ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"APLICAR LOS PRINCIPIOS DE LA SEGURIDAD DE INFORMACIÓN A LA BASE DE DATOS ACADÉMICA DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR CON MOTOR DB2 EN AMBIENTE DE PRODUCCIÓN"

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

MARCO GENARO CALLE JARAMILLO

GUAYAQUIL-ECUADOR

AÑO: 2015

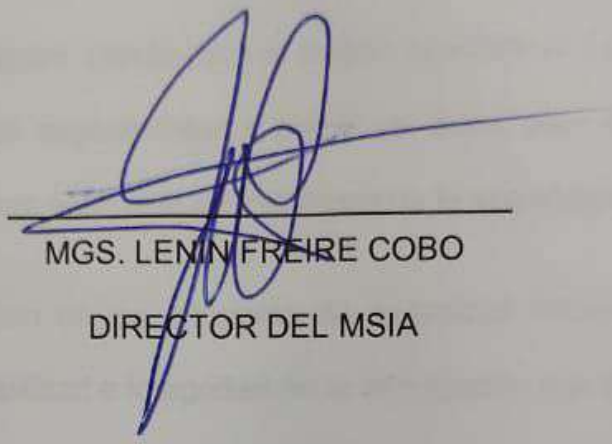
AGRADECIMIENTO

A Dios por las bendiciones que derrama sobre mí. A mis padres que han dado todo por mi superación profesional. A mi abuela por la formación de valores éticos y morales. A mis hermanos por el cariño incondicional. A mi esposa por todo el amor que me da, por estar a mi lado en todo momento y alentarme a seguir adelante en mis estudios.

DEDICATORIA

A Dios por poner en mi camino a todas las personas que me apoyaron moral, económicamente y con aportes de conocimiento para la culminación de este trabajo, sobre todo a mi esposa que incondicionalmente estuvo siempre a mi lado para apoyarme en las largas noches del desarrollo.

TRIBUNAL DE SUSTENTACIÓN



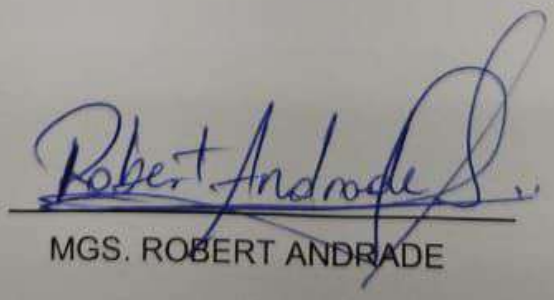
MGS. LENIN FREIRE COBO

DIRECTOR DEL MSIA

MGS. NÉSTOR ARREAGA

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA



MGS. ROBERT ANDRADE

PROFESOR DELEGADO

POR LA UNIDAD ACADÉMICA

RESUMEN

El presente trabajo pretende identificar y resolver problemas que se dan en una base de datos en producción, usada para el ámbito académico. Los problemas que la base de datos puede experimentar y como un buen plan de trabajo puede solucionar estos problemas aplicando los principios de la seguridad informática.

Se realizará la verificación de los principios de seguridad informática que son la confidencialidad, disponibilidad e integridad de la información con la ejecución de un plan de trabajo, y se pretende observar como el buen manejo de los principios de seguridad lleva a reducir al mínimo el impacto sobre una base de datos en producción y facilita la resolución de problemas.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BD	Base de datos
DBMS	Data Base Management System, sistema de gestor de bases de datos, el software encargado de administrar y producir base de datos
DDL	Lenguaje de definición de datos, el lenguaje que proporcionan las DBMS para definir la base de datos
DELL	Marca de equipos mundial reconocida en el mundo de las tecnologías
IBM	International Business Machines Corp., empresa multinacional de tecnología
ISO	Organización Internacional de Normalización
IXF	Integration Exchange Format, formato de archivo de datos para intercambiar entre arquitecturas diferentes o similares la base de datos debe reconocer este formato.
RAM	Radom Access Memory, la memoria de acceso aleatorio
SO	Sistema operativo
SQL	Structured Query Language, lenguaje de consulta estructurado

ÍNDICE DE FIGURAS

ÍNDICE TABLAS

INTRODUCCIÓN

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización [1].

Se debe tener un control sobre las seguridades de la información en las bases de datos, un control inadecuado puede producir pérdidas importantes o una mala toma de decisiones en el negocio, muchas empresas se rehúsan a invertir mucho en seguridad debido a que no se relaciona de manera directa con los ingresos de ventas. Sin embargo, proteger los sistemas de información es algo tan imprescindible para la operación de la empresa que merece reconsiderarse. [2]

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

La institución de educación superior cuenta con una base de datos relacional DB2 que es utilizada para llevar los registros académicos de la institución, desde 1998 se utiliza el motor de base de datos DB2 que es propiedad de IBM, la licencia con la que se cuenta es “DB2 Enterprise Server Edition” en este momento en su versión 10.5.5, en esta base de datos se tiene el registro de todos los datos personales de los estudiantes y profesores de la institución así mismo el historial académico, cursos, paralelos, y todo lo relacionado con el aspecto académico, es esencial que toda esta información sea confidencial, tenga integridad en sus datos y esté disponible en línea para su consulta ya que

es un sistema web 24/7 y además existen otros sistemas externos que consultan información de la base de datos académica.

Se ha requerido que sea analizada la seguridad de la información con el fin de que se solucione ciertos problemas que se han venido presentando como la duplicidad, veracidad e integridad de los datos ya que se han detectado varios problemas como datos personales ingresados varias veces, datos aberrantes en la fecha de nacimiento, personas que al ser buscadas no se las encuentra por sus nombres y apellidos, profesores que no se les refleja su carga horaria.

Dentro del análisis preliminar se encontró que las bases de datos fueron creadas con el codeset ISO8859-1 codepage 819 territory US, debido a estos parámetros configurados los datos de las tablas distinguen acentos, mayúsculas y minúsculas lo que quiere decir que “Maria” <> “MARIA” <> “María” como se ve en las figuras 1.1, 1.2, 1.3 y 1.4 , lo que llevaba a que cuando se consultaba una información a veces no era presentada si era escrita de manera diferente a como fue ingresada y esto causaba problemas ya que no solo una persona es la que ingresa la información; Existían casos como para los extranjeros que eran buscados con sus números de pasaporte y estos habían sido ingresados con minúsculas en la base por lo cual no se los encontraba en el momento de buscarlos, así también cuando un profesor extranjero había sacado cédula de identidad y era buscado por nombres y apellidos como no los encontraban eran ingresados nuevamente, todos estos problemas generaban también que cuando ellos ingresaban a un sistema no

eran reconocidos por el mismo ya que eran planificados con otros datos que no eran los correctos.

De igual forma se encontró que en algún momento los sistemas creados para la actualización de datos personales estaban enviando a guardar información errónea en las fechas de nacimiento o no enviaban datos, esto fue corregido a nivel de sistemas pero los datos guardados en las bases nunca fueron actualizados, por lo que ahora se encuentran a personas con fecha de nacimiento “1900-01-01” o “0001-01-01” o fechas de nacimiento del año 2001 en adelante.

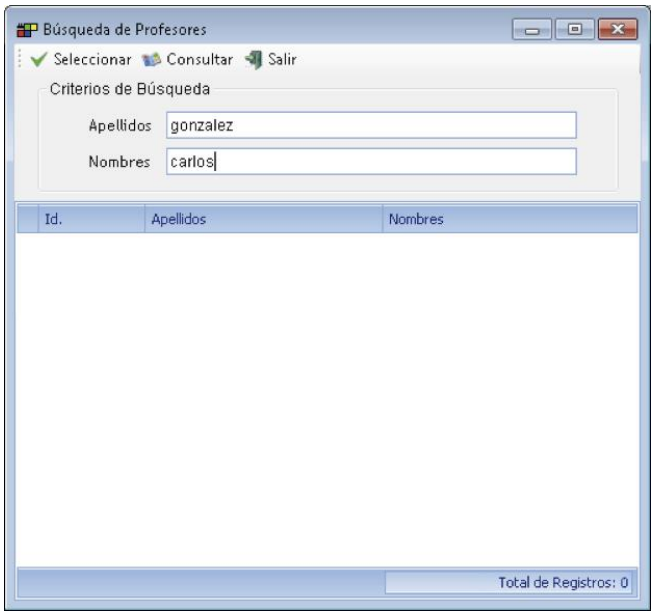


Figura 1.1 Búsqueda de datos del profesor en minúsculas

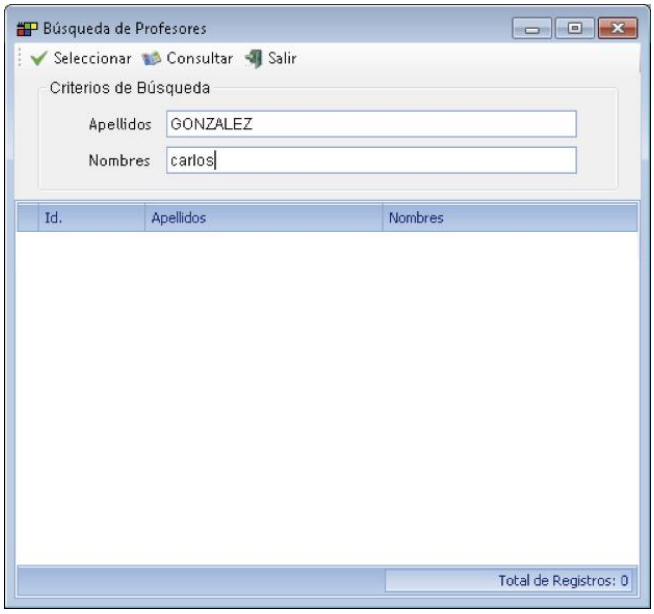


Figura 1.2 Búsqueda de datos del profesor Apellidos en Mayúsculas sin tilde

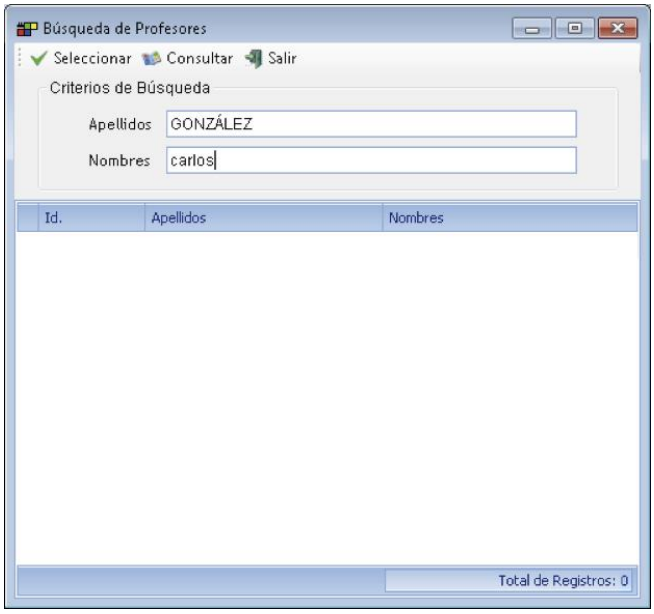


Figura 1.3 Búsqueda de datos del profesor Apellidos bien escritos en mayúsculas, Nombres bien escritos en minúsculas

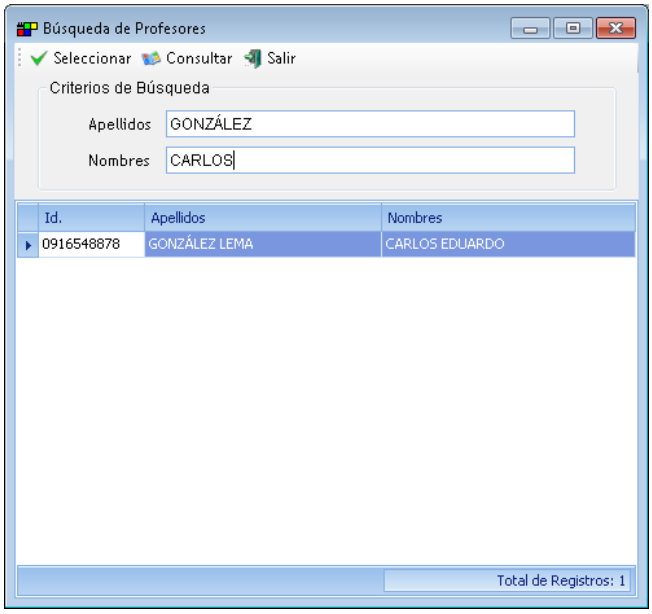


Figura 1.4 Búsqueda de datos del profesor Apellidos bien escritos en mayúsculas, Nombres bien escritos en mayúsculas

1.2 SOLUCIÓN PROPUESTA

Se ha requerido que se realice la solución lo más pronto posible de los problemas mencionados por lo cual se analizaron varias medidas como el cambio a nivel de programación de los sistemas pero esta propuesta fue descartada porque actualmente no se encuentran los desarrolladores disponibles y esto llevaría demasiado tiempo cambiar en todos los sistemas las consultas hacia la base de datos, de esta manera es que se eligió la solución que más se adaptaba y con menos impacto al esquema de negocio de la institución que fue realizar un plan de trabajo para resolver los problemas detectados y verificar que la base de datos cuente con los principios de la seguridad informática; principalmente se debe cambiar el collate en la base de datos, no obstante este parámetro no puede ser cambiado en caliente y

además no es soportado por el codeset iso8859-1 por lo cual se debió crear y diseñar un plan de actualización del codeset de la base de datos por el codeset “UTF-8 codepage 1208 Territory US” y definirle el collate “UCA500R1_LEN_S1”, es importante destacar que esta solución requiere que la base sea eliminada por lo cual se perdería demasiado tiempo del servicio, se requiere disminuir el tiempo que los sistemas se verían afectados por esta actualización, tener demasiado cuidado de mantener la consistencia de la información, mantener un plan de contingencia, mantener y definir el etiquetado de los respaldos antes y después de la actualización.

En cuanto al problema de la veracidad de la información se realizara un reporte con las novedades que existen comparando la información que se encuentra en la base de datos institucional y apoyándose con los servicios web de la institución pública del registro civil para poder actualizar la información en la base de datos académica.

Finalmente con este plan de trabajo bien estructurado y tomando en cuenta todas las observaciones se logrará resolver los problemas antes mencionados y verificar los principios de la seguridad informática en el menor tiempo, con mínimo impacto en la disponibilidad de los servicios de la institución, asegurando la continuidad del negocio y la integridad de la información.

CAPÍTULO 2

METODOLOGÍA DE DESARROLLO DE LA SOLUCIÓN

2.1 ANÁLISIS DEL MODELO DE LA BASE DE DATOS

La institución de educación superior cuenta con una base de datos IBM DB2, la base de datos comenzó como una base de datos enteramente relacional podríamos destacar “el modelo de datos relacional es el modelo de datos más ampliamente usado, y una amplia mayoría de sistemas de bases de datos actuales se basan en el modelo relacional” [3], con el tiempo y las nuevas tecnologías podríamos decir que se ha tenido que ajustar el modelo de bases a un modelo hibrido de bases relacional orientado a objetos y transaccional, en este análisis en particular tendremos en cuenta la base de datos académica de los estudiantes sus datos personales y la información académica.

Es necesario tener identificado y entender el modelo de la base de datos para poder realizar los cambios necesarios para aplicar los principios de la seguridad en la base de datos de la institución.

Tenemos la Figura 2.1 Modelo de datos personales, donde tenemos la información de la persona este modelo cuenta con dos tablas padres tbl_persona y estudiante_acad, tbl_persona guarda la información de todas las personas que tienen relación con la institución (profesor, estudiante), mientras que estudiante_acad tiene la información de solo los estudiantes esto para poder unirlo a los diferentes sistemas que tiene la institución.

Así también se tiene en la figura 2.2 el modelo de datos académicos, donde se guarda la información de toda la actividad académica del estudiante entiéndase esto como la información de cursos que existen quien es el profesor cual es el paralelo el horario, a que materias el estudiante se registró, los periodos académicos, la carreras de los estudiante, las unidades que existen y pueden pertenecer los estudiantes.

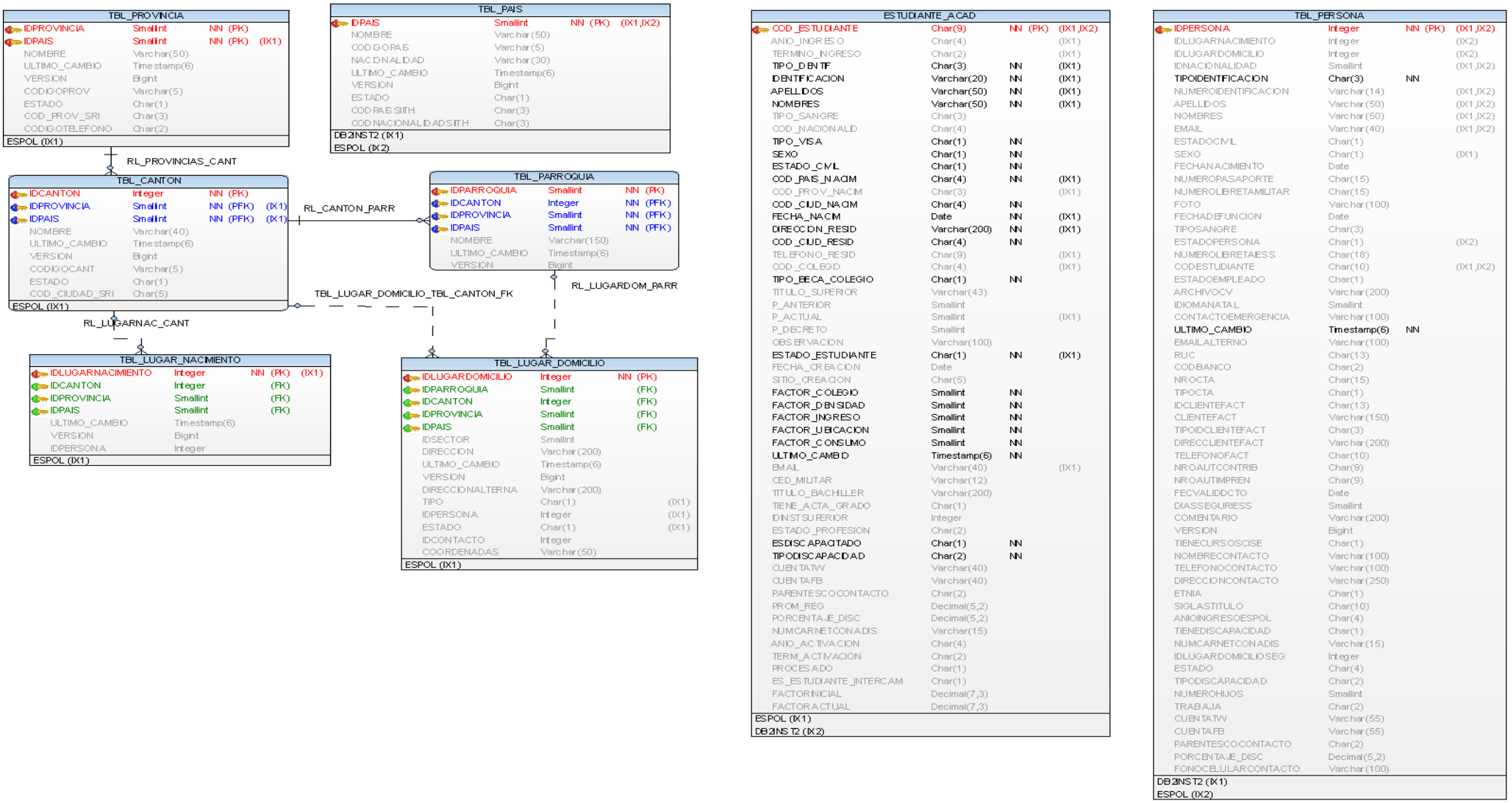


Figura 2.1 Modelo de datos personales

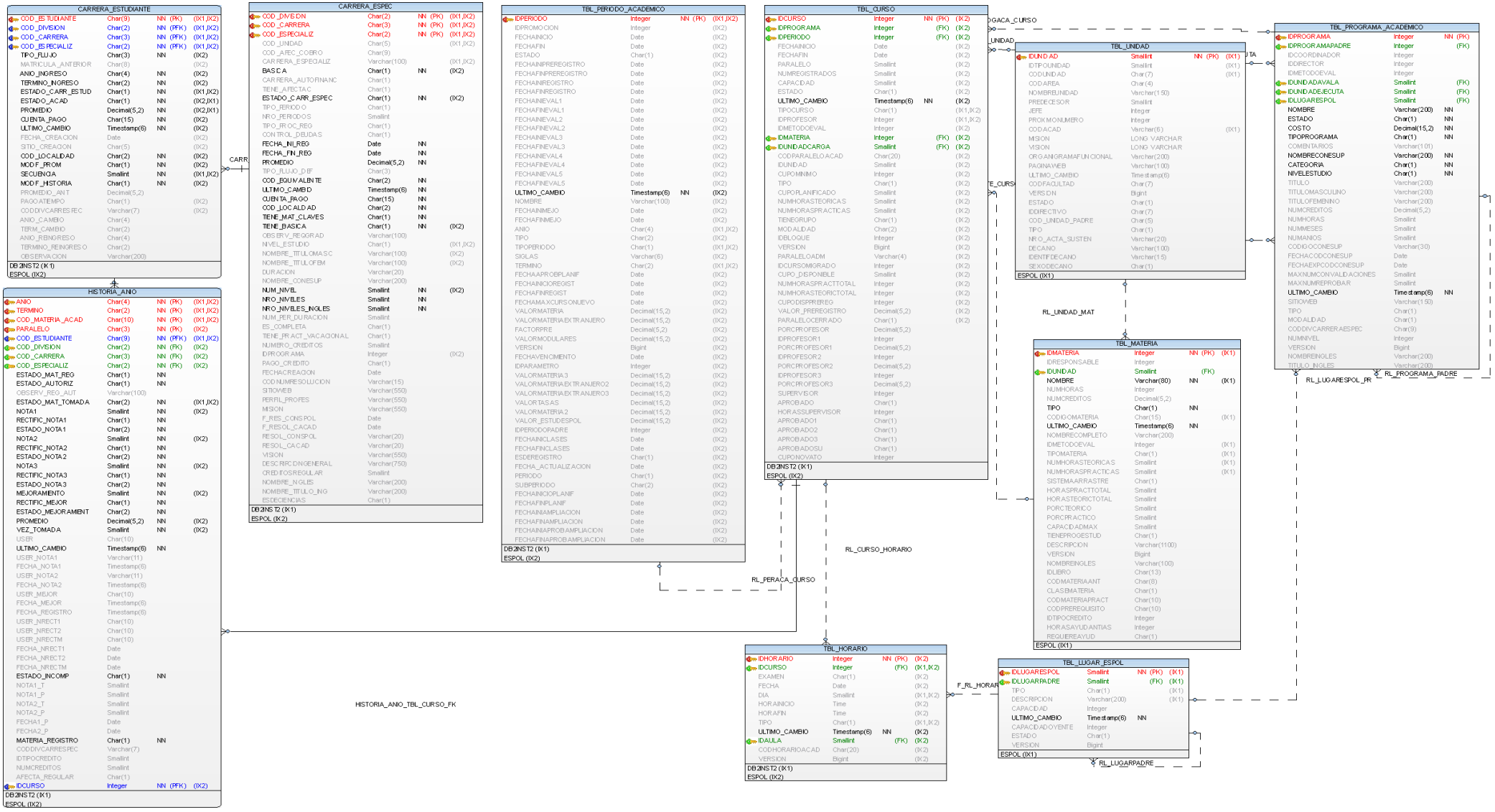


Figura 2.2 Modelo de datos académicos

2.2 RECURSOS NECESARIOS

Para el desarrollo del presente proyecto se hicieron uso de los siguientes recursos:

Tabla 1 Recursos necesarios

Recursos	Características
MATERIALES	
Servidor de Producción SUN SPARC	Modelo T5140 Sistema Operativo Solaris 5.10 Memoria RAM: 48GB Procesadores físicos: 2, UltraSPARC-T2+ Procesadores virtuales 48 c/p Discos Internos 300GB SAS Discos de Fibra 1 TB
Servidor de Desarrollo SUN SPARC	Modelo T2000 Sistema Operativo Solaris 5.10 Memoria RAM: 32GB Procesadores físicos: 1, UltraSPARC-T1 Procesadores virtuales 7 Discos Internos 240GB SAS Discos de Fibra 500 GB
Servidor Virtual Linux	Sistema operativo Centos 6.5 Memoria RAM: 8GB Procesadores: 1 Quaq core
Licencia DB2	DB2 Enterprise Server Edition Versión 10.5
Ordenador	Sistema Operativo Windows 7 Disco Duro mínimo de 250GB Memoria RAM: 4GB Procesador: Cualquiera Programa para conexión Remota a los servidores (PUTTY.EXE) Programa para administración de datos de los servidor (Filezilla)

HUMANO	
Personal	Especialista en Seguridad de la Información Conocimiento en Base de Datos DB2 Conocimiento en servidores Solaris Conocimiento en lenguajes de programación

2.3 CONSIDERACIONES

Debido que para solucionar ciertos problemas se debe realizar una eliminación total de la base de datos se debió contar con la elaboración de un documento que cuente con las medidas preventivas en caso de algún incidente para este caso en particular:

- Identificar y listar tareas a realizar y asignar los responsables.
- Restringir las operaciones durante la actualización de datos.
- Etiquetar debidamente los respaldos antes y después de la actualización de datos.
- Identificar a los afectados y comunicar la apertura de la ventana de mantenimiento.
- Identificar la fecha que va a tener menos impacto la suspensión de los servicios, para elegir la hora y fecha exacta de la apertura de la ventana de mantenimiento.
- Determinar el tiempo estimado que se van a demorar las tareas.
- Presentar las tareas a Gerencia para que sean aprobados los trabajos los respaldos OFFLINE debían realizarse el día sábado

2.4 DESARROLLO DEL PLAN

Tomando en cuenta las consideraciones que se deben tener se realizaron análisis de las actividades que deben revisarse y se sacaron las siguientes actividades:

- Revisar si se cuenta con herramienta de monitoreo en el servidor de base de datos
- Existen herramientas de alarmas en los servidores de bases de datos
- Verificar si se cuenta con generadores de respaldo de energía eléctrica
- Verificar si se realizaron las pruebas respectivas antes de realizar la migración al ambiente de producción
- Identificar el modelo utilizado en la programación de los sistemas
- Constatar herramientas de mantenimiento en la base de datos
- Verificar el listado de personas que tienen acceso a realizar UPDATE, SELECT, INSERT y DELETE en la base de datos
- Validar que se mantenga la integridad de los datos una vez realizado el cambio de Collate de la base de datos
- Validar que la información de datos personales como son el número de cedula, fecha y lugar de nacimiento sean las mismas que las registradas en el Registro Civil
- Verificar si existe un registro que demuestre que cambios fueron realizados y quien los realizo
- Verificar si se cuenta con manejo de programas de seguridad

- Revisar que solo los usuarios autorizados tienen acceso a la información confidencial de la base de datos
- Verificar si la base de datos cuenta con herramientas de encriptación de datos
- Verificar si se cuenta con la última actualización del sistema operativo y gestor de base de datos.

Estas actividades fueron planificadas para ser realizadas en 5 días donde primero se verificaran con las herramientas que se cuentan para mantener los sistemas disponibles, segundo se dará a entender las seguridades con las que se cuentan en los programas y como se conectan los sistemas, tercero se realizara el análisis de la información que se ha detectado que ha sido mal ingresada a las tablas y se verificara la consistencia de la misma para realizar un procedimiento para solucionar este problema teniendo cuidado de preservar la integridad de los datos y disponibilidad de los sistemas, cuarto se verificara las posibilidades de escalabilidad de la base para futuros proyectos para proteger los datos y quinto y último se verifico las actualizaciones de los servidores y motor de base de datos.

Tabla 2 Plan de trabajo

OBJETIVO	ALCANCE	ACTIVIDADES	DESCRIPCIÓN DE ACTIVIDADES
Verificar y validar la disponibilidad de la información de los servidores de la base de dato	Base de datos academica	Disponibilidad	Revisar si se cuenta con herramienta de monitoreo en el servidor de base de datos Existen herramientas de alarmas en los servidores de bases de datos Verificar si se cuenta con generadores de respaldo de energía electrica Verificar si se realizaron las pruebas respectivas antes de realizar la migración al ambiente de producción
Verificar y validar la integridad de la información de los servidores de la base de dato		Integridad	Identificar el modelo utilizado en la programación de los sistemas Constatar herramientas de mantenimiento en la base de datos Verificar el listado de personas que tienen acceso a realizar update, select, insert y delete en la base de datos Validar que se mantenga la integridad de los datos una vez realizado el cambio de Collate de la base de datos Validar que la información de datos personales como son el número de cedula, fecha y lugar de nacimiento sean las mismas que las registradas en el Registro Civil Verificar si existe un registro que demuestre que cambios fueron realizados y quien los realizo
Verificar y validar la confidencialidad de la información de los servidores de la base de dato		Confidencialidad	Verificar si se cuenta con manejo de programas de seguridad Revisar que solo los usuarios autorizados tienen acceso a la información confidencial de la base de datos Verificar si la base de datos cuenta con herramientas de encriptación de datos

Tabla 3 Cronograma de trabajo

Actividades	Responsables	Fecha				
		11/06/2015	12/06/2015	13/06/2015	14/06/2015	15/06/2015
Revisar si se cuenta con herramienta de monitoreo en el servidor de base de datos	Marco Calle					
Existen herramientas de alarmas en los servidores de bases de datos						
Verificar si se cuenta con generadores de respaldo de energía electrica						
Verificar si se realizaron las pruebas respectivas antes de realizar la migración al ambiente de producción						
Identificar el modelo utilizado en la programación de los sistemas						
Constatar herramientas de mantenimiento en la base de datos						
Verificar el listado de personas que tienen acceso a realizar update, select, insert y delete en la base de datos						
Validar que se mantenga la integridad de los datos una vez realizado el cambio de Collate de la base de datos						
Validar que la información de datos personales como son el número de cedula, fecha y lugar de nacimiento sean las mismas que las registradas en el Registro Civil						
Verificar si existe un registro que demuestre que cambios fueron realizados y quien los realizo						
Verificar si se cuenta con manejo de programas de seguridad						
Revisar que solo los usuarios autorizados tienen acceso a la información confidencial de la base de datos						
Verificar si la base de datos cuenta con herramientas de encriptación de datos						

CAPÍTULO 3

IMPLEMENTACIÓN Y ANÁLISIS DE RESULTADOS

3.1 IMPLEMENTACIÓN DEL PLAN

3.1.1 HERRAMIENTAS DE MONITOREO EN SERVIDOR DE BASE DE DATOS

Se ha detectado el uso de un software llamado nagios en su versión 3.4.1 que sirve para el monitoreo de red, vigila el rendimiento, salud y servicios del servidor, este servicio puede ser usado para monitorizar vía web y consultar memoria RAM libre, uso de procesador, espacio disponible en los discos, y otros parámetros de los sistemas operativos ver figura 3.1.

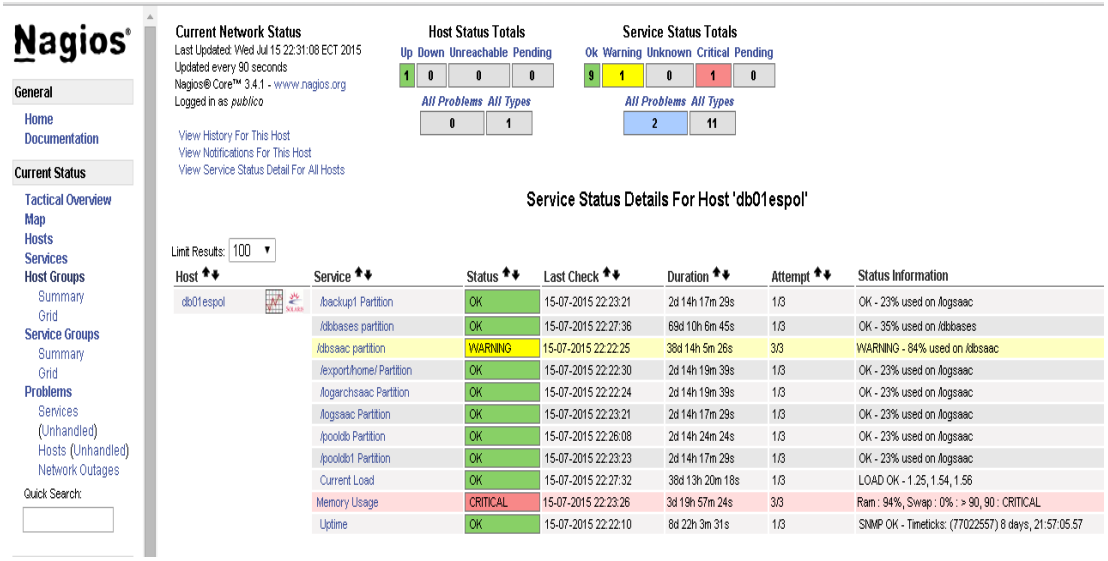
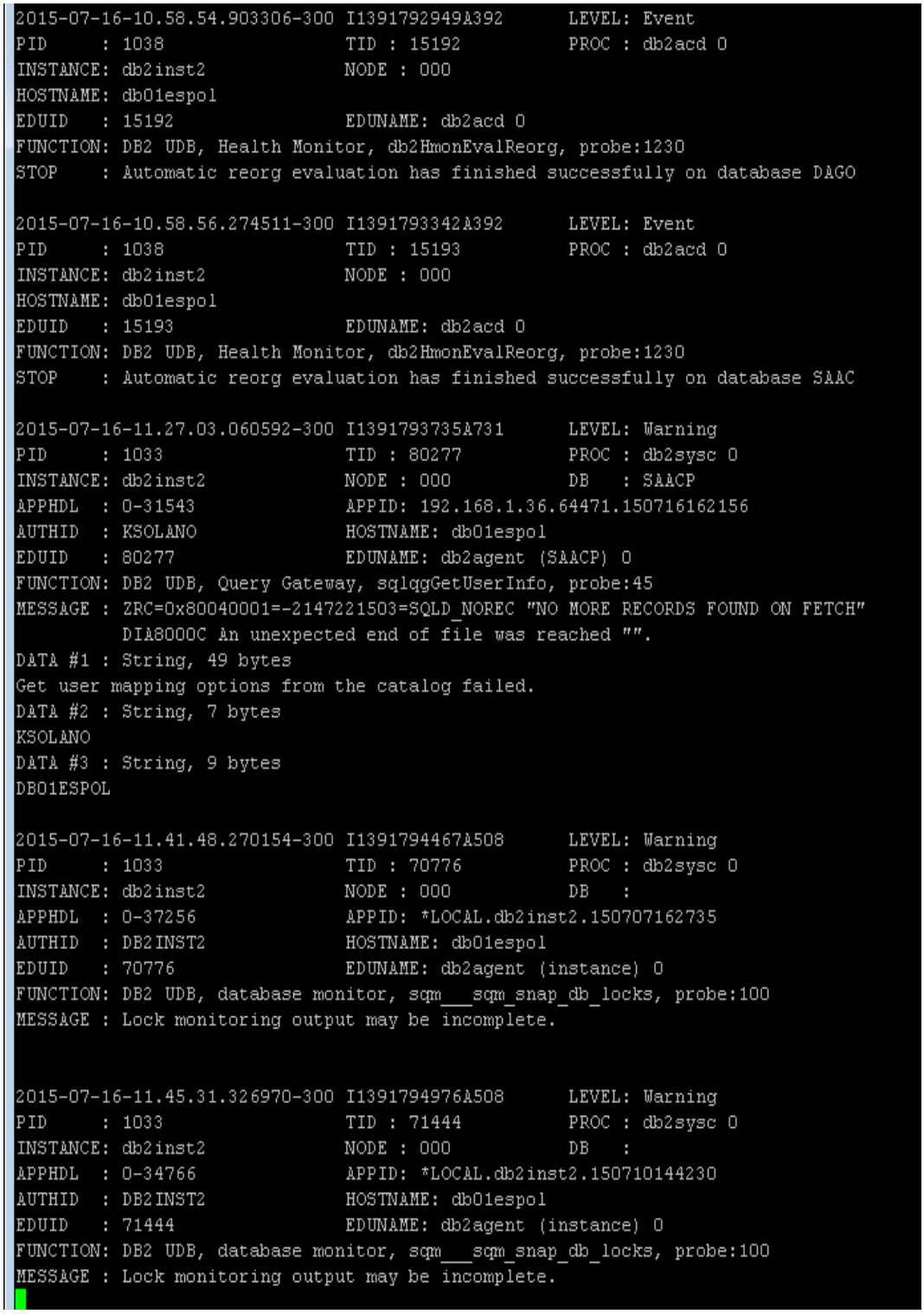


Figura 3.1 Herramienta de monitoreo Nagios

Se realiza un método de monitorización manual del log (db2diag) de la base de datos para poder revisar todos los eventos que ocurren en la base de datos los accesos fallidos, los errores de las bases, la asignación de recursos a la base, y otros eventos para el monitoreo de la base específicamente. Así también se monitorea con una herramienta propia de db2 que se llama “db2top” los recursos que la base de datos está consumiendo y que tiene asignado, se puede revisar el estado de la base de datos (cuando fue el último respaldo, cuando se lo reinicio, y otros), el estado de los bufferpools, el uso de la memoria RAM, las sesiones conectadas a la base, los bloqueos de la base, y algunos parámetros más ver figura 3.2 y 3.3.



```
2015-07-16-10.58.54.903306-300 I1391792949A392      LEVEL: Event
PID     : 1038                 TID : 15192          PROC : db2acd 0
INSTANCE: db2inst2             NODE : 000
HOSTNAME: db01espol
EDUID   : 15192                EDUNAME: db2acd 0
FUNCTION: DB2 UDB, Health Monitor, db2HmonEvalReorg, probe:1230
STOP    : Automatic reorg evaluation has finished successfully on database DAGO

2015-07-16-10.58.56.274511-300 I1391793342A392      LEVEL: Event
PID     : 1038                 TID : 15193          PROC : db2acd 0
INSTANCE: db2inst2             NODE : 000
HOSTNAME: db01espol
EDUID   : 15193                EDUNAME: db2acd 0
FUNCTION: DB2 UDB, Health Monitor, db2HmonEvalReorg, probe:1230
STOP    : Automatic reorg evaluation has finished successfully on database SAAC

2015-07-16-11.27.03.060592-300 I1391793735A731      LEVEL: Warning
PID     : 1033                 TID : 80277          PROC : db2sysc 0
INSTANCE: db2inst2             NODE : 000           DB   : SAACP
APPHDL  : 0-31543              APPID: 192.168.1.36.64471.150716162156
AUTHID  : KSOLANO              HOSTNAME: db01espol
EDUID   : 80277                EDUNAME: db2agent (SAACP) 0
FUNCTION: DB2 UDB, Query Gateway, sqlqgGetUserInfo, probe:45
MESSAGE : ZRC=0x80040001=-2147221503=SQLD_NOREC "NO MORE RECORDS FOUND ON FETCH"
          DIA8000C An unexpected end of file was reached "".
DATA #1 : String, 49 bytes
Get user mapping options from the catalog failed.
DATA #2 : String, 7 bytes
KSOLANO
DATA #3 : String, 9 bytes
DB01ESPOL

2015-07-16-11.41.48.270154-300 I1391794467A508      LEVEL: Warning
PID     : 1033                 TID : 70776          PROC : db2sysc 0
INSTANCE: db2inst2             NODE : 000           DB   :
APPHDL  : 0-37256              APPID: *LOCAL.db2inst2.150707162735
AUTHID  : DB2INST2             HOSTNAME: db01espol
EDUID   : 70776                EDUNAME: db2agent (instance) 0
FUNCTION: DB2 UDB, database monitor, sqm___sqm_snap_db_locks, probe:100
MESSAGE : Lock monitoring output may be incomplete.


2015-07-16-11.45.31.326970-300 I1391794976A508      LEVEL: Warning
PID     : 1033                 TID : 71444          PROC : db2sysc 0
INSTANCE: db2inst2             NODE : 000           DB   :
APPHDL  : 0-34766              APPID: *LOCAL.db2inst2.150710144230
AUTHID  : DB2INST2             HOSTNAME: db01espol
EDUID   : 71444                EDUNAME: db2agent (instance) 0
FUNCTION: DB2 UDB, database monitor, sqm___sqm_snap_db_locks, probe:100
MESSAGE : Lock monitoring output may be incomplete.
```

Figura 3.2 Monitoreo Manual del log db2diag

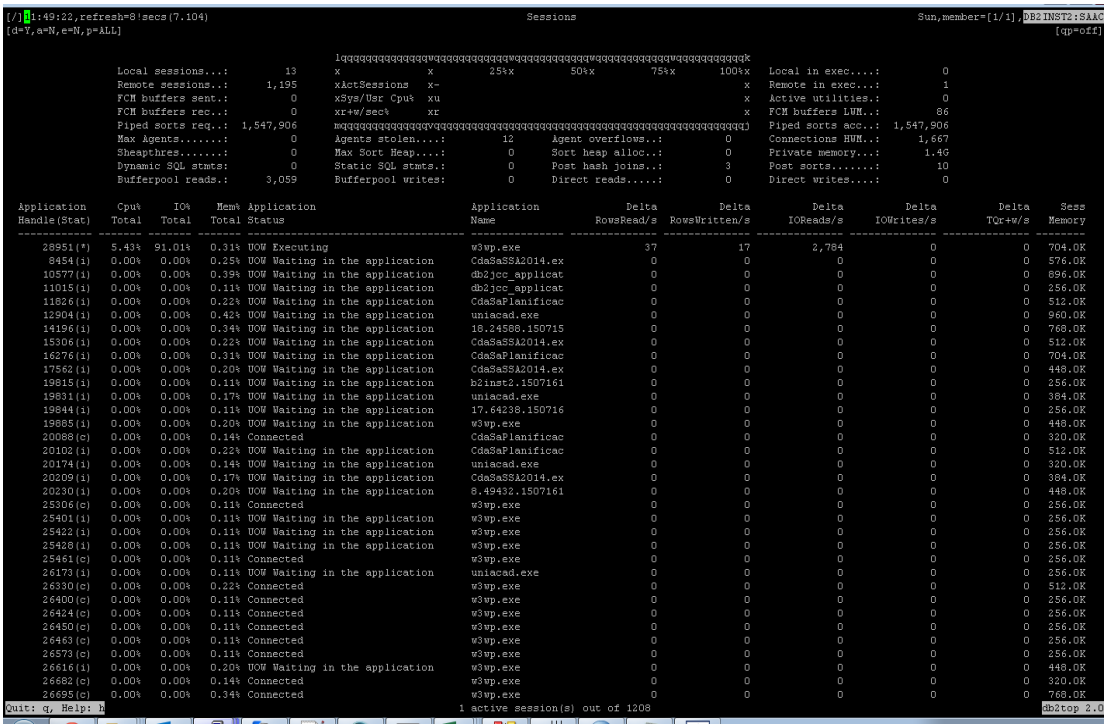


Figura 3.3 Monitoreo Manual de la base con “db2top”

Se instaló una nueva herramienta para el monitoreo que es mucho más amigable que con la que se cuenta, esta herramienta es de software propietario de DELL se llama Spotlight sirve para monitorear en tiempo real los recursos, de una manera más fácil e intuitiva incluyendo una representación arquitectónica del servidor ver figura 3.4. Se puede obtener un desglose detallado con tablas y gráficos. Su instalación es sencilla y los requerimientos no son exagerados.

Se pueden descargar el instalador desde la página oficial de DELL http://software.dell.com/products/spotlight-on-unix-linux/ una vez descargado ejecutar como administrador el ejecutable que se descargó y

seguir las instrucciones que salgan en la pantalla. Los requisitos para correr este software en un pc son:

Tabla 4 Requerimientos Spotlight

Sección	**Requerimiento**
Privilegios y Permisos	Administrador
Plataforma	Procesador 1.2 GHZ
Memoria RAM	512 MB
DISCO DURO	1GB libre
SO	Desde windows xp para arriba

Figura 3.4 Herramienta de monitoreo Spotlight

3.1.2 HERRAMIENTAS DE ALARMAS EN SERVIDOR DE BASE DE DATOS

Las herramientas ya revisadas tienen su propio software y configuración de parámetros de alertas el software nagios genera alertas cuando los parámetros definidos exceden de los límites señalados y pueden ser revisadas vía web, ser recibidas vía correo electrónico o vía mensajes de texto por celular ver figura 3.5. Los parámetros definidos para las alarmas son:

- Uso de memoria RAM
- Servidor este respondiendo
- Uso de los filesystems

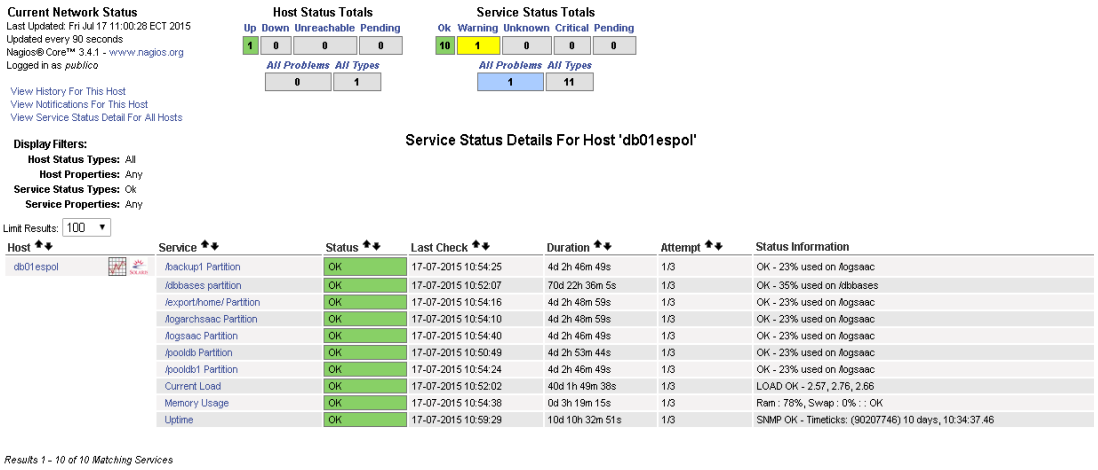


Figura 3.5 Nagios - Pantalla de estado de servidor

Así también Spotlight cuenta con alarmas en línea que se encienden intensificando los colores sobre el componente alertado mientras se

monitorea el servidor, da alertas audibles de precaución, y envía correos electrónicos ver figura 3.6. Las múltiples alarmas que se pueden revisar son:

- Bloqueo de procesos de lectura y escritura en disco o alto o bajo tráfico de la red.
- Alerta del espacio de la Swap
- Porcentaje de uso del disco duro
- Estado de los procesadores
- Alerta de aumento del porcentaje usado en la memoria RAM
- Memoria Virtual
- Espacio de la memoria Swap

Figura 3.6 Spotlight - Alarmas visuales

3.1.3 EQUIPOS DE PROTECCIÓN DE ENERGÍA ELÉCTRICA

Con respecto a la protección eléctrica de la base de datos para asegurar la continuidad de la energía eléctrica, todos los equipos están debidamente conectados a tierra, se tiene un equipo de UPS de 30 KVA que sirve para alimentar la primera fuente de poder del servidor, otro equipo un UPS de 10 KVA de respaldo conectado a la segunda fuente de poder del servidor, estos equipos de UPS son marca General Electric trifásicos con protección interna y nos dan 30 minutos de respaldo ante cualquier problema con la empresa eléctrica. Adicional a esto se cuenta con un generador Caterpillar a diésel de 139KVA con un panel automático que detecta la falta de energía eléctrica y en el lapso de 10 segundos comienza a distribuir la energía desde el mismo. No se ha reportado problemas con este sistema de protección.

3.1.4 GESTIÓN DE ACCESO A LA BASE DE DATOS

Dentro de la gestión de accesos tenemos las seguridades a la base de datos, se tiene que se trabaja con el directorio activo para autentificar los usuarios de la organización y a nivel de sistema operativo se los organiza por grupos para asignarle los determinados permisos a las tablas en la base de datos.

3.1.4.1 ADMINISTRACIÓN DE PERMISOS

Se cuenta con un sistema de administración de permisos que tiene una librería de control de acceso en los sistemas, el sistema de seguridades

lo maneja una sola persona y los permisos son requeridos por los jefes de las unidades. La única forma de entrar a los sistemas es estando registrados en este sistema y asignado el debido perfil y la unidad a la que pertenece.

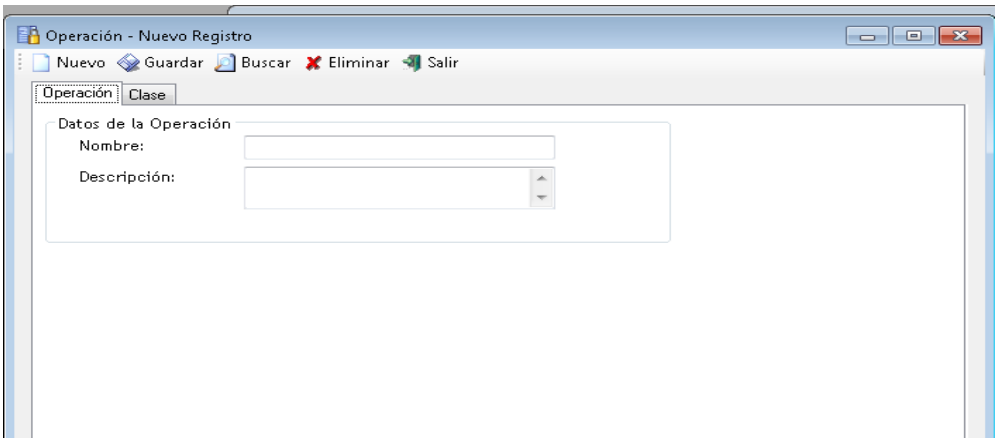


Figura 3.7 Módulo de Seguridad - Operación

En el sistema se manejan las operaciones donde son asignados los nombres de las clases, para que sirven y el nombre de la operación ver figura 3.7; Los permisos son manejados a nivel de perfil donde se detalla el nombre del perfil la descripción el horario de acceso, los días que pueden acceder y las operaciones que se les van a asignar a ese perfil ver figura 3.8.

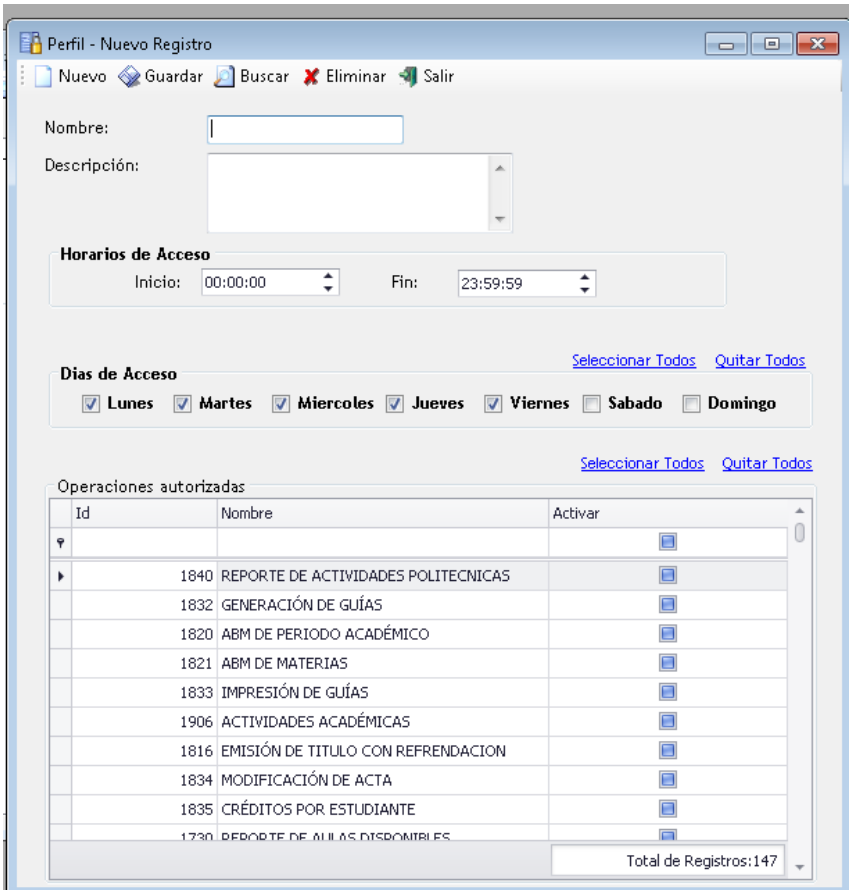


Figura 3.8 Módulo de Seguridad - Perfil

Así también el manejo de los usuarios donde se le asigna, busca y elimina el permiso que van a tener, la unidad que pertenece el usuario y si el perfil expira o es permanente ver figura 3.9.

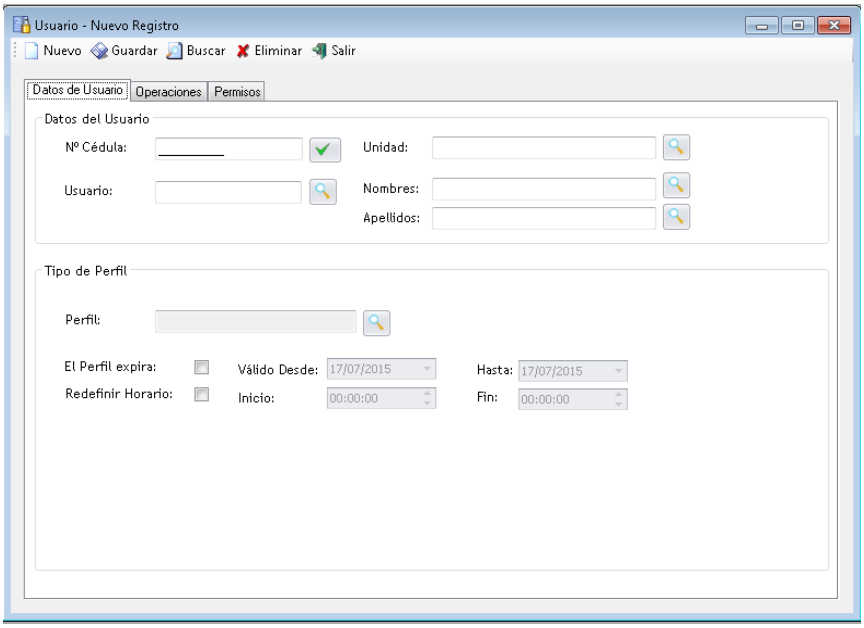


Figura 3.9 Módulo de Seguridad - Usuario

Y finalmente el módulo de usuarios conectados donde se puede ver el sistema, el usuario, el perfil con el que ingreso, los nombres del usuario y la hora de conexión y adicional una herramienta para poder desconectar a los usuarios del sistema ver figura 3.10.

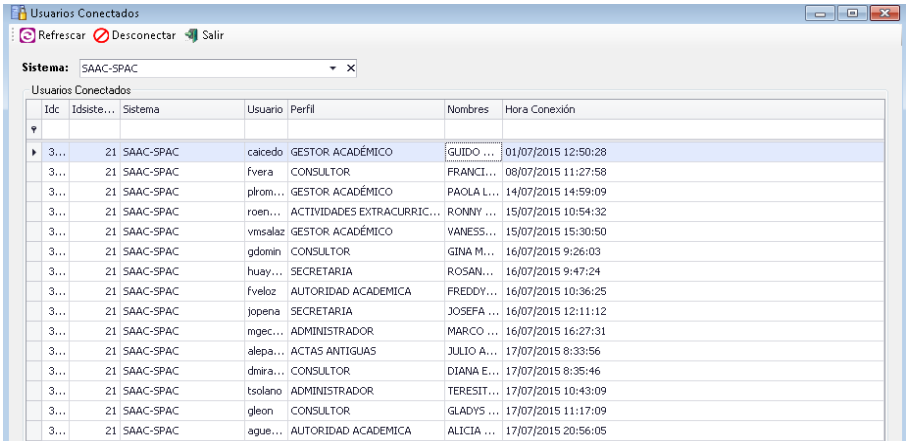


Figura 3.10 Módulo de Seguridad - Usuarios Conectados

3.1.4.2 PERMISOS ASIGNADOS EN LOS GRUPOS

Se lleva un control de asignación de permisos por año en una hoja de Excel, donde se tiene registrado la unidad, el nombre del usuario, el usuario que se le dio el permiso, el grupo a que fue asignado, el sistema que se pide el permiso, el perfil que se le asigno, la fecha de la operación, la acción (si se le asigna o quita) y la observación donde se ingresa la fecha y quien lo solicito ver figura 3.11.

Los grupos son creados en la base de datos y deben tener ciertas restricciones la principal que los nombres de grupo deben ser menor o igual a la longitud del nombre del grupo [4].

Figura 3.11 Hoja de control de grupos

Los grupos identificados fueron consultas y unidades, consultas que tiene permiso de SELECT sobre todas las tablas del sistema académico y el de unidades que tiene permisos de SELECT, INSERT, UPDATE y DELETE sobre las tablas ver figura 3.12.

Figura 3.12 Permisos en las tablas de los grupos

3.1.5 HERRAMIENTAS DE MANTENIMIENTO EN LAS BASES DE DATOS

Db2 cuenta con un sistema propio de administración de la base de datos llamado “IBM DATA STUDIO” se lo puede descargar de la página web de IBM, desde aquí se puede manejar todas las operaciones de consultas, creación, eliminación, configuración y mantenimiento. En cuanto al mantenimiento, el gestor de bases de datos proporciona capacidades de mantenimiento automático para realizar copias de seguridad de bases de datos, manteniendo vigentes las estadísticas, y la reorganización de tablas e índices según sea necesario. La realización de las actividades de mantenimiento de bases de datos es esencial para asegurar que están optimizados para un rendimiento y capacidad de recuperación [5].

Además de la configuración de la base para que realice de manera automática el mantenimiento también se puede correr de manera manual, es recomendable que después de la actualización de la estructura de una tabla sea ejecutado el debido mantenimiento de la tabla tomando en cuenta lo crítico y la cantidad de datos que maneje la misma ver figura 3.13.

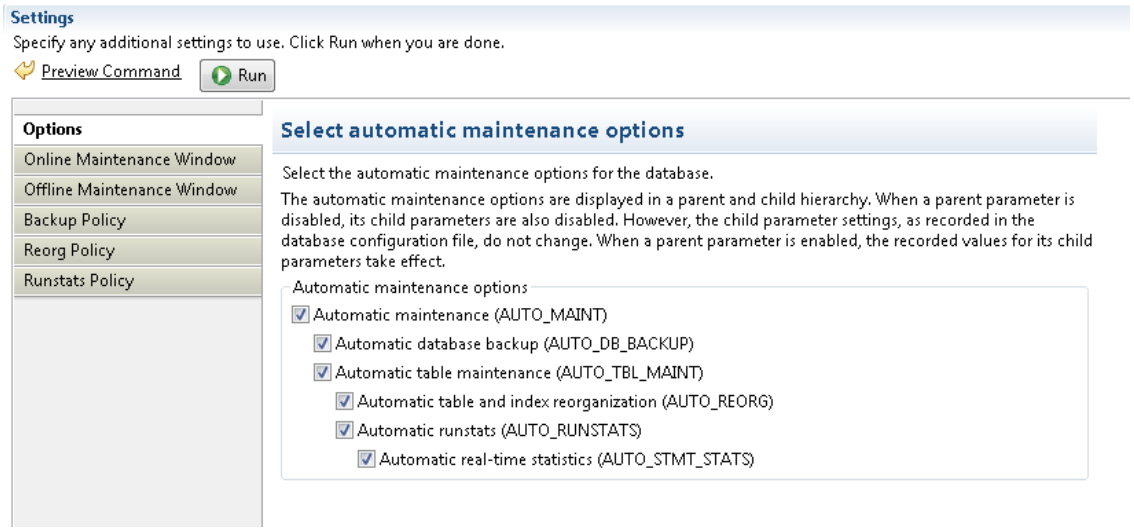


Figura 3.13 Mantenimiento Automático de la base

Las políticas de configuración actual esta de la siguiente manera, respaldo en línea de base de datos completa está planificado de lunes a domingo 3:30 am, no hay planificado automáticamente respaldos fuera de línea por lo que hay muchas conexiones desde los servidores web y para poder realizar un respaldo fuera de línea hay que desconectar a todos y esto por lo general se lo realiza manualmente cada 6 meses o en caso de realizar un cambio que afecte el funcionamiento total de la base como ejemplo puede ser alguna migración de bases. Los reordenamientos y estadísticas se corren automáticamente por requerimiento del gestor de base de datos.

3.1.6 CONEXIÓN DE LOS SISTEMAS CON LAS BASES DE DATOS

Como se había mencionado anteriormente se cuenta con un sistema de seguridades propio, el cual permite la conexión de los sistemas con la

base de datos si el usuario ha logrado autentificarse y si tiene el permiso de sistema correspondiente a la pantalla, podrá acceder a realizar las operaciones que el sistema le asigne.

Existen sistemas de escritorio y sistemas web desarrollados en visual.net, la arquitectura con la que se trabaja es webform que proporciona un gran nivel de abstracción con un modelo de programación familiar basado en eventos y controles que favorece la productividad mediante la programación declarativa reduciendo la cantidad de código necesaria para implementar una funcionalidad [6], se desarrolló con el tiempo una persistencia propia que es la encargada de realizar la conexión y consultas a la base de datos, esta persistencia hace uso de transacciones en caso de error toda la transacción es revertida para guardar la integridad de los datos así también si la transacción se realiza con éxito es grabada por completo.

En relación a cómo se maneja la conexión de los programas externos a la base de datos se usan dos formas la primera crear y dar el acceso a vistas con los permisos de SELECT para que puedan consultar datos y segundo el uso de servicios web provisto por la institución.

3.1.7 EVALUACIÓN DE LA INFORMACIÓN DE LA BASE DE DATOS

El manejo de la información es lo más importante de la institución por lo que se debe mantener a buen recaudo con respaldos, integridad de los datos, disponibilidad y otras formas, como también se debe mantener la

consistencia de la información es por esto que no es posible tener datos erróneos o duplicados. Se había venido reportando problemas que en los sistemas no era encontrada la información de algunas personas, luego que era ingresada se encontraba que los datos de las personas estaban duplicados o en caso específico de los profesores que no podían revisar sus cursos asignados. Se hizo el análisis de él porque estaban ocurriendo estos problemas y se llegó a la conclusión de que debido a la configuración con el cual fue creada la base de datos esta distinguía de mayúsculas, minúsculas y acentos. Se buscaron algunas formas de corregir estos parámetros pero dado que es una configuración que se da al crear la base de datos y esta no puede ser modificada, se llegó a la decisión que para corregir estos problemas la base debe ser nuevamente creada, tomando los parámetros de seguridad de la institución, se elaboró una lista de tareas para la migración y cambio del codeset de la base de datos. Se aprovechó la disponibilidad de un servidor de prueba con iguales configuraciones que el servidor de producción, lo que ayudo a realizar los cambios en este servidor y luego pasar al de producción mediante una restauración de un respaldo fuera de línea del servidor de prueba donde se realizó lo anteriormente indicado.

Tabla 5 Tareas migración y cambio de codeset de la bases de datos

TAREAS	ENCARGADO	CUMPLIMIENTO
MIGRACION Y CAMBIO DE CODESET DE LA BASE DE DATOS		
PREPARACIÓN		
PREPARAR SENTENCIA CREATE DE BASE DE DATOS CON UTF8 Y UCA500R1_LEN_S1	MC	
GENERAR DDL	MC	
COMPLETO	MC	
BUFFERPOOL	MC	
TABLESPACE	MC	
TABLAS	MC	
CLAVES PRIMARIAS	MC	
INDEX	MC	
FOREING KEY	MC	
IDENTITY	MC	
CONSTRAINS	MC	
VISTAS	MC	
TRIGGERS	MC	
STORE PROCEDURES	MC	
FUNCIONES	MC	
PERMISOS	MC	
GENERAR SENTENCIAS DROP DE IDENTITY	MC	
GENERAR SENTENCIA PARA GENERAR LOS LOAD Y EXPORT DE LOS IXF DE LAS TABLAS	MC	
DURANTE		
EN EL SERVIDOR DE PRODUCCIÓN SACAR LOS PERMISOS DE UPDATE, DELETE E INSERT A TODOS LOS USUARIOS Y GRUPOS	MC	
RESPALDAR LA BASE DE DATOS DE PRODUCCIÓN FUERA DE LINEA	MC	
RESPALDAR LOS LOG DE LA BASE DE DATOS DE PRODUCCIÓN	MC	
EJECUTAR SENTENCIA EXPORT DE LOS IXF DE LAS TABLAS DE PRODUCCIÓN	MC	
PASAR LOS ARCHIVOS AL SERVIDOR DE PRUEBA	MC	
ELIMINAR LA BASE DEL SERVIDOR DE PRUEBA	MC	
CREAR LA BASE DE DATOS EN EL SERVIDOR DE PRUEBA	MC	
EJECUTAR DDL DE CREACION DE TABLAS	MC	
EJECUTAR SENTENCIA DROP DE LOS IDENTITY	MC	
CARGAR DATOS CON SENTENCIA LOAD DE LOS IXF DE LAS TABLAS	MC	
EJECUTAR SENTENCIA DE CREACION DE PRIMARY KEY	MC	
EJECUTAR SENTENCIA DE CREACION DE IDENTITY	MC	
EJECUTAR SENTENCIA DE CREACION DE INDEX	MC	
EJECUTAR SENTENCIA DE CREACION DE FOREING KEY	MC	
EJECUTAR SENTENCIA DE CREACION DE CONSTRAINS	MC	
EJECUTAR SENTENCIAS DE CREACION DE VISTAS	MC	
EJECUTAR SENTENCIAS DE CREACION DE STORED PROCEDURE	MC	
EJECUTAR SENTENCIAS DE CREACION DE TRIGGERS	MC	
EJECUTAR SENTENCIAS DE CREACION DE FUNCIONES	MC	
EJECUTAR SENTENCIAS DE CREACION DE PERMISOS	MC	
CONTINGENCIA		
EN CASO DE QUE HUBIERA ALGÚN PROBLEMA EN EL MOMENTO DE LA EJECUCIÓN SE RESTAURARÁ DE LOS RESPALDOS OFFLINE REALIZADOS EN LA PREPARACIÓN.	MC	
OBSERVACIONES		

Las tareas fueron realizadas primero en el servidor de prueba con una tabla la de tbl_persona donde no se presentaron novedades y se realizaron con éxito todas las tareas en vista de esto se presentó a la jefatura el plan para realizar la migración de datos en el servidor de

producción y el cronograma. Una vez aprobado se procedió a la revisión de las tareas para ver que no se había pasado por alto alguna observación, se creó una carpeta en el servidor donde se guardaron todos los archivos generados, esta carpeta fue pasada a una maquina local desde donde se corrían los script para tener respaldo de los mismos localmente, la preparación de la migración se la realizo en un lapso de 8 horas sin mayores novedades, de ahí la carpeta fue subida al servidor de prueba y a las 8 de la noche se procedió a quitar todos los permisos de INSERT, UPDATE y DELETE a los usuarios y grupos de la base de datos, esto para prevenir que la información sea alterada y se la deja disponible solo para ser consultada, se desconectaron a todos los usuarios por 20 minutos para poder sacar el respaldo fuera de línea para en caso de contingencia pueda ser recuperada la información desde este respaldo. Se comenzaron a correr los script en el servidor de prueba para crear la base de datos, se crea primero las tablas para poder insertar la información esto se hace antes de crear los disparadores (triggers) ya que si no se insertarían registros en la tabla de logs, para poder controlar los cambios se realizó un archivo de texto por cada tabla migrada donde se registra cuantas filas fueron insertadas y si hubo algún problema con alguna fila. La migración de la base de datos duro aproximadamente 8 horas en el servidor de prueba una vez terminada se revisó los logs de cada tabla para ver si hubo algún problema en la migración, no se encontró novedades entonces se realizó un respaldo offline para poder pasarlo al servidor de producción, una vez pasado el

respaldo se procedió a realizar la restauración en la base de producción la cual demoro 2 horas, terminado este proceso se procedió a asignar nuevamente los permisos a los usuario y los grupos y posterior a esto la prueba de los sistemas de escritorio y web sin presentación de algún problema.

Así también fueron detectados errores en unos reportes solicitados por el vicerrectorado, donde los años de nacimiento de estudiantes eran del 2001, de 1900 o 0001 esta información se había ingresado mal cuando se había lanzado una actualización de un sistema para el ingreso de los datos personales y hubo problemas en la programación esto fue corregido a nivel del sistema pero nunca fue evaluado el impacto en la base de datos, se realizó el análisis de cuantos registros tenían este problema y se encontró que eran aproximadamente 6000 registros por lo cual no era posible actualizar a mano esta información, se realizó un listado de los números de cedulas de los estudiantes para sacar la información con un programa que usa los servicios web del registro civil donde se da un archivo con los números de cedulas y este devuelve un archivo con la información que nosotros le pidamos como fecha de nacimiento, dirección, estado civil, y otros datos personales. El programa fue ajustado para pedir fecha de nacimiento, dirección y estado civil, estos datos fueron cargados a una tabla temporal para poder comparar la información que se obtuvo del registro civil y la que está registrada en la tabla de producción, estas novedades fueron pasadas a los

encargados de mantener y actualizar esta información para que apruebe la actualización de los datos.

Una vez que se aprobó y reviso el archivo y para mantener un registro sobre los cambios se creó un usuario “usrregciv” con los permisos de SELECT y UPDATE sobre la tabla temporal y la tabla de datos personales “estudiante_acad” con el cual se realizó las actualizaciones para que quede registrado mediante los disparadores en la tabla de logs, así también se actualizara la información en la tabla principal “tbl_persona”. La actualización se la hizo mediante la generación del script de UPDATE con la información que se sacó del archivo revisado, y fue ejecutado en la noche en un tiempo aproximado de 1 hora sin novedades.

3.1.8 REGISTROS PARA AUDITORIA INFORMÁTICA A LA BASE DE DATOS

Se cuenta con módulos en los sistemas para realizar auditoría a ellos pero adicional a esto se tiene una tabla con todas las transacciones realizadas por los usuarios sobre las tablas de la base de datos, estas son manejadas por disparadores (triggers) en el momento de borrar, insertar o actualizar. La tabla log_academico guarda el usuario que realiza la transacción, la fecha, la hora, el nombre de la tabla, el tipo de transacción (I=INSERT; U=UPDATE; D=DELETE), un XML con los datos anteriores y un XML con los datos actuales.

El log_academico es respaldado mes a mes y guardado en cintas imation 4mm dds-150 con capacidad de 40 Gb comprimidos, y se libera cada 6 meses por la cantidad de información que maneja.

3.1.9 PROTECCIÓN DE DATOS

Para mantener la confidencialidad de los datos ya hemos visto que tenemos un programa de seguridad con el cual se le es asignado un perfil y este perfil solo puede tener acceso a la información y las opciones que se le fueron establecidas, de este modo se asegura que los usuarios solo puedan revisar la información a la que tienen permiso consultar. Pese a esto a veces no es suficiente con el control de permisos o el control de usuarios sino también es necesario tener cifrada la información dentro de la base de datos es por esto que debemos asegurarnos que la base de datos tenga soporte o haya una herramienta externa para encriptación de los datos.

En un futuro se requiere para un nuevo proyecto que los datos personales de los estudiantes y su información de ficha medica deba ir cifrada para que la información sensible no pueda ser revisada por otras personas fuera de las encargadas, la base de datos DB2 cuenta con las funciones ENCRYPT y DECRYPT que son las nativas de DB2 para cifrar y descifrar. Estas funciones trabajan con una clave semilla que es requerida para cifrar y descifrar los datos, cabe recalcar que sin esta clave la información se perdería y no pudiera ser revelada por ni un

método y además la función DECRYPT sólo puede descifrar valores que se han cifrado mediante la función ENCRYPT [7].

Ya que se cuenta con una herramienta nativa para el cifrado y descifrado de los datos no se ve necesario usar programas externos como protectDB ni ningún otro, a veces la utilización de estos programas puede llevar que en caso de algún incidente al momento de querer recuperar la información no pueda ser reconocida ya que se ha cambiado el ambiente donde originalmente fue cifrado.

3.1.10 MANTENER LOS SISTEMAS ACTUALIZADOS

Uno de los principios Informáticos es mantener siempre el sistema operativo actualizado y con sus respectivos parches así mismo el software que se usa, aunque esto siempre se lo ha visto orientado a Windows los sistemas UNIX también han venido presentando una serie de explotación de vulnerabilidades por lo cual se debe comprobar que los sistemas UNIX también estén siempre actualizados. Sin embargo un sistema en producción no debe ser actualizado sin un previo plan donde se indique que se debe hacer en caso de fallar o de corromperse el sistema y sus respectivas pruebas.

Actualmente verificando las actualizaciones del sistema operativo que usamos podemos apreciar que se encuentra instalada la última versión de Solaris 10 ver figura 3.14, por lo cual no necesitaremos ni un cambio o actualización del sistema operativo.

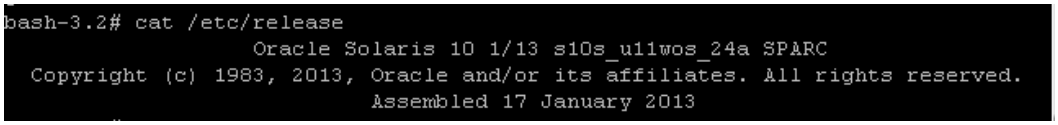


Figura 3.14 Última actualización de Solaris 10 1/13

En relación a la base de datos db2 tambien podemos constatar que la version instalada es la última version con el último fixpack aplicado ver figura 3.15, se puede leer en la web la documentacion de los últimos cambios que incluye este fixpack y que aún no ha salido otro fixpack para actualizar.

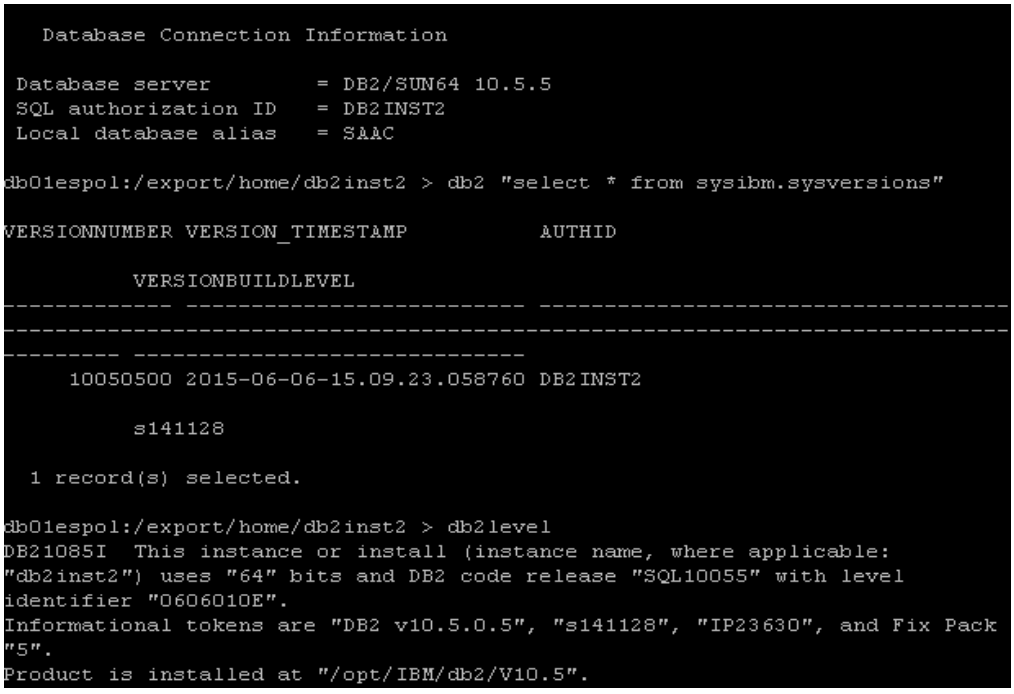


Figura 3.15 Última actualización de base de datos db2 v10.5.0.5

3.2 ANÁLISIS DE LOS RESULTADOS

Se han aplicado los principios de las seguridades en la base de datos académica principalmente se verifico las medidas que se tiene para mantener la disponibilidad, confiabilidad e integridad de la información se elaboró un plan de trabajo en cual se identificaba las principales actividades que debían evaluarse se ha cumplido con el plan de trabajo encontrando ciertas novedades.

Tabla 6 Cumplimiento de las actividades del plan

Actividades	Responsables	Cumplimiento	
		SI	NO
Revisar si se cuenta con herramienta de monitoreo en el servidor de base de datos	Marco Calle	x	
Existen herramientas de alarmas en los servidores de bases de datos		x	
Verificar si se cuenta con generadores de respaldo de energía electrica		x	
Verificar si se realizaron las pruebas respectivas antes de realizar la migración al ambiente de producción		x	
Identificar el modelo utilizado en la programación de los sistemas		x	
Constatar herramientas de mantenimiento en la base de datos		x	
Verificar el listado de personas que tienen acceso a realizar update, select, insert y delete en la base de datos		x	
Validar que se mantenga la integridad de los datos una vez realizado el cambio de Collate de la base de datos		x	
Validar que la información de datos personales como son el número de cedula, fecha y lugar de nacimiento sean las mismas que las registradas en el Registro Civil		x	
Verificar si existe un registro que demuestre que cambios fueron realizados y quien los realizo		x	
Verificar si se cuenta con manejo de programas de seguridad		x	
Revisar que solo los usuarios autorizados tienen acceso a la información confidencial de la base de datos		x	
Verificar si la base de datos cuenta con herramientas de encriptación de datos		x	
Verificar actualizaciones de los sistemas		x	

Es importante el uso de herramientas de monitoreo tanto de sistema operativo como de la base por eso debe tenerse herramientas que faciliten esta tarea ya que un DBA no solo debe realizar tareas de monitoreo sino también de generación de reportes, mantenimiento de datos y otras, la capacidad de estas herramientas viene medida por su facilidad de uso, el tiempo que disminuirá en

el monitoreo con el uso de la herramienta, la capacidad de emitir alarmas, si es o no multiplataforma, su facilidad de instalación y su costo.

Para mantener la disponibilidad de la información también es necesario mantener la disponibilidad de los equipos con sus respectivos mantenimientos preventivos periódicos, asimismo como todo equipo eléctrico es susceptible a fallos por lo cual se debe mantener un respaldo de energía en caso de problemas, si bien los equipos son servidores que su tecnología ayudan a autoprotegerse también es recomendable mantener la continuidad y calidad de energía que ingrese a los servidores, dando mantenimiento a las redes eléctricas, a los UPS y generadores.

Es importante destacar que mantener un control adecuado de los accesos a la base de datos nos ayuda a preservar los principios básicos de la información por esto es que se debe tener el inventario de los usuarios que acceden a la base de datos, los permisos que tienen sobre los datos, eliminar el uso de usuarios genéricos cada usuario debe acceder con su información y dejar un registro de las operaciones que realizo en su ingreso a sesión.

Mantener siempre los respaldos al día y realizar comprobaciones de los mismos, se encontró que la metodología para realizar respaldos no se ha actualizado desde hace 10 años por lo cual se sugiere revisar e implementar nuevos métodos de respaldo, como son los respaldos incrementales para no necesitar tanto almacenamiento ya que en este momento están usando por cada respaldo de la base 20GB de espacio en el disco duro, así también se

recomienda usar algún método automático de respaldo fuera del servidor para mantener los respaldos fuera del servidor de producción.

Se cambió la configuración de la base de datos volviendo a crearla una vez realizado el cambio se hicieron las pruebas y se verificó que la solución cumplió con el objetivo ver figuras 3.16 y 3.17 de que la información este siempre disponible para la búsqueda y que los usuarios no vuelvan a ingresar la información con lo cual mantendríamos la integridad.

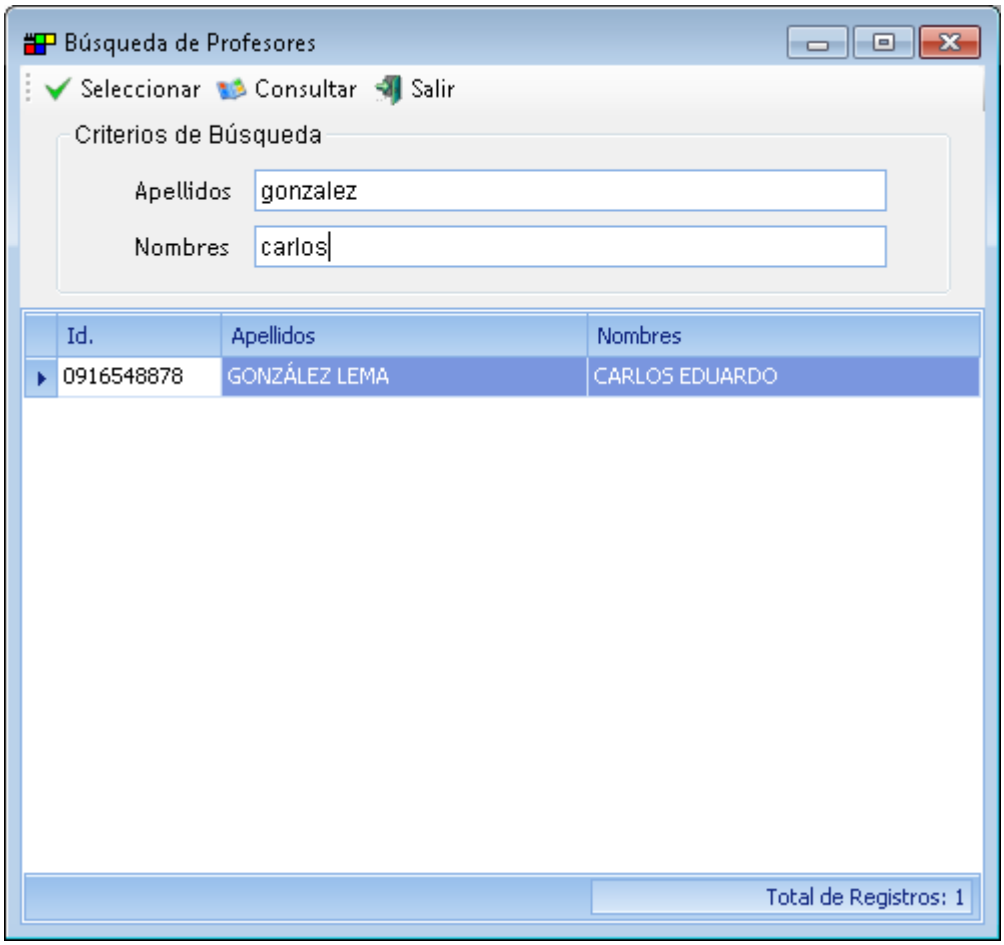


Figura 3.16 Consulta exitosa de apellidos y nombres en minúsculas y sin acentos

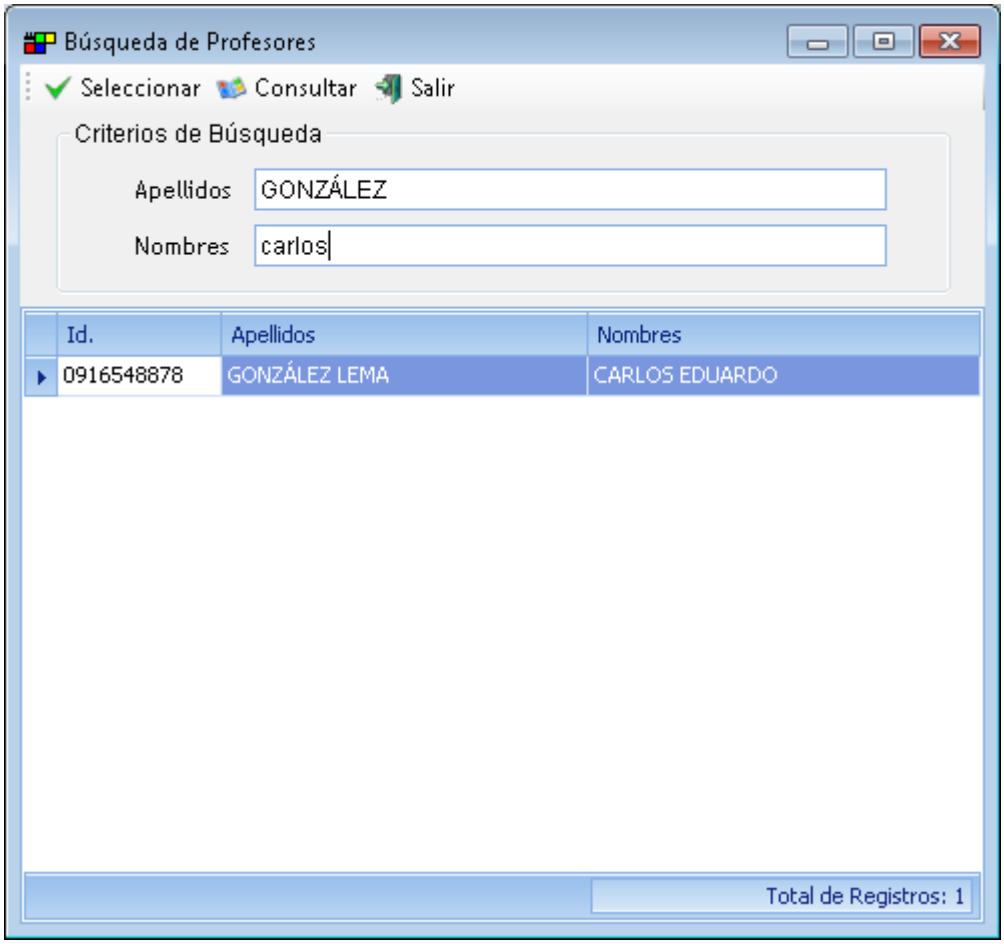


Figura 3.17 Consulta exitosa de apellidos con mayúsculas y nombres en minúsculas y acentos

Es importante mantener siempre un registro de las transacciones registradas en las tablas sobre todo de las que son críticas el uso de los disparadores es un buen método, pero esto genera que los log crezcan demasiado, se debe buscar un método para realizar la migración de estos datos para realizar minería de datos y la creación de cubos de datos o usar herramientas como IBM DB2 with BLU acceleration que es la nueva tecnología que aprovecha la computación in-memory, ofreciendo un extraordinario rendimiento y procesamiento de datos [8].

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Este trabajo ayudo a solucionar los problemas de búsqueda de información que estaba comenzando a causar problemas en las bases de datos, generando ya otros problemas más graves como falta de confiabilidad de la información.

2. La elección de una buena herramienta de monitoreo es esencial para cuidar el funcionamiento de los servidores y las bases de datos.

3. Se debe mantener los modelos de las bases de datos siempre actualizados y documentados para así poder llevar un control del flujo de la información que se maneja.

4. Es necesario contar siempre con un plan de trabajo y probarlo antes de realizar cualquier cambio en un ambiente de producción.

5. Se debe manejar en los sistemas las validaciones y las ayudas necesarias para evitar el ingreso erróneo de la información.

6. Se debe realizar un análisis de los requerimientos con el equipo de programación antes de crear una base de datos, para así poder evaluarlos y definir los parámetros iniciales con los que se los va a crear.

RECOMENDACIONES

1. Se debe aplicar las actualizaciones y parches estables en los sistemas periódicamente para mantener la seguridad de los programas y sistemas operativos.

2. La institución debe definir una política para realizar respaldos fuera de línea en intervalos de tiempo más cortos.

3. Es necesario documentar los registros de cambios y los respaldos de autorizaciones de los encargados para el uso en futuras auditorias.

4. Se debería considerar el uso de los servicios web del registro civil para cargar automáticamente la información personal y evitar información errónea.

BIBLIOGRAFÍA

[1] Estándar Internacional ISO/IEC 27001,Tecnología de la Información - Técnicas de seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos. Obtenido de http://www.iso27000.es/download/doc_iso27000_all.pdf, 15 de octubre de 2005.

[2] Laudon, K. C., & Laudon, J. P, Sistemas de información gerencial, Pearson, 2012

[3] Silberschatz, A., Korth, H. F., & Sudarshan, S, FUNDAMENTOS DE BASES DE DATOS, Concepción Fernández Madrid, 2002

[4] IBM, User, user ID and group naming rules. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.dbobj.doc/doc/c0007248.html?lang=en, Fecha de consulta abril del 2015

[5] IBM, Automatic maintenance. Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.dbobj.doc/doc/c0021757.html?cp=SSEPGG_10.5.0%2F3-0-0-2-1&lang=en, Fecha de consulta junio del 2015

[6] Mossberg, D, Modelos de programación en ASP.NET: Web Forms, MVC y Web Pages, Obtenido de http://blogs.msdn.com/b/daniem/archive/2012/05/10/modelos-de-programacion-en-aspnet.aspx, Fecha de consulta julio del 2015

[7] IBM, Funciones escalares DECRYPT_BIN y DECRYPT_CHAR, Obtenido de http://www-01.ibm.com/support/knowledgecenter/SSEPGG_9.7.0/com.ibm.db2.luw.sql.ref.doc/doc/r0004210.html?cp=SSEPGG_9.7.0%2F2-10-3-2-44&lang=es, Fecha de consulta abril del 2015

[8] IBM, BLU Acceleration. Obtenido de http://www-01.ibm.com/software/data/db2/linux-unix-windows/db2-blu-acceleration/, Fecha de consulta abril del 2015