate Holos version 7.0
Sterling Software (Business Intelligence Division), Eden Prairie, Minnesota, USA	Eureka:Suite comprising of Eureka:Strategy 5.7.8, Eureka:Analyst 4.5, Eureka:Intelligence 1.1, Eureka:Reporter 6.1.3 and Eureka:Portal 2.0
WhiteLight Systems, CA, USA	WhiteLight Analytic Application Server, version 2.0

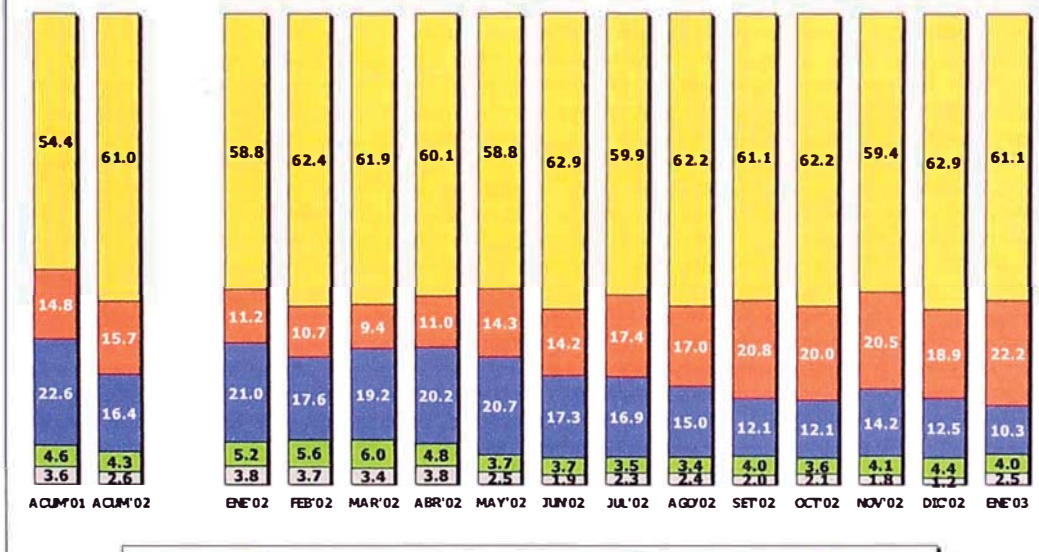
ANEXO 2: REPORTES Y PRESENTACIONES ENTREGADAS POR XYZ AUDIT A SUS CLIENTES

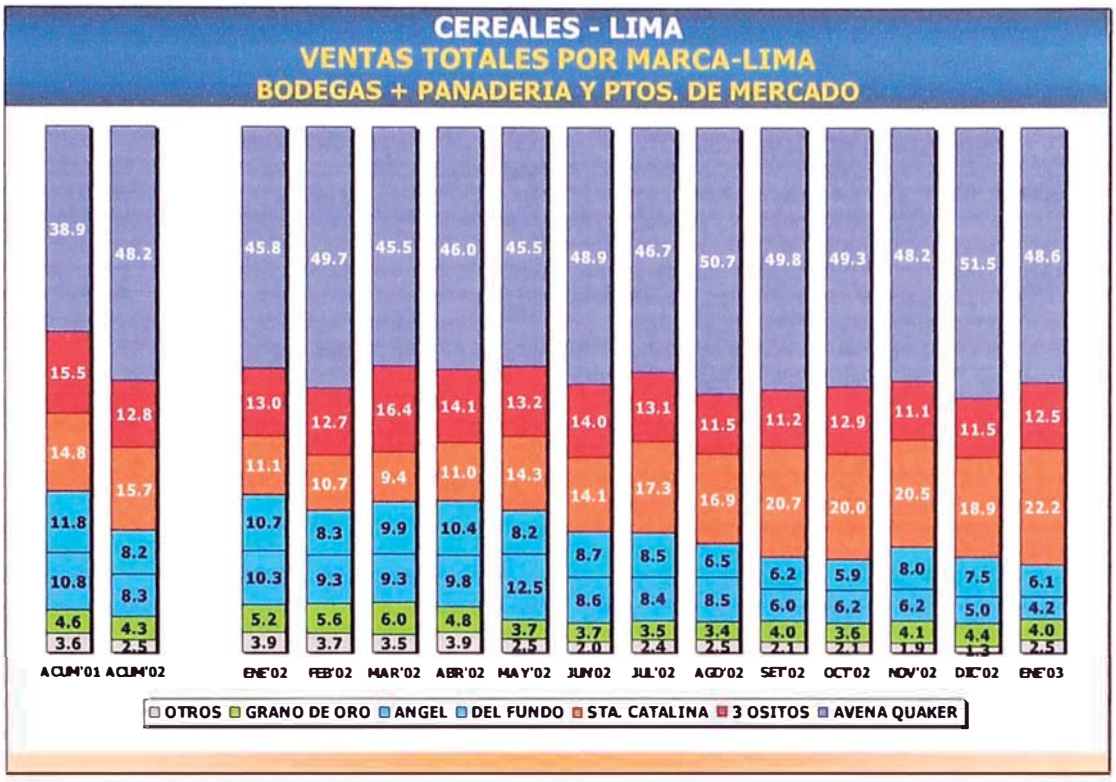
CEREALES - LIMA
FICHA TÉCNICA

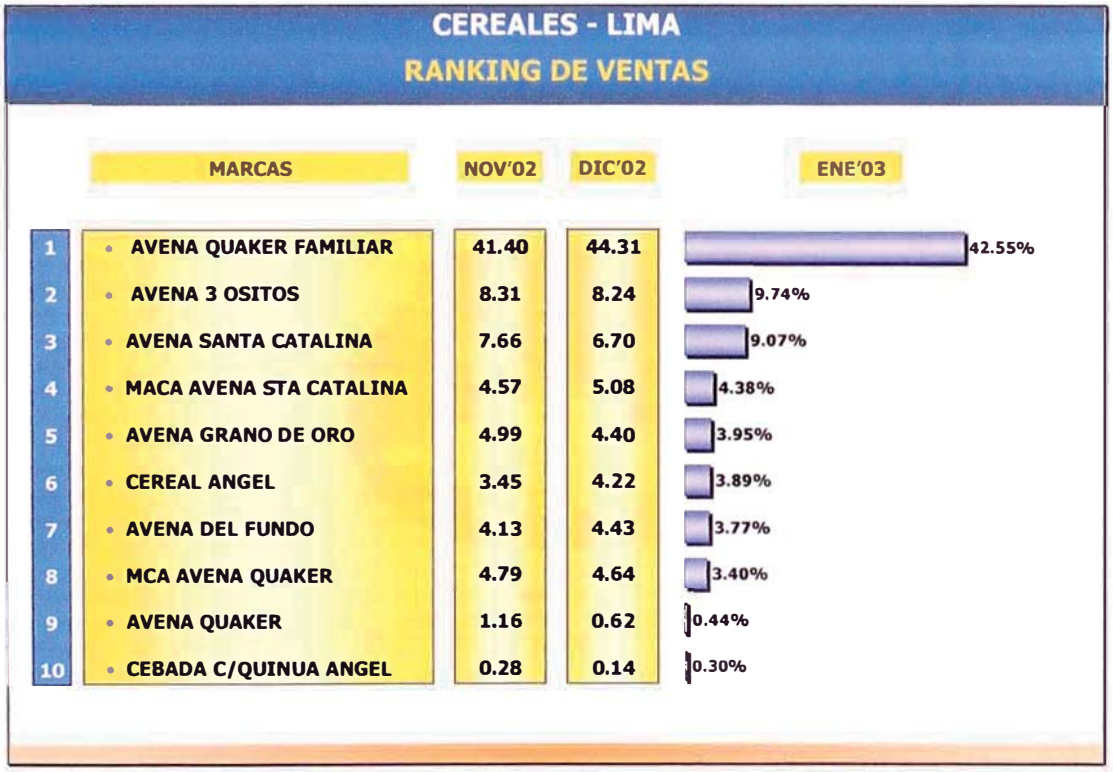
TIPO DE ESTUDIO	:	Auditoria de Producto
OBJETIVO	:	Contiene información a nivel minorista de las ventas y nos permite analizar y optimizar todas las variables que intervienen en el proceso de la comercialización y distribución de sus productos, a traves de la investigación sistemática. Nos proporciona información de las marcas segmentadas por tipo y cualquier otra división relevante para la categoría.
CANALES DE VENTA	:	Bodegas, Panaderías y Puestos de Mercado
TIPO DE MUESTREO	:	Aleatorio Estratificado, en función al volumen de ventas.
ERROR MUESTRAL	:	5%
NIVEL DE CONFIANZA	:	95%
FRECUENCIA	:	Bimestral
INFORMACIÓN A RECOGER	:	Inventario, Compras y Precios de venta al público

	BODEGAS	PANADERIAS	PTOS. MCDO.	TOTAL
Universo de Negocios	52412	2877	8328	60740
% de Penetración	76.9%	71.4%	82.6%	77.7%
Universo de Producto	40317	2055	6880	47197

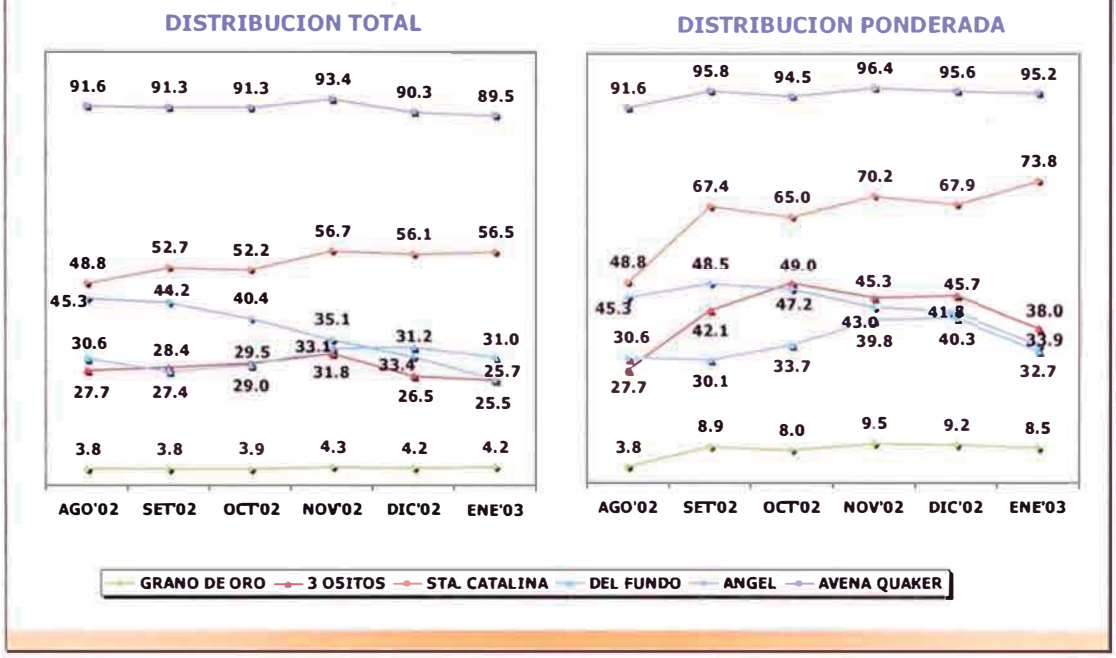
CEREALES - LIMA
VENTAS TOTALES POR FABRICANTE
BODEGAS + PANADERIA Y PTOS. DE MERCADO



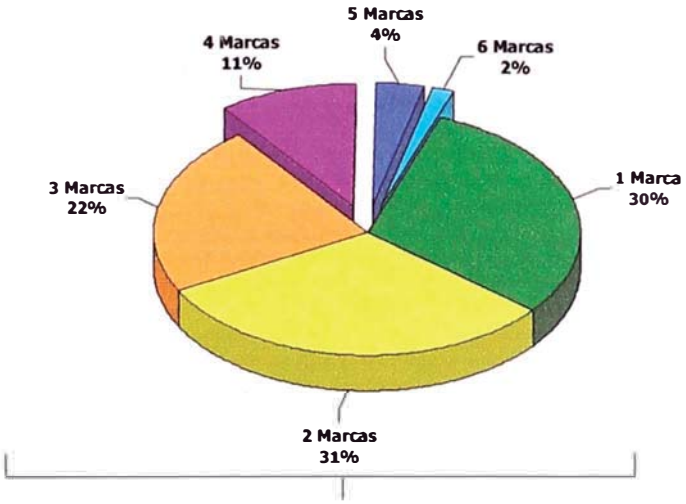

CEREALES - LIMA
VENTAS TOTALES POR MARCA-LIMA
BODEGAS + PANADERIA Y PTOS. DE MERCADO
38.9
15.5
14.8
11.8
10.8
4.6
3.6
48.2
12.8
15.7
8.2
8.3
4.3
2.5
45.8
13.0
11.1
10.7
10.3
5.2
3.9
49.7
12.7
10.7
8.3
9.3
5.6
3.7
45.5
16.4
9.4
9.9
9.3
6.0
3.5
46.0
14.1
11.0
10.4
9.8
4.8
3.9
45.5
13.2
14.3
8.2
12.5
3.7
2.5
48.9
14.0
14.1
8.7
8.6
3.7
2.0
46.7
13.1
17.3
8.5
8.4
3.5
2.4
50.7
11.5
16.9
6.5
8.5
3.4
2.5
49.8
11.2
20.7
6.2
6.0
4.0
2.1
49.3
12.9
20.0
5.9
6.2
3.6
2.1
48.2
11.1
20.5
8.0
6.2
4.1
1.9
51.5
11.5
18.9
7.5
5,0
4.4
1.3
48.6
12.5
22.2
6.1
4.2
4.0
2.5
ACUM'01
ACUM'02
ENE'02
FEB'02
MAR'02
ABR'02
MAY'02
JUN'02
JUL'02
AGO'02
SET'02
OCT'02
NOV'02
DIC'02
ENE'03
OTROS
GRANO DE ORO
ANGEL
DEL FUNDO
STA. CATALINA
3 OSITOS
AVENA QUAKER


CEREALES - LIMA
RANKING DE VENTAS
MARCAS
NOV'02
DIC'02
ENE'03
1 • AVENA QUAKER FAMILIAR 41.40 44.31 42.55%
2 • AVENA 3 OSITOS 8.31 8.24 9.74%
3 • AVENA SANTA CATALINA 7.66 6.70 9.07%
4 • MACA AVENA STA CATALINA 4.57 5.08 4.38%
5 • AVENA GRANO DE ORO 4.99 4.40 3.95%
6 • CEREAL ANGEL 3.45 4.22 3.89%
7 • AVENA DEL FUNDO 4.13 4.43 3.77%
8 • MCA AVENA QUAKER 4.79 4.64 3.40%
9 • AVENA QUAKER 1.16 0.62 0.44%
10 • CEBADA C/QUINUA ANGEL 0.28 0.14 0.30%

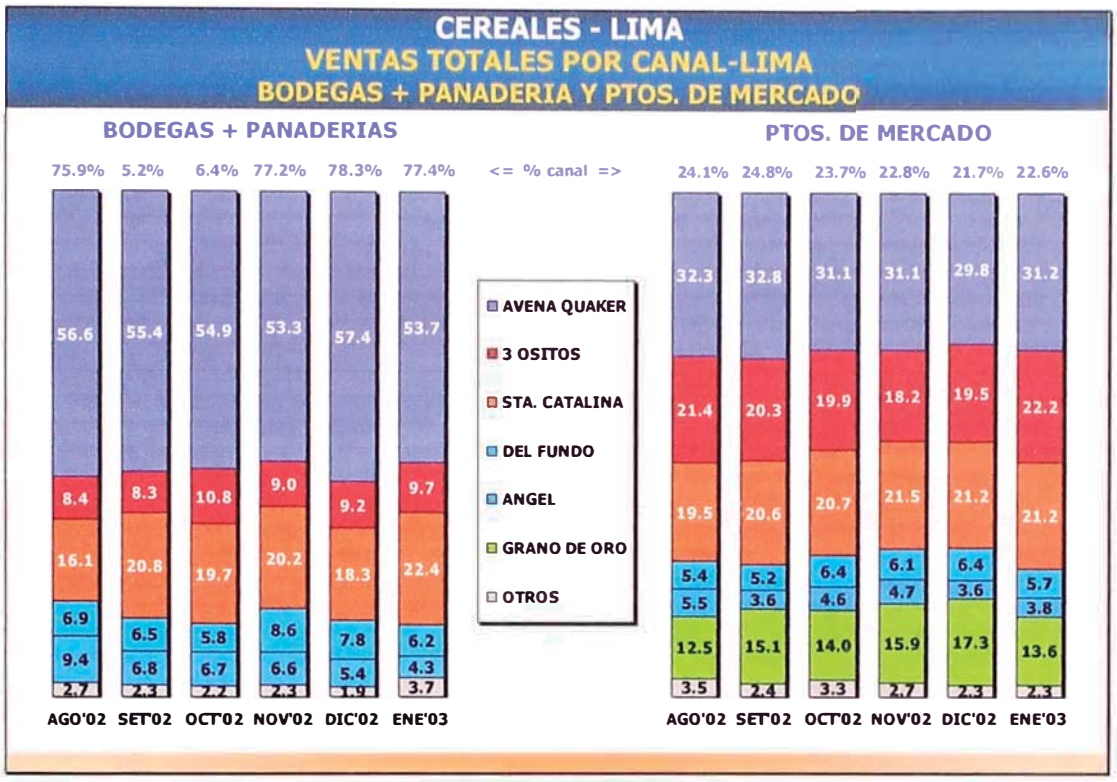
CEREALES - LIMA
DISTRIBUCION TOTAL Y PONDERADA POR MARCA
BODEGAS + PANADERIA Y PTOS. DE MERCADO

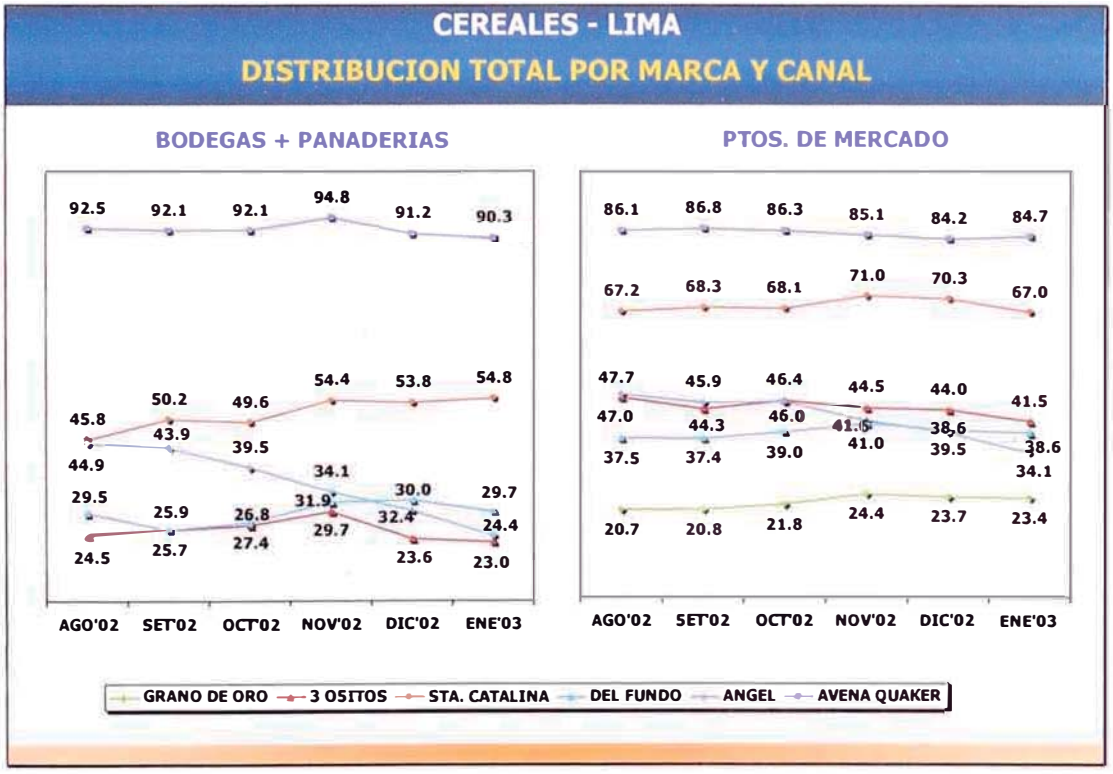


CEREALES - LIMA
NÚMERO DE MARCAS
QUE SE COMERCIALIZAN POR NEGOCIO

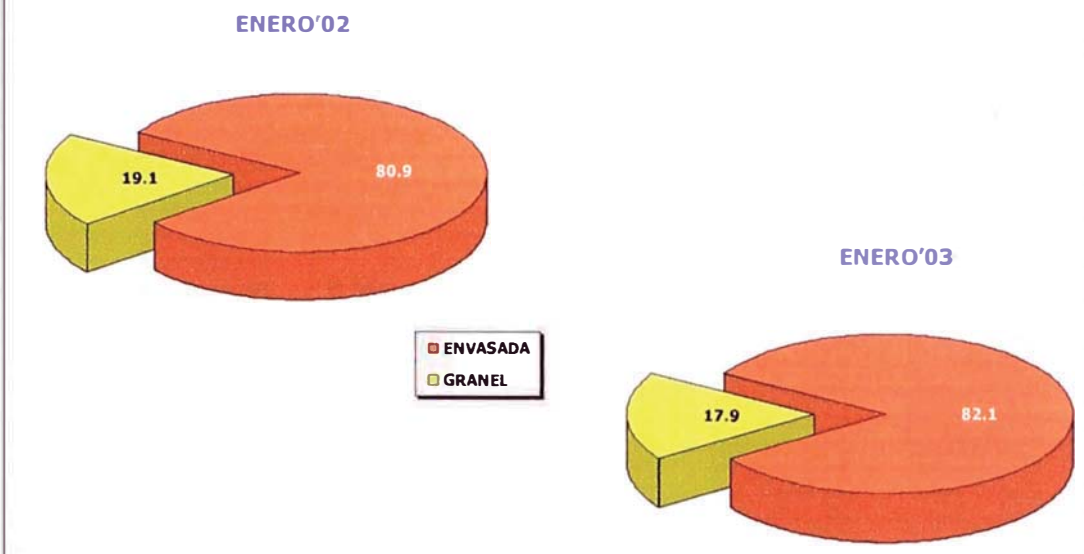


El 83.8% de los negocios comercializa de 1 a 3 marcas

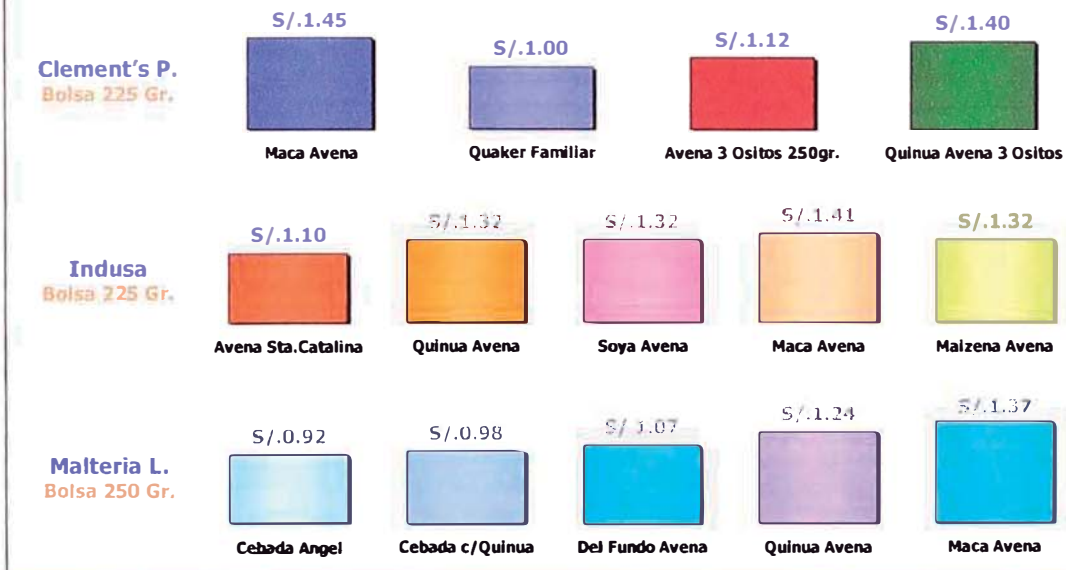

CEREALES - LIMA
VENTAS TOTALES POR CANAL-LIMA
BODEGAS + PANADERIA Y PTOS. DE MERCADO
BODEGAS + PANADERIAS
PTOS. DE MERCADO
75.9% 5.2% 6.4% 77.2% 78.3% 77.4%
<= % canal =>
24.1% 24.8% 23.7% 22.8% 21.7% 22.6%
56.6 8.4 16.1 6.9 9.4 2.7
55.4 8.3 20.8 6.5 6.8 2.3
54.9 10.8 19.7 5.8 6.7 2.2
53.3 9.0 20.2 8.6 6.6 2.3
57.4 9.2 18.3 7.8 5.4 1.9
53.7 9.7 22.4 6.2 4.3 3.7
32.3 21.4 19.5 5.4 5.5 12.5 3.5
32.8 20.3 20.6 5.2 3.6 15.1 2.4
31.1 19.9 20.7 6.4 4.6 14.0 3.3
31.1 18.2 21.5 6.1 4.7 15.9 2.7
29.8 19.5 21.2 6.4 3.6 17.3 2.3
31.2 22.2 21.2 5.7 3.8 13.6 2.3
AVENA QUAKER
3 OSITOS
STA. CATALINA
DEL FUNDO
ANGEL
GRANO DE ORO
OTROS
AGO'02 SET'02 OCT'02 NOV'02 DIC'02 ENE'03
AGO'02 SET'02 OCT'02 NOV'02 DIC'02 ENE'03

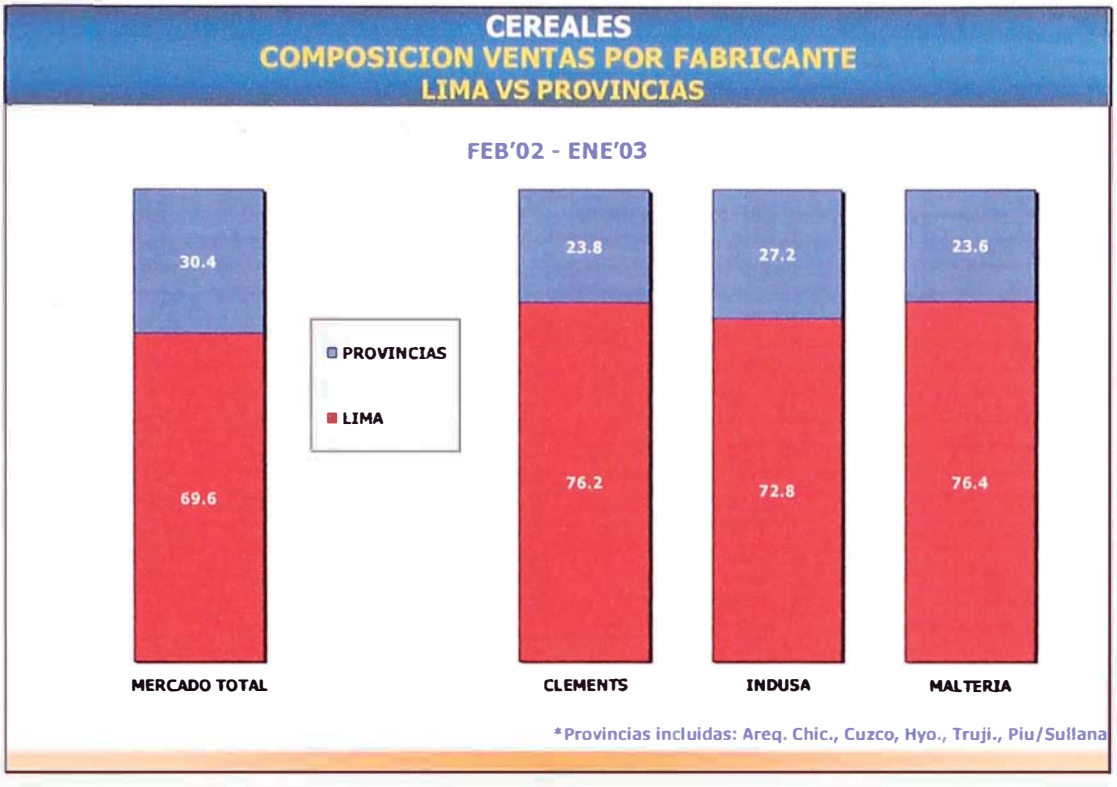

CEREALES - LIMA
DISTRIBUCION TOTAL POR MARCA Y CANAL
BODEGAS + PANADERIAS
PTOS. DE MERCADO
92.5 92.1 92.1 94.8 91.2 90.3
45.8 50.2 49.6 54.4 53.8 54.8
44.9 43.9 39.5 34.1 30.0 29.7
29.5 25.9 26.8 31.9 32.4 24.4
24.5 25.7 27.4 29.7 23.6 23.0
86.1 86.8 86.3 85.1 84.2 84.7
67.2 68.3 68.1 71.0 70.3 67.0
47.7 45.9 46.4 44.5 44.0 41.5
47.0 44.3 46.0 41.6 38.6 38.6
37.5 37.4 39.0 41.0 39.5 34.1
20.7 20.8 21.8 24.4 23.7 23.4
AGO'02 SET'02 OCT'02 NOV'02 DIC'02 ENE'03
AGO'02 SET'02 OCT'02 NOV'02 DIC'02 ENE'03
GRANO DE ORO
3 OSITOS
STA. CATALINA
DEL FUNDO
ANGEL
AVENA QUAKER

CEREALES - LIMA
PERFIL DE VENTAS POR PRESENTACION



CEREALES - LIMA
PRECIOS PROMEDIO
ENERO, 2003

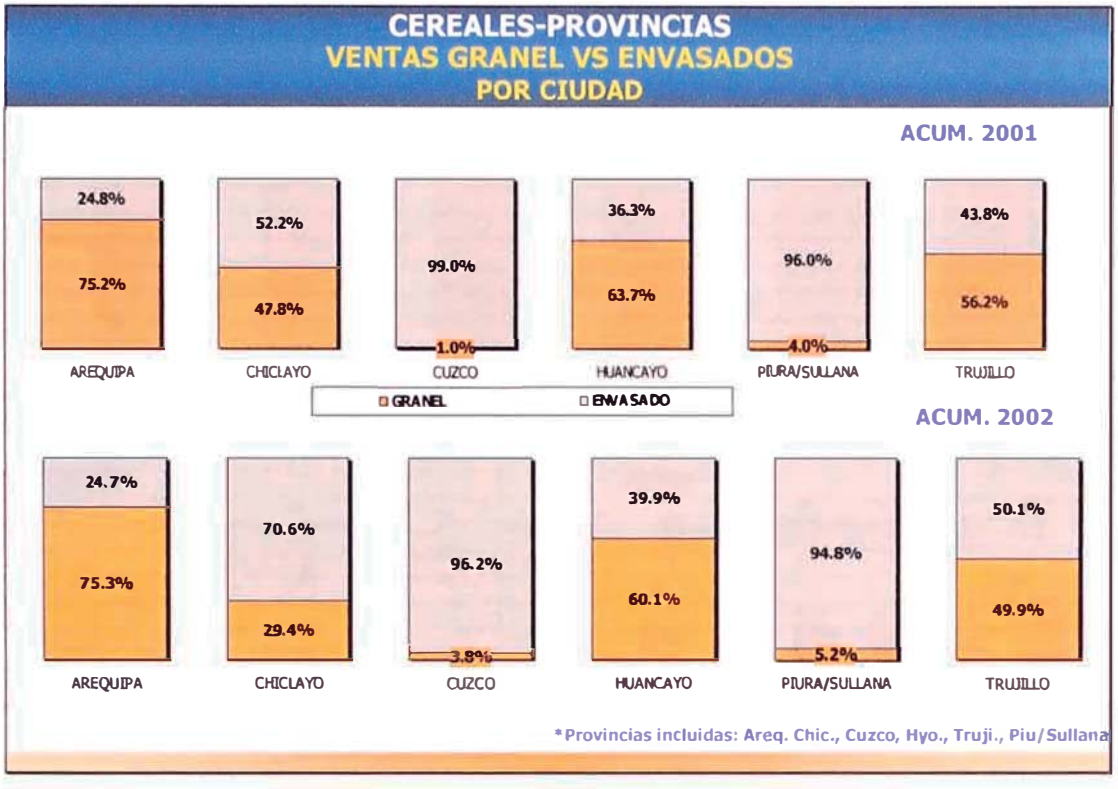


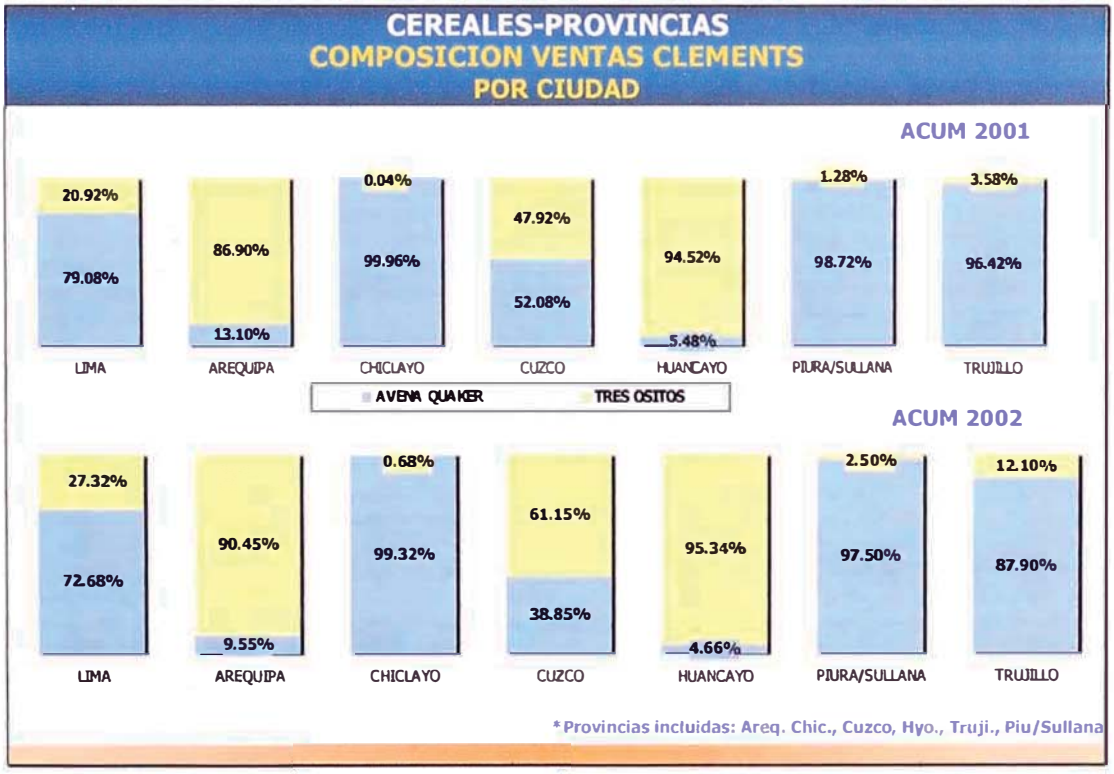


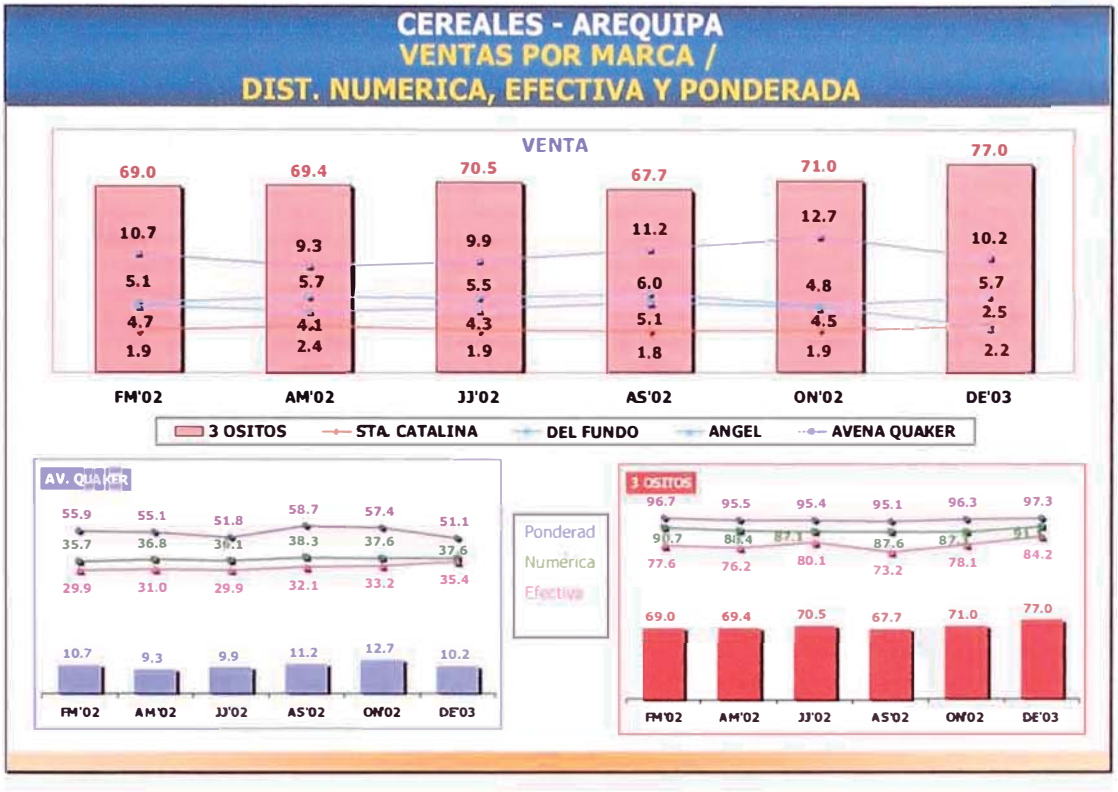
AUDITORIA DE PRODUCTO

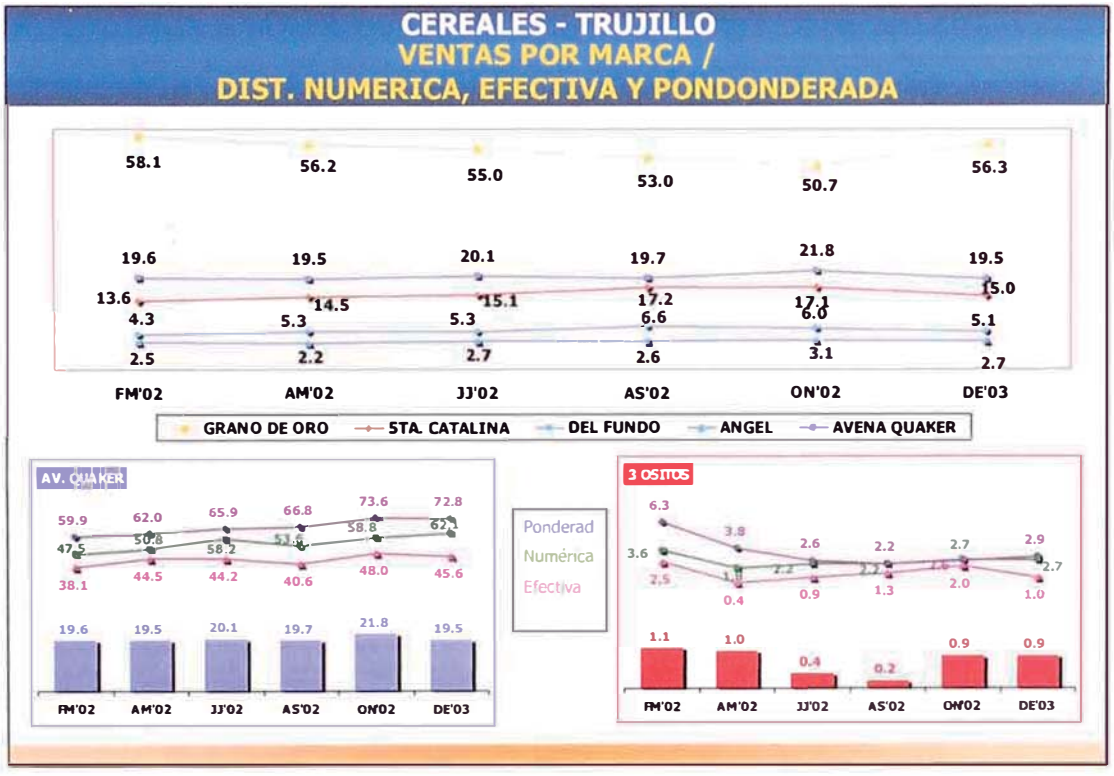
CEREALES
PROVINCIAS

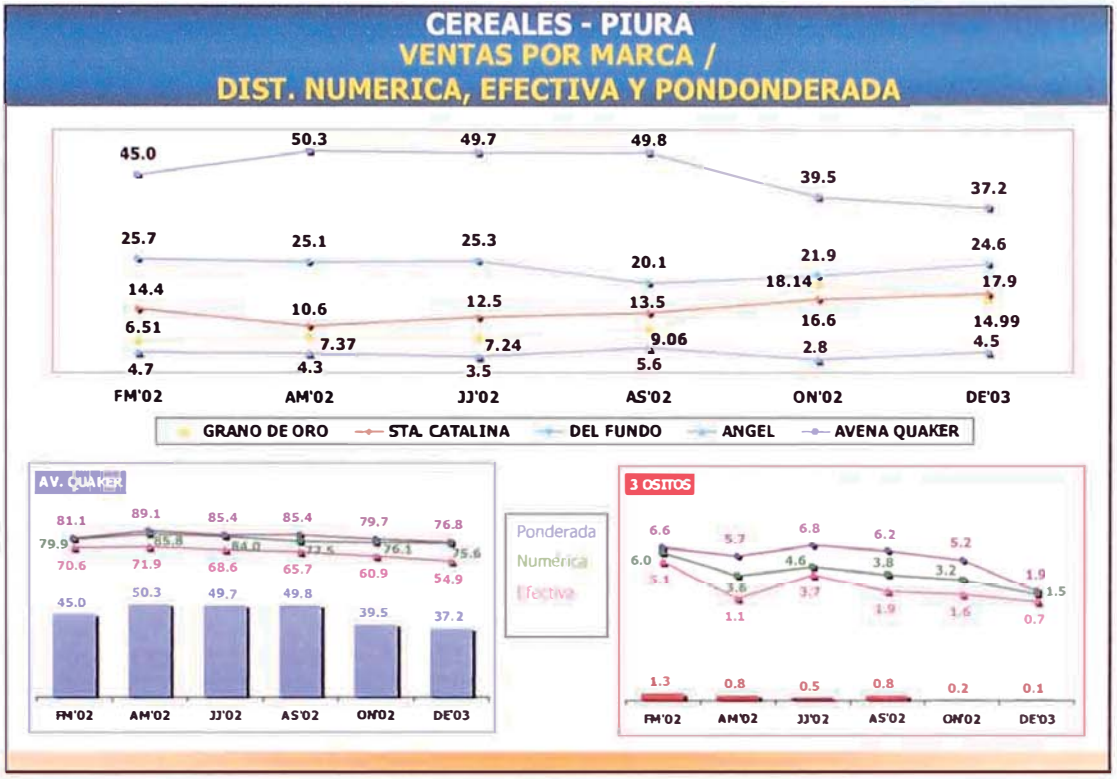
Diciembre, 2002 - Enero, 2003

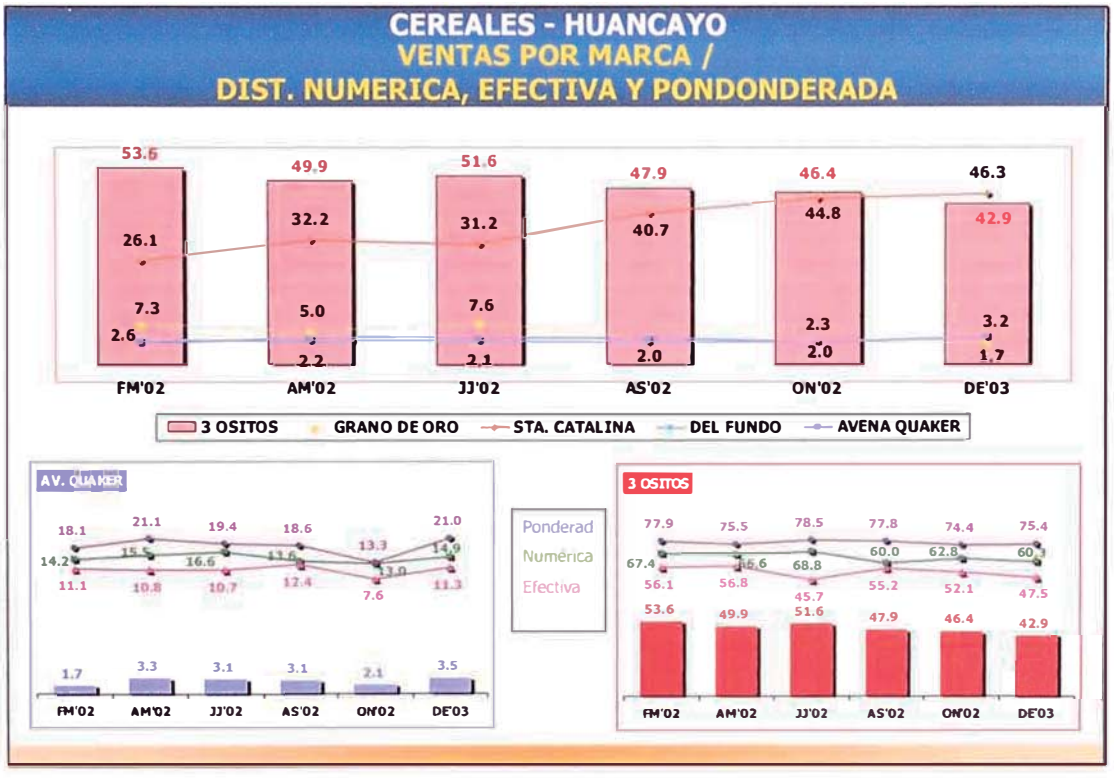

CEREALES-PROVINCIAS
VENTAS GRANEL VS ENVASADOS
POR CIUDAD
ACUM. 2001
24.8%
75.2%
52.2%
47.8%
99.0%
1.0%
36.3%
63.7%
96.0%
4.0%
43.8%
56.2%
AREQUIPA
CHICLAYO
CUZCO
HUANCAYO
PIURA/SULLANA
TRUJILLO
GRANEL
ENVASADO
ACUM. 2002
24.7%
75.3%
70.6%
29.4%
96.2%
3.8%
39.9%
60.1%
94.8%
5.2%
50.1%
49.9%
AREQUIPA
CHICLAYO
CUZCO
HUANCAYO
PIURA/SULLANA
TRUJILLO
*Provincias incluidas: Areq. Chic., Cuzco, Hyo., Truji., Piu/Sullana

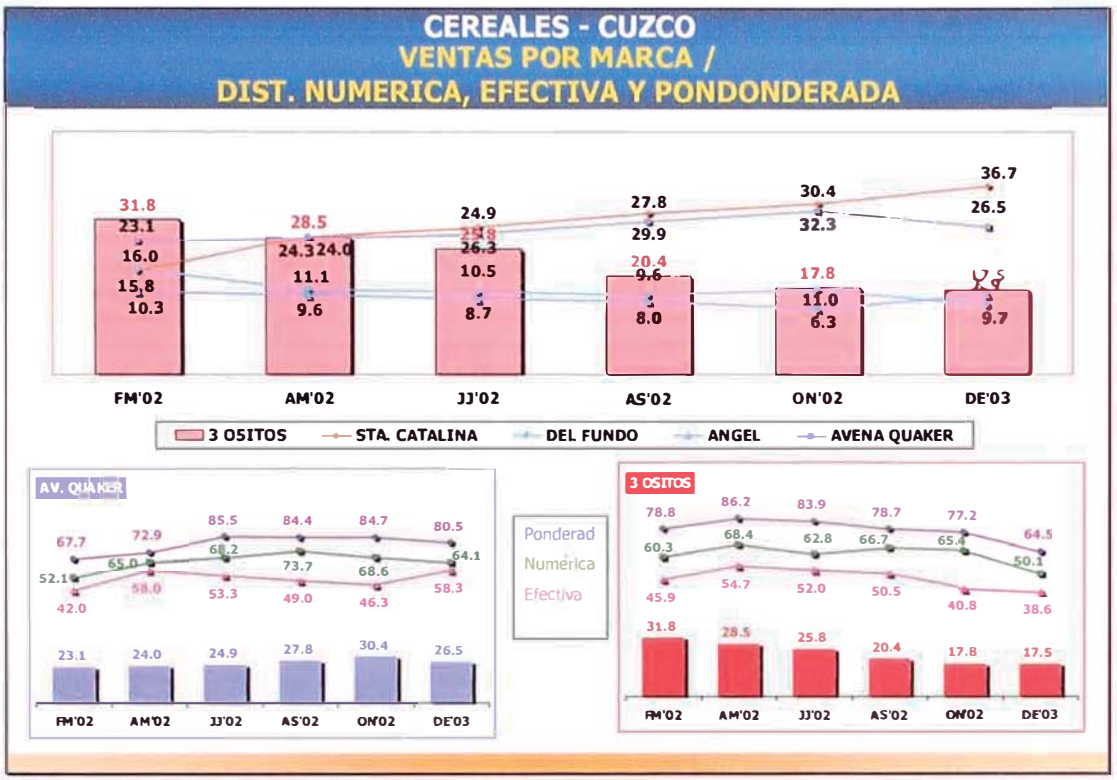

CEREALES-PROVINCIAS
COMPOSICION VENTAS CLEMENTS
POR CIUDAD
ACUM 2001
20.92%
79.08%
86.90%
13.10%
0.04%
99.96%
47.92%
52.08%
94.52%
5.48%
1.28%
98.72%
3.58%
96.42%
LIMA
AREQUIPA
CHICLAYO
CUZCO
HUANCAYO
PIURA/SULLANA
TRUJILLO
AVENA QUAKER
TRES OSITOS
ACUM 2002
27.32%
72.68%
90.45%
9.55%
0.68%
99.32%
61.15%
38.85%
95.34%
4.66%
2.50%
97.50%
12.10%
87.90%
LIMA
AREQUIPA
CHICLAYO
CUZCO
HUANCAYO
PIURA/SULLANA
TRUJILLO
*Provincias incluidas: Areq. Chic., Cuzco, Hyo., Truji., Piu/Sullana

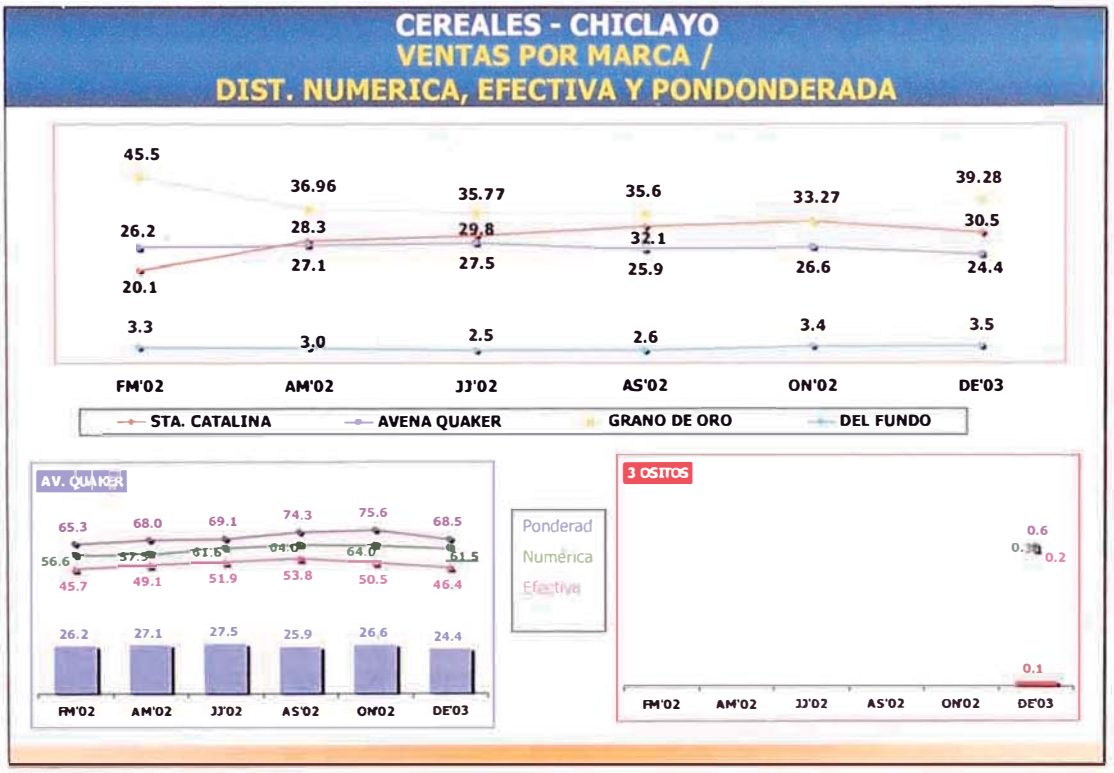

CEREALES - AREQUIPA
VENTAS POR MARCA /
DIST. NUMERICA, EFECTIVA Y PONDERADA
VENTA
69.0
69.4
70.5
67.7
71.0
77.0
10.7
5.1
4.7
1.9
9.3
5.7
4.1
2.4
9.9
5.5
4.3
1.9
11.2
6.0
5.1
1.8
12.7
4.8
4.5
1.9
10.2
5.7
2.5
2.2
FM'02
AM'02
JJ'02
AS'02
ON'02
DE'03
3 OSITOS
STA. CATALINA
DEL FUNDO
ANGEL
AVENA QUAKER
AV. QUAKER
Ponderad
Numérica
Efectiva
3 OSITOS


CEREALES - TRUJILLO
VENTAS POR MARCA /
DIST. NUMERICA, EFECTIVA Y PONDONDERADA
58.1
56.2
55.0
53.0
50.7
56.3
19.6
19.5
20.1
19.7
21.8
19.5
13.6
14.5
15.1
17.2
17.1
15.0
4.3
5.3
5.3
6.6
6.0
5.1
2.5
2.2
2.7
2.6
3.1
2.7
FM'02
AM'02
JJ'02
AS'02
ON'02
DE'03
GRANO DE ORO
STA. CATALINA
DEL FUNDO
ANGEL
AVENA QUAKER
AV. QUAKER
Ponderad
Numérica
Efectiva
3 OSITOS


CEREALES - PIURA
VENTAS POR MARCA /
DIST. NUMERICA, EFECTIVA Y PONDONDERADA
45.0 50.3 49.7 49.8 39.5 37.2
25.7 25.1 25.3 20.1 21.9 24.6
14.4 10.6 12.5 13.5 18.14 17.9
6.51 7.37 7.24 9.06 16.6 14.99
4.7 4.3 3.5 5.6 2.8 4.5
FM'02 AM'02 JJ'02 AS'02 ON'02 DE'03
GRANO DE ORO
STA. CATALINA
DEL FUNDO
ANGEL
AVENA QUAKER
AV. QUAKER
81.1 89.1 85.4 85.4 79.7 76.8
79.9 85.8 84.0 73.5 76.1 75.6
70.6 71.9 68.6 65.7 60.9 54.9
45.0 50.3 49.7 49.8 39.5 37.2
FM'02 AM'02 JJ'02 AS'02 ON'02 DE'03
Ponderada
Numérica
Efectiva
3 OSITOS
6.6 5.7 6.8 6.2 5.2
6.0 4.6 3.8 3.2 1.9
5.1 3.6 3.7 1.9 1.6 0.7
1.5
1.3 0.8 0.5 0.8 0.2 0.1
FM'02 AM'02 JJ'02 AS'02 ON'02 DE'03


CEREALES - HUANCAYO
VENTAS POR MARCA /
DIST. NUMERICA, EFECTIVA Y PONDONDERADA
53.6 49.9 51.6 47.9 46.4 46.3
26.1 32.2 31.2 40.7 44.8 42.9
7.3 5.0 7.6 2.3 3.2
2.6 2.2 2.1 2.0 2.0 1.7
FM'02 AM'02 JJ'02 AS'02 ON'02 DE'03
3 OSITOS
GRANO DE ORO
STA. CATALINA
DEL FUNDO
AVENA QUAKER
AV. QUAKER
18.1 21.1 19.4 18.6 13.3 21.0
14.2 15.5 16.6 13.6 13.0 14.9
11.1 10.8 10.7 12.4 7.6 11.3
1.7 3.3 3.1 3.1 2.1 3.5
FM'02 AM'02 JJ'02 AS'02 ON'02 DE'03
Ponderad
Numérica
Efectiva
3 OSITOS
77.9 75.5 78.5 77.8 74.4 75.4
67.4 65.6 68.8 60.0 62.8 60
56.1 56.8 45.7 55.2 52.1 47.5
53.6 49.9 51.6 47.9 46.4 42.9
FM'02 AM'02 JJ'02 AS'02 ON'02 DE'03


CEREALES - CUZCO
VENTAS POR MARCA /
DIST. NUMERICA, EFECTIVA Y PONDONDERADA
FM'02
AM'02
JJ'02
AS'02
ON'02
DE'03
3 OSITOS
STA. CATALINA
DEL FUNDO
ANGEL
AVENA QUAKER
AV. QUAKER
3 OSITOS
Ponderad
Numérica
Efectiva


CEREALES - CHICLAYO
VENTAS POR MARCA /
DIST. NUMERICA, EFECTIVA Y PONDONDERADA
FM'02
AM'02
JJ'02
AS'02
ON'02
DE'03
STA. CATALINA
AVENA QUAKER
GRANO DE ORO
DEL FUNDO
AV. QUAKER
3 OSITOS
Ponderad
Numérica
Efectiva

CEREALES

CONCLUSIONES

- A NIVEL DE FABRICANTES, HEMOS MANTENIDO EL NIVEL DE VENTAS A TRAVÉS DE TODO EL AÑO. INDUSA, EN CAMBIO, EXPERIMENTA UN CRECIMEINTO SOSTENIDO CON LO CUAL GANA MERCADO DIRECTAMENTE A MALETRIA LIMA

- A NIVEL DE MARCAS, EL LIDER ABSOLUTO ES AVENA QUAKER, CON SU PRESENTACIÓN DE AVENA FAMILIAR LO QUE BASICAMENTE ES UN REFLEJO DEL FACTOR PRECIO, SIENDO ESTA PRESENTACIÓN MUY ECONÓMICA.

- CONOCER QUE EL 84% DE NEGOCIOS OFRECEN ENTRE 1 A 3 MARCAS DE CEREAL, NOS ALERTA A NO DEJAR VACIOS EN LA DISTRIBUCIÓN DEL PRODUCTO POR SER FACILMENTE SUSTITUIDOS POR LA COMPETENCIA (POR EL NIVEL DE DISTRIBUCIÓN SERÍAMOS SUSTITUIDOS POR SANTA CATALINA O ANGEL).

ANEXO 3: LAS DIEZ VULNERABILIDADES DE SEGURIDAD MÁS CRÍTICAS EN APLICACIONES WEB

El siguiente es un breve sumario de las vulnerabilidades más significantes de la seguridad de aplicaciones Web.

A1 Entrada no validada

La información de llamadas Web no es validada antes de ser usadas por la aplicación Web. Los agresores pueden usar estas fallas para atacar los componentes internos a través de la aplicación Web.

A2 Control de Acceso Interrumpido

Las restricciones de aquello que tienen permitido hacer los usuarios autentificados no se cumplen correctamente. Los agresores pueden explotar estas fallas para acceder a otras cuentas de usuarios, ver archivos sensitivos o usar funciones no autorizadas.

A3 Administración de Autenticación y Sesión Interrumpida

Las credenciales de la cuenta y los tokens de sesiones no están propiamente protegidos. Los agresores que pueden comprometer las contraseñas, claves, cookies de sesiones u otro token, pueden vencer las restricciones de autenticación y asumir la identidad de otros usuarios.

A4 Fallas de Cross Site Scripting (XSS)

La aplicación Web puede ser usada como un mecanismo para transportar un ataque al navegador del usuario final. Un ataque exitoso puede comprometer el token de sesión del usuario final, atacar la maquina local o enmascarar contenido para engañar al usuario.

A5 Desbordamiento del Búfer

Los componentes de aplicaciones Web en ciertos lenguajes que no validan adecuadamente las entradas de datos pueden ser derribados y, en algunos casos, usados para tomar control de un proceso. Estos componentes pueden incluir CGI, bibliotecas, rutinas y componentes del servidor de aplicación Web.

A6 Fallas de Inyección

La aplicación Web puede pasar parámetros cuando accede a sistemas externos o al sistema operativo local. Si un agresor puede incrustar comandos maliciosos en estos parámetros, el sistema externo puede ejecutar estos comandos por parte de la aplicación Web.

A7 Manejo Inadecuado de Errores

Condiciones de error que ocurren durante la operación normal que no

son manejadas adecuadamente. Si un agresor puede causar que ocurran errores que la aplicación Web no maneja, éste puede obtener información detallada del sistema, denegar servicios, causar que mecanismos de seguridad fallen o tumbar el servidor.

A8 Almacenamiento Inseguro

Las aplicaciones Web frecuentemente utilizan funciones de criptografía para proteger información y credenciales. Estas funciones y el código que integran a el as han sido difíciles de codificar adecuadamente, lo cual frecuentemente redunda en una protección débil.

A9 Negación de Servicio

Los agresores pueden consumir los recursos de la aplicación Web al punto de que otros usuarios legítimos no puedan ya acceder o usar la aplicación. Los agresores también pueden dejar a los usuarios fuera de sus cuentas y hasta causar que falle una aplicación entera.

A10 Administración de Configuración Insegura

Tener una configuración de servidor estándar es crítico para asegurar una aplicación Web. Estos servidores tienen muchas opciones de configuración que afectan la seguridad y no son seguro desde la instalación original del software.

A1 ENTRADA NO VALIDA

Descripción:

Las aplicaciones Web usan entradas de l amadas HTTP (y

ocasionalmente archivos) para determinar cómo responder. Los atacantes pueden entrometerse con cualquier parte del l amado HTTP, incluyendo el URL, cadena de consulta (querystring), encabezados, cookies, campos de formularios (normales o escondidos), para tratar de pasar por encima de los mecanismos de seguridad del sitio. Nombres comunes para ataques de manipulación de entradas incluyen: navegación forzada, inserción de comandos, cross site scripting, desbordamiento de búfer, ataques de formato de cadena de caracteres, inyección de SQL, manipulación de cookies y campos escondidos. Cada uno de estos ataques es descrito detalladamente más adelante en este documento.

A4 Fallas de Cross Site Scripting trata sobre las entradas que contiene pequeños programas para ser ejecutados en el navegador de otros usuarios

A5 Desbordamiento de búfer trata sobre las entradas que ha sido diseñadas para sobrescribir el espacio de ejecución de un programa

A6 Fallas de inyección trata sobre las entradas que son modificadas para contener comandos ejecutables

Algunos sitios tratan de protegerse el os mismos por medio del filtrado de entradas maliciosas. El problema es que hay muchas formas diferentes de codificar información. Estos formatos de codificación no son como la encriptación, ya que éstos son triviales para decodificar. Aun así, los desarrolladores a veces olvidan decodificar todos los parámetros a su forma más simple antes de usarlos. Los parámetros tienen que ser convertidos a su forma más simple antes de ser validados, de otro modo, las entradas maliciosas puede ser enmascarado y pueden pasar a través de los filtros. El proceso de simplificar estas codificaciones es llamado "canonicalization". Ya que casi todas las entradas HTTP pueden ser representadas en múltiples formatos, esta técnica puede ser usada para obscurecer cualquier ataque utilizando las vulnerabilidades descritas en este documento. Esto hace el

filtrado muy difícil.

Un número sorprendente de aplicaciones Web utilizan sólo mecanismos de validación de entradas a nivel del cliente. Los mecanismos de validación a nivel del cliente son fácilmente sobrepasados, dejando la aplicación Web sin ninguna protección contra parámetros maliciosos. Los atacantes pueden generar sus propias l amadas HTTP usando herramientas tan simples como Telnet. Estos no necesitan poner atención a las cosas que el desarrollador tenía la intención de que ocurriesen a nivel del cliente. Hay que notar que la validación a nivel del cliente es una buena idea para el rendimiento y la usabilidad, pero no tiene ningún beneficio de seguridad. Las verificaciones a nivel del servidor son requeridas para defender contra los ataques de manipulación de parámetros. Ya estando éstas en funcionamiento, la verificación a nivel del cliente puede también ser incluida para mejorar la experiencia del usuario para usuarios legítimos y/o reducir la cantidad de tráfico inválido hacia el servidor.

Estos ataques están siendo cada vez más comunes, a la vez que el número de herramientas que soportan generación de parámetros (fuzzing), corrupción y fuerza bruta continúan creciendo. El impacto al usar datos de entrada no validados no debería ser subestimado. Una gran cantidad de ataques sería difícil o imposible si los desarrolladores simplemente pudieran validar la entrada de datos antes de usarla. A menos que una aplicación Web tenga un mecanismo fuerte y centralizado para validar todas las entradas para las llamadas HTTP (o cualquier otra fuente), las vulnerabilidades basadas en entradas maliciosas seguirán existiendo

Ambientes Afectados

Todos los servidores Web, servidores de aplicaciones, y ambientes de aplicación Web son susceptibles a la manipulación de parámetros

¿Cómo Determinara Si Usted Es Vulnerable?

Cualquier parte de una llamada HTTP usada por una aplicación Web sin ser cuidadosamente validada se conoce como parámetro "sucio". La manera más simple de encontrar el uso de un parámetro "sucio" es tener una revisión de código detallado, buscando todas las llamadas donde la información es extraída de una llamada HTTP. Por ejemplo, en una aplicación J2EE, estos son los métodos en la clase HttpServletRequest. Después se puede seguir el código para ver donde se ha utilizado esa variable. Si la variable no se revisa antes de ser usada, seguramente habrá un problema.

También es posible encontrar el uso de parámetros sucios empleando herramientas como OWASP's WebScarab. Al aceptar valores inesperados en l amadas HTTP y observando las respuestas de las aplicaciones Web, se pueden identificar los lugares donde se usan los parámetros sucios.

¿Cómo Autoprotegerse?

La mejor forma de prevenir la manipulación de parámetros es asegurando que todos los parámetros sean validados antes de que sean usados. Un componente centralizado o librería seria una de las formas más efectivas ya que el código que aplica la verificación debería estar en un sólo lugar. Cada parámetro debe ser verificado contra un formato estricto que especifica exactamente qué entrada de datos debe ser permitida. Es improbable que alcances "negativos" que involucran filtrado de entradas maliciosas o alcances basados en firmas (signatures) sean efectivos, además pueden ser difíciles de mantener.

Los parámetros deben ser validados contra una especificación "positiva" que define:

- Tipo de datos (string, integer, real, etc....)
- Conjunto de caracteres permitidos
- Longitud mínima y máxima
- Si nulo es permitido
- Si el parámetro es requerido o no
- Si los duplicados son permitidos
- El rango numérico
- Valores específicos permitidos (enumeración)
- Patrones específicos (expresiones regulares)

Una nueva clase de aparatos de seguridad conocidos como cortafuegos (firewalls) de aplicaciones Web pueden proveer algunos servicios de validación de parámetros. Sin embargo, para que éstos sean efectivos, el aparato debe estar configurado con una estricta definición de qué es válido para cada parámetro del sitio. Esto incluye proteger adecuadamente todos los tipos de entrada de las llamadas HTTP, incluyendo URLs, formularios, cookies, querystrings, campos escondidos y parámetros.

El proyecto *OWASP Filters* está produciendo componentes reutilizables en diferentes lenguajes para ayudar a evitar diferentes formas de manipulación de parámetros. El motor de validación de llamadas HTTP, Stinger (stinger.sourceforge.net), fue también desarrollado por OWASP para ambientes J2EE.

A2 CONTROL DE ACCESO INTERRUMPIDO

Descripción

El control de acceso, algunas veces llamado autorización, es el cómo una aplicación Web permite el acceso a contenido y funciones a

algunos usuarios y a otros no. Estas verificaciones son desarrolladas después de la autenticación, y gobiernan lo que pueden hacer los usuarios "autorizados". El control de acceso suena como un problema simple pero es insidiosamente difícil de implementar correctamente. El modelo de control de acceso de una aplicación Web tiene un lazo estrecho con el contenido y funciones que el sitio provee. Además, los usuarios pueden caer dentro de un número de grupos o roles con diferentes capacidades o privilegios.

Los desarrolladores frecuentemente menosprecian la dificultad de implementar un mecanismo de control de acceso confiable. Muchos de estos esquemas no fueron diseñados deliberadamente, sino simplemente han evolucionado junto con el sitio Web. En estos casos, las reglas de control de acceso son insertadas en varias locaciones en todo el código. Al acercarse el desplegado del sitio, la colección ad hoc de reglas se convierte tan difícil de manejar que es casi imposible de comprender.

Muchas de estas fallas en los esquemas de control de acceso no son difíciles de encontrar y explotar. Frecuentemente, todo lo que se requiere es hacer una petición por funciones o contenido que no debe ser concedido. Una vez que se descubre una falla, las consecuencias de un esquema de control de acceso con fallas pueden ser devastadoras. Además de visualizar contenido no autorizado, un atacante podría alterar o borrar contenido, realizar funciones no autorizadas, o aún tomar el control de la administración del sitio.

Un tipo específico de problema de control de acceso es la interfase administrativa que permite a los administradores del sitio manejar un sitio mediante Internet. Tales características son usadas frecuentemente para permitir a los administradores del sitio manejar eficientemente los usuarios, datos, y contenido en su sitio. En muchos casos, los sitios soportan una variedad de roles administrativos para permitir una granulación más fina de la administración del sitio. Debido a su poder, estas interfaces son

frecuentemente los objetivos primarios de un ataque ya sea por personas del exterior o del interior.

Ambientes Afectados

Todos los servidores Web conocidos, servidores de aplicación, y aplicaciones Web son susceptibles a por lo menos alguna de estas cuestiones. Aún si un sitio es completamente estático, si no está apropiadamente configurado, los piratas informáticos pueden obtener acceso a archivos sensibles y manipularlos o realizar otro tipo de daños

¿Cómo Determinara Si Usted Es Vulnerable?

Virtualmente todos los sitios tienen algunos requisitos de control de acceso. Por lo tanto, una política de control de acceso debe ser claramente documentada. También la documentación de diseño debe capturar una propuesta para reforzar esta política. Si esta documentación no existe, entonces es muy probable que el sitio sea vulnerable.

El código que implementa la política de control de acceso debe ser verificado. Tal código debe estar bien estructurado, ser modular y preferiblemente centralizado. Una verificación detallada del código debe ser realizada para validar la implementación correcta del control de acceso. Además, las pruebas de penetración pueden ser muy útiles para determinar si hay problemas en el esquema de control de acceso.

Investigue cómo es administrado su sitio Web. Querrá descubrir cómo son hechos los cambios a las páginas Web, dónde son probados y cómo son transportados al servidor de producción. Si los administradores pueden hacer cambios de forma remota, deseará saber cómo son protegidos esos canales de comunicación. Revise cuidadosamente cada interfase para asegurarse que solamente los

administradores autorizados tienen el acceso permitido. También, si existen diferentes tipos o grupos de datos a los que se puede acceder mediante la interfase, asegúrese que sólo se puede acceder a los datos autorizados. Si tales interfaces emplean comandos externos, verifique el uso de tales comandos para asegurar que no están sujetos a ninguna falla de inyección de comandos descritos en este documento

¿Cómo Autoprotegerse?

El paso más importante es pensar a partir de los requisitos de control de acceso de una aplicación y capturar este pensamiento en una política de seguridad para aplicaciones Web. Recomendamos encarecidamente el uso de una matriz de control de acceso para definir las reglas de control de acceso. Sin documentar la política de seguridad, no existe una definición de lo que significa estar seguro para ese sitio. La política debe documentar qué tipos de usuarios pueden acceder al sistema y a cuáles funciones y contenidos se les debería permitir el acceso a cada uno de estos tipos de usuarios. El mecanismo de control de acceso debe ser probado extensivamente para asegurar que no hay forma de evitarla. Estas pruebas requieren de una variedad de cuentas e intentos exhaustivos para acceder contenidos o funciones no autorizadas.

Algunos asuntos de control de acceso específico incluyen:

- Id's inseguros – la mayoría de los sitios Web utilizan alguna forma de id, llave o índice como una manera de referenciar usuarios, roles, contenido, objetos o funciones. Si un atacante puede adivinar estos id's y los valores provistos no son validados para asegurar que son autorizados para el usuario actual, el atacante puede ejercer libremente el esquema de control de acceso para ver a qué es lo que puede acceder. Las aplicaciones Web no deben depender del secreto de ningún id para su protección

- Navegación Forzada Saltando la Verificación del Control de Acceso – muchos sitios requieren que los usuarios pasen por ciertas verificaciones antes de que se les garantice el acceso a ciertos URLs que están típicamente colocados 'más profundamente' en el sitio. Estas verificaciones no deben ser evitables por un usuario que simplemente se salta la página que contiene la verificación de seguridad

- Cruce de Dirección de Fichero ("path traversal") – este ataque involucra proveer información relativa a la dirección de fichero (Ej., "./../target_dir/target_file") como parte de una petición por información. Tales ataques tratan de acceder archivos que normalmente no son accesibles para nadie o que podrían ser negados si se solicitan directamente. Tales ataques pueden ser enviados en URLs así como en cualquier otra entrada que en última instancia acceda a un archivo (Ej., llamadas a sistema y la interfase de comando "shell command").

- Permisos de Archivos muchos servidores y aplicaciones Web se basan en listas de control de acceso provistas por el sistema de archivos de la plataforma subyacente. Aun si casi todos los datos son almacenados en servidores de soporte DBMS ("backend servers"), siempre hay archivos almacenados localmente en el servidor y aplicación Web que no deben ser públicamente accesibles, particularmente archivos de configuración, archivos por defecto y scripts que son instalados en la mayoría de los servidores y aplicaciones Web. Solamente archivos que son específicamente diseñados para ser presentados a los usuarios Web deben ser marcados como legibles usando los mecanismos de permiso de los SO's, la mayoría de los directorios no deben ser legibles y muy pocos

archivos, si acaso existen, deben ser marcados como ejecutables.

- Cache del Lado Cliente ("client side caching") – muchos usuarios acceden a aplicaciones Web de computadoras compartidas localizadas en bibliotecas, escuelas, aeropuertos y otros puntos de acceso público. Los navegadores frecuentemente ponen en cache las páginas Web que pueden ser accedidas por atacantes para ganar acceso a partes o sitios de otra forma inaccesibles. Los desarrolladores deben usar múltiples mecanismos, incluyendo cabeceras HTTP y meta etiquetas ("meta tags"), para asegurarse que las páginas que contienen información sensitiva no sean capturadas en cache por el navegador del usuario.

Existen algunos componentes de seguridad a nivel aplicación que ayudan en el refuerzo apropiado de algunos aspectos de su esquema de control de acceso. Nuevamente, como con la validación de parámetro, para que sea efectiva, el componente debe ser configurado con una estricta definición de qué peticiones de acceso son válidas para su sitio. Cuando se utilice tal componente, debe ser cuidadoso para comprender exactamente qué ayuda puede proveer para usted la componente de control dada la política de seguridad de su sitio y qué parte de su política de control de acceso no puede manejar el componente y por lo tanto debe ser manejado apropiadamente en su propio código.

Para funciones administrativas, la recomendación primordial, si es del todo posible, es nunca permitir el acceso del administrador a través de la puerta principal de su sitio. Dado el poder de estas interfaces, la mayoría de las organizaciones no deben aceptar el riesgo de que estas interfaces estén disponibles para ataques externos. Si es absolutamente requerido el acceso del administrador remoto, esto puede ser logrado sin tener que abrir la puerta principal del sitio. El uso de la

tecnología VPN ("Virtual Private Network") puede ser utilizado para proveer el acceso del administrador externo al interior de la red de la compañía (o sitio) desde la cual un administrador puede entonces acceder al sitio a través de una conexión de soporte DBMS ("backend") protegida.

A3 ADMINISTRACION DE AUTENTICACIÓN Y SESION INTERRUMPIDA

Descripción

La administración de autenticación y sesión incluye todos los aspectos del manejo de la autenticación de usuario y la administración de sesiones activas. La autenticación es un aspecto crítico de este proceso, pero inclusive mecanismos de autenticación sólidos pueden ser minados por funciones de administración de credenciales defectuosas, incluyendo el cambio de contraseña, olvidé mi contraseña, recordar mi contraseña, actualización de cuenta y otras funciones relacionadas. Porque los ataques de paso ("walk by") son probablemente dirigidos a muchas aplicaciones Web, todas las funciones de administración de cuentas deben requerir re-autenticación aun si el usuario tiene un id de sesión válido.

La autenticación de usuario en Web típicamente involucra el uso de un id de usuario y una contraseña. Métodos más sólidos de autenticación tales como software y hardware basados en tokens criptográficos o biometría están comercialmente disponibles, pero tales mecanismos son de un costo prohibitivo para la mayoría de las aplicaciones Web. Una amplia colección de defectos en la administración de cuentas y sesiones puede traer como consecuencia el comprometer las cuentas de usuario o administración del sistema. Los equipos de desarrollo frecuentemente menosprecian la complejidad de diseñar un esquema de administración de autenticación y sesión que proteja adecuadamente las credenciales en todos los aspectos del sitio.

Las aplicaciones Web deben establecer sesiones para mantener el rastro del flujo de peticiones de cada usuario. HTTP no provee esta capacidad, así que las aplicaciones Web deben crearlas por sí mismas. Frecuentemente, los ambientes de aplicación Web proveen una capacidad de sesión, pero muchos desarrolladores prefieren crear sus propios tokens de sesión. En cualquier caso, si los tokens de sesión no están apropiadamente protegidos, un atacante puede apropiarse de una sesión activa y asumir la identidad del usuario. Diseñar un esquema para crear tokens sólidos de sesión y protegerlos a través de su ciclo de vida ha probado su efectividad para muchos desarrolladores.

A menos que todas las credenciales de autenticación e identificadores de sesión sean protegidos con SSL todo el tiempo y protegidas contra su revelación por causa de otras fallas, tales como "cross site scripting", un atacante puede apropiarse la sesión del usuario y asumir su identidad.

Ambientes Afectados

Todos los ambientes de servidores Web conocidos, servidores de aplicación y aplicaciones Web son susceptibles a los problemas de administración de autenticación y sesión interrumpida.

¿Cómo Determinara Si Usted Es Vulnerable?

Ambas pruebas de verificación de código y penetración pueden ser usadas para diagnosticar problemas de administración de autenticación y sesión. Cuidadosamente verifique cada aspecto de su mecanismo de autenticación para asegurar que las credenciales de usuario están protegidas en todo momento, mientras se encuentran detenidas (Ej., en disco) y mientras están en tránsito (Ej., durante la conexión inicial "login"). Revisa cada mecanismo disponible para cambiar las credenciales de usuario

con el fin de asegurar que sólo un usuario autorizado pueda cambiarlas. Revise su mecanismo de administración de sesión para asegurar que los identificadores de sesión siempre estén protegidos y sean utilizados de tal forma que se minimice la probabilidad de exposición accidental u hostil.

¿Cómo Autoprotegerse?

El uso apropiado y cuidadoso de mecanismos de administración de autenticación y sesión hechos a la medida o sacados del estante ("of the shelf") deben reducir significativamente la probabilidad de algún problema en ésta área. Definiendo y documentando la política de su sitio con respecto a la administración de forma segura de las credenciales de usuario es un buen primer paso. Asegurar que su implementación refuerza consistentemente esta política es la clave para tener un mecanismo de administración de autenticación y sesión seguro y robusto.

Algunas áreas críticas incluyen:

- Contraseñas Resistentes las contraseñas deben tener restricciones que impongan un tamaño y complejidad mínima. La complejidad típicamente requiere el uso de combinaciones mínimas de caracteres alfabéticos, numéricos, y/o no-alfanuméricos en la contraseña de usuario (Ej., por lo menos uno de cada uno). A los usuarios se les debe requerir cambiar su contraseña periódicamente. A los usuarios se les debe impedir re-utilizar contraseñas anteriores.

- Uso de Contraseña se debe restringir a los usuarios a un número definido de intentos de conexión por unidad de tiempo y los repetidos intentos de conexión fallidos deben ser registrados. Las contraseñas provistas durante los intentos fallidos de conexión no deben ser almacenados ya que

esto puede exponer una contraseña de usuario a cualquiera que logre acceder a este registro. El sistema no debe indicar si fue el nombre de usuario o la contraseña lo que estaba equivocado si falla un intento de conexión. Los usuarios deben ser informados de la fecha/hora de su última conexión exitosa y el número de intentos de acceso fallidos a su cuenta desde esa hora.

- Control de Cambios de Contraseña un solo mecanismo de cambio de contraseña debe ser usado donde sea que se permita cambiar a los usuarios su contraseña, independientemente de la situación. A los usuarios siempre se les debe solicitar el ingresar ambas contraseñas, la anterior y la actual, cuando cambian su contraseña (como todas las cuentas informáticas). Si las contraseñas olvidadas son enviadas por correo electrónico a los usuarios, el sistema debe requerir del usuario que se re-autentifique cuantas veces el usuario cambie su dirección de correo electrónico, de lo contrario un atacante que ha tenido acceso temporalmente a su sesión (Ej., acercándose a su computadora mientras está conectado) puede simplemente cambiar su dirección de correo electrónico y solicitar que una contraseña `olvidada' les sea enviada vía correo electrónico.

- Almacenamiento de Contraseña todas las contraseñas deben ser almacenadas ya sea de forma encriptada ("encrypted") o como hashes para protegerlas de ser expuestas, independientemente de donde son almacenados. La forma de hash es preferible ya que no es reversible. La encriptación debe ser usada cuando se necesita la contraseña en texto l ano, tal como cuando se utiliza la contraseña para conectarse a otro sistema. Las contraseñas

nunca deben ser insertadas directamente en el código fuente. Las l aves de descifrado deben ser protegidas fuertemente para asegurar que no puedan ser arrebatadas y usadas para descifrar el archivo de contraseñas.

- Protegiendo Credenciales en Tránsito la única técnica efectiva es encriptar completamente la transacción de acceso al sistema es usando algo como SSL. Las transformaciones sencillas de las contraseñas tales como aplicar un hash en el cliente antes de la transmisión provee poca protección ya que la versión cifrada puede simplemente ser interceptada y retransmitida aunque la contraseña en texto llano no pueda ser conocida.

- Protección del Id de Sesión idealmente, toda la sesión de usuario debe ser protegida mediante SSL. Si esto es hecho, entonces el id de sesión (Ej., cookie de sesión) no puede ser tomado de la red, lo cual es el mayor riesgo de exposición de un id de sesión. Si no es viable el uso de SSL por el desempeño u otras razones, entonces los id's de sesión deben ser protegidos de alguna otra forma. En primera instancia, éstos nunca deben ser incluidos en el URL ya que pueden ser capturados en memoria rápida ("cached") por el navegador, mandados en la cabecera referenciada o accidentalmente re-enviados a un `amigo'. Los id's de sesión deben ser números largos, complicados y aleatorios que no puedan ser fácilmente adivinados. Los id's de sesión pueden también ser cambiados frecuentemente durante una sesión para reducir el tiempo en que es válido un id de sesión. Los id's de sesión deben ser cambiados cuando se cambia a SSL, se autentifica u ocurre otra transacción importante. Los id's de sesión escogidos por un usuario nunca deben ser aceptados.

- Listas de cuentas los sistemas deben ser diseñados para evitar que los usuarios logren acceso a una lista de los nombres de cuentas del sitio. Si las listas de usuarios deben ser mostradas, es recomendable que alguna forma de pseudónimo ("screen name") que corresponda a la cuenta actual sea listada en su lugar. De esa forma el pseudónimo no puede ser usado durante un intento de conexión o algún otro intento de obtener la cuenta de usuario.

- Memoria Rápida ("Cache") del Navegador los datos de autenticación y sesión nunca deben ser suministrados como parte de un GET, en su lugar siempre debe ser utilizado POST. Las páginas de autenticación deben ser marcadas con todas las diversidades de etiquetas de no uso de memoria rápida para prevenir que alguien use el botón de retorno en el navegador del usuario para copiar la página de conexión y re-transmitir las credenciales previamente tecleadas. Muchos navegadores de hoy soportan la bandera ("flag") de `autocomplete=false' para prevenir el almacenamiento de credenciales en la memoria rápida ("cache") de auto completar.

- Relación de Confianza la arquitectura de su sitio debe evitar la confianza implícita entre componentes siempre que sea posible. Cada componente debe autentificarse por sí mismo con cualquier otro componente con el que esté interactuando, a menos que exista una fuerte razón para no hacerlo (tal como el desempeño o la falta de un mecanismo utilizable). Si las relaciones de confianza son requeridas, procedimientos sólidos y mecanismos arquitectónicos deben ser usados para asegurar que no se puede abusar de tal

confianza al evolucionar la arquitectura del sitio con el tiempo.

A4 FALLAS DE CROSS-SITE SCRIPTING (XSS)

Descripción

Las vulnerabilidades de cross-site scripting (algunas veces referido como XSS) ocurren cuando un atacante utiliza una aplicación Web para mandar código malicioso, generalmente en la forma de un *script*, a un usuario diferente. Estas fal as están muy generalizadas y ocurren donde quiera que una aplicación Web utilice entradas de datos de un usuario sin validar la salida que ésta genera.

Un atacante puede usar `cross site scripting' para mandar un *script* malicioso a un usuario ingenuo. El navegador del usuario final no tiene forma de saber que el *script* no debe ser confiable y lo ejecutará, porque piensa que vino de una fuente confiable, el *script* malicioso puede acceder a cualquier cookie, token de sesión u otra información sensitiva retenida por su navegador y utilizada con ese sitio. Estos pequeños programas pueden hasta re-escribir el contenido de una página HTML.

Los ataques XSS pueden generalmente ser clasificados en dos categorías: almacenados y reflejados. Los ataques almacenados son aquel os en donde el código inyectado es permanentemente almacenado en el servidor objetivo, tales como bases de datos, en un foro de mensajes, un archivo de visitante, campo comentado, etc. Entonces la víctima recupera el *script* malicioso del servidor cuando solicita la información almacenada. Los ataques reflejados son aquel os donde el código inyectado es reflejado desde el servidor, tal como un mensaje de error, resultado de una búsqueda o cualquier otra respuesta que incluya alguna o todas las entradas mandadas al servidor como parte de una petición. Los ataques reflejados

son entregados a las víctimas mediante otra ruta, tal como un mensaje de correo electrónico o algún otro servidor Web. Cuando un usuario es engañado para hacer clic a un enlace malicioso o ante la presentación artesanal de una forma, el código inyectado viaja al servidor Web vulnerable, el cual refleja el ataque de regreso al navegador del usuario. El navegador ejecuta el código porque viene de un servidor `confiable'.

La consecuencia de un ataque XSS son las mismas, independientemente de si es almacenado o reflejado. La diferencia es cómo llega el efecto destructivo al servidor. No se engañe al pensar que un sitio de "solo lectura" o de "presencia literaria corporativa en línea sin interacción" ("*brochureware*") no es vulnerable a ataques reflejados XSS serios. XSS puede causar una variedad de problemas al usuario final que varían en la severidad, desde una molestia hasta el comprometer completamente una cuenta. Los ataques XSS más severos involucran la divulgación de una cookie de sesión de usuario, permitiendo a un atacante secuestrar la sesión de usuario y apoderarse de la cuenta. Otros ataques dañinos incluyen la divulgación de los archivos del usuario final, instalación de programas de cabal os de Troya, re-dirigiendo al usuario a alguna otra página o sitio y modificando la presentación del contenido. Una vulnerabilidad XSS que permite a un atacante modificar un comunicado de prensa o un artículo de noticia puede afectar el precio de mercado de una compañía o disminuir la confianza del consumidor. Una vulnerabilidad XSS en un sitio farmacéutico podría permitir a un atacante modificar la información de dosificación resultando en una sobredosis.

Los atacantes usan frecuentemente una variedad de métodos para codificar la porción maliciosa de la etiqueta, tal como el utilizar Unicode (*código de 16 bits para exponer signos en el ordenador, parecido al ASCII pero con un número mayor de signos, lo que permite el uso de todos los idiomas mundiales*), de forma que la solicitud parezca menos sospechosa al usuario. Hay cientos de variantes de estos ataques, incluyendo versiones

que ni siquiera requieren ningún símbolo <>. Por esta razón el intentar "filtrar" estos *scripts* probablemente no tendrá éxito. En lugar de el o recomendamos validar las entradas contra una especificación positiva rigurosa de lo que es esperado. Los ataques XSS usualmente vienen en la forma de JavaScript incrustado. Sin embargo, cualquier contenido activo incrustado es una fuente potencial de daño, incluyendo: ActiveX (OLE), Vbscript, Shockwave, Flash y más.

Las cuestiones sobre XSS también pueden estar presentes en los servidores de aplicación y Web subyacentes. La mayoría de los servidores de aplicación y Web generan páginas Web simples para mostrar en caso de varios errores, tal como 404 `página no encontrada' o 500 `error interno del servidor'. Si estas páginas muestran como respuesta cualquier información de la solicitud del usuario, tal como la URL a la que trataban de acceder, pueden ser vulnerables a un ataque reflejado XSS.

La probabilidad de que un sitio contenga vulnerabilidades XSS es extremadamente alta. Hay una gran variedad de formas de engañar a las aplicaciones Web al transmitir *scripts* maliciosos. Los desarrolladores que intentan filtrar las partes maliciosas de estas solicitudes es muy probable que pasen por alto posibles ataques o codificaciones. Encontrar estas fallas no es enormemente difícil para los atacantes, ya que todo lo que necesitan es un navegador y algo de tiempo. Hay numerosas herramientas gratuitas disponibles que ayudan a los piratas informáticos a encontrar estas fallas así como a crear cuidadosamente ataques XSS e inyectarlos en los sitios objetivos.

Ambientes Afectados

Todos los servidores Web, servidores de aplicación y ambientes de aplicación Web son susceptibles de cross site scripting.

¿Cómo Determinara Si Usted Es Vulnerable?

Las fallas de XSS pueden ser difíciles de identificar y remover de una aplicación Web. La mejor manera de encontrar fallas es realizar una revisión de seguridad del código y buscar por todos aquel os lugares donde una entrada de una solicitud HTTP podría posiblemente hacerse camino hacia la salida de HTML. Note que una diversidad de diferentes etiquetas HTML puede ser usada para transmitir un JavaScript malicioso. Nessus, Nikto y algunas otras herramientas disponibles pueden ayudar a buscar estas fallas en un sitio Web, pero sólo pueden escarbar en la superficie. Si una parte del sitio Web es vulnerable, existe una alta probabilidad de que también existan otros problemas.

¿Cómo Autoprotegerse?

La mejor forma de proteger una aplicación Web de ataques XSS es asegurar que su aplicación desarrolla una validación de todas las cabeceras, *cookies*, cadenas de petición, campos de formularios y campos escondidos (Ej., todos los parámetros) contra una especificación rigurosa de lo que debe ser permitido. La validación no debe tratar de identificar contenido activo y removerlo, filtrarlo o desinfectarlo. Hay muchos tipos de contenido activo y también muchas formas de codificarlo para evitar los filtros para tal contenido. Recomendamos contundentemente una política de seguridad `positiva' que especifique lo que es permitido. Políticas basadas en identificación de ataques o `negativas' son difíciles de mantener y probablemente serán incompletas.

La salida codificada de usuario suministrada también puede abatir las vulnerabilidades XSS evitando que *scripts* insertados sean transmitidos a los usuarios en una forma ejecutable. Las aplicaciones pueden ganar una protección significativa contra los ataques basados en JavaScript al convertir, en todas las salidas generadas, los caracteres siguientes a la

entidad de codificación HTML apropiada:

De:	A:
<	&lt;
>	&gt;
(	&#40;
)	&#41;
#	&#35;
&	&#38;

El proyecto de Filtros de OWASP está produciendo componentes re-utilizables en varios lenguajes para ayudar a prevenir muchas formas de falsificación de parámetros, incluyendo la inyección de ataques XSS. OWASP también ha liberado CodeSeeker, una aplicación a nivel cortafuego. Además, el programa de entrenamiento WebGoat de OWASP tiene elecciones sobre Cross Site Scripting y codificación de datos.

A5 DESBORDAMIENTO DEL BUFER

Descripción

Los atacantes utilizan el desbordamiento del búfer para corromper la ejecución de la pila ("*stack*") de una aplicación Web. Mediante el envío de entradas hábilmente urdidas hacia una aplicación Web, un atacante puede causar que una aplicación Web ejecute código arbitrario tomando el control efectivo de una máquina. Los desbordamientos del búfer no son fáciles de descubrir y aun cuando uno es descubierto, es generalmente extremadamente difícil de explotar. No obstante, los atacantes se las han ingeniado para identificar los desbordamientos del búfer en una asombrosa

matriz de productos y componentes. Otra clase similar de fallas es conocida como ataques de cadena de formato

Las fallas de desbordamiento del búfer pueden estar presentes ya sea en los productos del servidor Web o en el servidor de aplicación que prestan el servicio del sitio para los aspectos estáticos y dinámicos o la aplicación Web en sí misma. Las fallas de desbordamiento del búfer encontradas en productos ampliamente utilizados en servidores probablemente serán extensamente conocidas y pueden exponer un riesgo significante a los usuarios de estos productos. Cuando las aplicaciones Web usan bibliotecas, tales como bibliotecas gráficas para generar imágenes, éstas se abren por sí mismas a ataques potenciales de desbordamiento del búfer.

El desbordamiento del búfer también puede ser encontrado en el código de aplicaciones Web hechas a la medida e incluso pueden tener una mayor probabilidad a ataques dada la falta de escrutinio por las cuales pasa típicamente una aplicación Web. Las fallas de desbordamiento del búfer en las aplicaciones Web hechas a la medida tienen menor probabilidad de ser detectadas porque normalmente habrá muchos menos piratas informáticos tratando de encontrar y explotar tales fallas en una aplicación específica. Si se descubre en una aplicación hecha a la medida, la habilidad de explotar las fallas (más que hacer que la aplicación deje de funcionar) es significativamente reducida por el hecho de que el código fuente y los mensajes de error detallados para la aplicación normalmente no están disponibles para el pirata informático.

Ambientes Afectados

Casi todos los servidores Web, servidores de aplicación y ambientes de aplicación Web conocidos son susceptibles de desbordamiento de memoria intermedia, la excepción notable son los ambientes Java y J2EE, los cuales son inmunes a estos ataques (excepto por los desbordamientos

propios de JVM).

¿Cómo Determinara Si Usted Es Vulnerable?

Para productos de servidor y bibliotecas, manténgase al día con los últimos reportes sobre errores para los productos que está utilizando. Para las aplicaciones de software hechas a la medida, todo código que acepte entradas de usuario mediante peticiones HTTP debe ser revisado para asegurar que puede manejar apropiadamente entradas arbitrariamente grandes.

¿Cómo Autoprotegerse?

Manténgase al día con los últimos reportes de errores para los productos de servidores Web y de aplicación y otros productos en su infraestructura de Internet. Aplique los últimos parches para estos productos. Periódicamente examine su sitio Web con uno o más de los buscadores (Scanners) comúnmente disponibles que buscan fal as de desbordamiento de memoria intermedia en sus productos para servidores y en sus aplicaciones Web hechas a la medida.

Para el código de sus aplicaciones hechas a la medida, necesitarás revisar todo código que acepte entradas de los usuarios mediante solicitudes HTTP y asegurar que se provee el tamaño apropiado para verificar todas esas entradas. Esto debe ser hecho aun para ambientes que no son susceptibles a tales ataques ya que entradas demasiado largas que no son capturadas podrían causar negación de servicio u otros problemas operacionales.

A6 FALLAS DE INYECCIÓN

Descripción

Las fal as de inyección permiten a los atacantes transmitir código malicioso a otro sistema a través de una aplicación Web. Estos ataques incluyen l amadas al sistema operativo mediante l amadas al sistema, el uso de programas externos vía interfaces de comando y también l amadas a servidores de soporte de bases de datos mediante SQL (Ej., Inyección SQL). *scripts* escritos en Perl, Python, y otros lenguajes pueden ser inyectados en aplicaciones Web pobremente diseñadas y ejecutadas. En cualquier momento en que una aplicación Web utiliza un interpretador de cualquier tipo hay peligro de un ataque por inyección.

Muchas aplicaciones Web utilizan características del sistema operativo y programas externos para realizar sus funciones. "Sendmail" es probablemente el programa externo más frecuentemente utilizado, pero muchos otros programas también son usados. Cuando una aplicación Web pasa información de una petición HTTP como parte de una solicitud externa, debe ser cuidadosamente examinada. De lo contrario, el atacante puede inyectar (meta) caracteres, comandos maliciosos o modificadores de comando en la información y la aplicación Web, sin dudarlo, pasa éstos al sistema externo para su ejecución.

La inyección SQL es una forma de inyección peligrosa y está particularmente generalizada. Para explotar una falla de inyección SQL, el atacante debe encontrar un parámetro que la aplicación Web pase hacia la base de datos. Mediante la inserción cuidadosa de comandos SQL en el contenido del parámetro, el atacante puede engañar a la aplicación Web para que envíe una solicitud maliciosa a la base de datos. Estos ataques no son difíciles de intentar y están surgiendo muchas herramientas que buscan estas fallas. Las consecuencias son particularmente dañinas ya que un

atacante puede obtener, corromper o destruir el contenido de una base de datos.

Los ataques por inyección pueden ser fáciles de descubrir y explotar, pero también pueden ser extremadamente obscuros. Las consecuencias también pueden ser de una variedad completa, desde triviales hasta comprometer completamente el sistema o destruirlo. En cualquier caso, el uso de llamadas externas está ampliamente extendido, así que la probabilidad de que una aplicación Web tenga fallas de inyección de comandos debe ser considerablemente alta.

Ambientes Afectados

Todo ambiente de aplicación Web permite la ejecución de comandos externos tales como l amadas al sistema, interfaces de comando y solicitudes SQL. La susceptibilidad de una llamada externa a una inyección de comando depende de cómo es hecho la llamada y el componente específico que está siendo llamado, pero casi todas las llamadas externas pueden ser atacadas si la aplicación Web no está apropiadamente codificada

¿Cómo Determinara Si Usted Es Vulnerable?

La mejor forma de determinar si es vulnerable a los ataques de inyección de comandos es buscar en el código fuente todas las l amadas a los recursos externos (Ej., system, exec, fork, Runtime.exec, solicitudes SQL o cualquiera sea la sintaxis para realizar solicitudes a los intérpretes de su ambiente). Note que muchos lenguajes tienen múltiples maneras de ejecutar comandos externos. Los desarrolladores deben revisar su código y buscar por todos los lugares donde la entrada de una petición HTTP podría posiblemente hacerse camino a través de cualquiera de estas l amadas. Debe examinar cuidadosamente cada una de estas llamadas para

asegurarse que los pasos de protección delineados anteriormente son seguidos.

¿Cómo Autoprotegerse?

La manera más simple de protegerse contra las inyecciones es evitar acceder a intérpretes externos siempre que sea posible. Para muchos comandos y l amadas al sistema, hay bibliotecas específicas de lenguajes que realizan las mismas funciones. Usar tales bibliotecas no involucra al intérprete de comandos y por lo tanto evita un gran número de problemas con comandos de sistema.

Para aquel as l amadas que forzosamente debe hacer, como l amadas a bases de datos, debe validar cuidadosamente los datos proveídos para asegurar que no almacenan algún contenido malicioso. También puede estructurar muchas peticiones de manera que aseguren que todos los parámetros proveídos son tratados como datos y no como código ejecutable potencial. El uso de procedimientos almacenados y sentencias preparadas ("prepared statements") proveerán protección significativa, asegurando que las entradas proveídas sean tratadas como datos. Estas medidas reducirán, pero no eliminarán completamente el riesgo relacionado a estas l amadas externas. De todas maneras debe validar siempre tales entradas para asegurarte que cumplen con las expectativas de la aplicación en cuestión.

Otro tipo de protección fuerte contra la inyección de comandos es asegurarse que la aplicación corre sólo con los privilegios indispensablemente necesarios para realizar su función. Así que no debería correr el servidor Web como administrador o acceder a la base de datos como DBADMIN, de otra manera un atacante puede abusar de los privilegios administrativos otorgados a la aplicación Web. Algunos de los ambientes J2EE permiten el uso de cajas de arena Java ("Java Sand Box") que pueden evitar la ejecución de comandos del sistema.

Si un comando externo debe ser usado, cualquier información del usuario que sea insertada dentro del comando debe ser rigurosamente revisada. Deben de usarse mecanismos para manejar cualquier error posible, tiempo de espera agotado o bloqueos durante las llamadas.

Todas las salidas, códigos de retorno y códigos de error de la l amada deben ser revisadas para asegurar que el procesamiento esperado sea realmente el que ocurrió. Al menos, esto permitirá determinar que algo salió mal. De otra manera el ataque puede ocurrir y nunca sería detectado.

El proyecto de Filtros OWASP está produciendo componentes reutilizables en diversos lenguajes para ayudar a evitar muchas formas de inyección. OWASP también ha liberado CodeSeeker, unos cortafuegos a nivel de aplicación.

A7 MANEJO INADECUADO DE ERRORES

Descripción

El manejo inadecuado de errores puede introducir variados problemas de seguridad a un sitio Web. El error mas común es cuando información detallada de mensajes error, como rastreos de pila, volcados de BD y códigos de error son mostrados al usuario (un pirata informático). Estos mensajes revelan detal es de la implementación que nunca deberían ser revelados. Tales detal es pueden proveer a los piratas informáticos de pistas importantes sobre potenciales fallas en el sitio y tales mensajes de error son también perturbadores para los usuarios normales.

Las aplicaciones Web frecuentemente generan condiciones de error durante su operación normal. Falta de memoria, excepciones por punteros nulos, l amadas fallidas a sistema, BD no disponible, tiempo de espera de red agotado y cientos de otras condiciones comunes pueden causar que los errores sean generados. Estos errores deben ser manejados de acuerdo a un esquema bien pensado que provea al usuario de un

mensaje de error con sentido, información de diagnostico para quienes mantienen el sitio, y ninguna información útil para un atacante.

Incluso cuando los mensajes de error no proveen muchos detal es, las inconsistencias en tales mensajes pueden revelar pistas importantes de cómo funciona un sitio y qué información esta presente bajo la cubierta. Por ejemplo, cuando un usuario trata de acceder a un archivo que no existe, el mensaje de error tradicionalmente indica "archivo no encontrado". Cuando se accede a un archivo al que el usuario no está autorizado, se indica "acceso negado". Se supone que el usuario no debe saber siquiera si existe el archivo, pero tales inconsistencias claramente revelan la presencia o ausencia de archivos inaccesibles o la estructura de directorios del sitio.

Un problema común de seguridad causado por el manejo inadecuado de errores es la prueba de seguridad de apertura de archivos. Todos los mecanismos de seguridad deben negar el acceso hasta que sea específicamente otorgado, y no otorgar acceso hasta que sea negado, lo cual es una razón común de porque ocurren los errores de apertura de archivos. Otros errores pueden causar que el sistema se caiga o consuma recursos significativos, negando o reduciendo efectivamente el servicio a usuarios legítimos.

Un buen mecanismo de manejo de errores debe ser capaz de manejar cualquier conjunto de entradas posible, mientras fomenta una seguridad apropiada. Mensajes de error simples deben ser producidos y registrados de tal manera que su causa, ya sea un error en el sitio o un intento de ataque, pueda ser revisada. El manejo de errores debe no sólo enfocarse en las entradas proveídas por el usuario, sino que deben también incluir cualquier error que pueda ser generado por componentes internos tales como llamadas al sistema, consultas de BD o cualquier otra función interna.

Ambientes Afectados

Todos los servidores Web, Servidores de aplicación y ambientes de aplicaciones Web son susceptibles a problemas de manejo de errores.

¿Cómo Determinara Si Usted Es Vulnerable?

Tradicionalmente una revisión simple puede determinar cómo responde su sitio a varios tipos de errores de entrada. Pruebas más profundas son usualmente requeridas para hacer que ocurran errores internos y ver cómo se comporta el sitio.

Otra estrategia importante es tener una revisión detallada del código que busque en éste la lógica en el manejo de errores. El manejo de errores debe ser consistente a través de todo el sitio y cada pieza debe ser parte de un esquema bien diseñado. Una revisión de código revelará cómo pretende el sistema manejar varios tipos de errores. Si encuentra que no hay organización en el esquema de manejo de errores o que parece que hay muchos esquemas diferentes, muy posiblemente hay un problema.

¿Cómo Autoprotegerse?

Una política especifica de cómo manejar errores debería ser documentada, Incluyendo los tipos de errores a ser manejados y, para cada uno de el os, qué información debe ser reportada al usuario y qué información será registrada. Todos los desarrolladores necesitan entender la política y asegurarse que su código la siga.

En la implementación, asegúrese de que el sitio está construido para manejar elegantemente todos los posibles errores. Cuando los errores ocurran, el sitio debe responder con un resultado específicamente diseñado

que sea de ayuda al usuario, sin que revele detal es internos innecesarios. Ciertas clases de errores deben ser registrados para ayudar a detectar errores de implementación en el sitio y/o intentos de ataque.

Muy pocos sitios tienen alguna habilidad de detección de intrusos en su aplicación Web, pero es ciertamente concebible que una aplicación Web pueda rastrear repetidos intentos fallidos y generar alertas. Note que la vasta mayoría de ataques a aplicaciones Web no son detectados nunca porque muy pocos sitios tienen la capacidad para hacerlo. Por lo tanto, el éxito de los ataques contra la seguridad de aplicaciones Web parece ser seriamente subestimado.

El proyecto de Filtros OWASP está produciendo componentes reutilizables en diversos lenguajes, los cuales ayudan a evitar revelar códigos de error dentro de las páginas Web de los usuarios ya que filtran las páginas cuando están construidas dinámicamente por la aplicación.

A8 ALMACENAMIENTO INSEGURO

Descripción

Muchas de las aplicaciones Web necesitan guardar información sensible, ya sea en una base de datos, en un sistema de archivos o en algún lugar. La información podría ser contraseñas, números de tarjetas de crédito, registros contables o información propietaria. Frecuentemente las técnicas de encriptación ("encryption") son usadas para proteger esta información sensible. Mientras que la encriptación se ha vuelto relativamente fácil de implementar y usar, los desarrolladores frecuentemente comenten errores aun cuando la integran dentro de una aplicación Web. Los desarrolladores pueden sobreestimar la protección ganada por el uso de la encriptación y no ser cuidadosos en asegurar otros aspectos del sitio. Unas pocas áreas donde los errores son comúnmente cometidos incluyen:

- Fallar al encriptar información crucial.
- Almacenamiento inseguro de llaves, certificados y contraseñas.
- Almacenamiento incorrecto de secretos en memoria.
- Fuentes pobres de aleatorización.
- Elección pobre de algoritmo.
- Intentar inventar el nuevo algoritmo de encriptación.
- Fallar al incluir soporte para cambios en las l aves de encriptación y otros procedimientos requeridos de mantenimiento.

El impacto de estas debilidades puede ser devastador para la seguridad del sitio Web. La encriptación es generalmente usada para proteger los activos más sensibles del sitio, los cuales pueden ser totalmente comprometidos por una debilidad.

Ambientes Afectados

La mayoría de los ambientes de aplicación Web incluyen alguna forma de soporte criptográfico. En el raro caso que tal soporte no esté disponible aún, hay una gran variedad de productos de terceros que pueden ser agregados. Sólo los sitios Web que usan encriptación para proteger información almacenada o en tránsito son susceptibles a estos ataques. Note que esta sección no cubre el uso de SSL, el cual es cubierto en la sección de Manejo de Configuración Segura. Esta sección menciona sólo la encriptación programática de datos en la capa de aplicación.

¿Cómo Determinara Si Usted Es Vulnerable?

Descubrir fallas criptográficas sin acceso al código fuente puede tomar muchísimo tiempo. Sin embargo, es posible examinar tokens, id's de sesión, cookies y otras credenciales para ver si obviamente no son aleatorias. Todas las estrategias cripto-analíticas pueden ser usadas para

intentar descubrir cómo es que un sitio Web usa las funciones criptográficas.

Por mucho, la estrategia más fácil es revisar el código para ver cómo están implementadas las funciones criptográficas. Una revisión cuidadosa de la estructura, calidad e implementación de los módulos criptográficos debe ser hecha. El revisor debe tener un fuerte conocimiento previo en el uso de la criptografía y las fallas comunes. La revisión debe cubrir también cómo las llaves, contraseñas y otros secretos son almacenados, protegidos, cargados, procesados y limpiados de la memoria.

¿Cómo Autoprotegerse?

La manera más fácil de protegerse contra las fallas criptográficas es minimizar el uso de la encriptación y sólo mantener la información que es absolutamente necesaria. Por ejemplo, más que encriptar los números de tarjetas de crédito y guardarlos, simplemente pida a los usuarios que los introduzcan nuevamente. También, en lugar de guardar las contraseñas encriptadas con un algoritmo que utilice llaves, use una función de una vía como SHA-1 para encriptar las contraseñas.

Si la criptografía debe ser usada, escoja una biblioteca que ha sido expuesta al escrutinio público y asegúrese de que no hay vulnerabilidades abiertas. Encapsule las funciones criptográficas que son usadas y revise el código cuidadosamente. Asegúrese de que los secretos, como las l aves, certificados y contraseñas son almacenados de forma segura. Para hacerlo más difícil para un atacante, un secreto maestro puede ser dividirla en al menos dos ubicaciones y ensamblarla en tiempo de ejecución. Tales ubicaciones pueden incluir archivos de configuración, un servidor externo o dentro del código mismo.

A9 NEGACIÓN DE SERVICIO

Las aplicaciones Web son especialmente susceptibles a ataques de negación de servicio. Toma nota de que los ataques de negación de servicio al nivel de red, como las inundaciones SYN (SYN Floods), son un problema independiente que está fuera del alcance de este documento

Las aplicaciones Web no pueden fácilmente identificar la diferencia entre un ataque y el tráfico ordinario. Hay muchos factores que contribuyen a esta dificultad, pero uno de los más importantes es que, por un número de razones, las direcciones IP no son útiles como una credencial de identificación. Porque no hay manera confiable para decir de dónde proviene una petición HTTP, es muy difícil filtrar tráfico malicioso. Para ataques distribuidos ¿Cómo una aplicación podría identificar la diferencia entre un ataque real, múltiples usuarios dando al mismo tiempo un clic en el botón recargar (lo cual puede suceder si hay un problema temporal con el sitio), o está siendo "derribado" ("slashdotted")?.

La mayoría de los servidores Web pueden manejar varios cientos de usuarios concurrentes bajo condiciones normales de uso. Sin embargo, un solo atacante puede generar suficiente tráfico desde una sola computadora para desplazar muchas aplicaciones. El balanceo de carga puede hacer estos ataques más difíciles, pero no imposibles, especialmente si las sesiones están ligadas a un servidor en particular. Esta es una buena razón para hacer los datos de sesión de la aplicación lo más pequeños posible y hacer un tanto difícil, de alguna manera, el iniciar una nueva sesión.

Cuando un atacante puede consumir completamente algún recurso requerido, puede impedir a los usuarios legítimos usar el sistema. Algunos recursos limitados incluyen el ancho de banda, las conexiones a BD, espacio en disco, CPU, memoria, hilos o recursos específicos de las aplicaciones. Todos estos recursos pueden ser consumidos por ataques que hagan blanco

en el OS. Por ejemplo, un sitio que permite a los usuarios sin autenticar solicitar tráfico de un tablero de mensajes, puede iniciar muchas consultas a la base de datos por cada petición HTTP que recibe. Un atacante puede fácilmente enviar tantas peticiones que la fila de conexiones de la base de datos las use todas y no quedará ninguna para los usuarios legítimos del servicio.

Otras variantes de estos ataques hacen blanco en los recursos del sistema relacionados a un usuario en particular. Por ejemplo, un atacante puede ser capaz de bloquear a un usuario legítimo enviando credenciales inválidas hasta que el sistema bloquee la cuenta. O el atacante puede pedir una nueva contraseña para el usuario, forzándolo a acceder a su cuenta de correo para volver a obtener acceso. Alternativamente, si el sistema bloquea alguno de los recursos de un usuario, entonces el atacante podría potencialmente interrumpir el acceso a éstos de manera que otros no pudieran usarlo.

Algunas aplicaciones Web son incluso susceptibles a ataques que las pondrán inmediatamente fuera de línea. Las aplicaciones que no manejan los errores apropiadamente pueden incluso tumbar el contenedor del servidor Web. Estos ataques son particularmente devastadores porque instantáneamente le impiden usar la aplicación a todos los usuarios.

Hay una amplia variedad de estos ataques, muchos de los cuales pueden fácilmente ser lanzados con unas pocas líneas de código Perl desde una computadora de bajo poder. Mientras no haya defensas perfectas para estos ataques, es imposible hacer más difícil que tengan éxito.

Ambientes Afectados

Todos los servidores Web, servidores de aplicación y

ambientes de aplicación Web son susceptibles a ataques de negación de servicio.

¿Cómo Determinara Si Usted Es Vulnerable?

Una de las partes difíciles de los ataques de negación de servicio es determinar si se es vulnerable. Herramientas de pruebas de carga, como el JMeter pueden generar tráfico Web de manera que puedas probar ciertos aspectos de cómo se desempeña su sitio bajo tráfico pesado. Ciertamente una prueba importante es cuantas peticiones por segundo puede manejar su aplicación. Probar desde una sola dirección IP es útil pues le da una idea de cuántas peticiones puede un atacante generar para dañar su sitio.

Para determinar si cualquier recurso puede ser usado para crear un ataque de negación de servicio, debe analizar cada uno para ver si hay alguna manera de agotarlo. Debe enfocarse particularmente en qué puede hacer un usuario autenticado y, a menos que confíe en todos tus usuarios, debe determinar también qué puede hacer un usuario no autenticado.

¿Cómo Autoprotegerse?

Defenderse de un ataque de negación de servicio es difícil, ya que no existe una manera perfecta de protegerse de estos ataques.

Como regla general, debe limitar al mínimo posible los recursos asignados a cualquier usuario. Para usuarios autenticados es posible establecer cuotas de manera que puedan limitar la cantidad de carga que un usuario en particular puede poner sobre el sistema. Particularmente puede considerar sólo manejar una petición por usuario cada vez, sincronizando la sesión del usuario.

Podría también considerar suspender cualquier petición de un usuario que se esté procesando cuando llegue otra petición de ese mismo usuario. Para usuarios no autenticados, debe evitar cualquier acceso innecesario a la base de datos u otro recurso caro. Trata de diseñar el flujo de su sitio de manera que un usuario no autenticado esté incapacitado para ejecutar alguna operación costosa. Puede considerar guardar en la memoria rápida el contenido recibido por usuarios no autenticados en lugar de generarlo o acceder a la base de datos para obtenerlo.

Debe también verificar su esquema para manejo de errores a fin de asegurar que un error no puede afectar la operación general de la aplicación.

A10 AMINISTRACION DE CONFIGURACIÓN INSEGURA

Descripción

El Servidor Web y el servidor de aplicación juegan un papel clave en la seguridad de una aplicación Web. Estos servidores son responsables de servir el contenido y ejecutar aplicaciones que generan contenido. Además, muchos servidores de aplicación proveen un número de servicios que los servidores Web pueden usar, incluyendo almacenamiento de información, servicios de directorio, correo, mensajería y más. Fallar al manejar la configuración apropiada de sus servidores puede llevar a una amplia variedad de problemas de seguridad.

Frecuentemente el grupo de desarrollo Web está separado del grupo que opera el sitio. De hecho, hay comúnmente un amplio trecho entre aquel os que escriben la aplicación y aquel os responsables del ambiente de operaciones. Lo relacionado a seguridad en aplicaciones Web frecuentemente acorta este trecho y requiere que los miembros de ambos

lados del proyecto afiancen apropiadamente la seguridad del sitio de la aplicación.

Hay una amplia variedad de problemas de configuración de servidores que pueden plagar la seguridad de un sitio. Estos incluyen:

- Fallas de seguridad no parchadas en el software del servidor.
- Fallas de seguridad en el software del servidor o malas configuraciones que permiten ataques de listado de directorio o atravesamiento de directorio.
- Innecesarios archivos por defecto, de respaldo o de ejemplo, incluyendo Scripts, aplicaciones, archivos de configuración y páginas Web.
- Permisos no adecuados en archivos y directorios.
- Servicios innecesarios habilitados, incluyendo manejo de contenido y administración remota.
- Cuentas por defecto con contraseñas por defecto.
- Funciones administrativas o de depuración que son habilitadas o accesibles. Mensajes de error demasiado informativos (más detal es en la sección de manejo de errores)
- Certificados SSL y opciones de encriptación mal configurados.
- Uso de certificados auto firmados para alcanzar la autenticación y protección sobre ataques de hombre-en-el-medio.
- Uso de certificados por defecto.
- Autenticación inadecuada con sistemas externos.

Algunos de estos problemas pueden ser detectados con herramientas de examinación de seguridad (security scanning tools) ampliamente disponibles. Una vez detectados, estos problemas pueden ser

fácilmente explotados y resultan en el compromiso total de un sitio Web. Los ataques exitosos pueden también resultar en el compromiso de los sistemas de respaldo incluyendo bases de datos y redes corporativas. Ambos, tener software seguro y una configuración segura, son requeridos para tener un sitio seguro.

Ambientes Afectados

Todos los servidores Web, servidores de aplicación y ambientes de aplicaciones Web son susceptibles a la mala configuración.

¿Cómo Determinara Si Usted Es Vulnerable?

Si no ha hecho un esfuerzo concienzudo para asegurar sus servidores Web y de aplicaciones, es muy probable que sea vulnerable. Pocos productos de servidor, sino es que ninguno, son seguros al sacarlos de la caja. Una configuración segura para su plataforma debe ser documentada y actualizada frecuentemente. Una revisión manual de la guía de configuración debe ser hecha regularmente para asegurar que ha sido mantenida actual y consistente. También es recomendable una comparación con los sistemas actualmente desplegados.

Además hay un número de productos de examinación disponibles que externamente buscan vulnerabilidades conocidas en una aplicación o servidor Web, incluyendo Nessus y Nikto. Debe correr estas herramientas regularmente, al menos mensualmente, para encontrar problemas tan pronto como sea posible. Las herramientas deben ser corridas tanto internamente como externamente. Las examinaciones externas deben correr desde una computadora localizada fuera de la red del servidor. Las examinaciones internas deben ser corridas desde la misma red de los servidores objetivo.

¿Cómo Autoprotegerse?

El primer paso es crear una guía de fortificación para su configuración particular de servidor Web y servidor de aplicación. Esta configuración debe ser usada en todas las computadoras corriendo la aplicación y también en los ambientes de desarrollo. Recomendamos empezar con cualquier guía existente que pueda obtener de su proveedor o aquellas disponibles por las organizaciones de seguridad como OWASP, CERT y SANS, y después adecuarlas a tus necesidades particulares. La guía de fortificación debe contener los siguientes temas:

- Configuración de todos los mecanismos de seguridad.
- Dar de baja todos los servicios no usados.
- Establecer roles, permisos y cuentas, incluyendo la deshabilitación de todas las cuentas por defecto o cambiando sus contraseñas.
- Registro de eventos y alertas.

Una vez que su guía ha sido establecida, úsela para configurar y mantener sus servidores. Si tiene un número grande deservidores que configurar, considere semi-automatizar o automatizar completamente el proceso de configuración. Use una herramienta de configuración existente o cree la suya propia. Un número de herramientas de este tipo ya existen. Puede también usar herramientas de replicación de discos como Ghost para hacer una imagen de un servidor fortificado existente y después replicar esa imagen a servidores nuevos. Tal proceso puede o no funcionar para su ambiente particular.

Mantener la configuración del servidor segura requiere vigilancia. Debe de asegurarse que la responsabilidad de mantener la configuración del servidor actualizada sea asignada a un individuo o equipo. El proceso de mantenimiento incluye:

- Monitorear las últimas vulnerabilidades publicadas
- Aplicar los parches más recientes.
- Actualizar la guía de configuración de seguridad.
- Búsqueda de vulnerabilidades frecuentes desde ambas perspectivas, interna y externa.
- Revisiones internas frecuentes de la configuración de seguridad del servidor comparada a la guía de configuración.
- Reportes de estado regulares a la gerencia superior, documentando la postura general de seguridad.