**AUDITORÍA INFORMÁTICA**

**Fases de la Auditoría.**

|  |  |  |
| --- | --- | --- |
| **Fase** | **Fecha de inicio** | **Fecha de término** |
| Planeamiento |  |  |
| Ejecución |  |  |
| Informe de Auditoría |  |  |

**Finalidad de Auditoría.**

El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto performance del SGBD, el procedimiento adecuado del acceso a la información y la emisión oportuna de sus resultados en la organización, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operación diaria de funcionarios y usuarios involucrados en los servicios que proporcionan los sistemas de BDs.

**Concepto de Auditoría Informática.**

Es una función que ha sido desarrollada para salvaguardar los activos de las TIC, mantener la integridad de los datos y lograr los objetivos de la organización de manera eficiente y eficaz.

Es la verificación de los controles en las siguientes tres áreas de la organización informática:

• Programas de aplicaciones (en ambiente de producción).

• Desarrollo de sistemas.

• Instalaciones del centro de procesos.

Es la revisión y evaluación de los sistemas y procedimientos de la información de los equipos de cómputo, su utilización, y seguridad de la organización, que participa en el procesamiento de la información.

**Objetivos de la Auditoría Informática.**

**Objetivo General.**

* Evaluación del ambiente en que residen las de bases de datos de IPS, lo que permitirá:
* Emitir una opinión sobre la fiabilidad de las BDs (diversas instancias Oracle e Informix) y su entorno físico (arquitectura/infraestructura) y de los procesos soportados por estos motores.
* Detectar posible deficiencias encontradas, para su análisis y fortalecimiento/corrección, tendiente a asegurar la continuidad del soporte de gestión de IPS.
* Elaborar un informe de recomendaciones y planes de acción.

**Objetivos Específicos.**

* El control de la función informática, en los SGBDs y la TI relacionadas.
* El análisis de la eficiencia de los Sistema de Información (SI) y la Tecnología de la Información (TI).
* La verificación/detección del cumplimiento de la normativa general de la organización.
* La verificación/detección de los planes y/o programas de las BDs.
* La revisión de la eficaz gestión de los recursos materiales y humanos informáticos.
* La revisión y verificación de controles técnicos generales y específicos de operatividad.
* La revisión y verificación de algunos aspectos del la seguridad.
* Cumplimiento de normas y estándares.
* Sistema Operativo.
* Seguridad de Comunicaciones.
* Seguridad de Base de Datos.
* Seguridad Física.
* Suministros y Reposiciones.
* Contingencias
* El análisis del control de resultados.
* El análisis de verificación y de exposición de debilidades y disfunciones.

**Alcance de la Auditoría Informática.**

* Enterarse de la situación actual del ambiente en donde residen las BDs, tanto para la diversas instancias Oracle, como para Informix
* No se considera auditoría de los datos de los SGBDs.
* No se considera auditoría de las aplicaciones que acceden a los datos de los motores de las BDs.

**Factores a considerar por su influencia en la Auditoría Informática.**

* Necesidad de controlar el uso de tecnologías (hardware, software) de última generación.
* Controlar el uso de éstas tecnologías, que cada día se vuelven más importantes y costosas.
* Uso y abuso de la tecnología.
* ~~Valor del hardware, software y personal.~~
* Toma de decisiones incorrectas.

En síntesis, se trata de un tema de Gobernanza de las TI

**Características con la Auditoría Tradicional**.

Existen ciertas características de la Auditoría Informática que se observan en la auditoría tradicional o financiera, las cuales se mencionan a continuación:

* Su función inicial, es estrictamente económico-financiero.
* Debe ser absolutamente independiente.
* No tiene carácter ejecutivo, ni son vinculantes sus conclusiones.
* Contiene elementos de análisis, verificación, exposición de debilidades y disfunciones.
* Todas las sugerencias se plasman en un documento que recibe el nombre de recomendaciones (informe corto).

**Síntomas de Necesidad de una Auditoría Informática.**

A continuación se mencionan los más comunes:

* Los estándares de productividad se desvían de los promedios conseguidos habitualmente.
  + Puede ocurrir con algún cambio masivo de personal, o en una reestructuración de alguna área o en la modificación de alguna norma importante.
* Síntomas de deterioro de la imagen institucional y/o insatisfacción de los usuarios:
  + No se atienden las peticiones de cambios de los usuarios.
  + No se reparan las fallas de hardware/software dentro los plazos estipulados ni se resuelven las incidencias en plazos razonables. El usuario percibe que no  está bien atendido.
  + No se cumplen en todos los casos los plazos de entrega de resultados periódicos. Pequeñas desviaciones pueden causar importantes desajustes en la actividad del usuario, en especial en los resultados de aplicaciones críticas y sensibles.
* Síntomas de debilidades económico-financieras:
  + Incremento desmesurado de costos.
  + Necesidad de justificación de inversiones informáticas ante la organización.
  + Desviaciones presupuestarias significativas.
  + Costos y plazos de nuevos proyectos (deben auditarse simultáneamente desarrollo de proyectos y al órgano que realizó la petición).
* Síntomas de Inseguridad: Evaluación de nivel de riesgos
  + Seguridad Lógica.
  + Seguridad Física.
  + Confidencialidad.

**Control Interno y Auditoría Informática.**

**Control.**

Consiste en verificar si todo ocurre de conformidad con lo adoptado, con las instrucciones emitidas y con los principios establecidos. Tiene como finalidad señalar las debilidades y errores, a fin de rectificarlos e impedir que se repitan.

**Control Interno.**

Es el plan de la organización de todos los métodos y procedimientos que son relativos y que están directamente relacionados principalmente con la salvaguardia de los activos y la confiabilidad de los registros financieros.

**Control Interno Informático.**

El control interno informático controla diariamente que todas las actividades de sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la dirección de la organización y la dirección de informática. Sus principales funciones son:

* Controlar que todas las actividades se rechazan cumpliendo los procedimientos y normas fijados.
* Asesorar sobre el conocimiento de las normas.
* Colaborar y apoyar la auditoría informática, así como de las auditorías externas al grupo.
* Definir, implantar y ejecutar mecanismos y controles para comprobar el logró de los grados adecuados del servicio informático.

**Tipos de Controles Internos.**

Los objetivos de los controles informáticos pueden ser clasificados en las siguientes categorías:

* Controles preventivos: para tratar de evitar la ocurrencia, como un software de seguridad que impida los accesos no autorizados al sistema.
* *C*ontroles reactivos: cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
* Controles correctivos*:* facilitan la vuelta a la normalidad cuando se ha producido una incidencia.

**Control interno y Auditoría informática: Campos Análogos**

Aunque ambas procesos tienen objetivos comunes, existen diferencias que conviene matizar:

**Tabla Nº 1. Las Similitudes y Diferencias entre el Control Interno y la Auditoría Informática.**

**Herramientas y Técnicas para la Auditoría Informática.**

Las herramientas que ayudan a examinar la eficiencia y eficacia a los controles establecidos sobre el objeto que se evalúa, son entre otras:

|  |  |
| --- | --- |
| **Herramienta** | **Utilización en Synapsis** |
| Cuestionarios | no |
| Entrevistas | sí |
| Formularios Checklist |  |
| Formularios Virtuales | no |
| Pruebas de consistencias |  |
| Inventarios y valorizaciones | si |
| Historias de cambios y mejoras | si |
| Reporte de bases de datos y archivos. | si |
| Reportes de estándares |  |
| Compatibilidades y uniformidades |  |
| Software de interrogación | no |
| Certificados, garantías, otros del software |  |
| Fotografías o tomas de valor (imágenes) | no |
| Diseño de flujos y la red de información | si |
| Planos de distribución e instalación (para estudio y revisión) | Si |
| Listado de proveedores |  |

**Técnicas de Evaluación.**

**Evaluación del software que posee IPS (Synapsis).**

Al utilizar un determinado software se debe evaluar lo siguiente:

b) Licencias. Verificar el tipo de licencia que se puede contratar (individual, múltiple, corporativa).

c) Compatibilidad con otros softwares.

e) Fácil de usar (usabilidad).

f) Capacidad de utilización en red.

h) Grado de sofisticación.

i) Requerimientos de memoria.

j) Seguridad y confidencialidad.

k) Costo.

l) Capacidad de trabajar en multiplataforma.

m) Demanda de Hardware.

**Evaluación del hardware que posee IPS (Synapsis).**

Evaluar su uso adecuado, resguardo, aprovechamiento y el estado en que se encuentran, a través de posibles cambios en el hardware a fin de proponer nivelar el sistema de cómputo ó de comparar la capacidad instalada de los Institutos con los planes de desarrollo del Ministerio de Educación. Al utilizar un determinado hardware se debe evaluar lo siguiente:

**Evaluación del sistema de comunicación (redes) posee IPS (Synapsis).**

Evaluar tenencia y/o necesidad de uso de red

Al utilizar una red se debe evaluar lo siguiente:

a) Servidor

b) Terminal o estación de trabajo

c) Modo de comunicación

d) Medio de comunicación.

e) Topología de la red

f) Compartir...

g) Compartir aplicaciones

h) Confiabilidad de la red y tiempo de respuesta.

i) Seguridad en la red.

**Análisis Infraestructura 1.0.**

Como punto inicial, definimos la arquitectura evidenciado en un entorno SAN (Storage Attached Network), en donde se enmarcan finalmente los ambientes de explotación Oracle e Informix. En función del entorno éste tiene como característica integrarse a metodología de alta disponibilidad, la cual se consigue primeramente por una definición clara de las directrices, políticas y procedimientos. Con ello se obtiene una estabilidad funcional a nivel del servicio, junto con la implementación técnica que da vida a esta sinergia. En base a lo anterior, se logró definir lo siguiente, para los ambientes Oracle e Informix:

* Entorno de alta disponibilidad para servicio IPS.
  + No se presenta ambiente de alta disponibilidad en la estructura de servicio ni como técnico.
    - Si bien los SLA, no presentan claramente que el servicio se entregue en este marco, como entidad tecnológica durante el periodo de servicio 2003-2013, proactivamente debió haber ofrecido o implementado sin costo el servicio, en compromiso de largo aliento de trabajo.

Ya definido la no existencia de un entorno de alta disponibilidad, lo visualizado para suplir esta deficiencia, fue lo siguiente:

* Definición clara de las entidades internas para las diferentes etapas de servicio que incurre el servir y mantener una infraestructura de la envergadura de IPS.
  + Infraestructura
  + Comunicaciones
  + Base de datos
  + Mesa de ayuda
* Definición clara de los cargos y roles, para la dirección, operación, explotación y mantención de cada una de las áreas.

No obstante, podemos revelar algunas deficiencias en este último:

* Dependencia del RRHH.
* Dominio aislado por cada una de las áreas.
* Estructura organizacional rígida y vertical.
* Falta de documentación técnica y diagramación de los entornos para una visión macro y micro del entorno.

Respecto a estos puntos, los más críticos para la continuidad del servicio son:

* La dependencia del RRHH, y en especial en el ambiente Informix para las versiones utilizadas en la explotación actual del IPS.
  + Se visualiza esta dependencia, por el hecho de la versión usada de Informix mantiene una data muy prolongada siendo el RRHH un recurso muy escaso el cual requiere una experticia de un nivel muy elevado.
  + El no contar con un entorno de alta disponibilidad agrava más la situación de dependencia, por la no existencia de procedimientos automáticos que suplanta la deficiencia.
* Documentación y diagramas, son un factor que eleva la criticidad del punto anterior. Por el hecho de que ante una eventual incidencia, si se obtuviera RRHH externo capacitado para suplir, este no estaría a cabalidad con el conocimiento requerido ralentizando los procesos de levantamiento para la contingencia. Sin poder acceder a documentación oficial y diagramación de los entornos.
  + Dentro del proceso de recolección de evidencia, este evento se describe en concreto para la revisión de comunicaciones, en el cual el líder de esta área informa que no cuentan con diagramas actualizados y se encuentran en el proceso de generación.
  + Se recomienda la implementación de un entorno de la gestión del conocimiento, de forma interna, como externa. Con el objetivo de minimizar este punto y maximizar el desarrollo del conocimiento generado en el tiempo, sin entorpecer los procesos cotidianos que implican la entrega del servicio.
  + Sin procedimientos, el *know-how* se encuentra encarnado en el recurso humano, no podrá ser accesado por otros con tal libertad
* Ausencia de procedimientos de la operación diaria

1.1 Evidencia Base

1.1.1 Servidores

1.1.2 Storage

1.1.3 Comunicación

**AUDITORÍA TÉCNICA DE SISTEMAS**

15. AUDITORÍA DE TÉCNICA DE SISTEMAS

**15.1.** Ámbito de técnica de sistemas

Instalaciones: datacenters, enlace físico (cableado)

Equipos de proceso: servidores, cintas de respaldo (cintoteca), elementos de enlace, routers

Software de base: sistemas operativos, SGBDs:

**Estado (del arte)**

Se define SAN (Storage Area Network) como la arquitectura en que Synapsis sustenta los servicios de explotación para los motores de base de datos Oracle e Informix de IPS.

Esta arquitectura se complementa con una serie de capas fisicas que soportar el servicio entregado por Synapsis hacie IPS de las cueles se desprenden:

* Hardware de Comunicación
* Hardware de Dato
* Servidores
* Storage

En donde fisicamente los aloja por ambientes geograficamente separadas definidas como:

* Entorno Productivo
  + Ubicación geografica: Paramericana norte
* Entorno de Contigencia
  + Ubicación geografica: Santa Rosa

Donde se desconoce la existencia del tipo de certidicación para ambos ambientes desde una mirada estructura y de seguridad en todo el sentido de la palabra.

Cada una de estas capas son administradas y gestionadas por diferentes areas especializadas, las cuales deben valar por el correcto funcionamiento en su marco de acción.

**Patrones de referencia(SLA, buenas practicas)**

El inicio de estos servicio datan del año 2003, principalmente con el desarrollo del “Centro de Servicios de Soporte de Aplicación ” (CSESA) comprendiendo una solución global de la plataforma tecnologica de Hardware y Software (Diseño, Desarrollo y Explotación basados en J2EE), así como los servicios de aplicación y soporte. Dentro de este marco se definiron un conjunto de SLA los que fueron modificados en el tranqcurso del 2004, por una ampliación del alcance del desarrollo, teniendo documento final el siguiente marco:

1. SLA Aplicaciones
   1. Análisis, diseño y construcción de componentes aplicaciones
   2. Diseño del modelo de datos corporativo
   3. Migración de datos
   4. Explotación de los componentes de aplicaciones
   5. Mantención y soporte de los componentes de aplicaciones
   6. Help Desk
   7. Capacitación
2. SLA CSESA
   1. Hardware y Software Básico
   2. Operación
   3. Desarrollo Ad Hoc
   4. Servicio

**~~15.2.~~** ~~Definición de la función~~

**15.3.** El nivel del servicio

SLAs

**15.4.** Los procedimientos

**15.4.1.** Instalación y puesta en servicio: direcciones IPs,

Planificación:

Documentación: inventarios

Parametrización

pruebas

**15.4.2.** Mantenimiento y soporte: operación diaria, interna y de terceros

Planificación: garantías

Documentación: como contactar al soperte

Parametrización

pruebas

**15.4.3.** Requisitos para otros componentes

Planificación: espacio en disco, nuevas instancias, impacto en llos backups del aumento del espacio, tiempo adicional

Documentación: efectos a considerar

Parametrización: adaptación de nuevos parámetros

pruebas

**15.4.4.** Resolución de incidencias: procedimientos para registrar, analizar, diagnosticar, calificar y seguimiento de incidencias

Registrar: Formulario en papel

Analizar:

Diagnosticar

Calificar: frecuencia de la ocurrencia

Resolución: mitigar el error

Seguimiento

**15.4.5.** Seguridad y control: proteger accesos a la información, acciones de daño fortuito o malintencionado, accesos no autorizados (por desarrolladores), administración de entornos desarrollo (borrado lógico o físico), registrar la autoría de los cambios, “pistas de auditoría” de la BD,

**15.4.6.** Información sobre la actividad

Evolución de la actividad

Comparar la realidad con los objetivos

Majorar la calidad de las tareas

Anticipación a actividades críticas, analizando tendencias

**15.5.** Los Controles: evitar comportamiento no deseado

H/W: inventario

S/W: licencias, versiones, rendimiento

Comunicaciones:

Conmutación

Enlace: ancho de banda

Seguridad: procedimientos, medidas tomadas

Información: procedimientos de backup, almacenamiento es el adecuado?, reutilización, procedimientos de reutilización de cintas,

Plan de contingencia: procedimientos?, tienen ensayos periódicos

**~~15.6.~~** ~~Auditoría de la función~~

**~~15.7.~~** ~~Consideraciones sobre la tecnología y su evolución~~

La metodología de evaluación de riesgos (*risk oriented approach),* propuesta por la organización

**AUDITORÍA DE BASES DE DATOS**

La metodología de evaluación de riesgos (*risk oriented approach),* propuesta por la organización ISACA, comienza fijando los objetivos de control que minimizan los riesgos potenciales a los que está sometido el entorno. Una lista de riesgos importantes son:

● Incremento de la “dependencia” del servicio informático de terceros, debido a la concentración de datos

● Mayores posibilidades de acceso en la figura del administrador de la base de datos

● Incompatibilidad entre sistemas de seguridad de acceso propios del SGBD y el general de la instalación.

● Mayor impacto de los errores en datos o programas que en los sistemas tradicionales

● Mayor impacto de accesos no autorizados al diccionario de la base de datos

● Mayor dependencia del nivel de conocimientos técnicos del personal que realice tareas relacionadas con el software de base de datos (DBAs, BDOs, usuarios especializados)

Recomendaciones:

Deben establecerse Objetivo-de-control, en nuestro caso:

El SGBD deberá preservar la confidencialidad de la base de datos. Una vez establecidos los objetivos de control,

Deben establecerse las Técnicas-de-control (que sostendrán al Objetivo-de-control), en nuestro caso:

* Se deberán establecer los tipos de usuarios,
* perfiles y privilegios necesarios para controlar el acceso a las bases de datos. Actualmente existe un único usuario de acceso a la BD y éste se conecta a través de una aplicación

Estas técnicas pueden ser

Preventivas/detectivas (como lo es el monitoreo de la BD) o

Correctivas (como lo es un backup).

Pruebas-de-cumplimiento. En caso de que las Técnicas-de-controles existan, se diseñan las pruebas-de-cumplimiento, que permiten verificar la consistencia de los mismos. Listar los privilegios y perfiles en el SGBD sería una.

Se diseñarán las Pruebas-sustantivas que permiten dimensionar el impacto de las deficiencias, Si las Pruebas-de-cumplimiento detectan inconsistencias en las Técnicas-de-control, o si éstos controles no existieran.

Controlando en el ciclo de vida de una BD

ESTUDIO PREVIO Y PLAN DE TRABAJO.

1°) A la hora de implantar o realizar un *upgrade* de un SGBD, es necesario realizar un estudio viabilidad-técnica en el cual se contemplen distintas alternativas para alcanzar los objetivos del proyecto, en conjunto con un análisis de costo/beneficio para cada una de las opciones en estudio.

Éstos estudios de viabilidad deciden seguir/abortar el proyecto. El plan-del-proyecto contempla lo siguiente:

* Formulación
* Estudio previo y plan de trabajo
* Concepción de la BD y selección del equipo
* Diseño y carga
* Explotación y mantenimiento
* Revisión Post-implantación
* Documentación
* Calidad

El seguimiento y gestión del proyecto será aquel que cumple con los procedimientos generales de gestión de proyectos que tengan aprobados la organización.

COBIT enfatiza la importancia de realizar gestión de riesgos.

2°) Otro aspecto importante en esta fase es la aprobación de la estructura orgánica del proyecto en particular, sino también de la unidad que tendrá la responsabilidad de la gestión y control de la base de datos; recordemos que, para que un entorno de base de datos funcione debidamente, esta unidad es imprescindible.

Tareas del DBA

* Realizar el diseño conceptual y lógico de la base de datos
* Apoyar al personal de sistemas durante el desarrollo de aplicaciones
* Formar al personal
* Establecer estándares de diseño de la BD. Desarrollo y contenido del diccionario de datos
* Desarrollar políticas de gestión de datos
* Desarrollar planes estratégicos y tácticos para la manipulación de los datos
* Desarrollar los requisitos de los elementos del diccionario de datos
* Desarrollar normas para la denominación
* Controlar la integridad y seguridad de los datos
* Planificar la evolución de la BD de la empresa
* Identificar oportunidades de compartición de datos
* Trabajar con los auditores en la auditoría de la base de d.
* Proporcionar controles de seguridad
* Realizar el diseño físico de la BD.
* Asesorar en la adquisición de H/W yS/W
* Soportar el SGBD
* Resolver problemas del SGBD y del software asociado
* Monitorizar el rendimiento del SGBD
* Ayudar en el desarrollo de planes que aseguren la capacidad H/W.
* Asegurar la integridad de los datos, comprobando que se implantan los controles adecuados
* Asegurar la seguridad y confidencialidad
* Proporcionar facilidades de prueba
* Integrar paquetes, procedimientos, utilidades, etc. De soporte para al SGND
* Desarrollar estándares, procedimientos y documentarlos

A la hora de detallar las responsabilidades de estas funciones hay que tener en cuenta uno de los principios fundamentales del control interno: la separación de funciones. Aunque no es imperativo, y sólo como un aspecto de control, se recomienda una separación de funciones entre:

* El personal de desarrollo de sistemas y el de explotación
* Explotación y control de datos
* DBA y desarrollo.
* El administrador de seguridad y el DBA.

La separación de funciones es difícil de verificar si la organización no cuenta con una descripción detallada de los puestos de trabajo, los cuales deslinden las responsabilidades y *expertise* de su personal.

Conceptualización de la BD

En esta fase se inicia el diseño de la BD. La metodología de diseño (físico & lógico) debería también emplearse para especificar los documentos fuentes, los mecanismos de control, las características de seguridad y las pistas-de-auditoría a incluir en el sistema, estos últimos aspectos generalmente se descuidan, lo que produce mayores costos e inconvenientes cuando se quieren incorporar una vez concluida la implementación de la base de datos y la programación de las aplicaciones.

La definición de la arquitectura de la información (puede abordarse con COBIT) contempla los siguientes objetivos de control:

* Modelo de arquitectura de información y su actualización, que es necesaria para mantener el modelo consistente con las necesidades de los usuarios y con el plan estratégico de tecnologías de la información
* Datos y diccionario de datos corporativo
* Esquema de clasificación de datos en cuanto a seguridad
* Niveles de seguridad para cada anterior clasificación de datos

Diseño y carga

El diseños lógico y físico de la BD, contempla además de su estructura, las asociaciones y las restricciones oportunas, así como las especificaciones de almacenamiento de datos y los aspectos de seguridad.

<Los elementos (tablas, vistas, índices) deben haber sido aprobada por el usuario y que el administrador de la base de datos participó en su establecimiento>

Explotación y mantenimiento.

Se establecen los procedimientos de explotación y mantenimiento que aseguren que los datos se tratan de forma congruente y exacta y que el contenido de los sistemas sólo se modifica mediante la autorización adecuada.

Para asegurar un rendimiento adecuado del SGBD, debe llevarse a cabo un proceso de ajuste y optimización continua que no sólo consiste en el rediseño físico o lógico de la BD, sino que también abarca ciertos parámetros del SO e incluso la forma en que acceden las transacciones a la BD. Recordemos que la “función de administración de la BD debe ser la responsable de monitorizar el rendimiento y la integridad de los sistemas de BD”.

Revisión post-implantación.

Se debería establecer el desarrollo de un plan para efectuar una revisión post-implantación de todo sistema nuevo o modificado con el fin de evaluar si:

* Se han conseguido los resultados esperados
* Se satisfacen las necesidades de los usuarios
* Los costos y beneficios coinciden con lo previsto

Aspectos claves de la BD

Deberán considerarse los datos compartidos por múltiples usuarios. Esto debe abarcar todos los componentes del entorno de Bd.

14.4.1. Sistema de Gestion de Base de Datos. (SGBD)

* Entre sus componentes podemos destacar, el Kernel, el catálogo (componente fundamental para asegurar la seguridad de la base de datos), las utilidad para el administrador ( crear usuarios, conceder privilegios ) y resolver otras cuestiones relativas a la confidencialidad.
* En cuanto a las funciones de auditoría que ofrece el propio sistema, prácticamente todos los productos del mercado permiten registrar la mayoría de las operaciones.
* “el requisito para la auditoria es que la causa y el efecto de todos los cambios de la base de datos sean veriificables”

14.4.3. SISTEMA DE MONITORIZACIÓN Y AJUSTE (tuning)

14.4.4. SISTEMA OPERATIVO (S.O)

14.4.5. MONITOR DE TRANSACCIONES

14.4.7. PAQUETES DE SEGURIDAD

14.4.8. Diccionario de Datos

Juegan un papel primordial en el ede ntorno de los SGBD en cuanto a la integración de componentes y al cumplimiento de la seguridad datos.

Los diccionarios de datos se pueden auditar de manera análoga a las bases de datos, ya que, después de todo, son bases de datos de metadatos

Un fallo en la BD puede atentar contra la integridad de los datos y producir un mayor riesgo financiero, mientras que un fallo en un diccionario (o repositorios), suele llevar consigo un perdida de integridad de los procesos; siendo más peligrosos los fallos en los diccionarios puesto que pueden introducir errores de forma repetitiva a lo largo del tiempo y son más difíciles de detectar.

14.4.11. Facilidades de Usuario

El auditor deberá investigar las medidas de seguridad que ofrecen estas herramientas (Interfaz gráfica de usuario) y bajo qué condiciones han sido instaladas; las herramientas de este tipo deberían proteger a los usuarios de sus propios errores.

Objetivos de control:

* La documentación de las aplicaciones desarrollada por usuarios finales debe ser suficiente para que tanto sus usuarios principales como cualquier otro pueda operar y mantenerlas.
* Los cambios de estas aplicaciones requieren la aprobación de la dirección y deben documentarse de forma completa.

14.4.12. Herramientas de Minería de Datos

Se deberá controlar la política de refresco y carga de los datos en el almacén a partir de las bases de datos operacionales existentes.

14.4.13. Aplicaciones

Se deberá controlar que las aplicaciones no atentan contra la integridad de los datos de la base.

**ANEXOS**

Proceso de la auditoría en IPS

**Metodología, Fases y Plan de la Auditoría Informática.**

**Metodología para llevar a cabo una Auditoría Informática:**

• Diseño del plan y método de trabajo.

• Alcance y objetivos de la auditoría informática.

• Estudio inicial del entorno o medio auditor.

• Determinación de los recursos necesarios para realizar la auditoría.

• Elaboración del plan y de los programas de trabajo.

• Actividades propiamente dichas de la auditoría.

• Confección y redacción del informe final.

• Determinación de las conclusiones y recomendaciones.

• Fijación del pliego de responsabilidades y valoración de gestión.

• Redacción de la carta del informe final

**a) Fases y Planificación de una Auditoría Informática.**

Fases previas:

• Recopilación de Información Básica.

• Programa de trabajo, identificación de riesgos y objetivos de control.

• Plan Específico de Auditoría, pruebas.

• Informe y Plan de mejoras.

**b) Plan para Realizar una Auditoría Informática.**

Para la realización de una auditoría informática se deben completar las siguientes fases y planificación de actividades:

**Toma de contacto.**

Primera toma de contacto con Ia empresa auditada para conocer características generales de la misma: sector industrial, organización y organigrama, relaciones externas, volumen de negocio.

**Definición del alcance.**

Se ha de definir con precisión el área y objetivos perseguidos por la auditoría. Se ha de indicar que parte del servicio de informática va a ser auditado así como hacer constar que elementos debe quedar fuera de la auditoría. Deben quedar recogidas, si existieran, excepciones que se deben tener cuenta al efectuar la revisión.

Desde el punto de vista del objetivo, debe quedar reflejado cuales son los motivos

y fines que persigue la auditoría:

**Recursos y tiempo.**

• Recursos personales (equipo auditor)

• Recursos materiales.

• Calendario de actuaciones.

**Plan de trabajo, recopilación de la información.**

Análisis de la información básica obtenida en la primera toma de contacto con la organización, conclusiones que se deducen. Estableciendo el programa de trabajo para realizar, ampliar y completar la información necesaria para la realización de la auditoría informática.

Esta recopilación de información se puede realizar de varias formas: entrevistas personales, cuestionarios, observación de las actividades.

**Identificación de los riesgos potenciales.**

Con toda la información obtenida en las fases anteriores, el equipo de auditoría estaría en condiciones de identificar los riesgos potenciales que pueden existir en el servicio informático, teniendo en cuenta el alcance que se ha definido para la realización de la auditoría.

**Definición de pruebas.**

El equipo de auditoría debe realizar pruebas para verificar la consistencia de los controles existentes o bien para medir el riesgo existente. Toda opinión o evaluación de un auditor debe estar basada en pruebas realizadas de acuerdo con mina normativa profesional. Las pruebas pueden ser de cumplimiento, que se utilizan para comprobar si el riesgo potencial es real.

**Obtención de resultados de las pruebas.**

Los resultados de cada prueba deben valorarse para obtener una conclusión, siempre teniendo en cuenta los objetivos y el alcance de la auditoría.

**Obtención de resultados de las pruebas.**

Las conclusiones obtenidas deben comentarse y discutirse con los responsables directos del área afectada por las razones que se expresan a continuación:

• Puede haber limitaciones en la realización de las pruebas.

• Puede haber controles alternativos que no hayan detectado en el proceso.

Todas las deficiencias o riesgos deben ser objeto de comentarios individuales y deben incluir:

• Descripción de la situación.

• Riesgo existente y deficiencia a solucionar.

• Si es preciso, sugerencia de solución.

**Revisión y cierre de papeles de trabajo.**

Tiene por objeto preparar la documentación del trabajo realizado y se debe realizar de acuerdo con unas normas básicas de auditoría que expresen:

• La metodología utilizada.

• Cobertura del objetivo de la auditoría.

• Pruebas realizadas y criterios utilizados.

• Resultado de las pruebas.

Antes de pasar a la realización del borrador del informe, los papeles de trabajo deben ser revisados, tratando de identificar:

• Las limitaciones en las tareas realizadas.

• Deficiencias en pruebas realizadas, que puedan requerir alguna extensión especial de la revisión.

• Falta de consistencia o claridad en las conclusiones.

• Documentación de todas las conclusiones obtenidas.

**Preparación del borrador del informe.**

El borrador del informe, es un resumen del trabajo efectuado durante la realización

de la auditoría y debe incluir:

• El alcance y objetivo de la auditoría.

• La metodología utilizada.

• Las posibles limitaciones y conclusiones.

**Discusión del informe.**

Es importante que el informe, antes de su emisión definitiva, sea comentado y discutido con los responsables del área auditada y en caso de discrepancia de opiniones con el área auditada, estas deberán ser incluidas en el texto final del informe.

**Emisión y distribución del informe.**

Finalizada la realización de la auditoría informática, se redactará el informe final y posteriormente se enviará a la dirección de la empresa.

**Plan de mejoras o recomendaciones.**

El informe puede ir acompañado de un plan de mejoras donde para cada uno de los problemas detectados se ofrezca un conjunto de posibles soluciones.

Estas soluciones pueden dividirse en tres tipos:

• Medidas a corto plazo (formación, cumplimiento de calendario)

• Medidas a medio plazo (mayor cantidad de recursos, mejoras en la estructura organizativa).

• Medidas a largo plazo (cambio de política en el servicio de informática, objetivos).

Anexos

Levantamiento de Evidencia

# Evidencia base

## Diagrama conceptual

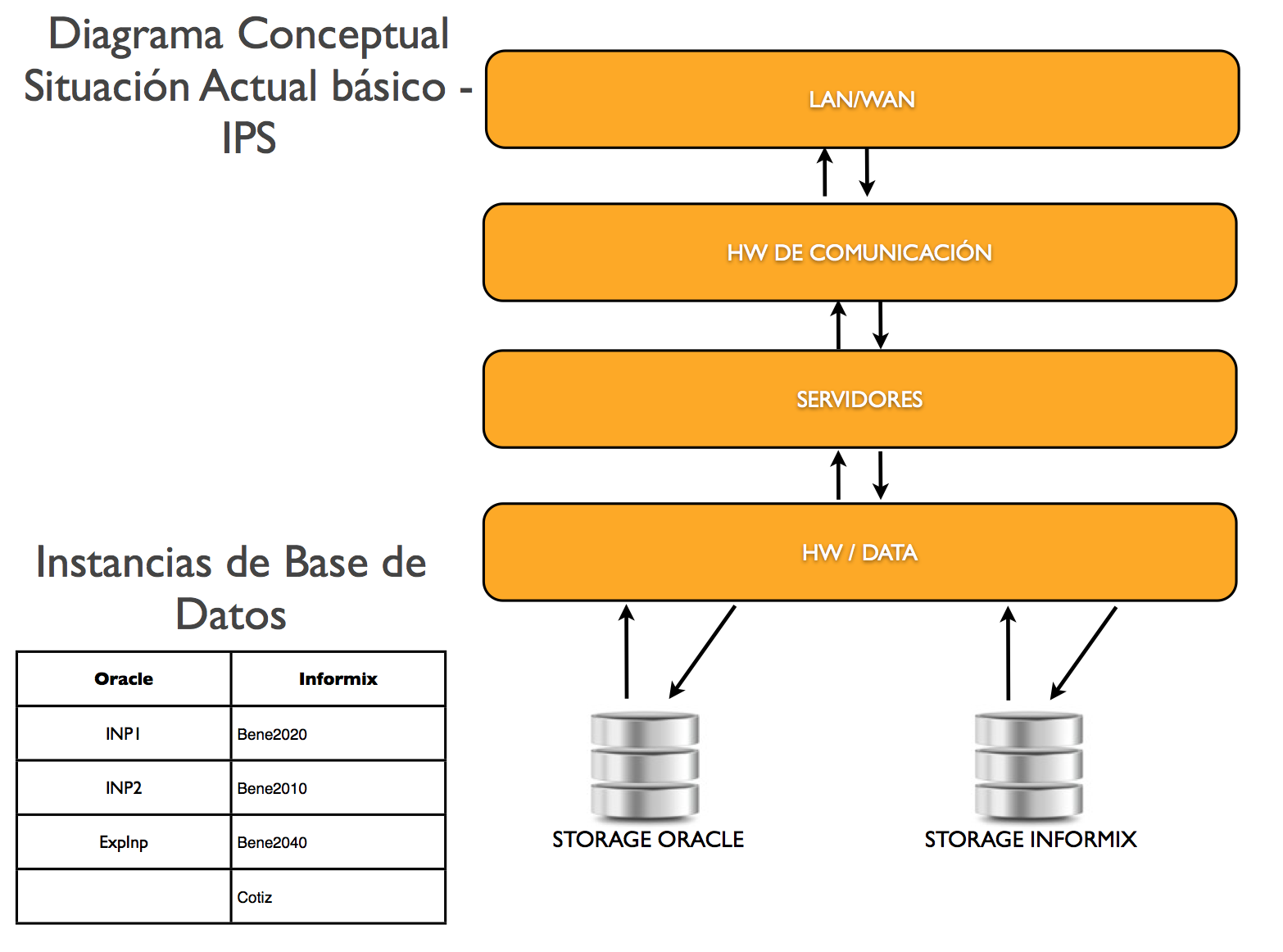


Imagen 1.0 Diagrama conceptual Situación Actual Básico- IPS

## Identificar toda la Infraestructura (hardware) que soporta las instancias ORACLE & INFORMIX (Servidores y Storage)

Se obtiene un 80.5% del total de la evidencia requerida (Anexo 1 – hoja SERVER\_STORAGE\_ORACLE & SERVER\_STORAGE\_INFORMIX) , teniendo como el restante no evidenciado lo siguiente:

* Hardware
  + Soporte
  + Garantía
    - Razón: No mantiene un soporte y garantía con los proveedores, y sumado a una falta de conocimiento real de esta situación.
* Discos Externos o Storage - Oracle
  + Utilizado
  + Libre
    - Razón: Los servicios se encuentran en un entorno compartido, lo que genera un desconocimiento en esta materia al entrar en un solo ambiente.
* Comunicaciones
  + IP PUB
  + IP BACK
    - Las comunicaciones, se realizan bajo un entorno en la Synapsis declaro no mantener esta estructura de IP’s

### Diagrama técnico y funcional

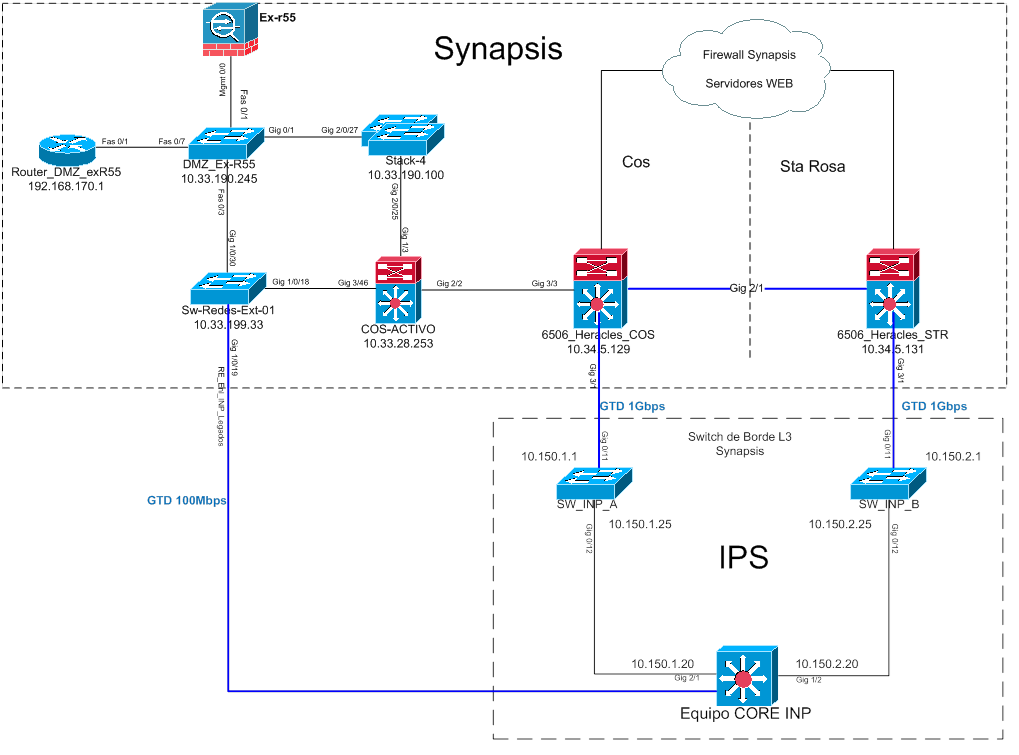
Evidencia no entregada, por no encontrarse disponible por parte de Synapsis.

## **Identificar toda la Infraestructura (hardware) que soporta las instancias ORACLE & INFORMIX (Periféricos de Comunicaciones y Datos)**

Se obtiene un 50% del total de la evidencia requerida (Anexo 1 – hoja HW\_COMUNIC\_DATOS\_ORACLE & HW\_COMUNIC\_DATOS\_INFORMIX) , teniendo como el restante no evidenciado lo siguiente:

* Comunicaciones
  + Tipo NIC
  + Velocidad
  + Cantidad
  + IP LAN
  + IP PUB
  + IP ADM
  + IP BACK
  + Redundancia
  + Stack
  + BGP
* Datos
  + Tipo FC
  + Marca
  + Modelo
  + Velocidad
  + Cantidad
* Razón: Como este ítem involucra la interacción de diferentes áreas dentro de Synapsis, no se logro dilucidar ciertamente el personal con el conocimiento global. Sumado a la aceleración del levantamiento de evidencia por concepto de atrasos.

### Diagrama técnico y funcional



## Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias ORACLE & INFORMIX (Servidores y Storage)

Se obtiene un 87.5% del total de la evidencia requerida (Anexo 1 – hoja SW\_SERVER\_STORAGE\_ORACLE & SW\_SERVER\_STORAGE\_INFORMIX , teniendo como el restante no evidenciado lo siguiente:

* Servidor
  + Tipo servidor
  + IOS
  + Configuración
* Sistema Operativo Servidor
  + Nombre volumen
* Razón: La información no fue devuelta a pesar de ser solicitad.

PLANILLA DE IDENTIFICACIÓN

|  |  |
| --- | --- |
| RECOLECCIÓN DE ANTECENTES TÉCNICOS | |
| AUDITORÍA BDATOS IPS 2013 | |
| SERVICIOS PROFESIONALES KROWTEN NETWORK | |
|  |  |
| MATRIZ DE EVIDENCIA BASE | |
| Item | Planilla |
| 1 | Diagrama conceptual Situación Actual |
| **2** | **Identificar toda la Infraestructura (hardware) que soporta las instancias ORACLE (Servidores y Storage)** |
| 3 | Diagrama técnico y funcional |
| **4** | **Identificar toda la Infraestructura (hardware) que soporta las instancias INFORMIX (Servidores y Storage)** |
| 5 | Diagrama técnico y funcional |
| **6** | **Identificar toda la Infraestructura (hardware) que soporta las instancias ORACLE (Periféricos de Comunicaciones y Datos)** |
| 7 | Diagrama técnico y funcional |
| **8** | **Identificar toda la Infraestructura (hardware) que soporta las instancias INFORMIX (Periféricos de Comunicaciones y Datos)** |
| 9 | Diagrama técnico y funcional |
| **10** | **Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias ORACLE (Servidores y Storage)** |
| 11 | Diagrama técnico y funcional |
| **12** | **Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias INFORMIX (Servidores y Storage)** |
| 13 | Diagrama técnico y funcional |
| **14** | ***Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias ORACLE (Periféricos de Comunicaciones)*** |
| 15 | Diagrama técnico y funcional |
| **16** | ***Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias INFORMIX (Periféricos de Comunicaciones)*** |
| 17 | Diagrama técnico y funcional |
| MATRIZ DE EVIDENCIA MEDIA | |
| 1 | Archivos LOGS (Sistemas Operativos, Oracle, Informix) |
| 2 | Archivos de CONFIG (Sistemas Operativos, Oracle, Informix) |
| 3 | Identificación de Accesos (Administración, Operación y Usuarios) |
| 4 | Organigrama de Servicios Transmisión Synapsis |
| 5 | Organigrama de Servicios Recepción IPS |
| 6 | Acuerdos de Niveles Servicios (SLA) |
| 7 | Contrato y anexos Servicio de Hosting |
| MATRIZ DE EVIDENCIA AVANZADA | |
| 1 | Plataforma de Respaldo y Recuperación (Hardware, Software, Procedimientos y Políticas) |
| 2 | Procedimientos de Administración |
| 3 | Procedimientos de Operación |
| 4 | Plataforma de Alta Disponibilidad |
| 5 | Procedimientos de Administración |
| 6 | Procedimientos de Operación |

SERVER\_STORAGE\_ORACLE

Infraestructura (hardware) que soporta las instancias ORACLE (Servidores y Storage)

Auditoría DB ORACLE - IPS MAYO 2013

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  | **Tipo de Arquitectura** | **Tipo Servidor** | **Hardware** | | | | | **Cantidad** |
| Ítem | Nombre Intancia Oracle | SAN/NAS/DAS | Físico/Virtual | Marca | Modelo | Soporte | Ganatía | Hostname | UR |
| 1 | INP1 | SAN | RX8640 -Fisico | HP | IA64 |  |  | HR3P1101 | 1 Rack Completo |
| 2 | INP1 | SAN | RX8640 -Fisico | HP | IA64 |  |  | HR3Pe1101 | 1 |
| 3 | Disc9i | SAN | Fisico | HP | 9000 |  |  | HR4P1101 | 4 |
| 4 | ExpInp | SAN | RX8640 -Fisico | HP | IA64 |  |  | Synora01 | 1 Rack Completo |
| 5 | Inp | SAN | RX8640 -Fisico | HP | IA64 |  |  | Synora01 | 1 Rack Completo |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **CELDA EN AMARILLO = PENDIENTE** | | | |  |  |  |  |  |  |
| **CELDA EN ROJO = NO HAY CONOCIMIENTO** | | | |  |  |  |  |  |  |
| **CELDA EN VERDE = DATO MUY RELEVANTE PARA SYNAPSIS** | | | |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cantidad** | **Tipo** | **Discos o Ejes Internos** | | | | **Discos Externos o Storage** | | |  |  |
| Fuente Poder | Raid | Tamaño GB | Velocidad RPM | Utilizado GB | Libre GB | Marca | Modelo | Cant. Fuente Poder | Cant. UR | Nombre Vol.Lóg. |
| 12 | 1 | 73 | 15000 | 72 | 1 | IBM | XIV | 36 | 1 Rack completo | Confirmar |
| 12 | 1 | 74 | 15000 | 71 | 2 | IBM | V7000 | 2 | 2U | Confirmar |
| 2 | 1 | 36 | 15000 | 33 | 3 | IBM | DS8100 | 19 | 1 Rack Completo | Confirmar |
| 12 | 1 | 73 | 15000 | 72 | 1 | IBM | DS5100 | 20 | 1 Rack completo | Confirmar |
| 12 | 1 | 73 | 15000 | 72 | 1 | IBM | DS5101 | 20 | 1 Rack completo | Confirmar |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Discos Externos o Storage | | | | |
| Raid | Tamaño TB | Velocidad | Utilizado | Libre |
| No aplica | 3,44 | 7200 2k RPM |  |  |
| 5 | 3,3 | 7500 RPM |  |  |
| 5 | 2.5 | 15000RPM |  |  |
| 5 | 1.1 | 15000RPM |  |  |
| 5 | 1.1 | 15000RPM |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Comunicaciones | | | | | | | |
| Tipo NIC | Velocidad | Cantidad | IP LAN | IP PUB | IP ADM | IP BACK | Redundancia |
| 1000 Base-T (GEthernet) | 1G | 4 | 10.34.3.20 |  | 10.34.3.20 |  | 2 |
| 1000 Base-T (GEthernet) | 1G | 4 | 10.33.1.239 |  | 10.33.1.239 |  | 2 |
| 1000 Base-T (GEthernet) | 1G | 2 | 10.34.2.22 |  | 10.34.2.22 |  |  |
| 1000 Base-T (GEthernet) | 1G | 6 | 10.33.2.103 |  | 10.33.2.103 |  | 2 |
| 1000 Base-T (GEthernet) | 1G | 6 | 10.33.2.103 |  | 10.33.2.103 |  | 2 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Canales de Fibra | | | |
| Tipo FC | Velocidad | Cantidad | Redundancia |
| HP AD 194-60001 | 4GB | 4 | 4 |
| HP AD 194-60001 | 4GB | 4 | 4 |
| HP Tachyon xl2 | 2GB | 2 | 2 |
| HP AD 194-60001 | 4GB | 2 | 2 |
| HP AD 194-60001 | 4GB | 2 | 2 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

SERVER\_STORAGE\_INFORMIX

Infraestructura (hardware) que soporta las instancias INFORMIX (Servidores y Storage)

Auditoría DB INFORMIX - IPS MAYO 2013

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Tipo de Arquitectura | Tipo Servidor | Hardware | | | | | Cantidad |
| Ítem | Nombre Intancia Informix | SAN/NAS/DAS | Físico/Virtual | Marca | Modelo | Soporte | Ganatía | Hostname | UR |
| 1 | Bene 2010 | SAN | Fisico | Fisico | 9000 |  |  | Syn11 | 1 Rack Completo |
| 2 | Bene 2020 |  |  |  |  |  |  |  |  |
| 3 | Bene 2040 |  |  |  |  |  |  |  |  |
| 4 | Cotiz |  |  |  |  |  |  |  |  |
| 5 | Cotiz His |  |  |  |  |  |  |  |  |
| 6 | Imponentes |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **CELDA EN AMARILLO = PENDIENTE** | | | |  |  |  |  |  |  |
| **CELDA EN ROJO = NO HAY CONOCIMIENTO** | | | |  |  |  |  |  |  |
| **CELDA EN VERDE = DATO MUY RELEVANTE PARA SYNAPSIS** | | | |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Cantidad | Tipo | Discos o Ejes Internos | | | | Discos Externos o Storage | | |  |
| Fuente Poder | Raid | Tamaño GB | Velocidad RPM | Utilizado GB | Libre GB | Marca | Modelo | Cant. Fuente Poder | Cant. UR |
| 2 PDU - (No visible fisicamente) | 1 | 36 | 15000 | 32,5 | 3,5 | IBM | DS8100 | 19 | 1 Rack Completo |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  |  | Discos Externos o Storage |
| Nombre Vol.Lóg. | Raid | Tamaño TB | Velocidad | Utilizado |
|  | 5 | 2,4 |  |  |
|  |  | 2,4 |  |  |
|  |  | 2,4 |  |  |
|  |  | 2,4 |  |  |
|  |  | 2,4 |  |  |
|  |  | 2,4 |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Comunicaciones | | | | | | | |
| Tipo NIC | Velocidad | Cantidad | IP LAN | IP PUB | IP ADM | IP BACK | Redundancia |
| HP A5 838A | 100 | 3 | 10.33.1.64 |  | 10.33.1.64 |  | 1 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Canales de Fibra | | | |
| Tipo FC | Velocidad | Cantidad | Redundancia |
| HP Tachyon xl2 | 2G | 2 | 2 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

HW\_COMUNIC\_DATOS\_ORACLE

Infraestructura (hardware) que soporta las instancias ORACLE (Periféricos de Comunicaciones y Datos)

Auditoría DB ORACLE - IPS MAYO 2013

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Nombre | Tipo HW | | | |
| Ítem | Nombre Intancia Oracle | Para todas las instancias | Hostname | Transciver | Router | Switch | IOS |
| 1 | INP1 | Stack\_IPS\_INP |  |  | x | 12.2(58)SE2 |
| 2 | INP1 | Stack\_IPS\_INP\_II |  |  | x | 12.2(53r)SE2 |
| 3 | Disc9i | Stack\_IPS\_INP\_III |  |  | x | 12.2(35)SE5 |
| 4 | ExpInp | ASA5540 |  |  | x | ASA 8.4(5) - ASDM 7.1(3) |
| 5 | Inp | Stack\_IPS\_Level3 |  |  | x | 12.2(55)SE5 |
|  |  | Sw\_ADM\_IPS |  |  | x | 12.1(22)EA9 |
|  |  | IPS\_SW-Pureflex\_ESX\_1.1 |  |  | x | 7.5.1 (FLASH image1) |
|  |  | IPS\_SW-Pureflex\_ESX\_1.2 |  |  | x | 7.5.1 (FLASH image1) |
|  |  | IPS\_SW-Pureflex\_Fisico\_1.1 |  |  | x | 7.5.1 (FLASH image1) |
|  |  | IPS\_SW-Pureflex\_Fisico\_1.2 |  |  | x | 7.5.1 (FLASH image1) |
|  |  | IPS\_SW-Pureflex\_L3\_1.1 |  |  | x | 7.5.1 (FLASH image1) |
|  |  | IPS\_SW-Pureflex\_L3\_1.2 |  |  | x | 7.5.1 (FLASH image1) |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **CELDA EN AMARILLO = PENDIENTE** | | | | |  |  |  |
| **CELDA EN ROJO = NO HAY CONOCIMIENTO** | | | | |  |  |  |
| **CELDA EN VERDE = DATO MUY RELEVANTE PARA SYNAPSIS** | | | | |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| Arquitectura | Marca | Modelo | Versión | Release | Configuración |
| Stack | Cisco | WS-C3750X-24T-L | C3750E-IPBASEK9-M | RELEASE SOFTWARE (fc1) | Stack de 3 Switch |
| Switch | Cisco | WS-C3750X-24T-L | C3750E-IPBASEK9-M | RELEASE SOFTWARE (fc1) | Switch |
| Switch | Cisco | WS-C3750G-24TS-1U | C3750-IPBASE-M | RELEASE SOFTWARE (fc1) | Switch |
| Firewall | Cisco | ASA5540 |  |  | Firewall HA |
| Stack | Cisco | WS-C3750X-24T-L | C3750E-UNIVERSALK9-M | RELEASE SOFTWARE (fc1) |  |
| Switch | Cisco | WS-C2950SX-24 |  | RELEASE SOFTWARE (fc1) | Stack de 3 Switch |
| Switch | IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  |  |
| Switch | IBM | BM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |
| Switch | IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |
| Switch | IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |
| Switch | IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |
| Switch | IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Comunicaciones | | | | | | | | | | Datos | | | | |
| Tipo NIC | Velocidad | Cantidad | IP LAN | IP PUB | IP ADM | IP BACK | Redundancia | Stack | BGP | Tipo FC | Marca | Modelo | Velocidad | Cantidad |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

HW\_COMUNIC\_DATOS\_INFORMIX

Infraestructura (hardware) que soporta las instancias INFORMIX (Periféricos de Comunicaciones y Datos)

Auditoría DB INFORMIX - IPS MAYO 2013

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | Nombre | Tipo HW | | | |  |
| Ítem | Nombre Intancia Oracle | Para todas las instancias | Hostname | Transciver | Router | Switch | IOS | Arquitectura |
| 1 | Bene 2010 | Stack\_IPS\_INP |  |  | x | 12.2(58)SE2 | Stack |
| 2 | Bene 2020 | Stack\_IPS\_INP\_II |  |  | x | 12.2(53r)SE2 | Switch |
| 3 | Bene 2040 | Stack\_IPS\_INP\_III |  |  | x | 12.2(35)SE5 | Switch |
| 4 | Cotiz | ASA5540 |  |  | x | ASA 8.4(5) - ASDM 7.1(3) | Firewall |
| 5 | Cotiz His | Stack\_IPS\_Level3 |  |  | x | 12.2(55)SE5 | Stack |
| 6 | Imponentes | Sw\_ADM\_IPS |  |  | x | 12.1(22)EA9 | Switch |
|  |  | IPS\_SW-Pureflex\_ESX\_1.1 |  |  | x | 7.5.1 (FLASH image1) | Switch |
|  |  | IPS\_SW-Pureflex\_ESX\_1.2 |  |  | x | 7.5.1 (FLASH image1) | Switch |
|  |  | IPS\_SW-Pureflex\_Fisico\_1.1 |  |  | x | 7.5.1 (FLASH image1) | Switch |
|  |  | IPS\_SW-Pureflex\_Fisico\_1.2 |  |  | x | 7.5.1 (FLASH image1) | Switch |
|  |  | IPS\_SW-Pureflex\_L3\_1.1 |  |  | x | 7.5.1 (FLASH image1) | Switch |
|  |  | IPS\_SW-Pureflex\_L3\_1.2 |  |  | x | 7.5.1 (FLASH image1) | Switch |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| **CELDA EN AMARILLO = PENDIENTE** | | | |  |  |  |  |  |
| **CELDA EN ROJO = NO HAY CONOCIMIENTO** | | | |  |  |  |  |  |
| **CELDA EN VERDE = DATO MUY RELEVANTE PARA SYNAPSIS** | | | |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | Comunicaciones | | |  |  |  |  |  |
| Marca | Modelo | Versión | Release | Configuración | Tipo NIC | Velocidad | Cantidad | IP LAN | IP PUB | IP ADM | IP BACK | Redundancia |
| Cisco | WS-C3750X-24T-L | C3750E-IPBASEK9-M | RELEASE SOFTWARE (fc1) | Stack de 3 Switch |  |  |  |  |  |  |  |  |
| Cisco | WS-C3750X-24T-L | C3750E-IPBASEK9-M | RELEASE SOFTWARE (fc1) | Switch |  |  |  |  |  |  |  |  |
| Cisco | WS-C3750G-24TS-1U | C3750-IPBASE-M | RELEASE SOFTWARE (fc1) | Switch |  |  |  |  |  |  |  |  |
| Cisco | ASA5540 |  |  | Firewall HA |  |  |  |  |  |  |  |  |
| Cisco | WS-C3750X-24T-L | C3750E-UNIVERSALK9-M | RELEASE SOFTWARE (fc1) |  |  |  |  |  |  |  |  |  |
| Cisco | WS-C2950SX-24 |  | RELEASE SOFTWARE (fc1) | Stack de 3 Switch |  |  |  |  |  |  |  |  |
| IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  |  |  |  |  |  |  |  |  |  |
| IBM | BM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |  |  |  |  |  |  |  |  |
| IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |  |  |  |  |  |  |  |  |
| IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |  |  |  |  |  |  |  |  |
| IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |  |  |  |  |  |  |  |  |
| IBM | IBM Flex System Fabric EN4093 10Gb Scalable Switch |  |  | Switch |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Comunicaciones | Datos | | | | |
| Stack | BGP | Tipo FC | Marca | Modelo | Velocidad | Cantidad |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

SW\_SERVER\_STORAGE\_ORACLE

Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias ORACLE (Servidores y Storage)

Auditoría DB ORACLE - IPS MAYO 2013

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Servidor | | | | | | | |
| Ítem | Nombre Intancia Oracle | Tipo Servidor | IOS | Arquitectura | Marca | Modelo | Versión | Release | Configuración |
| 1 | INP1 |  |  | 64bit | HP | IA64 | Rx | 8640 | Pendiente |
| 2 | INP1 |  |  | 64bit | HP | IA64 | Rx | 8640 | Pendiente |
| 3 | Disc9i |  |  | 64bit | HP | 9000 | 800 | L3000-8x | Pendiente |
| 4 | ExpInp |  |  | 64bit | HP | IA64 | Rx | 8640 | Pendiente |
| 5 | Inp |  |  | 64bit | HP | IA64 | Rx | 8640 | Pendiente |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **CELDA EN AMARILLO = PENDIENTE** | | | |  |  |  |  |  |  |
| **CELDA EN ROJO = NO HAY CONOCIMIENTO** | | | |  |  |  |  |  |  |
| **CELDA EN VERDE = DATO MUY RELEVANTE PARA SYNAPSIS** | | | |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Sistema Operativo Servidor | | | | | |  |  |
| Nombre | Distribución | Arquitectura | Versión | Kernel | Complilación | Particiones | Nombre volumen |
| HP-UX | N/A | 64 bits | 11.23 | B.11.23 U | N/A | Raw Device |  |
| HP-UX | N/A | 64 bits | 11.23 | B.11.23 U | N/A | Raw Device |  |
| HP-UX | N/A | 64 bits | 11.11 | B.11.11 U | N/A | dbspace1 | /dev/newvg02/lvol1 |
| HP-UX | N/A | 64 bits | 11.23 | B.11.23 U | N/A | Orainp | /dev/DS501/lvorainpDS5 |
| HP-UX | N/A | 64 bits | 11.23 | B.11.23 U | N/A | Orainp | /dev/DS501/lvorainpDS5 |
|  |  |  |  |  |  | export | /dev/DS501/lvexportDS5 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Base de datos Oracle | | | | | | Aplicación Cliente | | |
| Versión | Motor | Tipo | Release | Nº tablas | Tamaño TB | Nombre | Versión | Release |
| 9i | Oracle Enterprice edicion (64 bits) | Productivo | 2.0.7 | 2902 | 2,7923 | 10g (administración ) | 10.2 | 0.01 |
| 9i | Oracle Enterprice edicion (64 bits) | Testing | 2.0.7 | 2898 | 2,7856 | 10g (administración ) | 10.2 | 0.01 |
| 9i | Oracle Enterprice edicion (64 bits) | Productivo | 2.0.7 | 3139 | 0,2919 | 10g (administración ) | 10.2 | 0.01 |
| 9i | Oracle Enterprice edicion (64 bits) | Productivo | 2.0.6 | 617 | 0,0131 | 10g (administración ) | 10.2 | 0.01 |
| 9i | Oracle Enterprice edicion (64 bits) | Productivo | 2.0.6 | 771 | 0,0483 | 10g (administración ) | 10.2 | 0.01 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

SW\_SERVER\_STORAGE\_INFORMIX

Identificar toda la Arquitectura (software) que soporta y forma parte de las instancias INFORMIX (Servidores y Storage)

Auditoría DB INFORMIX - IPS MAYO 2013

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | | | | Servidor |  |  |
| Ítem | Nombre intancia Informix | Tipo servidor | IOS | Arquitectura | Marca | Modelo | Versión | Release | Configuración |
| 1 | Bene 2010 |  |  | 64Bits | HP | 900 | 800 | SD64A |  |
| 2 | Bene 2020 |  |  | 64Bits | HP | 900 | 800 | SD64A |  |
| 3 | Bene 2040 |  |  | 64Bits | HP | 900 | 800 | SD64A |  |
| 4 | Cotiz |  |  | 64Bits | HP | 900 | 800 | SD64A |  |
| 5 | Cotiz His |  |  | 64Bits | HP | 900 | 800 | SD64A |  |
| 6 | Imponentes |  |  | 64Bits | HP | 900 | 800 | SD64A |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
| **CELDA EN AMARILLO = PENDIENTE** | | | |  |  |  |  |  |  |
| **CELDA EN ROJO = NO HAY CONOCIMIENTO** | | | |  |  |  |  |  |  |
| **CELDA EN VERDE = DATO MUY RELEVANTE PARA SYNAPSIS** | | | |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sistema Operativo Servidor | | | | | |  |  | Base de datos Informix | | |
| Nombre | Distribución | Arquitectura | Versión | Kernel | Complilación | Particion | Nombre volumen | Versión | release | motor |
| HP-UX | N/A | 64Bits | 11.11 | B.11.11 U | N/A | Raw Device |  | 7 | 31.fc4 | Informix |
| HP-UX | N/A | 64Bits | 11.11 | B.11.11 U | N/A | Raw Device |  | 7 | 31.fc4 | Informix |
| HP-UX | N/A | 64Bits | 11.11 | B.11.11 U | N/A | Raw Device |  | 7 | 31.fc4 | Informix |
| HP-UX | N/A | 64Bits | 11.11 | B.11.11 U | N/A | Raw Device |  | 7 | 31.fc4 | Informix |
| HP-UX | N/A | 64Bits | 11.11 | B.11.11 U | N/A | Raw Device |  | 7 | 31.fc4 | Informix |
| HP-UX | N/A | 64Bits | 11.11 | B.11.11 U | N/A | Raw Device |  | 7 | 31.fc4 | Informix |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Aplicación Cliente | | |
| Nº tablas | Tamaño TB | Nombre | Versión | Release |
| 507 | 0,182 | Administración directa desde el servidor (En terminal ejecutando comando y usando algunos script y utilitarios) | | |
| 336 | 0,179 |
| 356 | 0,127 |
| 474 | 0,122 |
| 13 | 0,067 |
| 229 | 0,050 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |