



APLICACION DE PROTOCOLOS DE COPIAS DE RESPALDO

Monografía Diplomado Oracle



Autor:

DANIEL RICARDO ARIZA BARREA

Ingeniería de Sistemas

5 DE JULIO DE 2017
UNIVERSIDAD LIBRE DE COLOMBIA
Sede el Bosque

DEDICATORIA

Trabajo dedicado a mi hijo Santiago quien es mi inspiración y mi mayor razón para seguir creciendo y mejorando como padre, como persona y como profesional, a mi esposa por su apoyo incondicional, a mi madre por su apoyo y a mi padre que aunque ya no está con nosotros fue quien me motivo apoyo y colaboro para que yo iniciara mi carrera profesional.

AGRADECIMIENTOS

Los agradecimientos son para toda mi familia, a los docente y a mi compañeros que gracias a ellos comprendí y mejore en todo aspecto académico profesional y sobre todo personal.

INDICE

ITEM	Pág.
Portada	I
Dedicatorias	1
Agradecimientos	2
Índice	3
Síntesis	4
Introducción	5
Infraestructura Base	6
Tipos de Backup	8
Almacenamiento y retenciones para Backup	9
Seguridad general y en los Backup	10
Tiempos de Ejecución de Backup	11
Prueba de copias de Respaldo	13
Crecimiento de las Bases de Datos	13
Implementación de Protocolos en empresas	14
Implementación en Clínica del Occidente	15
Implementación en Banco de la Republica	19
Conclusiones	23
Bibliografía	24

SINTESIS

Los protocolos de seguridad en el tema de copias de seguridad están promulgados a nivel internacional y por medio de los procesos de acreditación se han estandarizado con el fin de que puedan y sean adoptados por las empresas siguiendo los parámetros básicos que facilitan su implementación, para ello se evalúan ciertas variables que analizaremos en este documento estas variables inciden en todo el proceso de generación de copias de respaldo de la información y se ajustan a todas las empresa, es esta la forma de garantizar que sean aplicadas sin importar el tipo de función que desempeñe la empresa.

VARIABLES como la infraestructura, los tipos de Backup, el almacenamiento y retención de los Backup, la seguridad en la información y en los Backup y el crecimiento de la información son las que más relevancia tienen en la implementación de los procesos y están ligadas de manera encadenada lo que permite que en el momento de la implementación todas deban ser consideradas y aplicadas.

Para demostrar este planteamiento estudiaremos 2 empresas que han trabajado procesos de acreditación y que han implementado los protocolos de seguridad informática y entre eso han adoptado los protocolos de seguridad de copias de respaldo de la información así como también tener en consideración que la plataforma gestora de bases de datos Oracle ha trabajado en desarrollar herramientas que permiten implementar estos protocolos con mayor eficiencia.

INTRODUCCION

La planeación es uno de los pilares de las empresas y se aplica a todas las áreas de gestión y producción, sin una apropiada planeación la ejecución de las labores cotidianas se presentarían problemas que podrían deteriorar o alterar los resultados esperados, al realizar una buena planeación se especifican protocolos que nos permiten estandarizar los procesos asegurando un proceso con calidad y un resultado esperado que de fiabilidad, seguridad, veracidad, en el manejo de la información estos protocolos son de mayor relevancia para mantener la integridad de los datos y la disponibilidad efectiva de estos para que puedan ser usados en la empresa.

Ante los actuales cambios en el entorno tecnológico y las posibles alteraciones de la información por daño, terrorismo, sabotaje y pérdida los estándares internacionales de manejo de información promulgaron el resguardo de la información como un pilar en la administración de la misma, este pilar encierra una variables que se deben estudiar y tener en cuenta para una óptima administración y es precisamente eso lo que se propone como tema en este trabajo, conocer las variables más importantes que se proponen en los estándares internacionales de las políticas de copias de respaldo de información, y como se aplican en dos empresas diferentes con sistemas gestores de bases de datos y de cómo ORACLE se ajusta más a este protocolo y ha desarrollado herramientas que permiten optimizar los procesos y ajustarlos al estándar internacional de seguridad en copias de respaldo.

Los protocolos de gestión de recursos y administración de respaldos de seguridad son un tema muy importante en las empresas que manejan gran cantidad de datos y que se deben manejar por medio de protocolos definidos que se han estandarizado gracias a los sistemas de acreditación, estos tienen unos aspectos ligados a los protocolos y los analizaremos en este escrito.

INFRAESTRUCTURA BASE

Actualmente la información es el activo más valioso de una compañía y del manejo de la información depende que la compañía perdure en el tiempo, no obstante la información está ligada a una buena infraestructura que permita un óptimo manejo de la misma por consiguiente entre más grande la empresa más información maneja lo que obliga a pensar en el resguardo de la información en caso de siniestros accidentes o fallas.

Ninguna empresa está exenta de situaciones en las que se pueda ver afectada la información por lo cual se debe pensar y actuar con eficiencia en el momento exacto, y se deben implementar acciones que permitan mantener la integridad y disponibilidad de la información en todo momento, para esto se han diseñado infraestructuras que permiten la alta disponibilidad del servicio de información en la compañías pero esto no asegura en la totalidad el resguardo de la información, aun la más sofisticadas infraestructuras que incorporan múltiples servidores, firewalls para evitar las intrusiones y/o ataques, un avanzado sistema antivirus o un cuerpo de ingenieros especializados no pueden asegurar en el 100% la protección y alta disponibilidad de la información en todo momento, para asegurar el 100% se debe tomar y ejecutar medidas de control sobre la información para mantener un respaldo a estas medidas se les llama Backup.

Los Backup de información son una copia exacta de la información al momento de su ejecución. Teniendo en cuenta que cuando hablamos de Backup de la información no solo referimos a los archivos almacenados en un servidor también a una base de datos (BASE DE DATOS) en la que se compila, guarda y procesa información de una empresa y de todas sus áreas de gestión y producción para su

procesamiento y entrega de resultados esta BASE DE DATOS es lo que realmente impacta en una empresa en cuanto a información.

La infraestructura que mantiene esta información debe estar administrada por Personal con conocimiento y experticia en la administración de los recursos y dispositivos por medio de los cuales se acceda a la información, este debe trabajar en compañía con el DBA (DATA BASE ADMINISTRATOR) quien es el responsable de la administración y resguardo de la información (DATA BASE), es el DBA quien debe asegurar que la información este siempre lista para su uso, que su almacenamiento debe tener integridad y fiabilidad en sus datos para esto el DBA usa métodos que permiten respaldar la información conservando su integridad y total recuperación ante una eventual falla o pérdida.

Las eventualidades más significativas que pueden generar riesgo de pérdida de datos a los que se ven inmersos los sistemas de información están representadas por Terrorismo y/o Sabotaje, Terremotos, inundaciones, agentes atmosféricos y fallas eléctricas. Estas eventualidades pueden afectar cualquier sistema de información y ORACLE no está exento.

En su infraestructura ORACLE ha implementado herramientas de recuperación y Backup que minimizan las consecuencias de una falla como RMAN (RECOVERY MANAGER) usando una infraestructura sólida y funcional usando el ARCHIVELOG MODE combinado con el FAST RECOVERY AREA (FRA), pero sin unas buenas prácticas de administración de datos no se puede asegurar al 100% el respaldo de la información, el hecho de que la base de datos este en modo ARCHIVE facilita el uso de la herramienta de administración de Backup (RMAN) que es la que permite realizar respaldos y restaurar los Backup, Por medio de ARCHIVE MODE y RMAN ORACLE proporciona al DBA una herramienta muy práctica para realizar los Backup de manera programada y eficaz ya que se hacen por tareas programadas en horas específicas para no afectar el performance de la DATABASE ni la operatividad de la compañía, aunque también se pueden realizar los Backup de manera manual sin RMAN pero esto implicaría sacar la DATABASE de funcionamiento o ponerla en modo offline para realizarlo.

TIPOS DE BACKUP

Lo anterior no define las opciones de Backup que se pueden aplicar inicialmente, ahora el Backup Online (Por Medio del ARCHIVELOG MODE) tiene varios modos de uso para las compañías, con ORACLE se tiene a disposición los Backup de tipo completo y de tipo incremental y/o diferencial, el FULL BACKUP o completo realiza un respaldo total de la DATABASE incluyendo los archivos de parámetros PFILE y SPFILE su tiempo de ejecución es el más alto y el performance de la BASE DE DATOS se afecta considerablemente durante el proceso.

El Backup incremental realiza respaldo de los datos desde el ultimo BACKUP independiente de si el último fue un Backup Completo, diferencial o incremental para ello usa los SCN, este tipo de Backup reduce los archivos a copiar así como el tiempo de ejecución del mismo.

El Backup diferencial realiza el respaldo de los datos modificados desde el ultimo FULL BACKUP (este es un prerequisite), y aunque su tiempo de ejecución es más largo no tiene un impacto tan alto en el performance del BASE DE DATOS durante su ejecución.

RMAN Backup Types

- A full backup contains all used data file blocks.
- A level 0 incremental backup is equivalent to a full backup that has been marked as level 0.
- A cumulative level 1 incremental backup contains only blocks modified since the last level 0 incremental backup.
- A differential level 1 incremental backup contains only blocks modified since the last incremental backup.

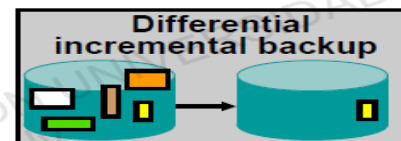
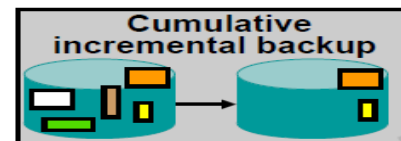
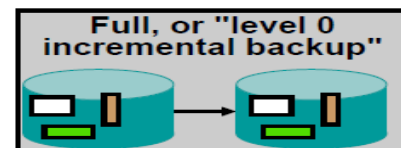


Imagen 1. (Oracle Database 11g: Administration WorkShop II 5, 2012, p. 8)

Ahora teniendo en cuenta que existen opciones para la realización de los Backup entra a trabajar la operación de donde se almacenan los Backup, si bien inicialmente al realizar los Backup estos quedan alojados en el FRA no se pueden dejar en esa ubicación de manera indefinida puesto que tarde o temprano esta área de almacenamiento se llenaría. Para minimizar este impacto en el almacenamiento se usa la extracción de los Backup a medios de almacenamiento externos (DISCOS o CINTAS), esta acción debe ir sujeta a un sistema de traslado a bóveda de cintas o discos dentro y fuera de la compañía para asegurar el buen almacenamiento e integridad de los datos respaldados en estos medios.

ALMACENAMIENTO Y RETENCIONES DE BACKUP

Asegurando un sistema de extracción de respaldos optimo no se puede dar por concluido el tema de los Backup aún hay temas por tratar como el tiempo de retención de los respaldos que aunque estén en CINTAS o DISCOS externos hay que mantener una copia disponible para una recuperación o restauración rápida en caso de algún incidente que obligue a devolver la base de datos a un punto anterior en el tiempo.

Lo anterior nos describe las opciones de almacenamiento de nuestros BACKUP aunque también entra en este tema que las POLITICAS de RETENCION son una particular manera de optimizar los procesos de RECOVERY en caso de una falla o incidente que nos obligue a realizar esta operación, si bien para asegurar la viabilidad y accesibilidad de los datos ante este tipo de eventualidades no es solo realizar el BACKUP y guardarlo en un medio confiable si no también poder acceder a estos datos de manera rápida y eficaz.

La función de las políticas de retención es precisamente facilitar al DBA el rápido acceso a los Backup para realizar las operaciones de Recovery en el menor tiempo posible para minimizar el impacto del mismo a las operaciones de producción de la empresa o compañía

Para poder realizar una retención de respaldos efectiva se deben tener en cuenta ciertas condiciones de la infraestructura como el espacio disponible en discos en este caso en el FAST RECOVERY AREA y el tamaño en disco que ocupa cada copia de respaldo para poder hacer el cálculo de cuantas copias se pueden mantener en dicha área si afectar las tareas propias de los Backup ya programados.

Otra herramienta de ORACLE que suele usarse como media en este aspecto del almacenamiento de respaldos y consumo de recursos de almacenamiento es el sistema de compresión de los Backup Set, desde la herramienta de RMAN (Recovery Manager) se presenta la opción para el nivel de compresión de los archivos de respaldo, aunque está condicionado a la Base de datos, configuración de red (Conexiones), recursos del Sistema y al tipo de sistemas de cómputo y sus capacidades. Aunque hay que tener en cuenta que realizar un Backup con compresión implica mayor uso de recursos de maquina en el proceso y mayor tiempo de ejecución.

Por eso ORACLE hace la siguiente recomendación en el caso del uso de compresión en los procesos de Backup *“Tenga en cuenta, sin embargo, que la operación de compresión y descompresión requiere recursos de la CPU, por lo tanto la creación y restauración de una copia de seguridad comprimida, por supuesto, probablemente tomará más tiempo y requieren más recursos del sistema; Al elegir un algoritmo, considere su espacio en Disco, además de los recursos dinámicos del sistema como la CPU y la Memoria”* (Oracle Database 11g: Administration WorkShop II 5, 2012, pág. 17)

Los niveles de compresión que se pueden usar por medio de RMAN son:

Using RMAN Backup Compression

Compression Ratio or Level	Considerations	Requires Advanced Compression Option
LOW	Fastest. Best suited to address backup: CPU resources	✓
MEDIUM	Fast. Good balance of CPU usage and compression ratio	✓
HIGH	Best compression ratio at the expense of high CPU consumption. Best suited to address backup constraint: network.	✓
BASIC	Fair. Compression ratio similar to MEDIUM at expense of additional CPU usage. Compression ratio between MEDIUM and HIGH	

Ilustración 2. (Oracle Database 11g: Administration WorkShop II 5, 2012, pág. 18)

SEGURIDAD GENERAL Y EN BACKUP

Otro punto importante al momento de realizar un Backup es la seguridad para lo cual ORACLE implementó el encriptamiento del Backup set, con tres opciones Encriptación transparente (default), encriptación con Password, y el Dual Mode Encryption que usa las dos opciones primarias y permite restaurar en modo transparente (default) o en modo con contraseña.

TIEMPOS DE EJECUCION DE BACKUP

Los tiempos de Backup están ligados al tipo de Backup y al tamaño de la BASE DE DATOS, es decir entre más grande la BASE DE DATOS más tiempo de ejecución

tomara la realización del Backup los Backup completos o FULL BACKUP son los que más demoran en su ejecución por lo cual se recomienda ejecutarlos en las horas en las que se procesen menos transacciones del sistema las horas más recomendadas son entre las 10 pm y las 5 am de los días sábados o domingos y según sea la actividad de la empresa por ejemplo en un banco lo más óptimo sería en un día no hábil en este horario mencionado pero si es una clínica cuya función es atención de pacientes 24 horas lo más recomendable sería el día miércoles entre las 10 pm y las 5 am puesto que los mayores días de flujo de pacientes están entre los días Jueves a martes incluyendo fines de semana que se tiene mayor afluencia de público con necesidad de atención.

Para los Backup diferencial o incremental se podría ejecutar en pleno procesó operativo de la empresa ya que tienen menor impacto en la funcionalidad del sistema y no afectarían el desarrollo de las actividades de producción aunque se recomienda ejecutarlos en los mismos horarios de los FULL BACKUP para minimizar el impacto lo más posible.

Otra variable de tiempos de ejecución adicional a la realización de Backup son los tiempos de restauración o recuperación de la BASE DE DATOS este tipo de operación tiene variables en su tiempo de ejecución, entran a afectar el o los tipos de Backup que se requiere usar para la operación, así como su ubicación de almacenamiento, si el Backup requerido está en cinta o en disco externo aumenta el tiempo a emplear mientras se copia del almacenamiento externo al FRA mas el tiempo mismo de la aplicación del recovery este tiempo de aplicación está ligado al tamaño de la BASE DE DATOS y a la cantidad de piezas de BACKUP a utilizar.

Lo anterior está sujeto al uso de los Backup online usando la opción del ARCHIVELOG MODE de ORACLE y que se tenga la BASE DE DATOS con tareas de realización de Backup programados ya sea completos o completos más diferenciales o incrementales.

Si la DB no tiene esta opción configurada el Backup se hace de manera OFFLINE o COLD BACKUP aunque se realice el recovery con el ultimo BACKUP si estaría sujeto a la perdida de información y de tiempo ya que se usaría una gran cantidad

de tiempo realizando el RECOVERY la DB no quedaría actualizada a la fecha del incidente si no a la fecha del ultimo COLD BACKUP lo que representa un gran riesgo de pérdida de información.

Otra herramienta que ORACLE incluye en su plataforma de administración de respaldos es el paralelismo que permite fraccionar el Backup Set en partes para transmitirlo a su destino de almacenaje por diferentes canales esto con el fin de consumir menos tiempo en la ejecución de las operaciones y mejorando el rendimiento del proceso en sí. Otras opciones que incluye ORACLE es que por medio de ejecución de comandos se pueden duplicar los Backup y enviarlos a diferentes ubicaciones de almacenamiento en una misma ejecución de un Backup proporcionando al DBA más opciones de administración de respaldos y optimización de los proceso de Backup.

PRUEBA DE COPIAS DE RESPALDO

Pruebas de respaldo es el proceso de tomar de manera aleatoria un Backup y restaurarlo en un ambiente de iguales características al de producción para verificar que los Backup generados en el proceso de respaldos de información estén bien hechos y que en caso de ser necesario desde estos se pueda restaurar y/o recuperar la información en su totalidad conservando su integridad y confiabilidad.

CRECIMIENTO DE LAS BASES DE DATOS

Estas herramientas que ORACLE le proporciona la DBA es lo que le permite tomar las decisiones a futuro para la administración de los respaldos de la información en el transcurso del tiempo para enfrentar las diferentes situaciones que se puedan presentar ya sean eventualidades que obliguen a realizar un RECOVERY o un RESTORE de la BASE DE DATOS aunque estas no son las únicas cosas que el DBA debe tener presentes para la gestión de la información, existe también el detalle del crecimiento exponencial al que se ven enfrentados los DBA, las BASE DE DATOS están continuamente en expansión y crecimiento todos los días debido a el ingreso constante de datos que alimentan la DB.

El crecimiento de la BASE DE DATOS es una problemática que para algunas empresas es un tema delicado ya que no solo hace más lenta la gestión de consulta sino que también afecta el proceso de respaldos ya que aumenta el tiempo del proceso y en ocasiones obliga a realizar inversiones adicionales en el futuro en infraestructura para el óptimo manejo de los datos así como más recursos para la gestión de los respaldos, ya que estos consumen más en cada proceso.

Aunque Oracle permite manejar sus áreas de almacenamiento de una manera eficaz si desde la implementación de la infraestructura no se realizan los cálculos de crecimiento de la DB al cabo del tiempo se pueden ver enfrentados a condiciones de difícil manejo para la realización de los respaldos generando gastos e inversiones que poder sobrepasar los presupuestos estimados de las empresas.

IMPLEMENTACION DE PROTOCOLOS DE COPIAS DE RESPALDO

Ya hemos abordado temáticas básicas de la teoría general de Backup que aplican en forma general a todos los sistemas de administración de bases de datos y denotado algunos puntos a favor que ORACLE proporciona en estas temáticas que se convierten en variables que hacen sobresalir a ORACLE como el más robusto y completo sistema gestor de bases de datos aunque no hemos ahondado ni profundizado en todas las herramientas de gestión que para el tema de Backup posee ORACLE vamos a mencionar con particularidad algunas que se aplican más en el proceso de políticas de Backup. La configuración de los Backup, que tipo de Backup se debe realizar con que periodicidad y como revisar si el respaldo que se realizado quedo correcto para tener la veracidad de que los respaldos pueden ser utilizados cuando se necesite recuperar o restaurar la base de datos.

Aunque estos temas se deben dejar registrados en los documentos de la administración, gestión de calidad, y seguridad informática de las empresas, presentaremos las políticas de Backup de 2 empresas una con un motor de base de datos en Oracle y otra con el motor de bases de datos en Microsoft SQLSEVER

para diferenciar las variables que hemos mencionado anteriormente en sus modelos de gestión de respaldos.

La empresa con Microsoft SQLSERVER es la CLINICA DEL OCCIDENTE de donde se adquirieron conocimientos de la administración de Backup e infraestructura por aproximadamente 5 años y la empresa que cuenta con ORACLE es el BANCO DE LA REPUBLICA donde se realizó un proyecto de actualización de software y se adquirieron datos de la infraestructura y procesos de tema que tratamos en este trabajo.

En principio se realizara la descripción del proceso de políticas de respaldo que se aplica en cada empresa para realizar un proceso comparativo entre ORACLE y Microsoft SQLSERVER para concluir con un análisis objetivo de prácticas de Backup.

IMPLEMENTACION EN LA CLINICA DEL OCCIDENTE

La Infraestructura Usada en la Clínica del Occidente se compone de servidor de Base de datos, servidor de Aplicaciones, infraestructura de redes y comunicaciones Hibrida entre fibra óptica y cobre, los servidores IBM X8350 con sistema Base VMWare esxi 5.0 para la virtualización de los servidores, enlazados a una NAS IBM DS3000 de 12 HDD de 6 HDD SAS y 6 HDD SATA para el almacenamiento de las máquinas y los repositorios de las Bases de Datos. Sistema operativo de los servidores Microsoft Windows Server 2008, motor de Base de Datos Microsoft SQLSERVER 2008.

Se maneja una Base de datos para el sistema de DGH (Dinámica Gerencial Hospitalaria) que se implementó en el año 2012 con la versión de DGH 3.5 y a la cual se le calculo un crecimiento de 2,5GB Mensuales, Para el manejo de los respaldos se optó por un Backup Full que se realiza de manera automática todos los días a las 2 AM, programación realizada desde la herramienta de SQL management.

Estos Backup se almacenaban inicialmente en el HDD secundario del servidor de Bases de Datos con una capacidad de 1 TB destinado para una retención de 15

días de Backup. Este Disco de almacenamientos estaba Ubicado en la NAS y era una porción de espacio de las unidades lógicas configuradas y destinadas para dicha función.

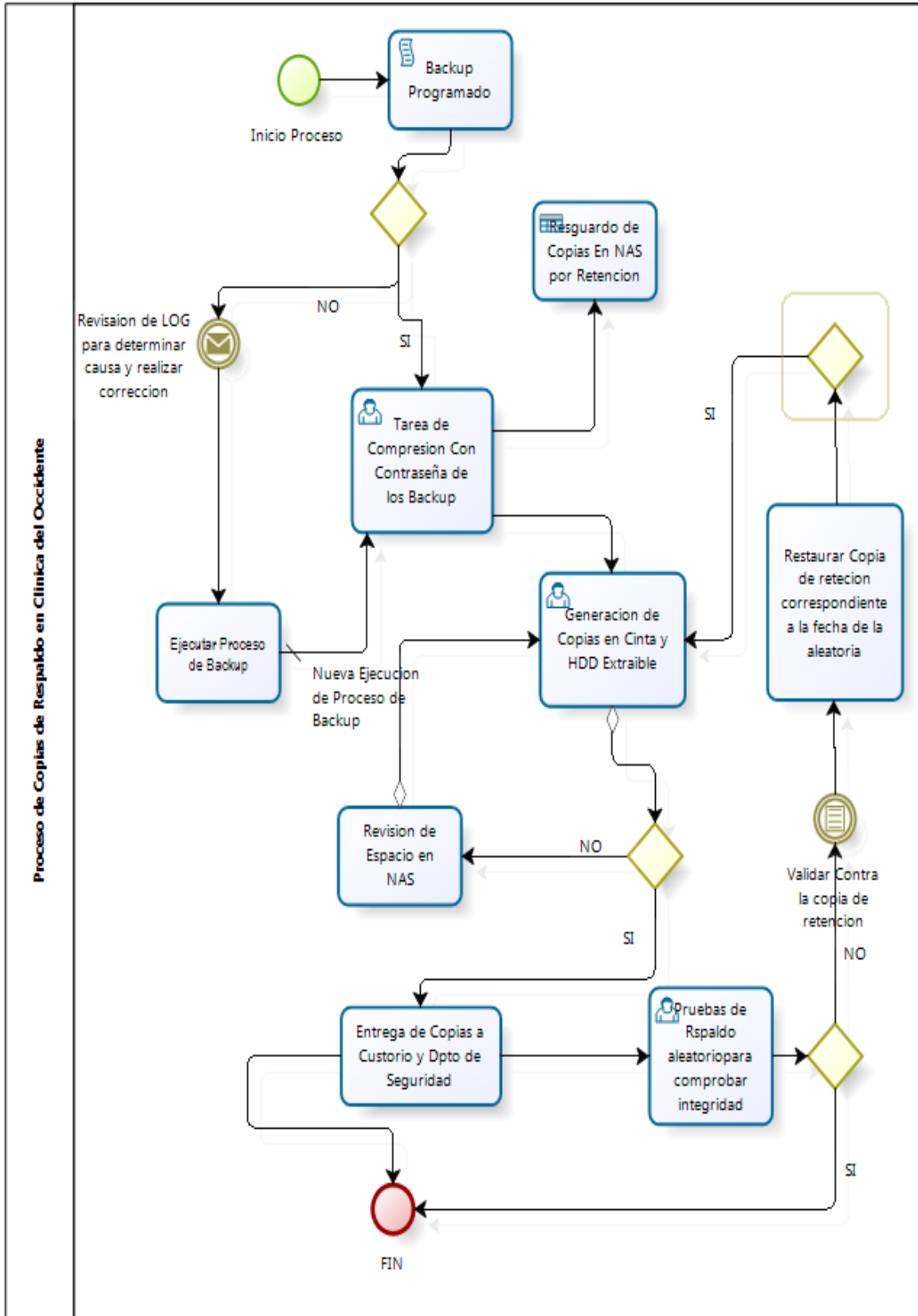
Para la seguridad de la información se optó por un dispositivo Físico que regulaba el acceso a internet (Fortinet) y creación de VPN para las distintas áreas de servicio de la entidad, las VPN permitían el acceso y comunicación a la Base de Datos, para el acceso directo a los ficheros del servidor se establecieron políticas desde el Active Directory del servidor DNS principal. Esto asociado a una plataforma de antivirus que proporcionaba control en los equipos de cómputo para el bloqueo de medios extraíbles (Unidades Ópticas y de Conexión USB) esto en términos de seguridad general, para la seguridad de los respaldos después de realizado el Backup se procedía de manera manual a la compresión con contraseña de los ficheros generados durante el proceso usando software licenciado de WINZIP, terminado el proceso de compresión con contraseña se procedía a trasladar los archivos de manera manual a un TAPE para su grabado en Cintas de seguridad para ser entregados al custodio externo (ALPOPULAR), estas cintas se generaban 1 vez a la semana con los Backup de 7 días de contenido, se generaba una segunda copia en un HDD Externo con el Backup del ultimo día que quedaba en custodia del departamento de seguridad de la clínica en caja fuerte.

El tiempo de Backup es una variable de cuidado aunque estaba programado para realizarse de manera automática y diaria esta inicialmente era un proceso rápido que no generaba impacto en las actividades de las áreas de servicio de la clínica de que obviamente funcionan durante las 24 horas del día, los procesos estaba programados para ejecutarse a las 2 Am a inicios del 2012 cuando se realizó la implementación del sistema el Backup consumía aproximadamente de 15 a 20 minutos para finales inicios del 2016 el proceso duraba aproximadamente 5 horas motivo por el cual se debió modificar la programación del Backup para que iniciara una hora antes de lo inicialmente programado.

Otro punto afectado en tiempos fue el proceso de restauración de la base de datos en las pruebas de respaldos inicialmente estas restauraciones de Backup aleatorios

tomaba un promedio de 1 hora a inicios del 2012 para principios del 2016 demoraban un promedio de 10 horas, estas pruebas se hacían en un servidor de pruebas de más mismas características del de producción pero como era una máquina virtual que también estaba alojada en la misma NAS generaban impacto en los procesos de producción por el consumo de recursos de I/O en la NAS, para mitigar este problema se optó por usar un tercer servidor sin virtualizar pero con características similares al principal y sin conexión a la NAS para realizar las pruebas de respaldos.

EL tema del crecimiento de la Base de datos se convirtió en una gestión crítica para finales del 2015 puesto que se abrieron nuevos servicios en la entidad durante el 2013 hasta el 2015 generando que el cálculo inicial del crecimiento de la base de datos dejara de ser fiable, si calculo un crecimiento de 2.5 GB mensuales pero con la puesta en funcionamiento de nuevos servicios la base de datos estaba creciendo a un rango de casi 6GB mensuales, este crecimiento afectó muchos procesos el que recibió el mayor impacto fue el de almacenamiento y retención de Backup, ya que para el 2016 la base de datos pesaba casi 380 GB para lo cual el espacio destinado para su almacenamiento solo permitía conservar 1 día y obligó a modificar también la entrega de cintas de seguridad al custodio de 1 semanal a 3 semanales generando sobre costos en procesos, esto conllevó a tomar medidas de contingencia como el cambio de la NAS y modificaciones al contrato con el custodio de las Cintas. (Ver Diagrama 1).



IMPLEMENTACION EN EL BANCO DE LA REPUBLICA

En la segunda empresa a describir BANCO DE LA REPUBLICA su infraestructura se compone de múltiples servidores de 2 servidores de interfaz que realizan la conexión al servidor de la base de datos que como se mencionó antes es ORACLE 11g uno se encuentra en el edificio principal y el otro en el centro de servicios alterno, interconectados con un balanceador de cargas para nivelar procesos de conexión y transacciones, sus servidores están en UNIX para la base de Datos de ORACLE 11g y los servidores de interfaz están en Windows Server 2008, el servidor de base de datos tiene adición de una NAS de 24 HDD híbrida entre SSD, SAS, no se encuentra virtualizado en ningún aspecto.

Su Base de datos está en ORACLE 11g y se dispuso de un protocolo para los Backup determinado así Diariamente a las 3 am se realiza un Backup Full, entre las 12 y las 2 pm se genera de manera manual un Backup Diferencial de nivel 1 al terminar las tareas de cierre de los procesos de los portafolios internacionales, y al terminar las tareas de los portafolios internos al final de la tarde se genera de manera manual un segundo Backup diferencial de nivel 1, estos procesos de Backup se repiten todos los días de Lunes a Viernes, para los días sábados se realiza Un Backup de Nivel 0 para cerrar el ciclo de Backup programados. Estos Backup son almacenados en la NAS que es la que tiene la estructura de configuración de ASM, y en esta está el FAST RECOVERY AREA FRA que recomienda ORACLE, se tiene asignado para retenciones de los Backup de 7 días completos, al cumplirse esta cláusula los Backup se trasladan a 2 copias en Cinta de Seguridad y 1 en HDD.

Para la seguridad de las copias se dispuso del siguiente protocolo externos los HDD se quedan en la caja de seguridad del área de Tecnología, 1 primera copia en Cinta es trasladada al centro de servicios alterno para su resguardo el cajas de seguridad y la segunda copia en cintas es entregada a un custodio externo, otros puntos de seguridad están asociados en gran parte a la infraestructura con 2 firewall Físicos y uno por software, los físicos controlan las salidas y entradas y flujo de navegaciones y accesos remotos, políticas de Active Directory para control de acceso a unidades

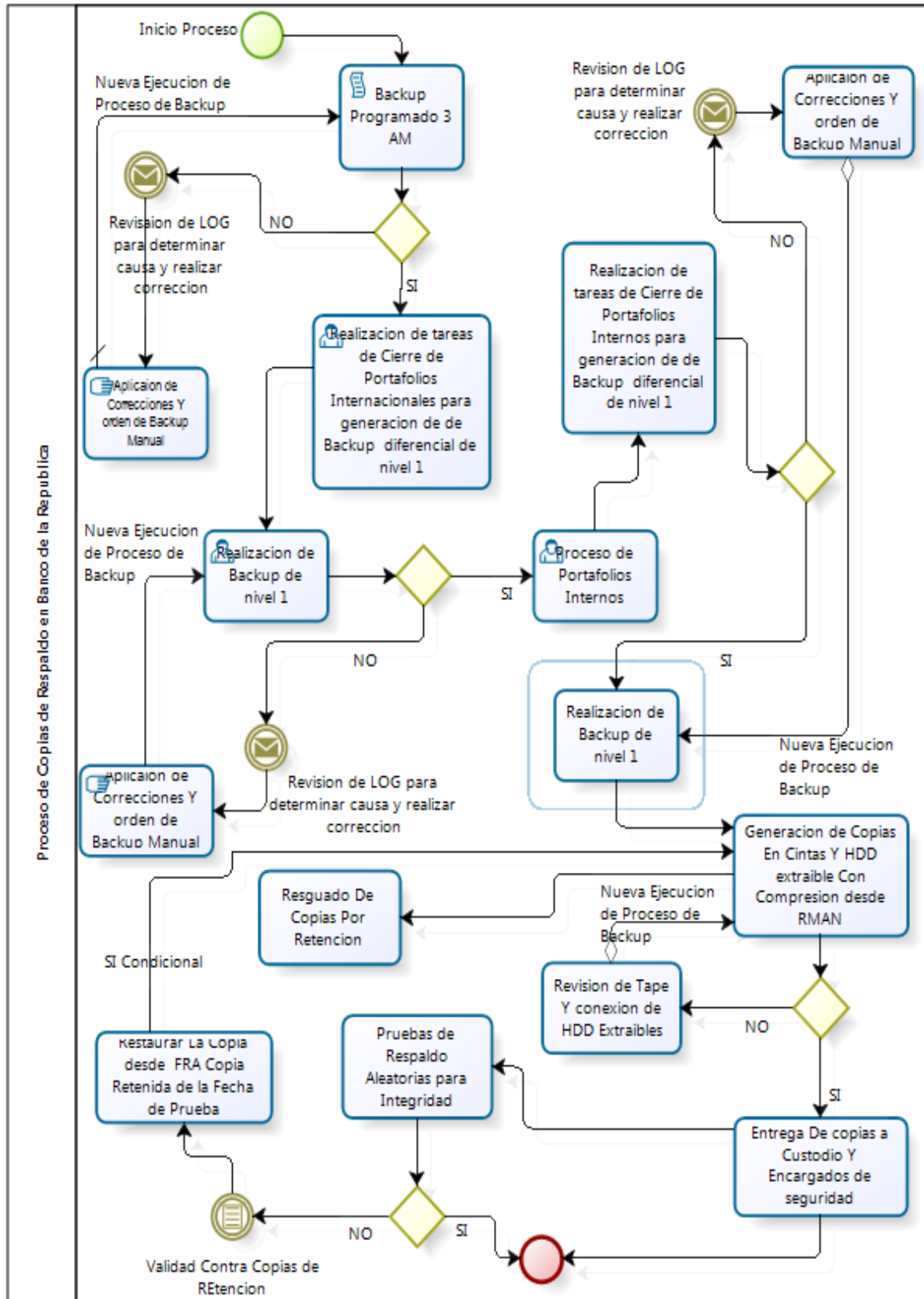
de red, y consola de antivirus MCAFFE para control de medios extraíbles (unidades ópticas y medios UBS)

Los tiempos de ejecución de los Backup son de aproximadamente 3 hora en el FULL Backup mientras los diferenciales tardan un aproximado de 15 a 30 minutos según la cantidad de transacciones que se registren en el sistema antes del cierre de procesos tanto externos como internos.

Para las pruebas de respaldó se implementó una estructura igual a la de producción con equipos con las mismas características lo que permite realizar los procesos de restauración de copias aleatorias sin que estos procesos afecten los de producción para este tipo de pruebas se realiza de dos maneras primero se realiza la restauración de una copia aleatoria aplicando todos los Backup set del día seleccionado, luego se valida que la información de ese día este completa y con integridad, luego se restaura nuevamente con la copia del ultimo Backup realizado estableciendo que el ambiente de pruebas este actualizado a la fecha de producción o con un máximo de 1 día de diferencia.

En cuanto al crecimiento de la base de datos del banco el DBA realizo cálculos donde determino que la base de datos crece en un promedio de 250 MB diarios y para evitar que a futuro se generaran dificultades o problemas con las políticas del almacenamiento y retención que se estimara el crecimiento de la base a un promedio de 1 GB mensual y se calculara el espacio para el tamaño de la base de datos aproximado al cabo de 5 años que es según el protocolo de tecnología cuando se deben actualizar todos los activos y el parque tecnológico del Banco.

(Ver Diagrama 2)



Todo lo anterior nos describe los protocolos estándar de políticas de copias de respaldó y como se han aplicado en 2 empresas diferentes, con sistemas de gestión de bases de datos diferentes que nos permite denotar ciertas diferencias y ventajas que ORACLE tiene respecto a otros sistemas, aunque en el banco no están virtualizados los sistemas tienen muy diferenciada su infraestructura de conexiones y accesos a la base de datos con 2 servidores de interfaz y uno con el motor de la base de datos, el de la clínica no lo tiene puesto que SQLSERVER no contempla servidores o nodos de conexión para el acceso a la base de datos, una de las diferencias más notables es en la gestión de Backup Oracle permite hacer Backup de niveles 0 y 1 que optimizan la gestión mientras que SQLSEVER solo tiene la Opción de Backup Full que en ocasiones no es óptimo más aun cuando la base de datos es muy grande generando impacto a los procesos productivos.

CONCLUSIONES

Teniendo en consideración que las dos empresas por medio de las cuales realizamos los análisis de la implementación de los protocolos de copias de respaldo de la información alcanzaron la acreditación por que han logrado llevar a cabo dicha implementación y cumplen con los requerimientos técnicos y documentales podemos concluir lo siguiente:

- En la Clínica se ha seguido los lineamientos de los protocolos pero aun así se presentan incidencias sobre los procesos de producción que han obligado a aplicar contramedidas con sobrecostos para la empresa demostrando que aún se pueden optimizar más los procesos, pero que su infraestructura y su gestor de bases de datos no tienen herramientas para alcanzar la optimización que se requiere.
- El Banco también ha seguido los lineamientos de los protocolos y ha minimizando el impacto en los proceso productivos dando uso de las herramientas que ORACLE ha desarrollado para optimizar estos procesos en cuanto a copias de respaldo de seguridad de la información.
- Concluimos también que ORACLE proporciona más herramientas para el control de procesos en copias de respaldo, pero a su vez estas herramientas tienen un costo adicional sobre el sistema de gestión de bases de Datos lo que los hace poco viable para las empresas que no tienen altos recursos económicos para la adquisición de estas.
- Por otro lado algunas empresas tampoco implementan ORACLE por el alto costo en su licenciamiento e implementación y el tema económico en un punto de que define en muchos casos en la decisión final a la hora de escoger el sistema gesto de bases de datos.

BIBLIOGRAFIA

Oracle Database 12c: Taller de Copia de Seguridad y Recuperación ed 2 (2013) [En línea] disponible en http://education.oracle.com/pls/web_prod-plq-dad/web_prod.view_pdf?c_id=D78850CS20&c_org_id=51&c_lang=US

Donna Cooksey, Gerente S nior de Productos de Oracle. Oracle Secure Backup: Optimizado para los Entornos de Oracle (Abril de 2006) Disponible en: <http://www.oracle.com/technetwork/es/documentation/317485-esa.pdf>

Oliver Heurtel. (2009) Oracle Administraci n, Espa a Ediciones ENI, colecci n Recursos inform ticos disponible en: <https://books.google.es/books?hl=es&lr=&id=y0cwa9hWGlwC&oi=fnd&pg=PT114&dq=copias+de+respaldo+ORacle&ots=XUFIN8tJzX&sig=1ibxAKFUKJPFb7Xjdrab8qDrTcg#v=onepage&q=copias%20de%20respaldo%20ORacle&f=false>

Ingrid Evelyn Cevallos Cevallos. (2014) An lisis comparativo de respaldo y recuperaci n de base de datos licenciada (Oracle Usando RMAN) Vs Open Source (MYSQL utilizando MYSQL Administrador) Tesis de Grado Ingeniero en sistemas Computacionales, Universidad De Guayaquil, Ecuador.

Esther Yacqueline Palma Urrutia, (2015) Implementaci n de un esquema de respaldo y recuperaci n de las bases de datos de una empresa comercial, Examen de grado Complexivo, Magister en Sistemas de Informaci n Gerencial, Escuela Superior Polit cnica del Litoral, Ecuador, disponible en: <http://www.dspace.espol.edu.ec/bitstream/123456789/36484/1/D-84980.pdf>

Oracle E-kit diplomado ORACLE Workshop 2 lesson 4 Configuring Backup Settings (2012) Oracle University

Oracle E-kit diplomado ORACLE Workshop 2 lesson 5 Creating Backups with RMAN (2012) Oracle University

Oracle E-kit diplomado ORACLE Workshop 2 lesson 6 Restore and Recovery Task (2012) Oracle University

Manual de Procedimientos y Protocolos del est ndar de sistemas (2014) Cl nica de occidente, Documentos de Acreditaci n de Alta Calidad

Documento Interno  rea de Tecnolog a (2012) Banco de la Republica, Soporte de documentaci n de Acreditaci n ISO 9000.