UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

MAESTRÍA EN GESTIÓN DE BASES DE DATOS

Tema: LAS CARACTERÍSTICAS DE SQL SERVER 2005 Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DATOS DE LA DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA UTA

Trabajo de Investigación, previo a la obtención del Grado Académico de Magíster en Gestión de Bases de Datos

Autor: Ing. Alex Ricardo Paucar Medina

Director: Ing. Edwin Hernando Buenaño Valencia, Mg.

Ambato – Ecuador

2018

A la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

El Tribunal receptor del Trabajo de Investigación presidido por la Ingeniera Elsa Pilar Urrutia Urrutia Magister, e integrado por los señores Ingeniero Edison Homero Álvarez Mayorga Magister, Ingeniero Clay Fernando Aldás Flores Magister, Ingeniero Carlos Israel Núñez Miranda Magister, designados por la Unidad Académica de Titulación de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, para receptar el Trabajo de Investigación con el tema: "LAS CARACTERÍSTICAS DE SQL SERVER 2005 Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DATOS DE LA DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA UTA.", elaborado y presentado por el señor Ingeniero Alex Ricardo Paucar Medina, para optar por el Grado Académico de Magister en Gestión de Bases de Datos; una vez escuchada la defensa oral del Trabajo de Investigación el Tribunal aprueba y remite el trabajo para uso y custodia en las bibliotecas de la UTA.

Ing. Elsa Pilar Urrutia Urrutia, Mg.
Presidente del Tribunal

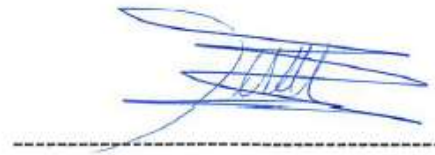
Ing. Edison Homero Álvarez Mayorga, Mg.
Miembro del Tribunal

Ing. Clay Fernando Aldás Flores, Mg.
Miembro del Tribunal

Ing. Carlos Israel Núñez Miranda, Mg.
Miembro del Tribunal

AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

La responsabilidad de las opiniones, comentarios y críticas emitidas en el Trabajo de Investigación presentado con el tema: LAS CARACTERÍSTICAS DE SQL SERVER 2005 Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DATOS DE LA DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA UTA**,** le corresponde exclusivamente a: Ingeniero Alex Ricardo Paucar Medina, Autor bajo la Dirección de Ingeniero Edwin Hernando Buenaño Valencia, Magister, Director del Trabajo de Investigación; y el patrimonio intelectual a la Universidad Técnica de Ambato.



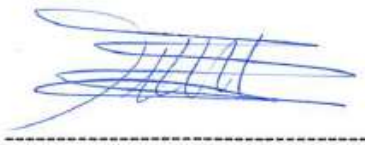
Ing. Alex Ricardo Paucar Medina
C.C.0604646117
AUTOR

Ing. Edwin Hernando Buenaño Valencia, Mg.
C.C. 1802662955
DIRECTOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que el Trabajo de Investigación, sirva como un documento disponible para su lectura, consulta y procesos de investigación, según las normas de la Institución.

Cedo los Derechos de mi trabajo, con fines de difusión pública, además apruebo la reproducción de éste, dentro de las regulaciones de la Universidad.



Ing. Alex Ricardo Paucar Medina
C.C. 0604646117

ÍNDICE GENERAL

PORTADA i
A la Unidad Académica de Titulación ii
AUTORÍA DEL TRABAJO DE INVESTIGACIÓN iii
DERECHOS DE AUTOR iv
ÍNDICE GENERAL v
ÍNDICE DE GRÁFICOS ix
ÍNDICE DE IMÁGENES xii
ÍNDICE DE CUADROS xiii
ÍNDICE DE TABLAS xiv
INTRODUCCIÓN 1
CAPÍTULO I 2
EL PROBLEMA DE INVESTIGACIÓN 2
1.1. Tema de investigación 2
1.2. Planteamiento del problema 2
1.2.1. Contextualización 2
1.2.1.1. Macro contextualización 2
1.2.1.2. Meso contextualización 2
1.2.1.3. Micro contextualización 3
1.2.2. Análisis crítico 3
1.2.3. Prognosis 4
1.2.4. Formulación del problema 4
1.2.5. Interrogantes 4
1.2.6. Delimitación del objeto de investigación 5
1.2.6.1. Delimitación espacial 5
1.2.6.2. Delimitación temporal 5
1.3. Justificación 5
1.4. Objetivos 6
CAPÍTULO II 7
MARCO TEÓRICO 7
2.1 Antecedentes investigativos 7
2.2 Fundamentación filosófica 8

2.3 Fundamentación legal 8
2.4 Categorías fundamentales 9
2.5 Hipótesis 33
2.6 Señalamiento de variables 33
CAPÍTULO III 34
METODOLOGÍA 34
3.1. Enfoque 34
3.2. Modalidad básica de investigación 34
3.3. Nivel o tipo de investigación 34
3.4. Población y muestra 35
3.5. OPERACIONALIZACIÓN DE LAS VARIABLES 36
3.1.1. Variable independiente: Características de SQL Server 2005. 36
3.1.2. Variable dependiente: Seguridad de los datos. 37
3.6. Recolección de información 38
3.7. Procesamiento y análisis 39
CAPITULO IV 40
ANÁLISIS E INTERPRETACIÓN DE RESULTADOS 40
4.1 Análisis e interpretación de resultados 40
4.2 Verificación de la hipótesis 46
4.2.1 Modelo estadístico 46
4.2.2 Definición del nivel de significancia 46
4.2.3 Frecuencias observadas 47
4.2.4 Frecuencias esperadas 48
4.2.5 Prueba Chi – Cuadrado 49
4.2.6 Especificación de los grados de libertad 49
4.2.7 Decisión estadística 50
CAPÍTULO V 51
CONCLUSIONES Y RECOMENDACIONES 51
5.1 Conclusiones 51
5.2 Recomendaciones 52
CAPÍTULO VI 53
LA PROPUESTA 53

6.1 Datos informativos 53
6.1.1 Título de la propuesta 53
6.1.2 Institución ejecutora 53
6.1.3 Beneficiarios 53
6.1.4 Ubicación 53
6.1.5 Equipo técnico responsable 53
6.2 Antecedentes de la propuesta 54
6.3 Justificación 54
6.4 Objetivos 55
6.5 Análisis de factibilidad 55
6.6 Fundamentación 56
6.6.1 Características de SQL Server 2016 Enterprise 56
6.6.1.1 Seguridad a nivel de fila 56
6.6.1.2 Always Encrypted 56
6.6.1.3 Enmascaramiento de datos dinámicos 57
6.6.1.4 Auditoría 57
6.6.1.5 Administración extensible de claves 58
6.6.1.6 Roles definidos por el usuario 58
6.6.1.7 Bases de datos independientes 59
6.6.1.8 Cifrados para copias de seguridad 59
6.6.1.9 Comparativa entre SQL Server 2005 y SQL Server 2016 60
6.6.2 Migración de base de datos 61
6.6.2.1 Tipos de migración de base de datos 62
6.6.2.2 Proceso de migración 64
6.6.2.3 Nivel de compatibilidad SQL Server 64
6.7 Metodología 66
6.7.1 Guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 66
6.7.1.1 Introducción 66
6.7.1.2 Alcance 67
6.7.1.3 Responsables 67
6.7.1.4 Definiciones 67

6.7.1.5 Procesos..... 67
6.7.2 Aplicación de la guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016, en las bases de datos de la DITIC de la UTA..... 80
6.7.3 Vulnerabilidades en la DITIC y SQL Server 2016..... 101
6.8 Conclusiones y recomendaciones 107
6.8.1 Conclusiones..... 107
6.8.2 Recomendaciones 107
Anexos..... 112

ÍNDICE DE GRÁFICOS

Gráfico 1. Relación Causa – Efecto 4
Gráfico 2. Inclusiones conceptuales – Organizador lógico de variables 10
Gráfico 3. Utilización exploit “mssql_login” 22
Gráfico 4. Configuración exploit “mssql_login” 23
Gráfico 5. Ejecución del exploit “mssql_login” 23
Gráfico 6. Ejecución del exploit “mssql_login” – caso exitoso 23
Gráfico 7. Utilización del exploit “mssql_payload” 24
Gráfico 8. Configuración del exploit “mssql_payload” 24
Gráfico 9. Parámetros configurados del exploit “mssql_payload” 25
Gráfico 10. Ejecución del exploit “mssql_payload” 25
Gráfico 11. Ejecución del exploit “mssql_payload” – caso exitoso 26
Gráfico 12. Ejecución comando ps 26
Gráfico 13. Listar programas instalados 27
Gráfico 14. Ejecución de comando 27
Gráfico 15. Usuarios del servidor local 27
Gráfico 16. Creación de usuarios desde línea de comandos 28
Gráfico 17. Asignación de usuario al grupo administradores 28
Gráfico 18. Utilización de “ms09_004_sp_replwritetovarbin” 29
Gráfico 19. Parametrización de “ms09_004_sp_replwritetovarbin” (A) 29
Gráfico 20. Parametrización de “ms09_004_sp_replwritetovarbin” (B) 30
Gráfico 21. Configuración de “ms09_004_sp_replwritetovarbin” 30
Gráfico 22. Ejecución de “ms09_004_sp_replwritetovarbin” 31
Gráfico 23. Listar archivos 31
Gráfico 24. Descargar archivos 32
Gráfico 25. Cargar archivos 32
Gráfico 26. Ejecución de comandos 32
Gráfico 27. Elevación de privilegios 33
Gráfico 28. Estándares SQL Server 2005 40
Gráfico 29. Exigencia de seguridad SQL Server 2005 41
Gráfico 30. Desactualización SQL Server 2005 42

Gráfico 31. Ataque informático 43
Gráfico 32. Vulnerabilidades SQL Server 2005 44
Gráfico 33. Medidas y control de seguridad 45
Gráfico 34. Zona de aceptación y rechazo según Chi – Cuadrado 50
Gráfico 35. Configuración COLLATE 73
Gráfico 36. Modo de usuario 74
Gráfico 37. Ejecución procedimiento 79
Gráfico 38. Cambio cadena conexión 87
Gráfico 39. Nueva instalación - SQL Server 2016 88
Gráfico 40. Selección de componentes - SQL Server 2016 89
Gráfico 41. Cuentas de servicio - SQL Server 2016 89
Gráfico 42. Configuración Collation - SQL Server 2016 90
Gráfico 43. Finalización de instalación - SQL Server 2016 90
Gráfico 44 Comprobación de Service Pack - SQL Server 2005 91
Gráfico 45. Respaldo utamatico - SQL Server 2005 91
Gráfico 46. Respaldo dbTutorias - SQL Server 2005 92
Gráfico 47. Respaldo dbPracticas - SQL Server 2005 92
Gráfico 48. Respaldo dbDistributivo - SQL Server 2005 93
Gráfico 49. Instalación - SQL Server 2008 R2 93
Gráfico 50. Selección de componentes - SQL Server 2008 R2 94
Gráfico 51. Finalización de instalación - SQL Server 2008 R2 94
Gráfico 52. Comprobación de Service Pack - SQL Server 2008 R2 94
Gráfico 53. Bases de datos restauradas – SQL Server 2008 R 95
Gráfico 54. Restauración dbPracticas - SQL Server 2016 96
Gráfico 55. Restauración dbTutorias - SQL Server 2016 96
Gráfico 56. Restauración dbDistributivo - SQL Server 2016 97
Gráfico 57. Restauración utamatico - SQL Server 2016 97
Gráfico 58. Usuarios huérfanos - SQL Server 2016 98
Gráfico 59. Inicios de sesión - SQL Server 2005 98
Gráfico 60. Ejecución script transferencia de logins 99
Gráfico 61. Script de logins 99
Gráfico 62. Asignación de usuarios huérfanos 100

Gráfico 63. Utilización de exploit “mssql_payload” - SQL Server 2016 101
Gráfico 64. Parametrizar “mssql_payload” - SQL Server 2016 102
Gráfico 65. Opciones configuradas “mssql_payload” - SQL Server 2016 102
Gráfico 66. Ejecución de "mssql_payload" - SQL Server 2016 103
Gráfico 67. Resultado ejecución "mssql_payload" - SQL Server 2016 103
Gráfico 68. Utilización de "ms09_004_sp_replwritetovarbin" 104
Gráfico 69. Seteo "ms09_004_sp_replwritetovarbin" (A) 105
Gráfico 70. Seteo "ms09_004_sp_replwritetovarbin" (B) 105
Gráfico 71. Parámetros seteados "ms09_004_sp_replwritetovarbin" 105
Gráfico 72. Ejecutar "ms09_004_sp_replwritetovarbin" 105

ÍNDICE DE IMÁGENES

Imagen 1. Niveles de seguridad 15

ÍNDICE DE CUADROS

Cuadro 1. Versiones de SQL Server 13
Cuadro 2. Boletines de seguridad – SQL Server 2005..... 20
Cuadro 3. Población..... 35
Cuadro 4. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE 36
Cuadro 5. OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE ... 37
Cuadro 6. Recolección de la información. 38
Cuadro 7. Estándares SQL Server 2005..... 40
Cuadro 8. Exigencia de seguridad SQL Server 2005..... 41
Cuadro 9. Desactualización SQL Server 2005..... 42
Cuadro 10. Ataque informático..... 43
Cuadro 11. Vulnerabilidades SQL Server 2005..... 44
Cuadro 12. Medidas de control y seguridad..... 45
Cuadro 13. Frecuencias observadas 47
Cuadro 14. Frecuencias esperadas (1)..... 48
Cuadro 15. Frecuencias esperadas (2)..... 48
Cuadro 16. Cálculo del Chi – Cuadrado 49
Cuadro 17. Comparativa SQL Server 2005 – SQL Server 2016 60
Cuadro 18. Matriz de planificación..... 69
Cuadro 19. Listado de base de datos..... 80
Cuadro 20. Especificaciones software 81
Cuadro 21. Especificaciones hardware 82
Cuadro 22. Planificación de migración..... 82
Cuadro 23. Tipos de datos descontinuados..... 84
Cuadro 24. JOINS NO CALIFICADOS..... 85
Cuadro 25. Clausula Order By..... 86
Cuadro 26. Objetos externos..... 100

ÍNDICE DE TABLAS

Tabla 1. Tabla de distribución de frecuencias..... 49
Tabla 2. Niveles de compatibilidad SQL Server..... 65
Tabla 3. Palabras reservadas SQL Server 65

AGRADECIMIENTO

Un especial agradecimiento a Dios por ser mi amparo y mi fortaleza en todo momento, gracias Dios porque para ti todo es posible.

A mis padres por el cariño, apoyo y sabios consejos.

A mi Esposa e Hijo, por el apoyo brindado a lo largo de esta meta.

A la Universidad Técnica de Ambato por ofrecerme nuevas oportunidades que me han permitido mejorar profesionalmente.

Gracias al Ing. Hernando Buenaño y al Ing. Robert Vaca por el apoyo incondicional para el desarrollo del presente trabajo de investigación.

Alex Ricardo Paucar Medina

DEDICATORIA

Este trabajo de investigación lo dedico principalmente a Dios por ser el pilar fundamental de mi vida y por permitirme culminar esta etapa de mi vida profesional.

A mi hijo Gael por ser la fuente de inspiración y por motivarme a realizar mi mayor esfuerzo.

Alex Ricardo Paucar Medina

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO
MAESTRÍA EN GESTIÓN DE BASES DE DATOS

TEMA:

"LAS CARACTERÍSTICAS DE SQL SERVER 2005 Y SU INCIDENCIA EN LA SEGURIDAD DE LOS DATOS DE LA DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN DE LA UTA"

AUTOR: Ing. Alex Ricardo Paucar Medina
DIRECTOR: Ing. Edwin Hernando Buenaño Valencia, Mg.
FECHA: 23 de noviembre de 2017

RESUMEN EJECUTIVO

El presente trabajo de investigación tiene por objeto determinar la incidencia de las características de SQL Server 2005 en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación (DITIC) de la Universidad Técnica de Ambato (UTA).

La DITIC es la encargada del control, almacenamiento y seguimiento de la información generada por los sistemas de información de la universidad, gestión que se la realiza casi en su totalidad a través del Sistema Gestor de Base de Datos (SGBD) SQL Server 2005, cuyas características no permiten salvaguardar la integridad, consistencia y disponibilidad de los datos en la DITIC.

Se detectaron vulnerabilidades en SQL Server 2005 que comprometen la seguridad de los datos en la DITIC, vulnerabilidades que pueden ser aprovechadas por atacantes para causar daños en los datos de la dirección.

Se plantea como propuesta de solución al problema planteado, una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 en la DITIC de la UTA; que direccione y asegure de alguna manera el éxito de una migración, y por ende permita la migración a SQL Server 2016 de las bases de datos de la DITIC.

Descriptores: Base de Datos, Migración de Base de Datos, Seguridad de Base de Datos, Auditoría de Base de Datos, Vulnerabilidades, Amenazas, SQL Server, ETL, Guía, Traslado de Datos.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL / DIRECCIÓN DE POSGRADO
MAESTRÍA EN GESTIÓN DE BASES DE DATOS

THEME:

"THE CHARACTERISTICS OF SQL SERVER 2005 AND ITS INCIDENCE IN THE DATA SECURITY OF THE DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY OF THE UTA"

AUTHOR: Ing. Alex Ricardo Paucar Medina
DIRECTED BY: Ing. Edwin Hernando Buenaño Valencia, Mg.
DATE: November 23, 2017.

EXECUTIVE SUMMARY

The purpose of this research work is to determine the incidence of the SQL Server 2005 characteristics in the data security of the Department of Information and Communication Technology (DITIC) of the Technical University of Ambato (UTA).

The DITIC, is responsible of the control, storage and monitoring of the information generated by the information systems of the university, management that is carried out almost entirely through the Database Management System (SGBD) SQL Server 2005, whose characteristics do not allow to safeguard the integrity, consistency and availability of data in the DITIC.

Vulnerabilities were detected in SQL Server 2005 that compromise the security of the data in the DITIC, vulnerabilities that can be exploited by attackers to cause damage to the address data.

It is proposed as a solution proposal to the problem, a guide for secure data migration, from SQL Server 2005 to SQL Server 2016 in the DITIC of the UTA; that directs and assures in some way the success of a migration, and therefore allows the migration to SQL Server 2016 of the databases of the DITIC.

Keywords: Database, Database Migration, Database Security, Database Audit, Vulnerabilities, Threats, SQL Server, ETL, Guide, Data Transfer.

INTRODUCCIÓN

La presente investigación es de mucha importancia porque se analizará el rendimiento, escalabilidad, disponibilidad, seguridad y demás características de SQL Server 2005; y su incidencia en la seguridad de los datos de la DITIC, con la finalidad de plantear una propuesta factible que satisfaga las necesidades de esta Dirección y por ende de la Universidad Técnica de Ambato.

En el CAPÍTULO I se identifica el problema a investigar, además se plantea la justificación y los objetivos.

En el CAPÍTULO II se presentan los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de variables.

En el CAPÍTULO III se determina la metodología de investigación a utilizar, el enfoque, la modalidad básica de la investigación, el tipo de investigación, la población y muestra.

En el CAPÍTULO IV se realiza el análisis e interpretación de los resultados obtenidos de las diversas técnicas y métodos utilizados en la presente investigación (Entrevistas, Encuestas etc.)

En el CAPÍTULO V se plantea las conclusiones y recomendaciones de la investigación del problema planteado.

En el CAPÍTULO VI se desarrolla la propuesta, la misma que contiene: antecedentes, objetivos de la propuesta, análisis de factibilidad, fundamentación, metodología de desarrollo de la propuesta, conclusiones y recomendaciones.

Finalmente se encuentra la bibliografía y los respectivos anexos.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. Tema de investigación

Las características de SQL Server 2005 y su incidencia en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

1.2. Planteamiento del problema

1.2.1. Contextualización

1.2.1.1. Macro contextualización

Desde la década de los sesenta y con más énfasis en los últimos 20 años, las universidades en el mundo han puesto énfasis en que la información originada en sus operaciones y actividades es un activo sumamente valioso y el mejor acceso a la misma se ha convertido en un ingrediente para la evolución de la educación (Barcos, 2008). Lo que ha originado una mayor inversión en recursos para mejorar los sistemas de información, el rendimiento y accesibilidad de los datos, y evitar ataques que vulneren la seguridad de los mismos.

1.2.1.2. Meso contextualización

Desde el año 2009 organismos de control como el CONESUP actualmente SENESCYT, CES, CEAACES y SENPLADES han solicitado a las Universidades del Ecuador información referente a estudiantes, docentes, administrativos, infraestructura, vinculación con la sociedad, investigación, servicios universitarios, graduados, carreras, obligando a éstas a mejorar sus sistemas de información, frente a estos nuevos requerimientos.

1.2.1.3. Micro contextualización

La Universidad Técnica de Ambato con la finalidad de poder cumplir con los requerimientos solicitados por varios organismos de control, se encuentra integrando sus bases de datos, desarrollando nuevos sistemas de información, pero con una visión integrada, evaluando (el rendimiento, la tolerancia a fallos, la capacidad de procesamiento, etc.) sus SGBD, dejando en evidencia las características en la seguridad de la información y el rendimiento.

1.2.2. Análisis crítico

La DITIC utiliza a SQL Server 2005 para la gestión de los datos académicos de la Universidad Técnica de Ambato, SGBD que a partir de abril de 2016 dejó de recibir soporte (actualizaciones y revisiones de seguridad muy importantes); exponiendo a las bases de datos gestionadas por mencionado motor a posibles ataques informáticos exitosos y robo de información.

La integración de los sistemas de información académica y el incremento o evolución de los requerimientos en la universidad han ocasionado el deterioro en el rendimiento del SGBD SQL Server 2005, se ha hecho notorio el aumento de los tiempos de respuestas en el procesamiento de información; mayor consumo de hardware en operaciones de: consulta, actualización, eliminación e inserción de datos, entre otras.

SQL Server 2005 es un motor muy potente desarrollado bajo las exigencias de su época, almacenamiento, procesamiento, capacidad de respuesta, entre otras; capacidades que con el tiempo dejan en evidencia su discontinuidad y han obligado a la DITIC a solventar de alguna manera esta problemática incrementando recursos (hardware y software) en el mantenimiento de esta versión de SGBD utilizada para la gestión de los datos académicos.

En el gráfico 1, se ilustra el árbol del problema.

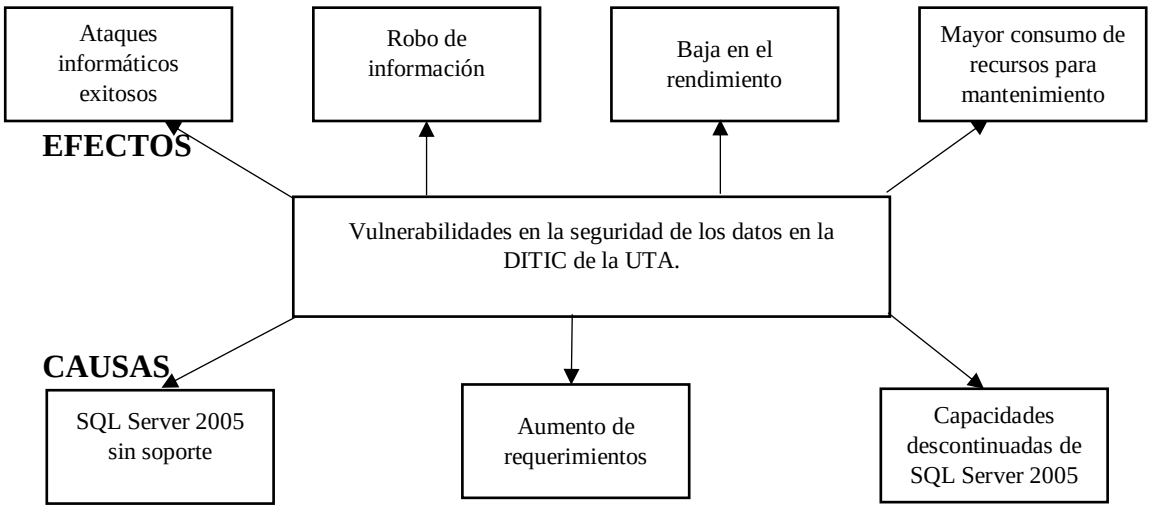


Gráfico 1. Relación Causa – Efecto
Elaborado por: Investigador

1.2.3. Prognosis

Si el problema persiste se puede tener consecuencias más graves como: robo y copias no autorizadas de los datos, adulteración, sabotaje, fallas críticas en el software y hardware; que concluirían en la suspensión de los servicios académicos proporcionados por la DITIC de la UTA.

1.2.4. Formulación del problema

¿Incide las características de SQL Server 2005 en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA?

1.2.5. Interrogantes

¿Cuáles son las características de SQL Server 2005?
¿Cuáles son las vulnerabilidades en la seguridad de los datos de la DITIC?
¿Se puede implementar una solución factible al problema planteado?

1.2.6. Delimitación del objeto de investigación

Campo: Base de datos
Área: Características de SQL Server 2005
Aspecto: Seguridad de los datos de la DITIC

1.2.6.1. Delimitación espacial

Dirección de Tecnología de Información y Comunicación de la UTA.

1.2.6.2. Delimitación temporal

Desde noviembre 2016 a noviembre 2017.

1.3. Justificación

La información es parte fundamental del desarrollo de toda organización y su correcta gestión va de la mano con la utilización de herramientas tecnológicas adecuadas, herramientas que con el paso del tiempo pueden descontinuarse y no ofrecer las garantías que años atrás lo hicieron. En el caso de los SGBD, es de vital importancia que éstos brinden la escalabilidad y seguridad requerida por la organización.

Hoy en día la diversidad de entornos, las múltiples plataformas y la evolución de las redes; han provocado que cada vez sea más complejo el resguardo de los datos; los sistemas de información tienen que enfrentar constantes ataques informáticos. Las empresas proveedoras de software invierten más recursos en la seguridad de sus productos, reflejándose en actualizaciones o desarrollo de nuevas versiones.

La presente investigación será de mucho beneficio e interés, porque se buscará determinar la incidencia de las características de SQL Server 2005 en la seguridad de los datos de la DITIC de la UTA.

El proyecto es factible técnicamente porque, la DITIC cuenta con el hardware y el licenciamiento necesario del software a utilizar, en cuanto a la investigación se cuenta con las facilidades de la información por parte del personal de gestión como por las autoridades universitarias.

El proyecto es factible económicamente porque, se dispone de los recursos y el equipo necesario para la investigación.

EL proyecto de investigación es factible operativamente porque, basado en la experiencia del investigador y en los conocimientos adquiridos en gestión de bases de datos, la investigación se la puede realizar.

1.4. Objetivos

1.4.1. Objetivo general

Determinar la incidencia de las características de SQL Server 2005 en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

1.4.2. Objetivos específicos

- Analizar las características de SQL Server 2005.
- Determinar las vulnerabilidades en la seguridad de los datos de la DITIC.
- Implementar una solución factible al problema planteado.

CAPÍTULO II

MARCO TEÓRICO

2.1 Antecedentes investigativos

Luego de revisar información del problema investigado se encontró la siguiente información:

En la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, en el año 2012, la investigadora Susana Caraguay, investigó en la empresa VSYSTEMS, el tema: "METODOLOGÍA PARA MIGRACIÓN DE DATOS QUE PERMITA ASEGURAR Y CONSERVAR LA INTEGRIDAD Y CONSISTENCIA DE LA INFORMACIÓN ADMINISTRADA POR LA EMPRESA VSYSTEMS", la investigadora hizo una investigación de campo en la empresa con el objetivo de establecer una metodología de migración de datos que asegure la conservación de integridad y consistencia de información administrada por la empresa VSYSTEMS, llegando a la conclusión de que la aplicación de una metodología desarrollada a medida permite ahorro de costos, ya que reduce tiempos improductivos de los sistemas asociados a la base de datos migrada.

En la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, en el año 2014, el investigador Milton Navas, investigó en la Universidad de las Fuerzas Armadas (ESPE) extensión Latacunga, el TEMA; "LA ADMINISTRACIÓN DE LOS SGBD'S DE LOS SISTEMAS DE INFORMACIÓN Y SU INCIDENCIA EN EL CONTROL DE LAS SEGURIDADES DE LAS BASES DE DATOS DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE EXTENSIÓN LATACUNGA", llegando a la conclusión de que los sistemas de información de la ESPE extensión Latacunga deberían ser migrados a herramientas de última generación o SGBD's que dispongan de seguridades propias.

2.2 Fundamentación filosófica

La presente investigación se enmarca en el paradigma Critico Propositivo, es crítico porque realiza un análisis crítico del problema, y es Propositivo porque busca proponer una solución factible al problema.

2.3 Fundamentación legal

La Ley del Sistema Nacional de Registro de Datos públicos en el Capítulo II Principios Generales del Registro de Datos públicos establece:

- Art. 4. "Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando ésta o éste provee toda la información".

- Art. 26. "Toda base informática de datos debe contar con su respectivo archivo de respaldo, cumplir con los estándares técnicos y plan de contingencia que impidan la caída del sistema, robo de datos, modificación o cualquier otra circunstancia que pueda afectar la información pública".

En el reglamento de estudios de posgrado (CEPOS) de la Universidad Técnica de Ambato, en el Capítulo II De la Organización, establece:

- Art. 75. "Para optar por el Título de Diploma Superior, Especialista o el grado académico de Magíster, los estudiantes tendrán que realizar un trabajo de investigación para cada caso y sustentarlo ante un tribunal. (Res. 881-CU-P-2009, de julio 15/2009)"

- Art. 76. “Previo a la realización del trabajo de investigación para Titulación o Graduación se deberá planificar el mismo mediante un Proyecto de Trabajo Investigación para Titulación o Graduación, de acuerdo con el esquema de elaboración de Proyectos de Investigación aprobado por el H. Consejo Universitario…”

2.4 Categorías fundamentales

Las categorías fundamentales se ilustran en el gráfico 2.

Categorías de la variable independiente

Base de datos relacionales

Una base de datos relacional consiste en un conjunto de tablas, a cada una de las cuales se le asigna un nombre exclusivo. Cada fila de la tabla representa una relación entre un conjunto de valores. Dado que cada tabla es un conjunto de dichas relaciones, hay una fuerte correspondencia entre el concepto de tabla y el concepto matemático de relación, del que toma su nombre el modelo de datos relacional (Silberschatz, Korth & Sudarshan, s.f., p.53).

Jiménez (2015), señala que el modelo de datos relacional consta de 3 aspectos fundamentales:

> Estructura de los datos: compuesta por dominio, atributos, tuplas (registros o filas) y relaciones.
>
> Integridad de los datos: reglas que se aplican a relaciones base e informan al Sistema Gestor de Base de Datos de ciertas restricciones.
>
> Manipulación de datos: la manipulación de relaciones se realiza a través de un lenguaje de consulta, que consiste en un lenguaje que utiliza el usuario para manejar la información (p. 7).

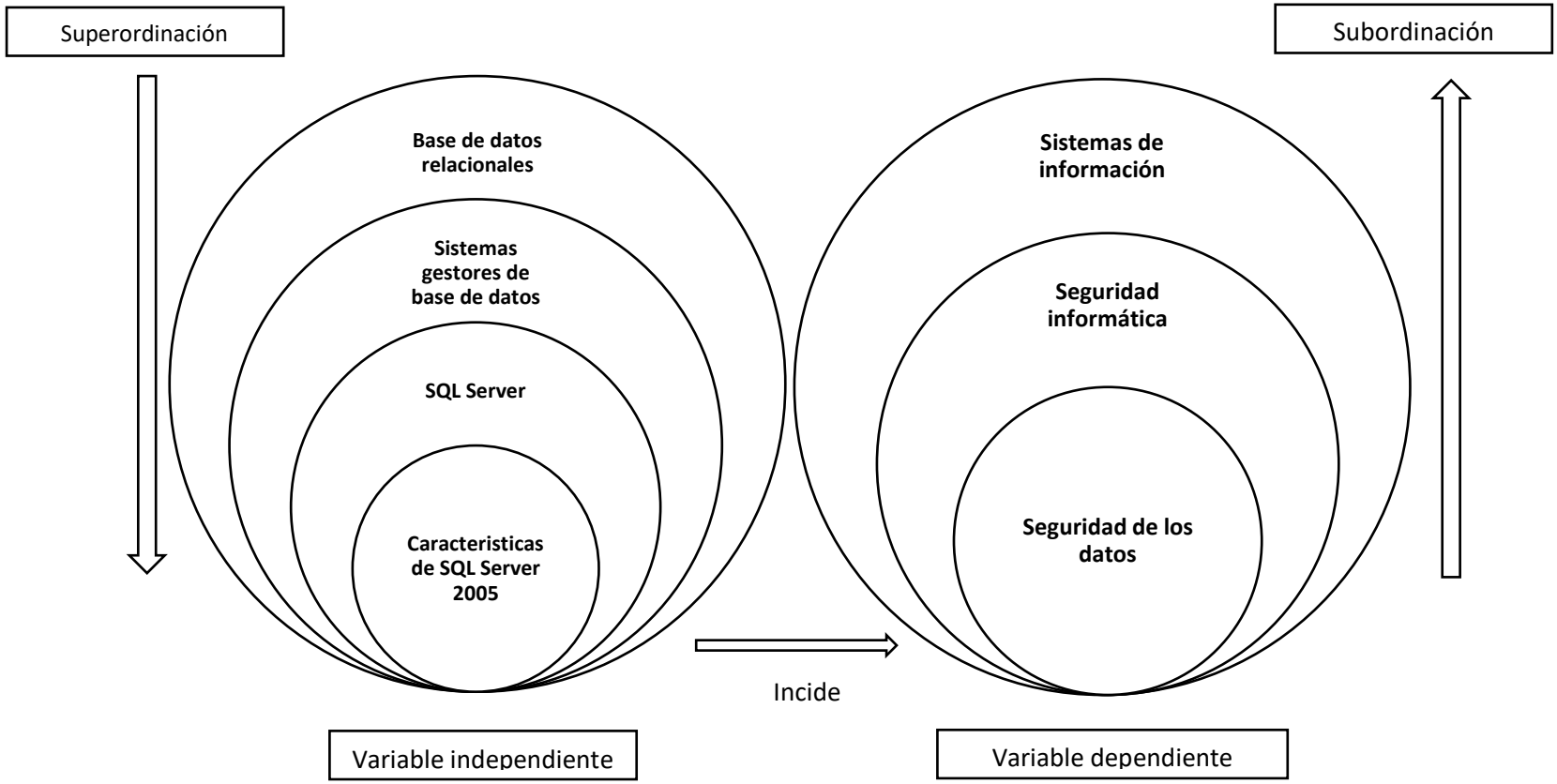


Gráfico 2. Inclusiones conceptuales – Organizador lógico de variables
Elaborado por: Investigador

Básicamente un modelo relacional es un conjunto de tablas relacionadas entre sí, cuya estructura de datos está compuesta por: dominio, atributos, tuplas y relaciones; su estructura está orientada a la integridad de datos.

Sistemas gestores de base de datos

Heredero y López (2004), definen a los SGBD como:

> Un conjunto de programas que gestionan la estructura de la base de datos y controlan los posibles accesos de los datos allí albergados. Los sistemas gestores de bases de datos permiten compartir los datos de una determinada base de datos a un conjunto de aplicaciones o usuarios. El sistema gestor de base de datos es en realidad un intermediario entre el usuario y la base de datos. Traduce los requerimientos del usuario del lenguaje complejo que se requiere para conseguir esa información (p. 272).

Cobo (s.f.), define a los SGBD como:

> Un software o conjunto de programas que permite crear y mantener una base de datos. El SGBD actúa como interfaz entre los programas de aplicación (usuarios) y el sistema operativo. El Objetivo Principal de un SGBD es proporcionar un entorno eficiente a la hora de almacenar y recuperar la información de la base de datos (p. 7).

Un SGBD es un software que permite al usuario interactuar con la base de datos; facilita el acceso, brinda seguridad, permite operaciones de almacenamiento, actualización, eliminación y consulta de los datos; en definitiva, permite la gestión de la o las bases de datos. Existen varios SGBD disponibles en el mercado, su selección dependerá de las necesidades y recursos de la institución u empresa que lo requiera.

Cobo (s.f.), manifiesta que los objetivos de un SGBD son los siguientes:

> **Abstracción de la información**
> Consiste en proporcionar a los usuarios una visión abstracta de la información, es decir, el sistema ahorra al usuario la necesidad de conocer los detalles de cómo se almacena los datos.

Independencia
Es la capacidad para modificar un esquema de definición sin afectar a los programas de aplicación.

Redundancia mínima
Consisten en evitar el almacenamiento múltiple de una misma información para uso de distintas aplicaciones.

Consistencia
Consiste en impedir que exista información inconsistente o contradictoria en la base de datos.

La inconsistencia surge cuando existen varias copias del mismo dato y tras la modificación de una de ellas, las demás no son actualizadas, o sí los son, pero de forma incorrecta.

Seguridad
El SGBD debe garantizar la protección de la información, controlando el acceso y la manipulación de las distintas aplicaciones y usuarios.

El SGBD debe disponer de un robusto Subsistema de seguridad y autorización, mediante el cual el Administrador pueda crear usuarios y niveles de seguridad.

Integridad
Mantener la integridad es asegurar que la información almacenada y utilizada por una aplicación es correcta, es decir, refleja fielmente la realidad (p. 9).

SQL Server

Definiciones:

"Es un sistema para administracion de bases de datos que posee una arquitectura cliente/servidor. Utiliza el lenguaje de consulta Transact-SQL para recibir comandos desde los clientes que se conecten a él, y ofrece una gran variedad de herramientas y servicios para desarrollar y administrar bases de datos de distintos tamaños y complejidad" (Gradi, 2008, p. 161).

"SQL Server es el sistema de base de datos profesional de Microsoft. Contiene una variedad de características y herramientas que se pueden utilizar para desarrollar y administrar bases de datos y soluciones de todo tipo basadas en ellas" (Pérez, 2011, p.13).

Versiones:

SQL Server fue desarrollado por Microsoft, empresa que habitualmente crea nuevas versiones de SQL Server cada cierto tiempo y cada versión es mejorada mediante Service Packs, en el cuadro 1, queda notorio la finalización del soporte del último Service Pack (mejora) de la versión 2005 de SQL Server.

Versión	Último service pack	Fecha lanzamiento	Finalización soporte extendido	Cuenta con soporte
SQL Server 2016	SQL Server 2016 SP1	1/6/2016	14/7/2024	SI
SQL Server 2014	SQL Server 2014 SP2	5/6/2014	9/7/2024	SI
SQL Server 2012	SQL Server 2012 SP3	20/5/2012	12/7/2022	SI
SQL Server 2008 R2	SQL Server 2008 R2 SP3	10/7/2010	9/7/2019	SI
SQL Server 2008	SQL Server 2008 SP4	7/11/2008	9/7/2019	SI
SQL Server 2005	SQL Server 2005 SP4	14/1/2006	12/4/2016	NO

Cuadro 1. Versiones de SQL Server
Elaborado por: Investigador
Fuente: https://support.microsoft.com/en-us/lifecycle/search?alpha=Microsoft%20SQL%20Server%202016

Características de SQL Server 2005

- **Soporte**

El 12 de abril de 2016 llegó el final del soporte extendido de SQL Server 2005 y Microsoft no lanzará parches para vulnerabilidades de seguridad u otros errores en la versión. Esto significa que SQL Server 2005 será cada vez más vulnerable a ataques (Snodgrass, 2014).

Snodgrass (2014), manifiesta que:

> SQL Server 2005 ha seguido recibiendo parches de seguridad durante el último año, por lo que es probable que las vulnerabilidades aún no sean descubiertas y explotadas por los atacantes. Los sistemas sin parches también podrían presentar nuevos problemas de compatibilidad a medida que una organización actualiza configuraciones y aplicaciones, lo que podría poner en

peligro la capacidad de seguir ejecutando las aplicaciones de la organización en el motor de base de datos.

SQL Server contiene muchos componentes y menudo se conecta a una gama de otras aplicaciones y dispositivos, todos los cuales pueden estar expuestos a riesgos a través de una conexión no admitida. Los riesgos potenciales incluyen el robo de datos, la corrupción y la destrucción de datos, acceso no supervisado y la imposibilidad de ejecutar las aplicaciones necesarias (p. 3).

- **Niveles de seguridad**

Microsoft (s.f.-a), señala sobre los niveles de seguridad que:

SQL Server 2005 administra una colección jerárquica de entidades que se pueden proteger mediante permisos. A dichas entidades se las conoce como "asegurables".

Las entidades asegurables más destacadas son los servidores y las bases de datos, aunque se pueden definir permisos discretos con un mayor nivel de precisión. SQL Server regula las acciones de los principales sobre las entidades asegurables comprobando que se les ha otorgado los permisos adecuados.

Las entidades asegurables son aquellos recursos cuyo acceso está regulado por el sistema de autorizaciones de SQL Server. Algunas entidades asegurables pueden estar contenidas dentro de otras, dando lugar a jerarquías anidadas llamadas "ámbitos" que, a su vez, se pueden proteger. Los ámbitos se clasifican en:

Servidor:

Contiene las siguientes entidades asegurables:

- Inicios de sesión
- Bases de datos
- Notificaciones de eventos

Base de datos

Contiene las siguientes entidades asegurables:

- Usuarios
- Funciones
- Funciones de aplicación

- Esquema
- Ensamblados

Esquema

Contiene las siguientes entidades asegurables:

- Tabla
- Vista
- Función
- Procedimiento
- Tipo
- Regla
- Valor por defecto
- Sinónimos

- **Cifrado de datos**

"SQL Server 2005 tiene una infraestructura de cifrado jerárquica y administración de claves. Cada capa se encarga de cifrar a las capas inferiores utilizando una combinación de certificados, claves simétricas y asimétricas" (Dueñas, s.f.).

El cifrado de datos se lo realiza a nivel de servidor. En la imagen 1, se ilustra el proceso de cifrado:

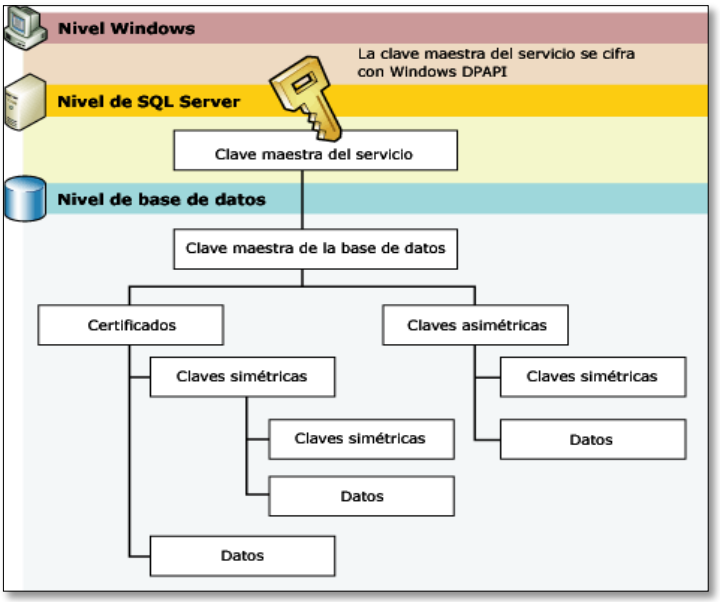


Imagen 1. Niveles de seguridad
Fuente: https://msdn.microsoft.com/es-es/library/bb972194.aspx

- **Modo auditoría C2**

Según, Clemente (2010), SQL Server 2005 cuenta con el modo auditoría c2 para realizar auditoría, el mismo que:

> Registra tanto los intentos sin éxito como los intentos con éxito de accesos a instrucciones y objetos del servidor y base de datos, es decir, registra el apagado y encendido del SGBD, los intentos de inicio de sesión de los usuarios, el acceso de los usuarios a los diferentes objetos de la base de datos (tablas, vistas, registros, etc.) teniendo en cuenta los permisos que tienen, la sentencias de los lenguajes de manipulación de datos (DML) o de definición de datos (DDL) o de control de acceso (DCL); el hecho de recoger tanta información tiene como consecuencia el rápido crecimiento del tamaño del fichero de almacenamiento y una disminución en el rendimiento del SGBD (p. 25).

En este tipo de auditoría no es posible elegir qué auditar, básicamente audita todo o nada.

- **Roles de servidor**

Los roles de servidor son roles fijos preestablecidos por SQL Server 2005 (no se puede agregar más roles), cada miembro de este role puede agregar otros inicios de sesión a éste. Los roles fijos de servidor son: bulkadmin, dbcreator, diskadmin, processadmin, securityadmin, serveradmin, setupadmin, sysadmin y public (Microsoft, s.f.-b).

- **Bases de datos dependientes**

Las bases de datos en SQL Server 2005 no son objetos independientes, cuentan con metadatos y configuraciones que para su funcionamiento dependen de otros objetos, un claro ejemplo, son: los inicios de sesión y contraseñas. Problemática que se denota en la migración de base de datos a otras instancias en las que si una base de datos es transferida a otra instancia lo más probable es que no se pueda acceder a ella, hasta que también los inicios de sesión y contraseñas sean transferidos (Microsoft, s.f.-c).

- **Copias de seguridad**

"SQL Server provee un componente denominado "Copia de seguridad" y en esencia es utilizado para para proteger los datos almacenados en las bases de datos. Las copias de seguridad se las puede utilizar para restaurar y recuperar los datos después de un error" (Microsoft, 2016a).

Según, Microsoft (2006), señala los siguientes tipos de copias de seguridad:

Completa

Una copia de seguridad completa incluye todos los datos de una base de datos determinada o un conjunto de grupos de archivos o archivos, así como una cantidad suficiente del registro como para permitir la recuperación de datos.

Diferencial

Una copia de seguridad diferencial se basa en la última copia de seguridad completa de los datos. Una copia de seguridad diferencial incluye sólo los datos que han cambiado desde la última base diferencial.

El uso de copias de seguridad diferenciales acelera el proceso de realización de copias de seguridad. En el momento de la restauración, se restaura primero la copia de seguridad completa, seguida de la copia de seguridad diferencial más reciente.

Registro de transacciones

Gracias a las copias de seguridad de registros es posible recuperar la base de datos en el punto en que se haya producido el error o en un momento dado.

Es aconsejable realizar copias de seguridad de registros suficientemente regulares para ajustarse a los requisitos de la empresa o institución, específicamente a la tolerancia de la pérdida de trabajo que una unidad de registro dañada podría provocar.

Las copias de seguridad son un mecanismo de defensa que ofrece SQL Server 2005, que sumado a una buena administración de base de datos, permiten reducir el riesgo de perdida de información ante un desastre.

Categorías de la variable dependiente

Seguridad de los datos

González (2014), señala que:

> La seguridad de los datos tiene como fin la protección de éstos y de los sistemas de la información, el acceso, uso, divulgación, la no interrupción y evitar la destrucción no autorizada.
>
> La seguridad de los datos, seguridad informática y garantía de la información son términos que, aunque su significado no sea el mismo, buscan una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información.
>
> La seguridad de los datos conlleva crear y aplicar una serie de estrategias que cubran los procesos de donde los datos son el activo primordial. Estas estrategias deben fijar el establecimiento de políticas, controles de seguridad, y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dichos datos; es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que almacenan y gestionan.

Seguridad informática

García, Hurtado y Alegre (2011), señalan que:

> La seguridad informática se puede definir como un conjunto de procedimientos, dispositivos y herramientas encargadas de asegurar la integridad, disponibilidad y privacidad de la información en un sistema informático e intentar reducir las amenazas que pueden afectar al mismo.
> Dentro de la seguridad informática podemos encontrar elementos y técnicas tanto hardware, como software, así como dispositivos físicos y medios humanos (p. 21).

Avilés (2015), señala que:

> La seguridad de base de datos hereda las mismas dificultades a las que enfrenta la seguridad informática y es garantizar la integridad, disponibilidad y confidencialidad de la información. Un Sistema Gestor de Base de Datos debe suministrar los mecanismos que ayuden es esta tarea.

> A modo general, los mecanismos de seguridad se refieren a las reglas impuestas por el subsistema de seguridad del SGBD, que verifica todas las solicitudes de acceso, comparándolas con las restricciones de seguridad almacenadas en el catálogo del sistema.
>
> Sin embargo, existen brechas en el sistema y amenazas externas que pueden comprometer a un servidor de base de datos o crear la posibilidad de robo de datos confidenciales (p. 20).

En base a la gestión de información en la DITIC y la utilización de SQL Server 2005, se lograron determinar vulnerabilidades que pondrían en riesgo la confiabilidad, integridad y disponibilidad de sus datos; cabe recalcar que es imposible determinar todas las vulnerabilidades que podrían afectar la seguridad de los mismos. A continuación, se detalla las vulnerabilidades encontradas:

- **Copias de seguridad de datos no cifradas.**

Las copias de seguridad de las bases de datos en SQL Server 2005 se las realiza periódicamente (diarias, quincenales, mensuales, etc.) dependiendo de la criticidad de la información que gestionen mencionadas bases de datos, éstas pueden ser completas o diferenciales. Una vez realizadas las copias de seguridad, éstas son almacenadas en el mismo servidor de base de datos y en medios de almacenamiento externos (DVD y discos duros externos). Por las características de SQL Server 2005 no se puede cifrar las copias de seguridad y por ende su seguridad depende de las medidas de almacenamiento y conservación que se den a los medios de almacenamiento.

Se denota que una copia de seguridad no cifrada puede ser fácilmente vulnerada, ésta puede ser simplemente abierta desde un editor de texto (bloc de notas).

- **Auditoria débil**

La DITIC cuenta con mecanismos personalizados para auditar sus datos considerados de mayor importancia, a través de la ejecución de disparadores a nivel de base de datos. Los disparadores almacenan en tablas de auditoria las operaciones

(INSERT, UPDATE y DELETE) realizadas en las tablas auditadas, adicionalmente se guarda el usuario que realizó la operación y la fecha. Solución de auditoría básica que no considera todos los objetos de las bases de datos y además no contempla objetos a nivel de servidor que podrían ser cruciales en la superación de incidentes.

- **Terminación de soporte**

SQL Server 2005 desde el inicio de su ciclo de vida ha sido constantemente actualizado y monitoreado por Microsoft, se han detectado y corregido vulnerabilidades que comprometían la integridad, consistencia y disponibilidad de los datos gestionados por mencionada versión. La explotación de estas vulnerabilidades permitía la elevación de privilegios, denegación de servicios, ejecución de malware entre otras.

Las actualizaciones y revisiones de seguridad descritos en el cuadro 2 han permitido que SQL Server 2005 siga funcionado y dando las garantías necesarias a sus usuarios hasta el final de su ciclo de vida. Actualizaciones que también dan a notar que el software esta propenso a nuevas amenazas que revelen nuevas vulnerabilidades o errores no detectados en la versión, y por ende se vea afectada la seguridad de los datos en la DITIC.

Boletín	Fecha	Descripción
MS09-004	2/10/2009	Vulnerability in Microsoft SQL Server Could Allow Remote Code Execution
MS11-049	6/14/2011	Vulnerability in the Microsoft XML Editor Could Allow Information Disclosure
MS12-060	8/14/2012	Vulnerability in Windows Common Controls Could Allow Remote Code Execution
MS12-027	4/12/2012	Vulnerability in Windows Common Controls Could Allow Remote Code Execution

Cuadro 2. Boletines de seguridad – SQL Server 2005
Elaborado por: Investigador
Fuente: https://docs.microsoft.com/en-us/security-updates/securitybulletins/securitybulletins

Boletín	Fecha	Descripción
MS12-070	10/9/2012	Vulnerability in SQL Server Could Allow Elevation of Privilege
MS15-034	4/14/2015	Vulnerability in HTTP.sys Could Allow Remote Code Execution
MS10-086	10/12/2010	Vulnerability in Windows Shared Cluster Disks Could Allow Tampering
MS09-062	10/13/2009	Vulnerabilities in GDI+ Could Allow Remote Code Execution
MS15-058	7/14/2015	Vulnerabilities in SQL Server Could Allow Remote Code Execution
MS14-044	8/12/2014	Vulnerabilities in SQL Server Could Allow Elevation of Privilege

Cuadro 2. (cont.)

En la DITIC, SQL Server 2005 cuenta con la instalación de todas las actualizaciones proporcionadas por Microsoft, pero aún con estas actualizaciones se pudo detectar vulnerabilidades que pondrían en peligro la seguridad de los datos, las mismas que se detallan a continuación:

Vulneración del procedimiento extendido "xp_cmdshell"

Herramientas utilizadas

Sistema operativo: Kali Linux
Software: Metasploit v4

Descripción de la vulnerabilidad

La vulnerabilidad permite la escala de privilegios a través del procedimiento extendido "xp_cmdshell", es decir, un usuario con privilegios "sysadmin" puede a través del procedimiento extendido "xp_cmdshell" apoderarse del sistema operativo donde reside el SGBD.

Obtención del usuario con privilegios “sysadmin” en SQL Server

Para la vulneración del procedimiento extendido “xp_cmdshell” es necesario contar con los privilegios “sysadmin” en el SGBD, y existe un usuario predeterminado con esos permisos, el usuario “sa”.

El exploit “mssql_login” permite realizar ataques de fuerza bruta utilizando diccionarios para descifrar contraseñas, en este caso se descifrará la contraseña del usuario “sa” de SQL Server; desde luego el éxito dependerá de la robustez del diccionario y la complejidad de la contraseña del usuario buscado.

A manera de prueba se ilustra la manera como un atacante puede obtener la contraseña “sa” de SQL Server.

1. Utilizar el exploit “mssql_login” para realizar el ataque. Ver gráfico 3

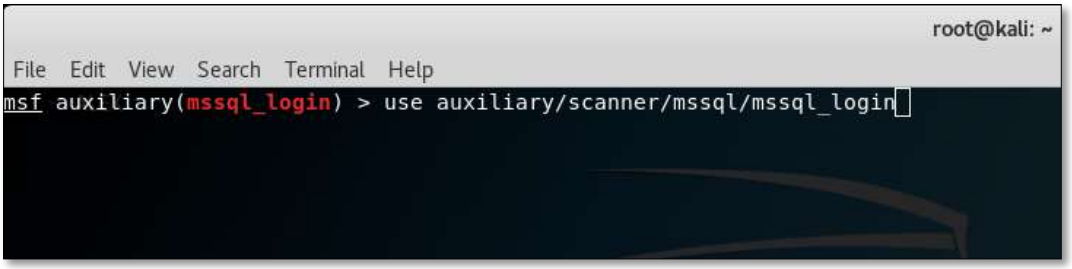


Gráfico 3. Utilización exploit “mssql_login”
Elaborado por: Investigador

2. Parametrizar el exploit “mssql_login” con los siguientes parámetros**:**

RHOSTS: IP del SGBD
USERNAME: Usuario a buscar la contraseña
PASS_FILE: Archivo con el diccionario de contraseñas a comparar
RPORT: Puerto utilizado por el servicio de SQL Server (utilizar NMAP para el escaneo de puertos del servidor). El puerto por defecto es: 1433.

En el gráfico 4, se ilustra los parámetros registrados en el exploit “mssql_login”

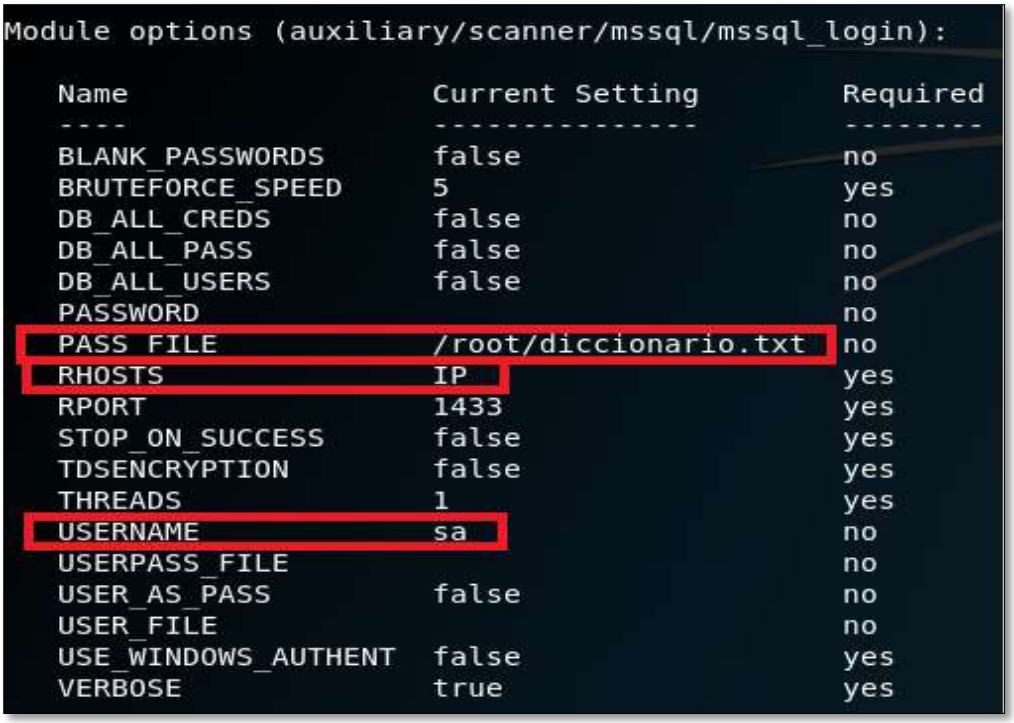


Gráfico 4. Configuración exploit "mssql_login"
Elaborado por: Investigador

3. Ejecutar el exploit. Ver gráficos 5 y 6.

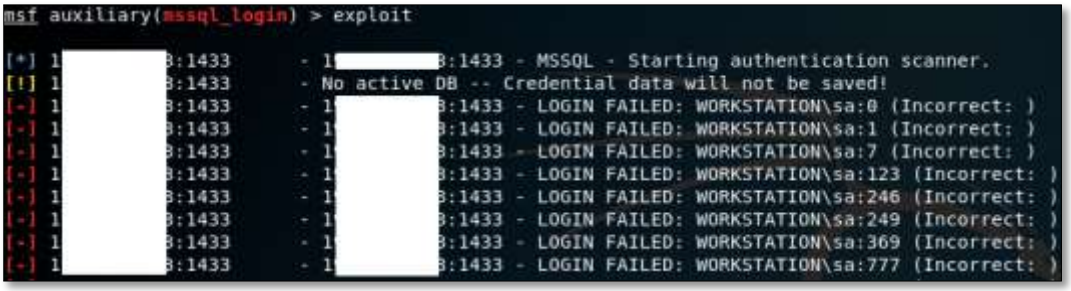


Gráfico 5. Ejecución del exploit "mssql_login"
Elaborado por: Investigador

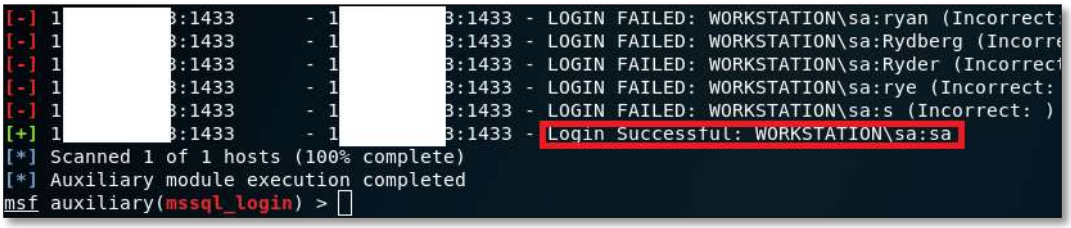


Gráfico 6. Ejecución del exploit "mssql_login" – caso exitoso
Elaborado por: Investigador

Explotación de la vulnerabilidad

Pasos

1. Utilizar el exploit “mssql_payload”. Ver gráfico 7.

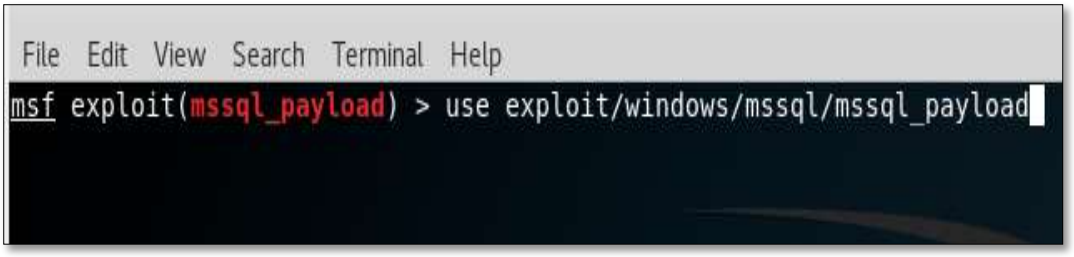


Gráfico 7. Utilización del exploit “mssql_payload”
Elaborado por: Investigador

2. Parametrizar el exploit “mssql_payload” (ver gráficos 8 y 9), con los siguientes parámetros:

RHOSTS: IP del SGBD
USERNAME: Usuario del SGBD
PASSWORD: Password del SGBD
LHOST: IP atacante
LPORT: Puerto atacante (los atacantes utilizan puertos conocidos para no causar sospechas).

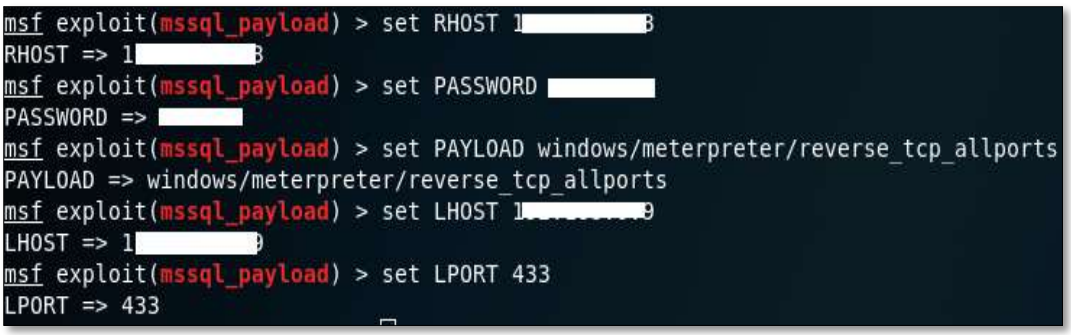


Gráfico 8. Configuración del exploit “mssql_payload”
Elaborado por: Investigador

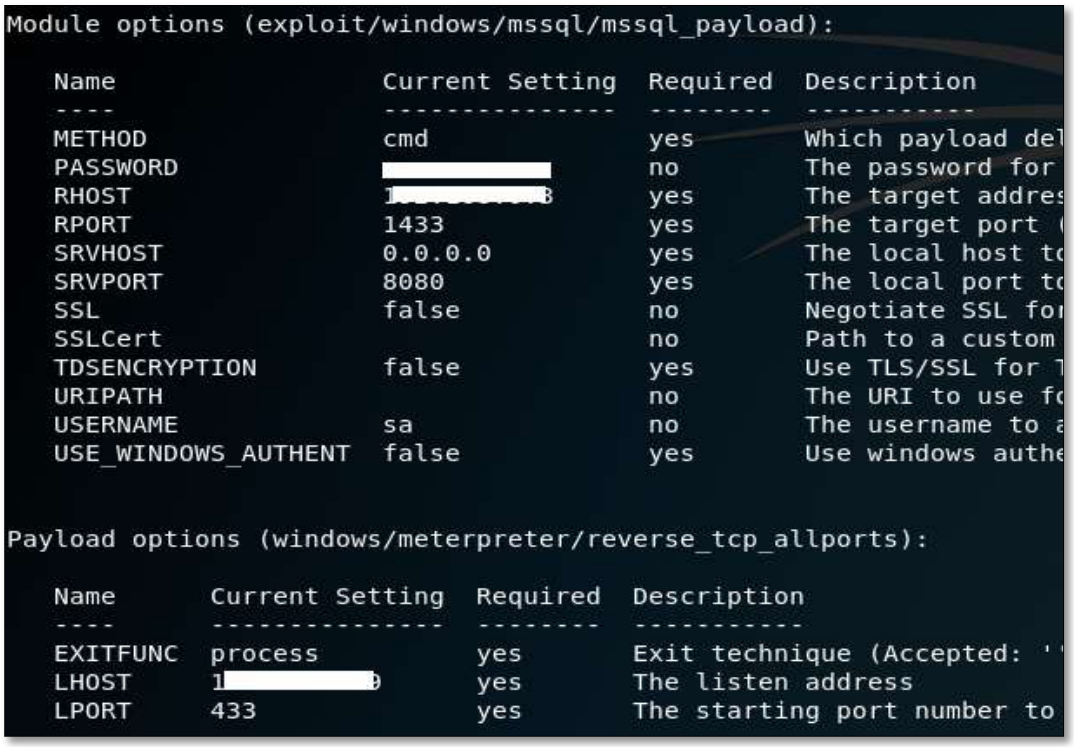


Gráfico 9. Parámetros configurados del exploit "mssql_payload"
Elaborado por: Investigador

3. Ejecutar el exploit "mssql_payload"

El resultado de la ejecución del exploit "mssql_payload" fue exitoso, se logró acceder al sistema operativo, como lo muestra el gráfico 10 y 11.

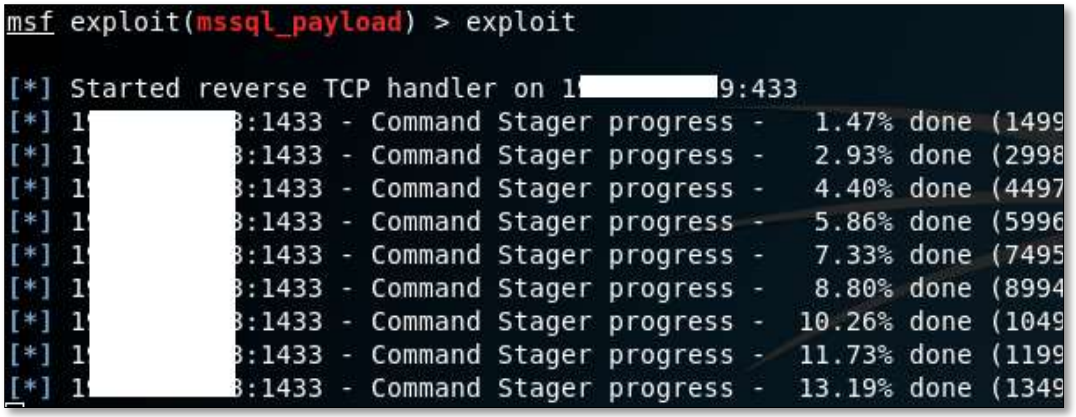


Gráfico 10. Ejecución del exploit "mssql_payload"
Elaborado por: Investigador

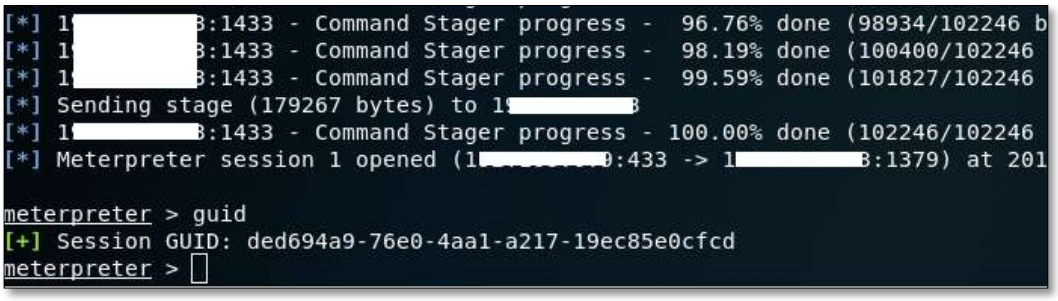


Gráfico 11. Ejecución del exploit "mssql_payload" – caso exitoso
Elaborado por: Investigador

Una vez dentro, el atacante tendrá disponible todos los permisos de NTAUTHORITY\SYSTEM (privilegio de nivel más alto) en el servidor local. Recordemos que todo usuario de base de datos asignado al role sysadmin cuenta con los permisos NTAUTHORITY\SYSTEM en el servidor local.

Entre la cantidad de acciones que el atacante podría realizar en el servidor local, están:

Visualización de procesos (ver gráfico 12). Ejecutar el comando "ps"

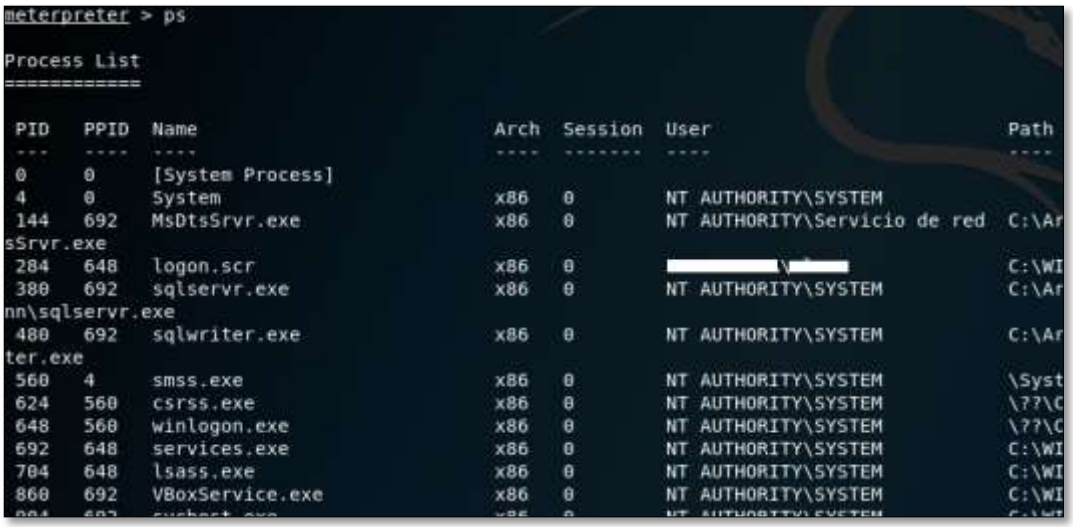


Gráfico 12. Ejecución comando ps
Elaborado por: Investigador

Listado de procesos (ver gráfico 13). Ejecutar el comando "run post/windows/gather/enum_applications"

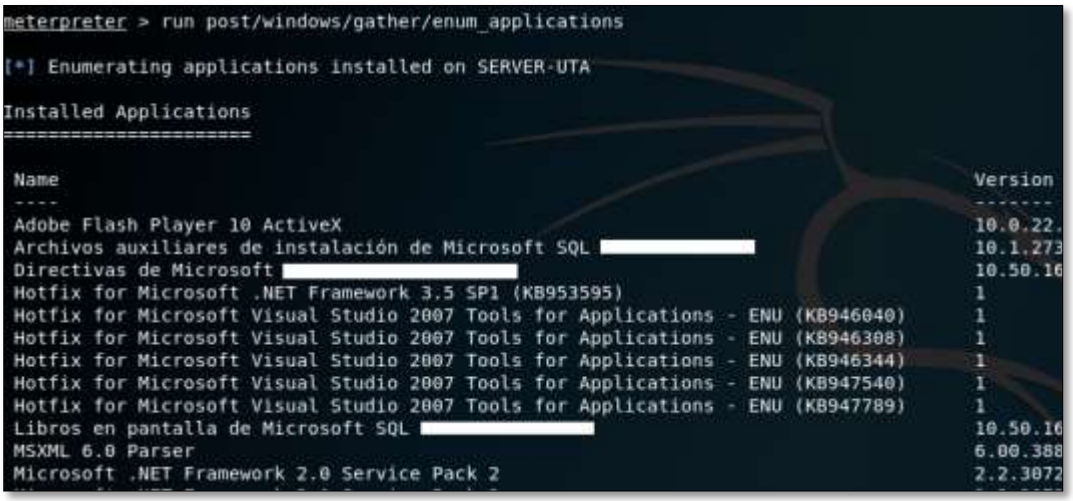


Gráfico 13. Listar programas instalados
Elaborado por: Investigador

A continuación, se muestra un ejemplo de cómo un atacante puede visualizar y crear usuarios en el servidor local.

Acceso a cmd del servidor local (ver gráfico 14). Ejecutar el comando "execute -f cmd.exe -i -H"

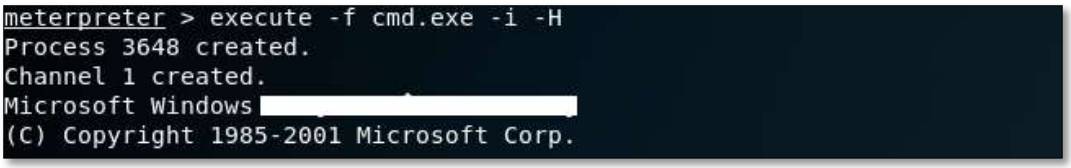


Gráfico 14. Ejecución de comando
Elaborado por: Investigador

Visualización de usuarios del servidor local (ver gráfico 15). Ejecutar el comando "net user"

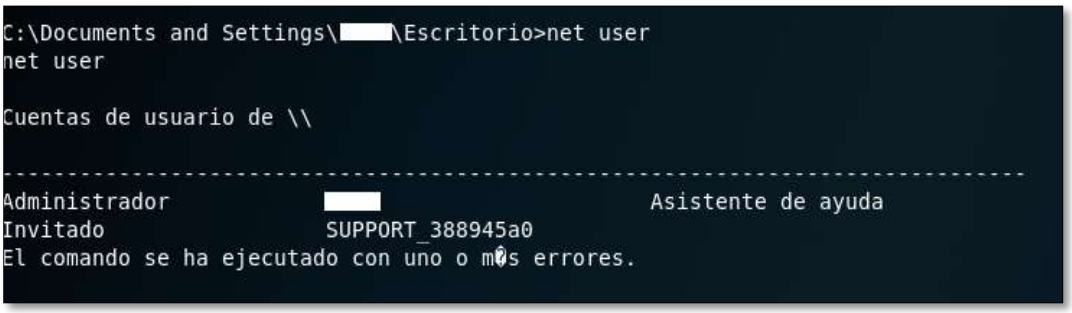


Gráfico 15. Usuarios del servidor local
Elaborado por: Investigador

Creación de usuarios (ver gráfico 16). Ejecutar el comando “net /add user password”

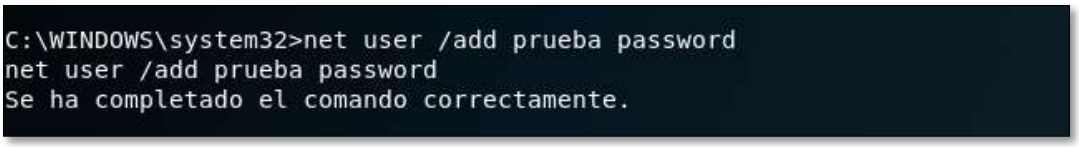


Gráfico 16. Creación de usuarios desde línea de comandos
Elaborado por: Investigador

Asignación de usuarios al grupo administradores (ver gráfico 17). Ejecutar el comando “net localgroup grupo usuario /add”. Mencionado usuario que podría permitir que el atacante se adueñe del servidor, simplemente cambiando las contraseñas de los usuarios del grupo administradores utilizadas por la dirección.

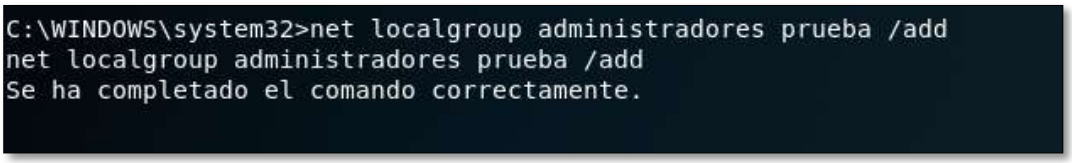


Gráfico 17. Asignación de usuario al grupo administradores
Elaborado por: Investigador

Vulneración del procedimiento extendido “sp_replwritetovarbin”

Herramientas utilizadas

Sistema operativo: Kali Linux
Software: Metasploit v4

Descripción de la vulnerabilidad

La vulnerabilidad permite el acceso remoto y escala de privilegios a través del procedimiento extendido “sp_replwritetovarbin”.

El procedimiento “sp_replwritetovarbin” puede ser ejecutado por cualquier usuario y nivel de privilegios del SGBD, el atacante puede aprovechar esta ventaja y

combinando técnicas de inyección SQL puede obtener el acceso remoto al servidor que aloja el SGBD. Incluso funcionarios malintencionados con acceso al servidor (usuario y contraseña de ingreso) podrían explotar esta vulnerabilidad.

Explotación de la vulnerabilidad

Pasos

1. Utilizar el exploit "ms09_004_sp_replwritetovarbin"**.** Ver gráfico 18

Gráfico 18. Utilización de "ms09_004_sp_replwritetovarbin"
Elaborado por: Investigador

2. Parametrizar el exploit "ms09_004_sp_replwritetovarbin" (ver gráficos 19, 20 y 21), con los siguientes parámetros:

RHOSTS: IP del SGBD
USERNAME: Usuario del SGBD
PASSWORD: Password del SGBD
LHOST: IP atacante
LPORT: Puerto atacante (los atacantes utilizan puertos conocidos para no causar sospechas).

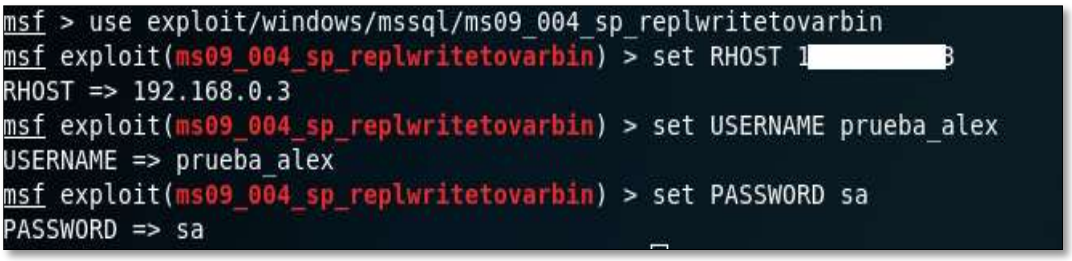


Gráfico 19. Parametrización de "ms09_004_sp_replwritetovarbin" (A)
Elaborado por: Investigador

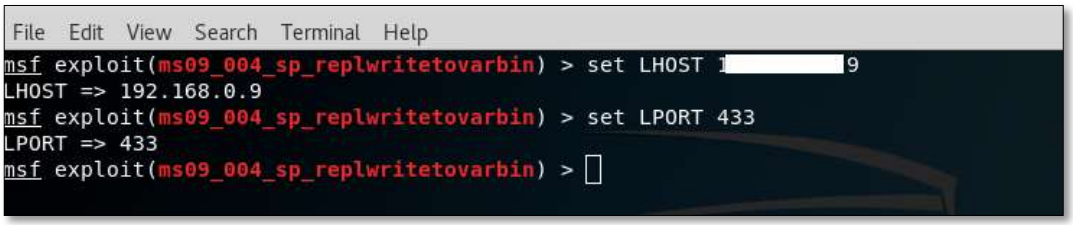


Gráfico 20. Parametrización de "ms09_004_sp_replwritetovarbin" (B)
Elaborado por: Investigador

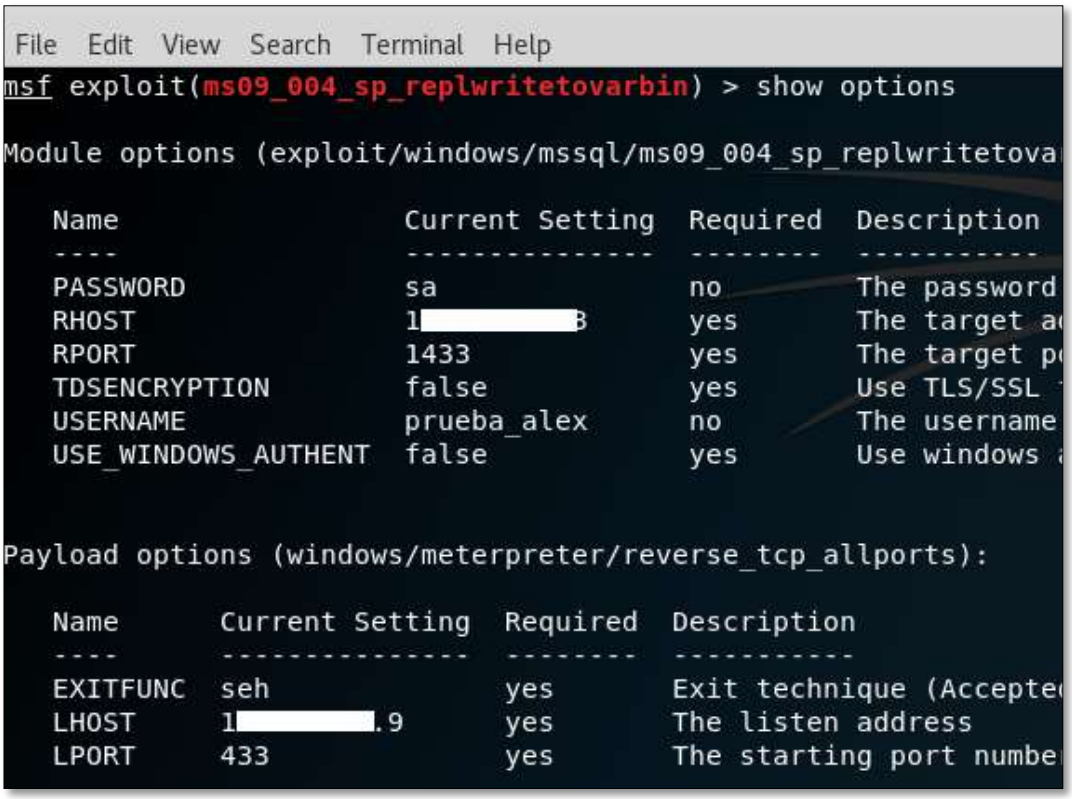


Gráfico 21. Configuración de "ms09_004_sp_replwritetovarbin"
Elaborado por: Investigador

3. Ejecutar el exploit "ms_09_004_sp_replwritertovarbin"

El resultado de la ejecución del exploit "ms_09_004_sp_replwritertovarbin" en SQL Server 2005 (versión utilizada en la DITIC) fue exitoso, se logró acceder al sistema operativo remotamente, como lo muestra el gráfico 22.

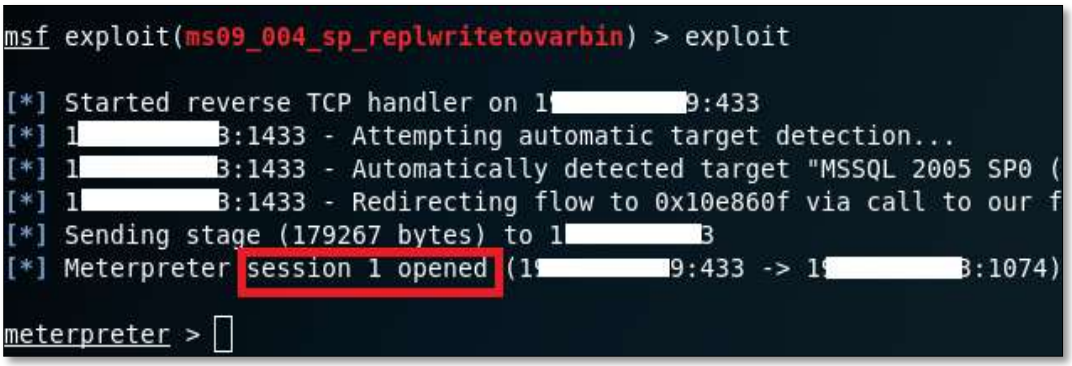


Gráfico 22. Ejecución de "ms09_004_sp_replwritetovarbin"
Elaborado por: Investigador

Ya en el servidor, el atacante dispone de los permisos de NTAUTHORITY\ SYSTEM sin importar con que usuario de SQL Server realizó el ataque.

A continuación, se lista algunas acciones que podría realizar el atacante en el servidor:

Listar archivos. Ver gráfico 23

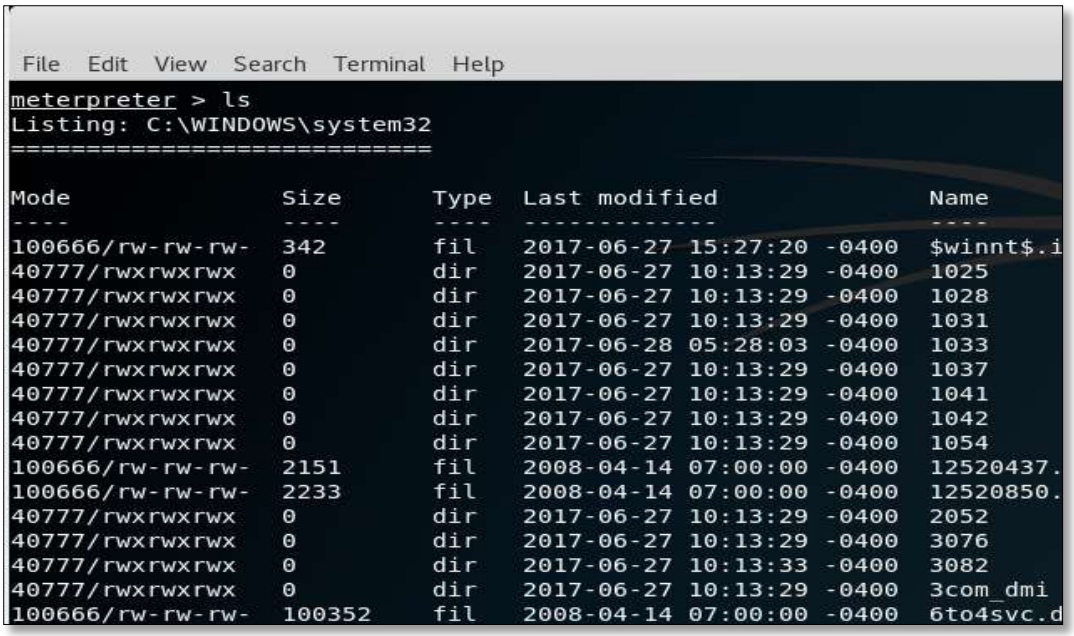


Gráfico 23. Listar archivos
Elaborado por: Investigador

Descargar archivos. Ver gráfico 24

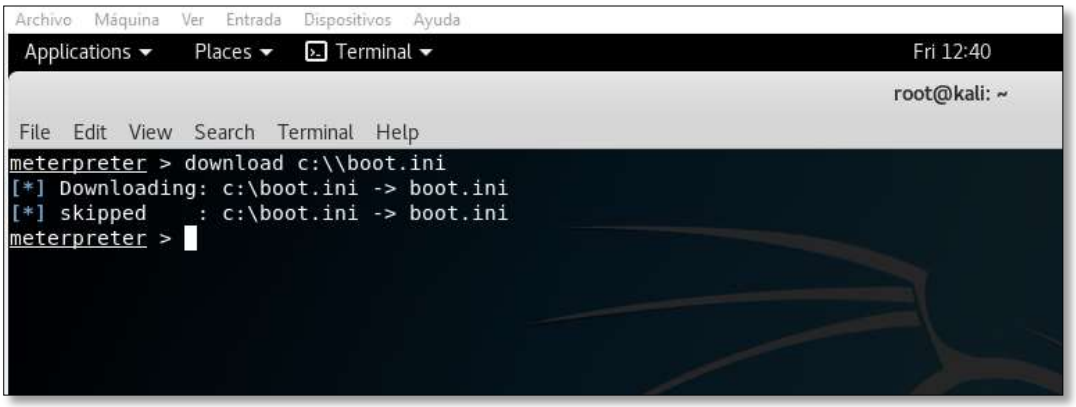


Gráfico 24. Descargar archivos
Elaborado por: Investigador

Cargar archivos. Ver gráfico 25

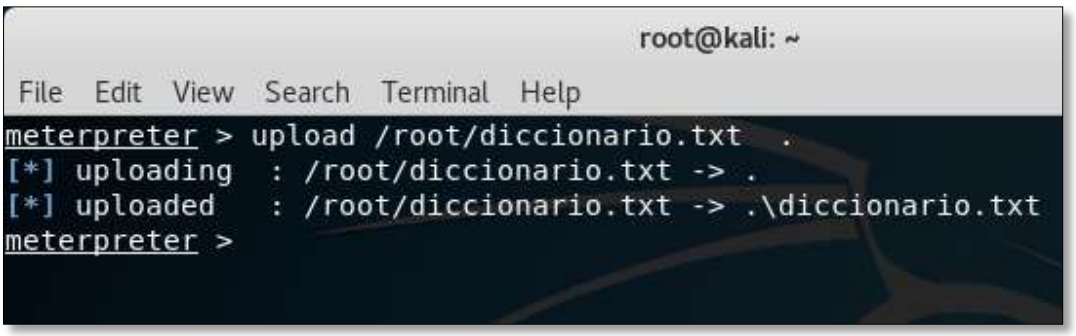


Gráfico 25. Cargar archivos
Elaborado por: Investigador

Ejecutar comandos (ver gráfico 26 y 27). A través del acceso al "cmd" del servidor local y la creación de usuarios con privilegios de administrador, el atacante puede apropiarse del servidor.

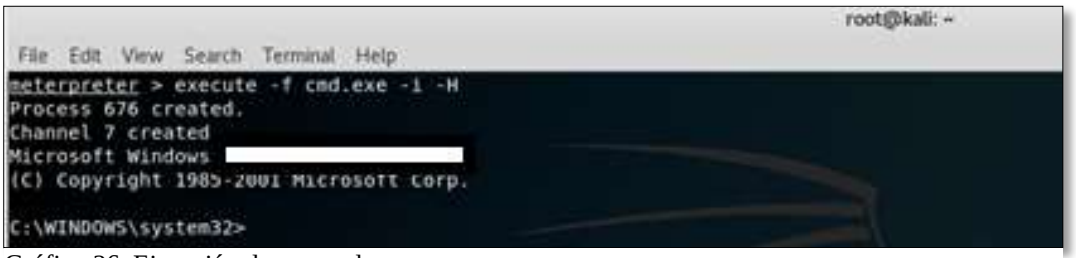


Gráfico 26. Ejecución de comandos
Elaborado por: Investigador

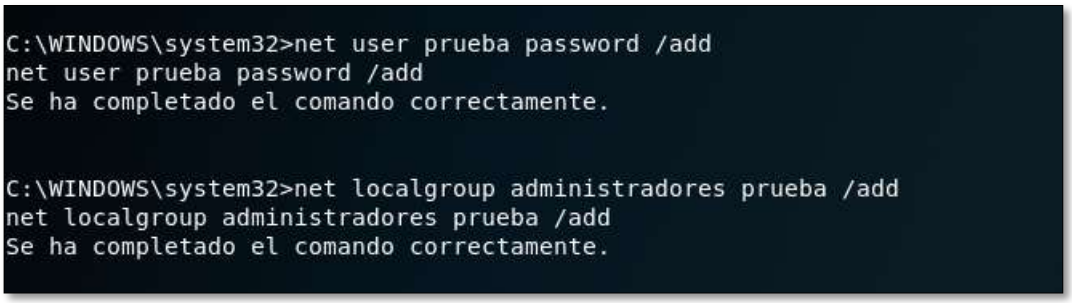


Gráfico 27. Elevación de privilegios
Elaborado por: Investigador

Sistemas de información

Laudon y Laudon (2004 citado en Fernández, 2006), definen a los sistemas de información como:

> Un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control de una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores a analizar problemas, a visualizar asuntos complejos y a crear productos nuevos (p. 12).

2.5 Hipótesis

Las características de SQL Server 2005 inciden en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

2.6 Señalamiento de variables

Variable Independiente: Características de SQL Server 2005

Variable Dependiente: Seguridad de los datos

CAPÍTULO III

METODOLOGÍA

3.1. Enfoque

La investigación es cuantitativa porque se utilizó parámetros de medición para la variable dependiente y es cualitativa porque se emitió juicios de valor sobre la investigación.

3.2. Modalidad básica de investigación

La investigación es bibliográfica porque se utilizó fuentes como libros, documentos, artículos, revistas, etc., para la construcción del marco teórico tanto de las características de SQL Server 2005 como de la seguridad de los datos de la DITIC de la UTA.

La investigación además tiene la modalidad de campo porque se buscó obtener la información de las características de SQL Server 2005 y la seguridad de los datos de la DITC de la UTA en el lugar de los hechos.

3.3. Nivel o tipo de investigación

Investigación exploratoria

Porque se analizó el problema y se buscó obtener una posible solución.

Investigación descriptiva

Porque se procesó y analizó la información obtenida de la aplicación de encuestas, cuestionarios, etcétera para la especificación del problema.

Investigación explicativa

Porque se buscó la razón del porque las vulnerabilidades en la seguridad de los datos de la DITIC de la UTA, partiendo de lo general a lo especifico (Método inductivo) y de lo específico a lo general (Método deductivo).

Investigación correlacional

Porque busco medir el grado de relación existente entre las características de SQL Server 2005 y la seguridad de los datos en la DITIC de la UTA.

3.4. Población y muestra

El presente proyecto trabajó con la población total, que es el grupo de profesionales encargados de la administración de base de datos y desarrolladores de software de la Dirección de Tecnología de Información y Comunicación de la UTA. (Ver cuadro 3)

PROBLACIÓN	NUMERO(FRECUENCIA)	PORCENTAJE
Administradores de Base de Datos	4	57,14%
Director DITIC	1	14,29%
Administrador de Seguridad Informática.	2	28,57%
TOTAL	7	100.00 %

Cuadro 3. Población
Elaborado por: Investigador

3.5. OPERACIONALIZACIÓN DE LAS VARIABLES

3.1.1. **Variable independiente:** Características de SQL Server 2005.

CONCEPTUALIZACIÓN	DIMENSIONES	INDICADORES	ITEMES BÁSICOS	TÉCNICAS E INSTRUMENTOS
SQL Server 2005, es un SGBD que fue desarrollado bajo altos estándares de seguridad y en todo su ciclo de vida fue constantemente supervisado y soportado po0r Microsoft.	Estándar	Estándar	¿Las características del SQL Server 2005 le permiten cumplir con los actuales estándares internacionales de seguridad de la información?	Encuesta – Cuestionario dirigida a: Administradores de BD Director DITIC Administradores de Seguridad Informática
	Seguridad	Seguridad	¿En matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad. SQL Server 2005 está dotado para cumplir esos requerimientos?	
	Soporte	Soporte	¿Al finalizar el contrato de soporte con SQL Server 2005, la desactualización de la herramienta generaría que los datos de la DITIC queden vulnerables para ataques informáticos exitosos?	

Cuadro 4. OPERACIONALIZACIÓN DE LA VARIABLE INDEPENDIENTE
Elaborado por: Investigador

3.1.2. **Variable dependiente:** Seguridad de los datos**.**

CONCEPTUALIZACIÓN	**DIMENSIONES**	**INDICADORES**	**ITEMES BÁSICOS**	**TÉCNICAS E INSTRUMENTOS**
Son medidas de control que permiten asegurar el acceso autorizado a las bases de datos y reducir de alguna manera ataques informáticos exitosos. El administrador de base de datos es el encardado del mantenimiento preventivo de los SGBD con la finalidad de corregir nuevas vulnerabilidades que podrían presentarse.	Ataque informático	Ataque informático	¿Las bases de datos en SQL Server 2005 de la UTA han sufrido algún tipo de ataque informático?	Encuesta – Cuestionario dirigida a: Administradores de BD Director DITIC Administradores de Seguridad Informática.
	Mantenimiento	Mantenimiento	¿Existe algún proceso de mantenimiento preventivo frente a nuevas vulnerabilidades que podría presentar SQL Server 2005?	
	Medidas de Control	Control	¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?	

Cuadro 5. OPERACIONALIZACIÓN DE LA VARIABLE DEPENDIENTE
Elaborado por: Investigador.

3.6. Recolección de información

En el cuadro 6, se ilustra la recolección de información

PREGUNTAS BÁSICAS	EXPLICACIÓN
¿Para qué?	Para alcanzar los objetivos de la investigación
¿De qué personas u objetos?	Administradores de BD Director DITIC Administradores de Seguridad Informática.
¿Sobre qué aspectos?	Sobre los indicadores (Matriz de operacionalización de variables)
¿Quién, Quiénes?	Paucar Medina Alex Ricardo
¿Cuándo?	Cuarto trimestre del 2016
¿Dónde?	Universidad Técnica de Ambato
¿Cuántas veces?	Una
¿Qué técnicas de recolección?	Encuesta Observación Revisión de documentación
¿Con qué?	Cuestionario Guía de Entrevista Inspecciones
¿En qué situación?	Mientras cumplen sus funciones

Cuadro 6. Recolección de la información.
Elaborado por: Investigador

3.7. Procesamiento y análisis

Procesamiento de la información

1. Revisión crítica de la información recogida; es decir, limpieza de la información defectuosa: contradictoria, incompleta, no pertinente, etc.

2. Repetición de la recolección, en ciertos casos individuales, para corregir fallas de contestación.

3. Tabulación o cuadros según variables de cada hipótesis: cuadros de una sola variable, cuadro con cruce de variables, etc.

4. Manejo de información (reajuste de cuadros con casillas vacías o con datos tan reducidos cuantitativamente, que no influyen significativamente en los análisis).

5. Estudio estadístico de datos para presentación de resultados.

Análisis de Resultados

6. Análisis de los resultados estadísticos, destacando tendencias o relaciones fundamentales de acuerdo con los objetivos e hipótesis.

7. Interpretación de los resultados, con apoyo del marco teórico, en el aspecto pertinente.

8. Comprobación de hipótesis para la verificación estadística conviene seguir la asesoría de un especialista.

9. Establecimiento de conclusiones y recomendaciones.

CAPITULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1 Análisis e interpretación de resultados

A continuación, se muestra los resultados obtenidos de la aplicación de la encuesta; a los Administradores de Base de Datos, Administradores de Seguridad Informática y al Director de la Dirección de Tecnología de Información de la UTA.

Pregunta 1

¿Las características del SQL Server 2005 le permiten cumplir con los actuales estándares internacionales de seguridad de la información?

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	0	0
NO	7	100
TOTAL	**7**	**100**

Cuadro 7. Estándares SQL Server 2005
Elaborado Por: Investigador

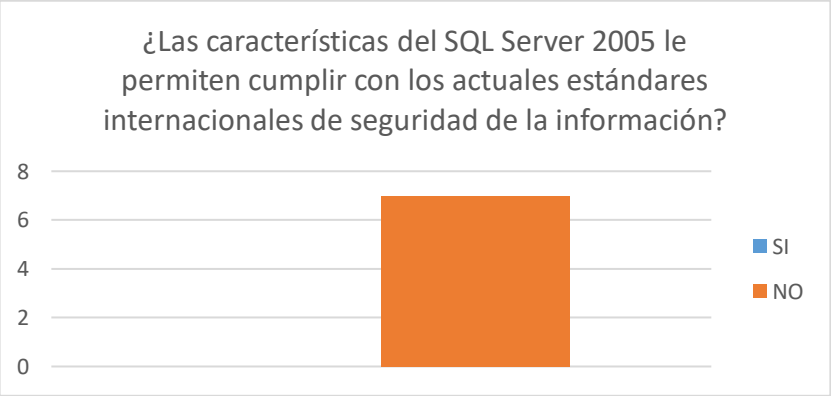


Gráfico 28. Estándares SQL Server 2005
Elaborado por: Investigador

Análisis

El 100% de los encuestados afirma que las características del SQL Server 2005 no le permiten cumplir con los actuales estándares internacionales de seguridad de la información.

Interpretación

SQL Server 2005 no cumple con los actuales estándares internacionales de seguridad de la información que permitan garantizar el aseguramiento, la confidencialidad e integridad de los datos de la DITIC.

Pregunta 2.

¿En matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad. SQL Server 2005 está dotado para cumplir esos requerimientos?

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	0	0
NO	7	100
TOTAL	7	100

Cuadro 8. Exigencia de seguridad SQL Server 2005
Elaborado por: Investigador

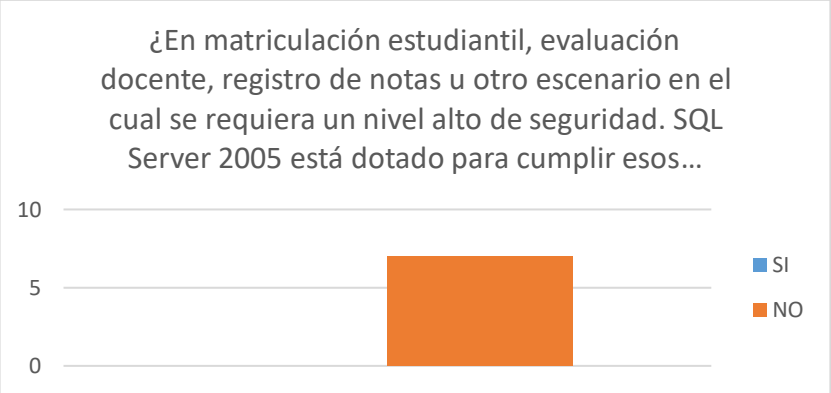


Gráfico 29. Exigencia de seguridad SQL Server 2005
Elaborado por: Investigador

Análisis

El 100% de los encuestados afirma que, en matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad; SQL server no está dotado para cumplir con los requerimientos.

Interpretación

Se ratifica que SQL Server 2005 no está dotado con las características que le permitan ofrecer un alto nivel de seguridad en todo escenario.

Pregunta 3.

¿Al finalizar el contrato de soporte con SQL Server 2005, la desactualización de la herramienta generaría que los datos de la DITIC queden vulnerables para ataques informáticos exitosos?

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	7	100
NO	0	0
TOTAL	7	100

Cuadro 9. Desactualización SQL Server 2005
Elaborado por: Investigador

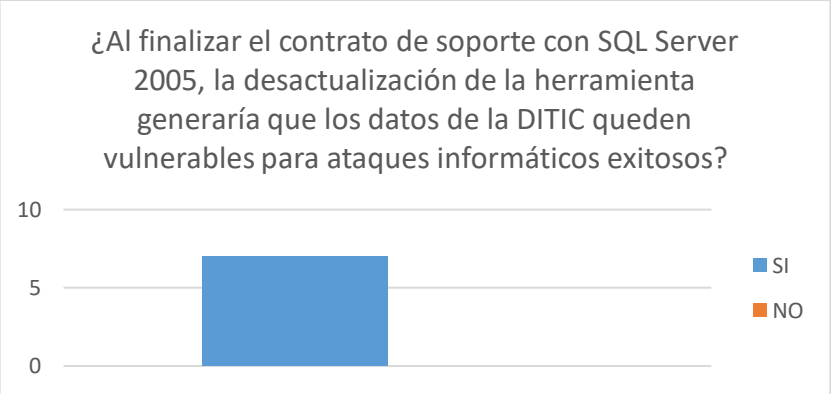


Gráfico 30. Desactualización SQL Server 2005
Elaborado por: Investigador

Análisis

El 100% de los encuestados afirma que, al finalizar el contrato de soporte con SQL Server 2005, la desactualización de la herramienta generaría que los datos de la DITIC queden vulnerables para ataques informáticos exitosos.

Interpretación

La finalización del contrato de soporte con SQL Server 2005 y en consecuencia la desactualización de la herramienta, dejarían a los datos de la DITIC vulnerables para ataques informáticos exitosos.

Pregunta 4.

¿Las bases de datos en SQL Server 2005 han sufrido algún tipo de ataque informático?

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	6	85,71
NO	1	14,29
TOTAL	**7**	**100**

Cuadro 10. Ataque informático.
Elaborado por: Investigador

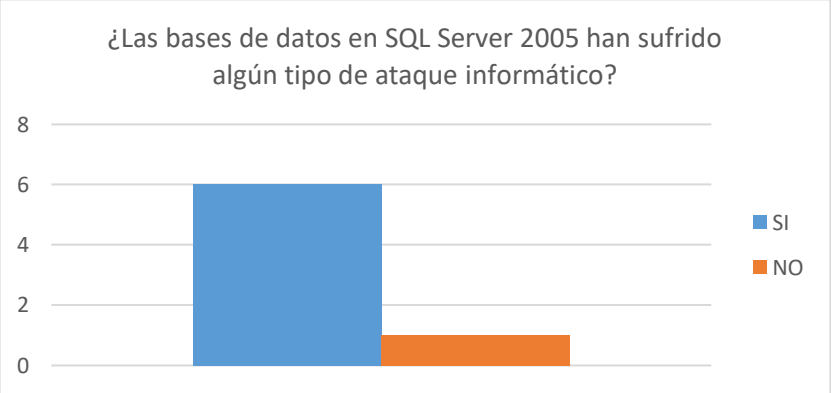


Gráfico 31. Ataque informático
Elaborado por: Investigador

Análisis

Del 100% de los encuestados, el 85.71% afirma que, las bases de datos en SQL Server 2005 han sufrido algún tipo de ataque informático; mientras que el 14.29% afirma que, las bases de datos en SQL Server 2005 no han sufrido algún tipo de ataque informático.

Interpretación

Se evidencia que las bases de datos en SQL Server 2005, en un momento dado han sufrido un cierto tipo de ataque informático que no necesariamente fue exitoso. Factor de riesgo que pone en evidencia la importancia de la correcta gestión de la seguridad en la DITIC.

Pregunta 5

¿Existe algún proceso de mantenimiento preventivo frente a nuevas vulnerabilidades que podría presentar SQL Server 2005?

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	0	0
NO	7	100
TOTAL	**7**	**100**

Cuadro 11. Vulnerabilidades SQL Server 2005
Elaborado por: Investigador

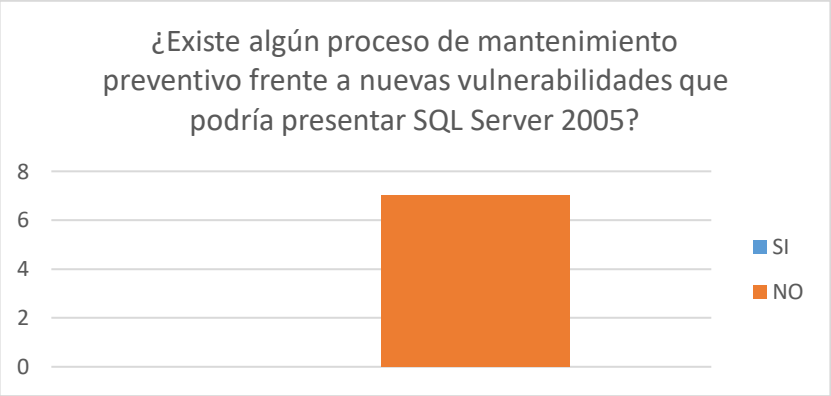


Gráfico 32. Vulnerabilidades SQL Server 2005
Elaborado por: Investigador

Análisis

El 100% de los encuestados afirma que, no existe algún proceso de mantenimiento preventivo frente a nuevas vulnerabilidades que podría presentar SQL Server 2005.

Interpretación

Los resultados evidencian que la DITIC no cuenta con procesos de mantenimiento preventivo frente a nuevas vulnerabilidades que podría presentar SQL Server 2005, vulnerabilidades que podrían ser la puerta de acceso para ataques informáticos exitosos y un serio problema en la seguridad de la información.

Pregunta 6.

¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?

ALTERNATIVAS	FRECUENCIA	PORCENTAJE
SI	0	0
NO	7	100
TOTAL	**7**	**100**

Cuadro 12. Medidas de control y seguridad
Elaborado por: Investigador

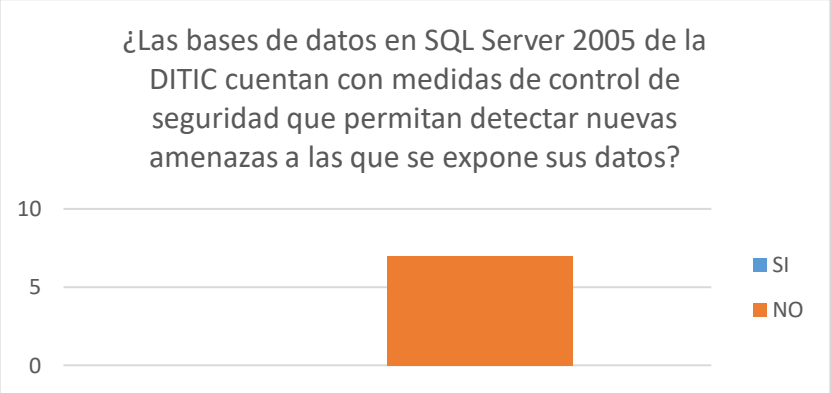


Gráfico 33. Medidas y control de seguridad
Elaborado por: Investigador

Análisis

El 100% de los encuestados afirma que, las bases de datos en SQL Server 2005 de la DITIC no cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos.

Interpretación

Se evidencia que las bases de datos en SQL Server 2005 de la DITIC no cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos.

Interpretación de resultados

4.2 Verificación de la hipótesis

Las características de SQL Server 2005 inciden en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

H_0: Las características de SQL Server 2005 **NO** inciden en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

H_1: Las características de SQL Server 2005 **SI** inciden en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

4.2.1 Modelo estadístico

Se aplicó la prueba de Chi – Cuadrado para la comprobación de la hipótesis.

Fórmula aplicada:

$$x^2 = \sum \left[\frac{(O-E)^2}{E}\right]$$

En donde:

x^2 = Chi – Cuadrado

O = Frecuencias observadas

E = Frecuencias esperadas

$\sum$ = Sumatoria

4.2.2 Definición del nivel de significancia

El nivel de significancia que se trabajó en la presente investigación es del 5%, α = 0,05

Para determinar la relación existente entre las Características de SQL Server 2005 y la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA, se procedió a seleccionar dos preguntas del cuestionario planteado, a continuación, se listan mencionadas preguntas.

Pregunta 2. ¿En matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad. SQL Server 2005 está dotado para cumplir esos requerimientos?

Pregunta 6. ¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?

4.2.3 Frecuencias observadas

En el cuadro 13, se ilustra las frecuencias observadas.

VARIABLE	PREGUNTAS	FRECUENCIAS		
		SI	NO	TOTAL
Variable Independiente	¿En matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad. SQL Server 2005 está dotado para cumplir esos requerimientos?	0	7	7
Variable Dependiente	¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?	7	0	7
	TOTAL	7	7	14

Cuadro 13. Frecuencias observadas
Elaborado por: Investigador

4.2.4 Frecuencias esperadas

En el cuadro 14 y cuadro 15, se ilustra las frecuencias esperadas.

VARIABLE	PREGUNTAS	FRECUENCIAS		
		SI	NO	TOTAL
Variable Independiente	En matriculación estudiantil, evaluación docente u otro escenario en la UTA donde mayor seguridad se exija a SQL Server 2005; éste puede cumplir estos requerimientos	(0+7)*(0+7)/14	(7+0)*(7+0)/14	
Variable Dependiente	¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?	(7+0)*(7+0)/14	(0+7)*(0+7)/14	
	TOTAL			

Cuadro 14. Frecuencias esperadas (1)
Elaborado por: Investigador

VARIABLE	PREGUNTAS	FRECUENCIAS		
		SI	NO	TOTAL
Variable Independiente	¿En matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad. SQL Server 2005 está dotado para cumplir esos requerimientos?	3,5	3,5	7
Variable Dependiente	¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?	3,5	3,5	7
	TOTAL	7	7	14

Cuadro 15. Frecuencias esperadas (2)
Elaborado por: Investigador

4.2.5 Prueba Chi – Cuadrado

Una vez determinadas las frecuencias esperadas, se procedió a calcular el Chi - Cuadrado, ver cuadro 16.

VARIABLE	PREGUNTAS	CÁLCULOS				
		O	E	(O - E)	(O - E)2	(O - E)2/E
VI	SI	0	3,5	-3,5	12,25	3,5
	NO	7	3,5	3,5	12,25	3,5
VD	SI	7	3,5	3,5	12,25	3,5
	NO	0	3,5	-3,5	12,25	3,5
TOTAL		**14**	**14**	**0**	**49**	**14,00**

Cuadro 16. Cálculo del Chi – Cuadrado
Elaborado por: Investigador

El Chi – Cuadrado Calculado es: 14,00

4.2.6 Especificación de los grados de libertad

Para determinar los grados de libertad, se aplicó la siguiente formula:

gl = (Número de columnas - 1) * (Número de filas -1)
gl = (2 – 1) * (2 - 1)
gl = 1

Con el grado de libertad obtenido, el valor del Chi Cuadrado de acuerdo a la tabla de distribución de frecuencias es de 3,8415, en la tabla 1 se ilustra el valor obtenido.

v/p	0,001	0,0025	0,005	0,01	0,025	0,05	0,1	0,15
1	10,8274	9,1404	7,8794	6,6349	5,0239	3,8415	2,7055	2,0722
2	13,8150	11,9827	10,5965	9,2104	7,3778	5,9915	4,6052	3,7942
3	16,2660	14,3202	12,8381	11,3449	9,3484	7,8147	6,2514	5,3170
4	18,4662	16,4238	14,8602	13,2767	11,1433	9,4877	7,7794	6,7449
5	20,5147	18,3854	16,7496	15,0863	12,8325	11,0705	9,2363	8,1152
6	22,4575	20,2491	18,5475	16,8119	14,4494	12,5916	10,6446	9,4461
7	24,3213	22,0402	20,2777	18,4753	16,0128	14,0671	12,0170	10,7479
8	26,1239	23,7742	21,9549	20,0902	17,5345	15,5073	13,3616	12,0271
9	27,8767	25,4625	23,5893	21,6660	19,0228	16,9190	14,6837	13,2880

Tabla 1. Tabla de distribución de frecuencias
Fuente: http://labrad.fisica.edu.uy/docs/tabla_chi_cuadrado.pdf

4.2.7 Decisión estadística

En el gráfico 34, se representa los valores obtenidos según Chi - Cuadrado.

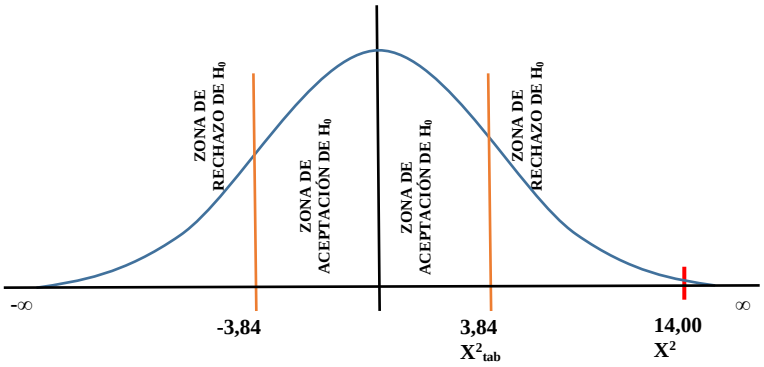


Gráfico 34. Zona de aceptación y rechazo según Chi – Cuadrado
Elaborado por: Investigador

X^2_{tab} = Valor obtenido de la tabla de distribución de Chi – Cuadrado. (Ver Tabla 1. Tabla de distribución de frecuencias)

X^2 = Valor obtenido del cálculo de Chi – Cuadrado. (Ver Cuadro 16. Cálculo del Chi – Cuadrado)

Si $X^2 > X^2 t_{ab}$ se rechaza H_0 y se acepta H_1.

14,00 > 3.84

Entonces se rechaza H_0 y se acepta H_1, lo que determina que, las características de SQL Server 2005 **SI** inciden en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- SQL Server 2005 no cumple con los actuales estándares internacionales de seguridad de la información que permitan garantizar el aseguramiento, la confidencialidad e integridad de los datos de la DITIC.

- SQL Server 2005 no está dotado con las características que le permitan ofrecer un alto nivel de seguridad en escenarios en donde la universidad más lo requiera.

- La finalización del contrato de soporte con SQL Server 2005 y en consecuencia la desactualización de la herramienta, dejarían a los datos de la DITIC vulnerables para ataques informáticos exitosos.

- La DITIC no cuenta con procesos de mantenimiento preventivo frente a nuevas vulnerabilidades que podría presentar SQL Server 2005, vulnerabilidades que podrían ser la puerta de acceso a intromisiones y un serio problema en la seguridad de la información.

- SQL Server 2005 en la DITIC, permite elevación de privilegios y ejecución remota de código en el sistema, a través de vulnerabilidades detectadas en los procedimientos extendidos: xp_cmdshell y sp_replwritetovarbin.

- Los resultados de la investigación confirmaron la hipótesis “Las Características de SQL Server 2005 SI influyen en la seguridad de los datos de la Dirección de Tecnología de Información y Comunicación de la UTA”, factor que deja en evidencia los potenciales riegos a los que esta expuestos los datos que se maneja en la DITIC.

5.2 Recomendaciones

- Implementar mecanismos de revisión y verificación del software utilizado en la gestión de información de la DITIC con la finalidad de prevenir la utilización de herramientas sin soporte e incluso con características descontinuadas.

- Se recomienda realizar un cambio a la versión de SQL Server 2016, última versión de SQL Server que cuenta con características de alta seguridad de la información según estándares internacionales actuales y además cuenta con actualizaciones y revisiones de seguridad (soporte). Factores que permitirán mejorar a la DITIC el aseguramiento, la consistencia e integridad de sus datos.

- Elaborar una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016.

CAPÍTULO VI

LA PROPUESTA

6.1 Datos informativos

6.1.1 Título de la propuesta

Guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016, caso práctico Dirección de Tecnología de Información y Comunicación de la UTA.

6.1.2 Institución ejecutora

Universidad Técnica de Ambato

6.1.3 Beneficiarios

Dirección de Tecnología de Información y Comunicación de la UTA
Estudiantes
Docentes

6.1.4 Ubicación

País: Ecuador
Provincia: Tungurahua
Cantón: Ambato
Dirección: Av. Colombia y Chile

6.1.5 Equipo técnico responsable

Investigador: Ing. Alex Paucar
Personal de la DITIC de la UTA

6.2 Antecedentes de la propuesta

La DITIC es la encargada del desarrollo de varios sistemas académicos para la UTA, sistemas cuya información en su mayoría se encuentra almacenada y gestionada por SQL Server 2005.

Una vez realizado el análisis sobre la utilización de SQL Server 2005 en la DITIC, se logró determinar que sus características no brindan la confianza necesaria en cuanto a seguridad de información, factor que sumado a la terminación de soporte (actualizaciones y revisiones de seguridad) no permite cumplir con estándares internacionales de aseguramiento (integridad, confidencialidad y disponibilidad) de datos.

Se plantea como una propuesta de solución al problema planteado, la implementación de una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 en la DITIC de la UTA; que direccione y asegure de alguna manera el éxito de una migración entre estas versiones de SQL Server.

6.3 Justificación

Una migración de base de datos no es sencilla, no es suficiente el conocimiento de toda la infraestructura que rodea la base de datos (hardware y software), sino también de la utilización y seguimiento de una guía que sirva de soporte y apoyo en todo el proceso de migración; y permita ayudar en el aseguramiento de la integridad, consistencia y disponibilidad de los datos migrados.

La implementación de una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 en la DITIC de la UTA, permitirá a la Dirección no solo asegurar los datos al realizar la migración entre estas dos versiones, sino también servirá de base para futuras migraciones en donde las características de la versión utilizada de SQL Server no garanticen la seguridad de los datos en la Dirección.

6.4 Objetivos

General

- Implementar una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 en la Dirección de Tecnología de Información y Comunicación de la UTA.

Específicos

- Analizar los tipos de migración de base de datos que se pueden realizar entre versiones de SQL Server.
- Desarrollar una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016.
- Aplicar la guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016, en las bases de datos en la Dirección de Tecnología de Información y Comunicación de la UTA.

6.5 Análisis de factibilidad

6.5.1 Factibilidad técnica

Para implementar una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 en la DITIC de la UTA, el investigador cuenta con el conocimiento necesario sobre migración de base de datos y la DITIC cuenta con el software y el licenciamiento requerido.

6.5.2 Factibilidad organizacional

La DITIC de la UTA preocupada por la seguridad de sus datos, ofrece las facilidades de información y apoyo a través del personal dedicado a la gestión de base de datos en la Dirección, para que la implementación de una guía para

migración segura de datos desde SQL Server 2005 a SQL Server 2016 se la pueda realizar.

6.5.3 Factibilidad económica

La DITIC de la UTA, cuenta con el talento humano requerido y el equipamiento necesario para poder implementar una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016.

6.6 Fundamentación

6.6.1 Características de SQL Server 2016 Enterprise

6.6.1.1 Seguridad a nivel de fila

Stacia, Cherry y D'Anthony (2016), al respecto, señalan que:

> SQL Server 2016 maneja la seguridad a nivel de fila (SNF), las misma que permite configurar tablas de manera que los usuarios vean solo las filas a las que se les otorga acceso. Esta función limita las filas que se devuelven al usuario, independientemente de las aplicaciones que las utilice. Puede usar predicados para filtrar silenciosamente las filas a las que puede acceder el usuario cuando ejecuta instrucciones INSERT, UPDATE o DELETE.
>
> Además, puede usar los siguientes predicados de bloque para evitar que el usuario escriba datos: después de insertar, después de actualizar, antes de actualizar y antes de eliminar. Estos predicados de bloque devuelven un error a la aplicación que indica que el usuario está intentando modificar filas que no tiene acceso.

6.6.1.2 Always Encrypted

Para Stacia, Cherry y D'Anthony (2016), Always Encrypted es una tecnología de cifrado del lado de la cliente manejada en SQL Server 2016, en la que:

> Los datos se encriptan automáticamente no solo cuando se escriben, sino también cuando se leen por una aplicación. A diferencia del cifrado de datos

> transparente, que cifra los datos en el disco, pero permite que los datos sean leídos por cualquier aplicación que los consulte, Always Encrypted requiere que su aplicación cliente use un controlador habilitado con cifrado permanente para comunicarse con la base de datos.

Al usar este controlador, la aplicación traslada de forma segura los datos encriptados a la base de datos que luego puede descifrar solo la aplicación que tenga acceso a la clave de cifrado. Cualquier otra aplicación que consulte los datos puede recuperar los valores encriptados, pero no podrá usar los datos sin la clave de cifrado. Debido a esta arquitectura de cifrado, la instancia de SQL Server nunca ve la versión descifrada de los datos.

6.6.1.3 Enmascaramiento de datos dinámicos

Microsoft (2016b), manifiesta que, en SQL Server 2016:

> El enmascaramiento dinámico de datos (DDM) limita la exposición de información confidencial ocultándolos a los usuarios sin privilegios. Se puede usar para simplificar considerablemente el diseño y la codificación de la seguridad en la aplicación.
>
> El enmascaramiento dinámico de datos evita el acceso no autorizado a información confidencial permitiendo que los clientes designen la cantidad de información confidencial que se debe revelar, con un impacto mínimo en la capa de aplicación. DDM se puede configurar en la base de datos para ocultar la información adicional de los conjuntos de resultados de las consultas de campos designados de una base de datos, sin modificar los datos de esta última. El enmascaramiento dinámico de datos resulta fácil de usar con las aplicaciones existentes, ya que las reglas de enmascaramiento se aplican en los resultados de la consulta. Muchas aplicaciones pueden enmascarar información confidencial sin modificar las consultas existentes.

6.6.1.4 Auditoría

Peter (2016), manifiesta que:

> La auditoría de una instancia de motor de base de datos de SQL Server 2016 o de una base de datos individual implica el seguimiento y registro de los eventos que se producen en el motor de base de datos.

> La auditoría de SQL Server 2016 puede asociarse con una o más especificaciones de auditoría de servidor y especificaciones de auditoría de base de datos. Las especificaciones definen la actividad que captura la auditoría a nivel de instancia y de base de datos, respectivamente. (p. 35)

Los eventos auditados se pueden escribir en los registros de eventos o en los archivos de auditoría.

6.6.1.5 Administración extensible de claves

"SQL Server 2016 proporciona las funciones de cifrado de datos junto con la Administración Extensible de Claves (EKM). Las claves de cifrado utilizadas para cifrar datos y claves se crean en contenedores transitorios de claves y se deben exportar desde un proveedor antes de que se almacenen en la base de datos" (Microsoft, 2017a).

La Administración extensible de claves habilita las claves de cifrado que protegen los archivos de base de datos para que se almacenan en un dispositivo externo, como puede ser una tarjeta inteligente, un dispositivo USB o un módulo EKM/Módulo de seguridad por hardware (HSM). Los datos se pueden cifrar utilizando claves de cifrado a las que solo tiene acceso el usuario de la base de datos en el módulo EKM/ HSM externo.

6.6.1.6 Roles definidos por el usuario

"SQL Server 2016 proporciona un conjunto de funciones de servidor integradas. Estas funciones permiten asignar permisos de nivel de instancia a los inicios de sesión que tienen requisitos comunes. Se llaman roles fijos del servidor y son: sysadmin, bulkadmin, dbcreator, diskadmin, processadmin, public, securityadmin, serveradmin y setupadmin" (Peter, 2016, p. 24).

Adicionalmente a los roles fijos de servidor, SQL Server 2016 permite crear roles de servidor personalizados, para ayudarle al administrador a otorgar un conjunto

personalizado de permisos a un grupo de inicios de sesión, simplificado y ayudando en la tarea de proporcionar y administrar el SGBD.

6.6.1.7 Bases de datos independientes

Microsft (2016c), manifiesta que, en SQL Server 2016:

> Una base de datos totalmente independiente incluye todos los metadatos y opciones de configuración necesarios para definirla y no tiene dependencias de configuración de la instancia de Motor de base de datos donde esté instalada. En versiones anteriores de SQL Server, la separación de una base de datos de la instancia de SQL Server podría necesitar mucho tiempo y un conocimiento detallado de la relación entre la base de datos y la instancia de SQL Server.
>
> Cualquier entidad definida por el usuario que solo se base en las funciones que residen dentro de la base de datos se considera totalmente independiente. Cualquier entidad definida por el usuario que se base en funciones que residen fuera de la base de datos se considera dependiente.

Las ventajas de usar una base de datos independientes son:

- Cuando se mueve una base de datos de una instancia a otra no hay inconvenientes para su funcionamiento adecuado, porque la base de datos trasladada cuenta con toda la información (metadatos y demás configuraciones) definida dentro de la misma base de datos.

- La creación de usuarios contenidos permite al usuario conectarse directamente a la base de datos independiente. Esta es una característica muy importante en escenarios de alta disponibilidad y recuperación ante desastres. Los usuarios podrán conectarse al servidor secundario sin crear nuevos inicios de sesión.

6.6.1.8 Cifrados para copias de seguridad

“SQL Server tiene la capacidad de cifrar los datos mientras crea una copia de seguridad. Al especificar el algoritmo y el sistema de cifrado (un certificado o una

clave asimétrica) al crear una copia de seguridad, puede crear un archivo de copia de seguridad cifrado" (Microsoft, 2016d).

Es muy importante realizar una copia de seguridad del certificado o la clave asimétrica, y preferiblemente en almacenarlo en una ubicación diferente de la que se usó para cifrar el archivo de copia de seguridad. Sin el certificado o la clave asimétrica, no se podrá restaurar la copia de seguridad, lo que deja inutilizable el archivo de copia de seguridad.

6.6.1.9 Comparativa entre SQL Server 2005 y SQL Server 2016

En el cuadro 17, se ilustra una comparativa de las características de seguridad entre SQL Server 2005 y SQL Server 2016.

SQL Server 2016	**SQL Server 2005**
Seguridad a nivel de fila	Seguridad a nivel de Tabla, vista, función, etc.
Always Encrypted (cifrado permanente), tecnología de cifrado del lado del cliente.	Cifrado a nivel de servidor.
Enmascaramiento de datos dinámicos	No soporta, se lo puede hacer mediante programación.
SQL Server Audit Permite realizar auditoría para eventos de servidor y base de datos Se puede especificar las actividades o eventos a auditar.	Auditoría modo C2 No es parametrizable, se audita todo o nada. Mayor consumo de especio en disco Disminución en el rendimiento del SGBD
Administración extensible de claves, almacenamiento externo de claves: EKM, HSM, dispositivo USB, etc.	El motor de base de datos posee una infraestructura interna de cifrado y administración de claves.
Roles definidos por el usuario	Cuenta con roles fijos de servidor. No se puede agregar ni eliminar roles a nivel de servidor.
Bases de datos independientes	Los metadatos y configuraciones de las bases de datos pueden provenir de objetos externos. Bases de datos Dependientes
Cifrados para copias de seguridad	No soporta el cifrado de copias de seguridad
Cuenta con soporte	EL soporte finalizo en abril de 2016

Cuadro 17. Comparativa SQL Server 2005 – SQL Server 2016
Elaborado por: Investigador

Se denota en el cuadro 17, mejoras en las características de seguridad ofrecidas por SQL Server 2016 respecto a SQL Server 2005, como; mayor granularidad en los niveles de seguridad, cifrado permanente, auditoría personalizable, administración extensible de claves y cifrado de respaldos; todo esto sumado a que Microsoft únicamente ofrece soporte (actualizaciones y revisiones de seguridad) a SQL Server 2016.

6.6.2 Migración de base de datos

Definiciones

"La migración de base de datos es la selección, preparación, extracción, transformación y el movimiento de datos apropiado; con la calidad adecuada, en el lugar propicio y en el momento correcto" (Morris, 2012).

"La migración de base de datos es el proceso de transferencia de datos entre almacenes, en otras palabras, es el proceso de mover los datos de la antigua base de datos a una nueva base de datos" (Paygude & Devale, 2013, p.599).

"También supone reescribir sentencias de lenguaje de consulta estructurada (SQL) o incluso procedimientos almacenados (SP) de lógica de negocio, con la finalidad de adaptarlos al nuevo servidor de destino" (Celis, 2014, p.142).

Los proyectos de migración de datos pueden surgir de varias formas.

La forma clásica es cuando un nuevo sistema está siendo implementado y necesita ser alimentado con datos del sistema anterior. También hay programas de consolidación de sistemas, que pueden ser generados por fusiones de empresas o por normalización. Hay actualizaciones del sistema, y éstas también requieren la migración de datos (Morris, 2012).

6.6.2.1 Tipos de migración de base de datos

Microsoft (2017b), considera que:

Existen varios enfoques que se deben considerar a la hora de planear la actualización o migración del Motor de base de datos de una versión previa de SQL Server a una nueva versión con el objetivo de minimizar el tiempo de inactividad y los riesgos.

- Actualización local
- Migración a una nueva instalación
- Actualización gradual

Actualización local

Con este tipo de actualización, el programa de instalación de SQL Server actualiza la instalación existente reemplazando la instancia de SQL Server por la nueva versión, después, actualiza cada una de las bases de datos de usuario y del sistema. Este tipo de actualización es el más sencillo, conlleva la menor cantidad de tiempo de inactividad, pero no se aplica en todos los escenarios (Micosoft, 2016e).

En el caso de SQL Server 2016, Micosoft (2016e), detalla los siguientes escenarios no admitidos en una actualización local:

- No se admiten instancias de SQL Server 2016 de distintas versiones. Los números de versión de Motor de base de datos, Analysis Services y Reporting Services deben ser los mismos en una instancia de SQL Server 2016.

- SQL Server 2016 solo está disponible para plataformas de 64 bits. No puede actualizar una instancia de 32 bits de SQL Server a 64 bits nativo con el programa de instalación de SQL Server.

- No puede agregar características nuevas durante la actualización de una instancia existente de SQL Server. Después de actualizar una instancia de SQL Server a SQL Server 2016, puede agregar características mediante el programa de instalación de SQL Server 2016.

Además, SQL Server solo admite la actualización local de las siguientes versiones:

- SQL Server 2008 SP4 o posterior
- SQL Server 2008 R2 SP2 o posterior
- SQL Server 2012 SP2 o posterior
- SQL Server 2014 o posterior

Se puede denotar que la versión de SQL Server 2005 no permite mencionada actualización local.

Migración a una nueva instalación

"Con este enfoque, se conserva el entorno actual a la vez que se crea un entorno de SQL Server nuevo, con frecuencia en nuevo hardware y con una nueva versión del sistema operativo. Después de instalar la nueva versión, debe realizar una serie de pasos a fin de poder realizar la migración y minimizar el tiempo de inactividad" (Microsoft, 2017b).

"Algunas aplicaciones dependen de información, entidades u objetos que se encuentran fuera del ámbito de una sola base de datos de usuario, a los que se denomina objetos de sistema. Cualquier elemento almacenado fuera de la base de datos de usuario que sea necesario para el funcionamiento correcto de dicha base de datos debe estar disponible en la instancia del nuevo servidor" (Microsoft, 2017b).

"Una vez que el nuevo entorno de SQL Server cuente con los mismos objetos de sistema que el antiguo, deberá migrar las bases de datos de usuario con un método que minimice el tiempo de inactividad en dicho sistema" (Microsoft, 2017b).

Actualización gradual

"Una actualización gradual consiste básicamente en la actualización de varias instancias de SQL Server en un orden determinado, ya sea mediante una

actualización local en cada instancia de SQL Server existente o efectuando una actualización con una nueva instalación a fin de facilitar la actualización del hardware o el sistema operativo como parte del proyecto de actualización" (Microsoft, 2017b).

6.6.2.2 Proceso de migración

Según González (2014), para la realización de una migración segura se debe descomponer el proceso de migración en tres pasos:

> Extracción, Transformación y Carga (ETL): en este proceso, es donde realmente se trasladan los datos desde las bases de datos iniciales. Se realiza una transformación y purga de datos para ponerlos en un formato compatible y aceptable para el sistema al cual se migran los datos y, finalmente, se realiza la carga a la nueva base de datos.
>
> Extracción
> Es el primer paso del proceso, en el que se procede a extraer los datos que se quiere migrar.
>
> Transformación
> En esta fase de transformación se aplica a una serie de reglas o funciones sobre los datos, que previamente se han extraído para transformarlos en otros que se pueden cargar.
>
> Carga
> Aquí los datos procedentes de la fase de transformación se cargan en la base de datos destino

"Todo proceso de migración acostumbra a disponer de tres pasos: extracción de la información, transformación de la información y carga de la información". (Vilela, 2016).

6.6.2.3 Nivel de compatibilidad SQL Server

Según (Microsoft, 2017), el nivel de compatibilidad es una opción que ofrece toda versión de SQL Server, y fue implementada con la finalidad de ayudar en los procesos de migración.

En la tabla 2, se puede observar las versiones de SQL Server y su nivel de compatibilidad, junto a los niveles soportados.

Versión	Nivel de compatibilidad asignado	Soporta
SQL Server 2016	130	130, 120, 110, 100
SQL Server 2014	120	120, 110, 100
SQL Server 2012	110	110, 100, 90
SQL Server 2008 R2	100	100, 90, 80
SQL Server 2008	100	100, 90, 80
SQL Server 2005	90	90, 80
SQL Server 2000	80	80

Tabla 2. Niveles de compatibilidad SQL Server
Fuente. https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-database-transact-sql-compatibility-level

Cada nivel de compatibilidad registra algún cambio, aumento o eliminación de características (palabras reservadas, tipos de datos, incremento de funciones, procedimientos, etcétera); las mismas que deben ser analizadas cuando se produzca una migración y se modifique el nivel de compatibilidad de las bases de datos.

Palabras reservadas

Las palabras reservadas son uno de los cambios que generalmente es evidente en los diferentes niveles, en la tabla 3 se detalla las palabras reservadas introducidas en cada nivel de compatibilidad:

Nivel de compatibilidad	Palabras reservadas
130	No determinado
120	Ninguna
110	WITHIN GROUP, TRY_CONVERT, SEMANTICKEYPHRASETABLE, SEMANTICSIMILARITYDETAILSTABLE, SEMANTICSIMILARITYTABLE
100	CUBE, MERGE, ROLLUP
90	EXTERNAL, PIVOT, UNPIVOT, REVERT, TABLESAMPLE

Tabla 3. Palabras reservadas SQL Server
Fuente: https://docs.microsoft.com/en-us/sql/t-sql/statements/alter-database-transact-sql-compatibility-level

6.7 Metodología

Para la implementación de una guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016, se optó por seguir etapas estándares que todo proyecto de migración las tiene, las etapas de extracción, transformación y carga. Además, se incluyeron las etapas de análisis, pruebas y control de desastres, con la finalidad de asegurar el traslado seguro de datos.

6.7.1 Guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016

6.7.1.1 Introducción

La DITIC de la Universidad Técnica de Ambato es la encargada del control, almacenamiento y seguimiento de la información generada por los sistemas de información de la universidad, gestión que se la realiza en su mayoría a través del SGBD SQL Server.

SQL Server es un producto soportado por Microsoft y que a través de versiones es lanzado al mercado, versiones cuyo ciclo de vida puede llegar a su fin y es necesario una migración o actualización hacia nuevas versiones soportadas y mejoradas según requerimientos actuales. La seguridad es la mayor preocupación al terminar el ciclo de vida de SQL Server ya que el software no contará con parches o actualizaciones de seguridad y le dejarán vulnerable a nuevas formas de ataques informáticos y a fallos por errores no detectados.

Un proceso de migración de base de datos puede resultar bastante complejo e incluso llegar al fracaso, si es que no se siguen los debidos procedimientos, que permitan garantizar que la base de datos migrada muestre características de confiabilidad, integridad, veracidad y consistencia en sus datos; en otras palabras, que se logre una base de datos migrada con éxito.

6.7.1.2 Alcance

La presente guía aplica a la migración de base de datos desde SQL Server 2005 a SQL Server 2016.

6.7.1.3 Responsables

El **Director de Tecnología** de la empresa o institución es el responsable de hacer cumplir los procedimientos detallados en la presente guía.

El **Responsable del Área de Gestión de Bases de Datos** junto con su personal, son los encargados de coordinar y de aplicar los procedimientos de la presente guía.

6.7.1.4 Definiciones

Instancia
Es un servicio de SQL Server que administra varias bases de datos. Las aplicaciones se conectan a la instancia para realizar el trabajo en una base de datos.

Service Pack
Es un conjunto de actualizaciones que corrigen y mejoran aplicaciones y sistemas operativos.

Script
Es un conjunto de órdenes guardadas en un archivo de texto, generalmente muy ligero, que es ejecutado por lotes o línea a línea, en tiempo real por un intérprete.

6.7.1.5 Procesos

Para la realización de la migración se contempla los siguientes procesos:

a. Análisis

b. Pruebas
c. Control de desastres
d. Extracción, transformación y carga de datos

a. Análisis

Levantamiento de requerimientos

Una vez acogida la solicitud formal de migración o actualización de bases de datos SQL Server, el área de Gestión de Base de Datos, deberá realizar el correspondiente levantamiento de requerimientos.

Para realizar el levantamiento de requerimientos, el responsable deberá basarse en los siguientes aspectos:

- Que bases de datos serán migradas

- Períodos de mayor demanda, ¿con qué frecuencia? y ¿qué? aplicaciones utilizan las bases de datos a ser migradas. Con el objetivo de identificar y establecer periodos de inactividad necesarios en un proceso de migración.

- Identificar los componentes internos de la o las bases de datos a ser migradas.

    - Tablas
    - Procedimientos
    - Triggers
    - Funciones
    - Reglas
    - Tipos de datos
    - Vistas
    - Usuarios de base de datos
    - Roles de base de datos

- Identificar los componentes externos de la o las bases de datos a ser migradas.

    - Inicios de sesión
    - Roles de servidor
    - Vistas externas: Consultas con fuentes (tablas o vistas) que pudieran estar en diferentes bases de datos y que pudieran no estar presentes en el nuevo entorno.
    - Servidores vinculados: Enlaces a bases de datos gestionadas en diferentes servidores
    - Trabajos: Procesos automáticos ejecutados por SQL Server.
    - Tablas maestras
    - Sinónimos
    - Otros

- Se va a realizar una depuración de los datos inconsistentes o se moverán todos los datos.

Planificación de la migración

En esta etapa se debe especificar el alcance que tendrá la migración, se debe considerar que bases de datos se van a migrar y el tipo de migración que se va a realizar.

El responsable de la migración de base de datos deberá realizar una planificación basada en objetivos, en la que deberá constar tiempos, responsables y actividades.

Se recomienda que la planificación deba ser concisa y precisa, según el cuadro 18.

Objetivos	Actividad	Fecha Inicio	Fecha Fin	Responsables

Cuadro 18. Matriz de planificación
Elaborado por: Investigador

El Director de Tecnología será el encargado de monitorear el cumplimiento de la planificación de la migración, que todas las actividades y objetivos se cumplan de acuerdo con los tiempos establecidos. Si existiera algún retraso en las actividades planificadas, éstas deberán contar con su respectiva justificación debidamente documentada.

Requerimientos de hardware y software

El responsable de la migración se encargará de identificar y especificar las características del hardware donde se implementará SQL Server 2016. En este procedimiento se identificará: disco duro (capacidad de almacenamiento y tecnología), memoria RAM, procesador (Velocidad, tipo, cache interna, número de núcleos, etc.).

El responsable de la migración se encargará de identificar y especificar las características del software donde se implementará SQL Server 2016. En este procedimiento se identificará: el sistema de archivos (NTFS, ReFS, etc.); el particionamiento; la arquitectura, versión y edición del Sistema Operativo. Es necesario que la plataforma del sistema operativo sea Windows, versión servidor y con arquitectura de 64 bits (debido SQL Server 2016 y futuras versiones no están disponibles para sistemas operativos de 32 bits), además es necesario que el hardware también soporte mencionadas requerimientos.

b. Pruebas

La fase de pruebas se encuentra presente en todo el proceso de migración, se propone al responsable de la migración crear escenarios intermedios en donde valide y someta a los datos a ciclos de pruebas y simulaciones de carga, antes de realizar la carga de datos final al nuevo servidor de base de datos y que los datos migrados lleguen al destino en forma segura.

Los posibles problemas que se pudieran detectar están relacionados a los niveles de compatibilidad entre estas dos versiones (características en desuso o características no incluidas en SQL Server 2016) y las características de las bases de datos migradas. Se recomienda utilizar pruebas de unidad para la detección de errores.

Pueden existir errores de fácil detección, que ocasionen la no ejecución o la no restauración del respaldo en SQL Server 2016 y su solución es necesaria para la continuidad de la migración; pero puede existir errores que provoquen que el resultado entregado no sea el correcto y no generen alertas, por lo que es importante verificar que cada uno de los componentes de las bases de datos migradas entreguen los resultados esperados.

c. Control de desastres

Transportar datos de una plataforma a otra implica riesgos en la seguridad de los mismos, riesgos que comprometen el activo más valioso que puede tener una empresa o institución. A continuación, se detallan medidas que permitirán reducir el riesgo en la seguridad de los datos:

1. Respaldos de base de datos

El último respaldo de la base de datos, el que será cargado en el nuevo entorno (SQL Server 2016), no deberá contener transacciones en línea generadas por usuarios que en ese instante estén conectados a mencionada base de datos. La omisión de esta medida podría ocasionar que el nuevo entorno no contenga la base de datos con toda la información, ocasionando perdida e inconsistencias en los datos.

Para asegurar que la base de datos origen (SQL Server 2005) no contenga transacciones en línea, configurar la base de datos en modo “SINGLE USER” antes de realizar el respaldo a ser migrado.

2. Base de datos origen y destino en funcionamiento

Otra medida a tomar en cuenta es nunca dejar en funcionamiento las base de datos origen (SQL Server 2005) y destino (SQL Server 2016), se recomienda que, cuando la base de datos destino entre en producción necesariamente la base de datos origen debe ser deshabilitada, por lo menos hasta asegurarnos que todas las cadenas de conexión que vinculan a la base de datos origen hayan sido actualizadas, con esto garantizamos que ninguna aplicación consuma o escriba en la base de datos origen y por ende cause inconsistencias en los datos.

3. Seguridad de respaldos

En un proceso de migración los respaldos de las bases de datos se encuentran más vulnerables o expuestos a terceros que en otras situaciones, es posible que, por el hecho de realizar validaciones, simulación de escenarios en ambientes de prueba, el responsable de la migración se encuentre proclive a errores que permitan el acceso no autorizado. Se recomienda seguir estrictamente las políticas de la dirección en cuento al manejo de respaldos y si no hubiera una política o norma, seguir las siguientes medidas:

- Los respaldos generados o entregados al personal deberán ser registrados en documentos para el efecto, en el que conste el responsable, fecha de entrega y motivo.

- Los ambientes de prueba creados para la migración deberán contar con controles de acceso (usuario y contraseña) y deberán ser eliminados luego de la culminación del proceso de migración.

- La migración deberá siempre realizarse en el área de trabajo, bajo ningún motivo los respaldos podrán salir de la institución.

d. Extracción, Transformación y Carga de datos

Realmente no existe una ruta de migración directa a SQL Server 2016 desde SQL Server 2005, pero se puede llegar mediante el uso de SQL Server 2008 como el paso intermedio o provisional de migración de forma segura.

Los siguientes pasos ayudaran a migrar las bases de datos desde SQL Server 2005 a SQL Server 2016, estos pasos son esencialmente para poder cumplir los objetivos dentro de las necesidades de la empresa o institución.

1. Instalar una copia separada de SQL Server 2016

El primer paso es instalar una instancia independiente de SQL Server 2016. Este será típicamente en el hardware y sistema operativo especificado en el paso "Requerimientos de hardware y software". Si la nueva instalación se encuentra en la misma red que el sistema original, se necesitará un nombre de instancia diferente, la misma que puede ser cambiada más adelante.

Se recomienda que la codificación de caracteres del servidor SQL Server 2016 sea la misma respecto al servidor SQL Server 2005 (servidor origen). Ver gráfico 35.

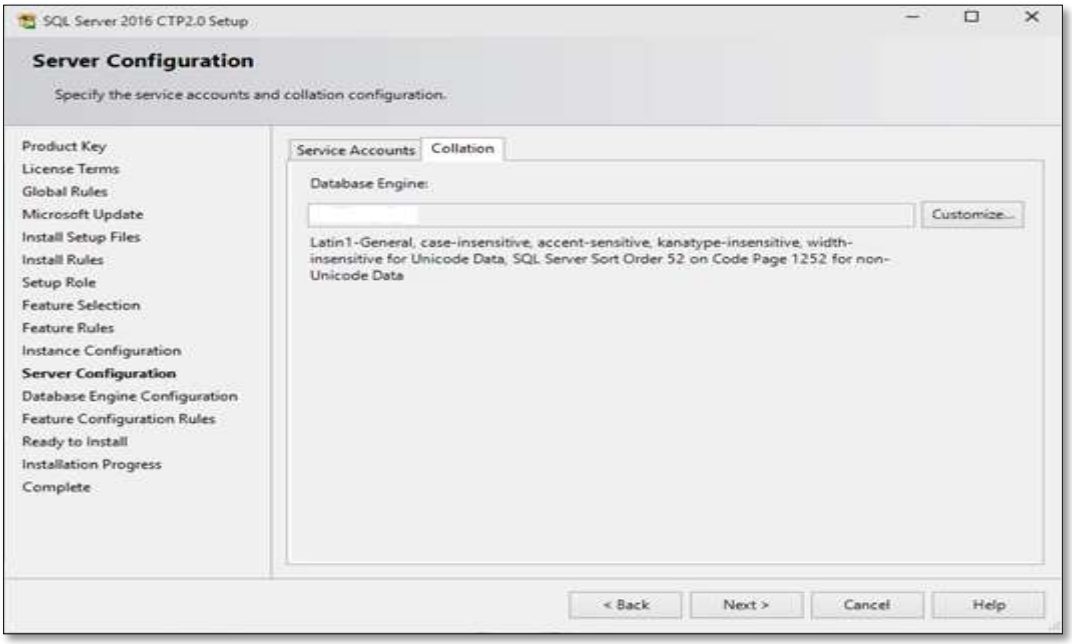


Gráfico 35. Configuración COLLATE
Elaborado por: Investigador

2. Asegurar que SQL Server 2005 está en el último Service Pack (Service Pack 4). Se puede comprobar el nivel del Service Pack utilizado por SQL Server, realizando la siguiente consulta:

SELECT SERVERPROPERTY ('productversion'), SERVERPROPERTY ('ProductLevel'), SERVERPROPERTY ('edición')

Si el nivel del Service Pack es inferior a 4, entonces se necesitará la actualización de Service Pack antes de continuar. Con esto se asegura que el nivel de compatibilidad de SQL Server 2005 tenga las actualizaciones y correcciones necesarias para la migración.

3. Realizar una copia de seguridad de todas las bases de datos a ser migradas

Después de haber actualizado el sistema de origen a SQL Server 2005 Service Pack 4, se debe realizar una copia de seguridad completa de todas las bases de datos que se migrarán. Ver gráfico 36

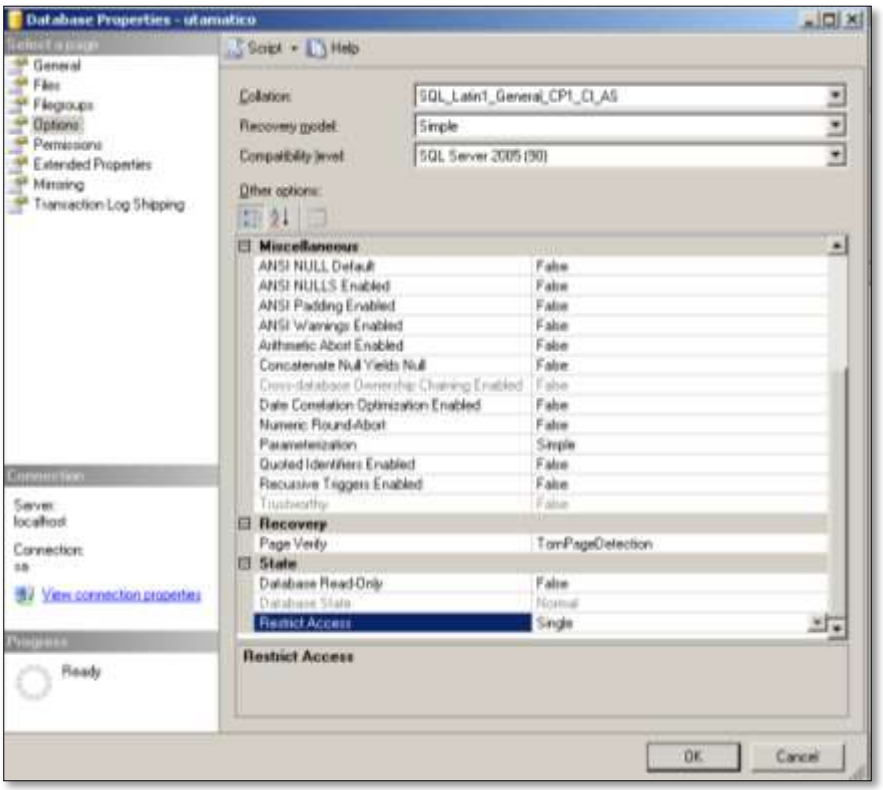


Gráfico 36. Modo de usuario
Elaborado por: Investigador

4. Instalar una copia intermedia de SQL Server 2008 o SQL Server 2008 R2.

Esta copia sólo será utilizada para convertir las copias de seguridad del formato anterior de SQL Server 2005 (nivel de compatibilidad 90) que no pueden ser restauradas a SQL Server 2016 a un formato compatible. La instalación de la instancia SQL Server 2008 / R2 se la puede realizar en cualquier sistema operativo, pero sería más conveniente que la instalación de ésta se la haga en el mismo sistema operativo donde se encuentra SQL Server 2016 (servidor destino).

5. Instalar el Service Pack adecuado en SQL Server 2008 o SQL Server 2008 R2 provisional.

Se puede comprobar el nivel del Service Pack utilizado por SQL Server, realizando la siguiente consulta:

SELECT SERVERPROPERTY ('productversion'), SERVERPROPERTY ('ProductLevel'), SERVERPROPERTY ('edición')

Si se utiliza SQL Server 2008, entonces se debe instalar el Service Pack 2. Si se utiliza SQL Server 2008 R2, entonces se necesita el Service Pack 1.

6. Restaurar la copia de seguridad de base de datos SQL Server 2005 en el sistema provisional SQL Server 2008/R2 que ha sido instalado provisionalmente.

7. En este punto las bases de datos SQL Server 2005 se habrán restaurado al 100% en SQL Server 2008/R2 y se habrán convertido en un formato más reciente. El siguiente paso es realizar una copia de seguridad de estas bases de datos provisionales (SQL Server 2008/R2) para su posterior restauración en SQL Server 2016. Una vez completada estas copias de seguridad, es recomendable eliminar la instancia.

8. El siguiente paso es tomar las copias de seguridad de las bases de datos de SQL Server 2008 / R2 y restaurarlas a SQL Server 2016.

9. Trasladar los inicios de sesión

Todas las bases de datos migradas y que se encuentran en el servidor SQL Server 2016 tienen usuarios huérfanos (se denomina usuario huérfano al usuario de base de datos que no cuenta con un inicio de sesión), debido a que únicamente fueron trasladadas las bases de datos al nuevo servidor y no sus componentes externos.

Para garantizar que la base de datos en el nuevo servidor (SQL SERVER 2016) no tenga usuarios huérfanos, es necesario transferir los inicios de sesión y contraseñas.

Para lo cual se debe:

- Ejecutar en SQL Server 2005 (origen) el siguiente script.

```
USE master
GO
IF OBJECT_ID ('sp_hexadecimal') IS NOT NULL
  DROP PROCEDURE sp_hexadecimal
GO
CREATE PROCEDURE sp_hexadecimal
    @binvalue varbinary(256),
    @hexvalue varchar (514) OUTPUT
AS
DECLARE @charvalue varchar (514)
DECLARE @i int
DECLARE @length int
DECLARE @hexstring char(16)
SELECT @charvalue = '0x'
SELECT @i = 1
SELECT @length = DATALENGTH (@binvalue)
SELECT @hexstring = '0123456789ABCDEF'
WHILE (@i <= @length)
BEGIN
  DECLARE @tempint int
  DECLARE @firstint int
  DECLARE @secondint int
  SELECT @tempint = CONVERT(int, SUBSTRING(@binvalue,@i,1))
  SELECT @firstint = FLOOR(@tempint/16)
  SELECT @secondint = @tempint - (@firstint*16)
  SELECT @charvalue = @charvalue +
    SUBSTRING(@hexstring, @firstint+1, 1) +
    SUBSTRING(@hexstring, @secondint+1, 1)
```

```
  SELECT @i = @i + 1
END

SELECT @hexvalue = @charvalue
GO

IF OBJECT_ID ('sp_help_revlogin') IS NOT NULL
  DROP PROCEDURE sp_help_revlogin
GO
CREATE PROCEDURE sp_help_revlogin @login_name sysname = NULL AS
DECLARE @name sysname
DECLARE @type varchar (1)
DECLARE @hasaccess int
DECLARE @denylogin int
DECLARE @is_disabled int
DECLARE @PWD_varbinary  varbinary (256)
DECLARE @PWD_string  varchar (514)
DECLARE @SID_varbinary varbinary (85)
DECLARE @SID_string varchar (514)
DECLARE @tmpstr  varchar (1024)
DECLARE @is_policy_checked varchar (3)
DECLARE @is_expiration_checked varchar (3)

DECLARE @defaultdb sysname

IF (@login_name IS NULL)
  DECLARE login_curs CURSOR FOR

     SELECT p.sid, p.name, p.type, p.is_disabled, p.default_database_name,
l.hasaccess, l.denylogin FROM
sys.server_principals p LEFT JOIN sys.syslogins l
     ON ( l.name = p.name ) WHERE p.type IN ( 'S', 'G', 'U' ) AND p.name <> 'sa'
ELSE
  DECLARE login_curs CURSOR FOR


     SELECT p.sid, p.name, p.type, p.is_disabled, p.default_database_name,
l.hasaccess, l.denylogin FROM
sys.server_principals p LEFT JOIN sys.syslogins l
     ON ( l.name = p.name ) WHERE p.type IN ( 'S', 'G', 'U' ) AND p.name =
@login_name
OPEN login_curs

FETCH NEXT FROM login_curs INTO @SID_varbinary, @name, @type, @is_disabled,
@defaultdb, @hasaccess, @denylogin
IF (@@fetch_status = -1)
BEGIN
  PRINT 'No login(s) found.'
  CLOSE login_curs
```

```
  DEALLOCATE login_curs
  RETURN -1
END
SET @tmpstr = '/* sp_help_revlogin script '
PRINT @tmpstr
SET @tmpstr = '** Generated ' + CONVERT (varchar, GETDATE()) + ' on ' +
@@SERVERNAME + ' */'
PRINT @tmpstr
PRINT ''
WHILE (@@fetch_status <> -1)
BEGIN
  IF (@@fetch_status <> -2)
  BEGIN
    PRINT ''
    SET @tmpstr = '-- Login: ' + @name
    PRINT @tmpstr
    IF (@type IN ( 'G', 'U'))
    BEGIN -- NT authenticated account/group

      SET @tmpstr = 'CREATE LOGIN ' + QUOTENAME( @name ) + ' FROM WINDOWS
WITH DEFAULT_DATABASE = [' + @defaultdb + ']'
    END
    ELSE BEGIN -- SQL Server authentication
       -- obtain password and sid
          SET @PWD_varbinary = CAST( LOGINPROPERTY( @name, 'PasswordHash' ) AS
varbinary (256) )
       EXEC sp_hexadecimal @PWD_varbinary, @PWD_string OUT
       EXEC sp_hexadecimal @SID_varbinary,@SID_string OUT

       -- obtain password policy state
       SELECT @is_policy_checked = CASE is_policy_checked WHEN 1 THEN 'ON' WHEN
0 THEN 'OFF' ELSE NULL END FROM sys.sql_logins WHERE name = @name
       SELECT @is_expiration_checked = CASE is_expiration_checked WHEN 1 THEN
'ON' WHEN 0 THEN 'OFF' ELSE NULL END FROM sys.sql_logins WHERE name = @name

          SET @tmpstr = 'CREATE LOGIN ' + QUOTENAME( @name ) + ' WITH PASSWORD
= ' + @PWD_string + ' HASHED, SID = ' + @SID_string + ', DEFAULT_DATABASE = [' +
@defaultdb + ']'

       IF ( @is_policy_checked IS NOT NULL )
       BEGIN
         SET @tmpstr = @tmpstr + ', CHECK_POLICY = ' + @is_policy_checked
       END
       IF ( @is_expiration_checked IS NOT NULL )
       BEGIN
         SET @tmpstr = @tmpstr + ', CHECK_EXPIRATION = ' + @is_expiration_checked
       END
    END
    IF (@denylogin = 1)
```

```
  BEGIN -- login is denied access
   SET @tmpstr = @tmpstr + '; DENY CONNECT SQL TO ' + QUOTENAME( @name )
  END
  ELSE IF (@hasaccess = 0)
  BEGIN -- login exists but does not have access
   SET @tmpstr = @tmpstr + '; REVOKE CONNECT SQL TO ' + QUOTENAME( @name )
  END
  IF (@is_disabled = 1)
  BEGIN -- login is disabled
   SET @tmpstr = @tmpstr + '; ALTER LOGIN ' + QUOTENAME( @name ) + ' DISABLE'
  END
  PRINT @tmpstr
 END

 FETCH NEXT FROM login_curs INTO @SID_varbinary, @name, @type, @is_disabled,
@defaultdb, @hasaccess, @denylogin
  END
CLOSE login_curs
DEALLOCATE login_curs
RETURN 0
GO
```

El resultado de la ejecución del script genera dos procedimientos almacenados en la base de datos master, denominados sp_hexadecimal y sp_help_revlogin

- Ejecutar en SQL Server 2005 (origen) el procedimiento "sp_help_revlogin" generado en el paso anterior. La ejecución del procedimiento genera un script con la información de inicios de sesión de servidor con sus respectivas contraseñas. Ver gráfico 37.

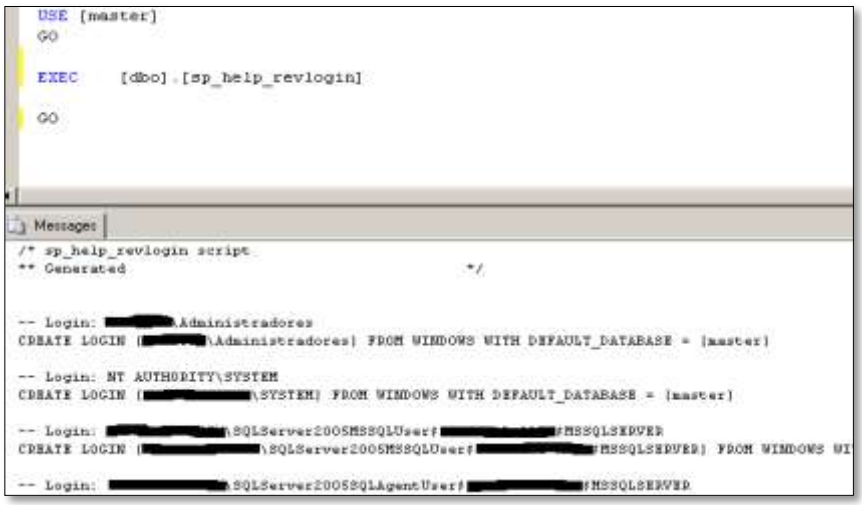


Gráfico 37. Ejecución procedimiento
Elaborado por: Investigador

- Copiar el resultado de la ejecución del procedimiento almacenado sp_help_revlogin y ejecutarlo en SQL Server 2016; se generar todos los inicios de sesión y demás información relacionada con los usuarios de las bases de datos migradas.

10. Identificar y crear manualmente: servidores vinculados, trabajos, tablas maestras y otros componentes externos.

11. Si se llegó a este punto significa que las bases de datos fueron migradas con éxito desde SQL Server 2005 a SQL Server 2016, las bases de datos funcionan en la nueva versión.

6.7.2 Aplicación de la guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016, en las bases de datos de la Dirección de Tecnología de Información y Comunicación de la UTA.

a. Análisis

Especificación de requerimientos

La DITIC de la UTA requiere realizar una migración de sus bases de datos, desde SQL Server 2005 hacia SQL Server 2016, según los siguientes requerimientos:

1. Migrar las bases de datos del cuadro 19

Base de Datos	Descripción
dbDistributivo	Contiene información referente al distributivo docente de la Universidad Técnica de Ambato.
dbPracticas	Contiene información referente a los proyectos de prácticas pre profesionales de formación académica de la Universidad Técnica de Ambato y proyectos de vinculación de la facultad de Ciencias de la Salud de la Universidad Técnica de Ambato.

Cuadro 19. Listado de base de datos
Elaborado por: Investigador

Base de Datos	Descripción
DbTutorias	Contiene información referente a tutorías de docentes y estudiantes de la Universidad Técnica de Ambato.
Utamatico	Contiene la mayor parte de información académica generada en la Universidad Técnica de Ambato.

Cuadro 19. (cont.)

2. Debido a las altas exigencias de disponibilidad y la criticidad de la información que se gestiona en las bases de datos a migrar, los periodos de inactividad necesarios para la migración deberán estar contemplados para los fines de semana y con previa autorización del director.

3. Se migrarán todos los componentes internos de cada una de las bases de datos, como: tablas, procedimientos, triggers, funciones, reglas, tipos de datos, vistas, etc.

4. Se migrarán todos los componentes externos que se encuentren relacionados con las bases de datos, como: inicios de sesión, roles de servidor, vistas externas, servidores vinculados, trabajos, etc.

5. El nuevo servidor de base de datos (SQL Server 2016) será implementado en el hardware y software descrito en los cuadros 20 y 21.

Software

Sistema Operativo	Windows Server 2016 Data Center 64Bits
Sistema Gestor de Base de Datos	SQL Server 2016 Enterprise Edition 64Bits
Sistema de Archivos	NTFS

Cuadro 20. Especificaciones software
Elaborado por: Investigador

Hardware

Memoria RAM	64 Gb
Disco Duro	Tecnología SAS, capacidad 2 TB
Procesador	8 nucleos

Cuadro 21. Especificaciones hardware
Elaborado por: Investigador

EL desarrollo de la migración se la realizará de acuerdo con la planificación detallada en el cuadro 22.

Objetivos	Actividad	Fecha Inicio	Fecha Fin	Responsables
Analizar los requerimientos	Recolección de Información	02/05/2017	31/05/2017	Responsable migración, administradores de base de datos
Analizar los requerimientos	Especificación de requerimientos	01/06/2017	16/06/2017	Responsable migración, administradores de base de datos
Extraer la información	Realización de copias de seguridad de las bases de datos (SQL Server 2005)	19/06/2017	12/09/2017	Responsable migración
Extraer la información	Realización de pruebas de funcionalidad de respaldos	19/06/2017	12/09/2017	Responsable migración
Extraer la información	Realización de inventario de componentes	22/06/2017	17/07/2017	Responsable migración
Transformar la información	Adecuación de la información para la nueva versión.	17/07/2017	07/09/2017	Responsable migración

Cuadro 22. Planificación de migración
Elaborado por: Investigador

Objetivos	Actividad	Fecha Inicio	Fecha Fin	Responsables
Carga de información	Realizar Pruebas de Carga	08/09/2017	28/08/2017	Responsable migración
Cargar la información	Restaurar copias de seguridad de las bases de datos (SQL Server 2016)	29/08/2017	12/09/2017	Responsable migración
Pruebas	Realizar pruebas de detección de errores	16/05/2017	12/09/2017	Responsable migración

Cuadro 22. (cont.)

Pruebas

Como dispone la guía, se realizaron pruebas en todo el proceso de migración. A continuación, se detalla las acciones tomadas:

- Verificación y validación de copias de seguridad.

Se verificó y valido, que todas las copias y restauraciones de seguridad sean generadas con éxito, tanto en los ambientes de prueba como en el escenario de producción (copia y restauración final).

- A través de pruebas de unidad se verifico y validó cada componente de la base de datos. Los inconvenientes encontrados se detallan a continuación:

Características descontinuadas

Se detectó la utilización de los tipos de datos: text, image y ntext; los mismos que son considerados como obsoletos en SQL Server 2016. En el cuadro 23, se puede observar las tablas que utilizan campos con estos tipos de datos, adicionalmente se

muestra la columna sugerencia, la misma que indica el tipo de datos por el cual fue cambiado.

Base de datos	Tabla	Campo	Tipo dato	Sugerencia
bdDistributivo	carreras_lineamientos_diferentes	cld_observacion	text	varchar(max)
bdDistributivo	DistributivoDetalleDEAV	dd_observacion	text	varchar(max)
bdDistributivo	DistributivoDetalleDEAV	dd_observacion1	text	varchar(max)
bdDistributivo	tipo_personal_opcion	tpo_descripcion	text	varchar(max)
dbPracticas	Observations	description_obs	text	varchar(max)
dbPracticas	Projects	activity_summary_pro	text	varchar(max)
dbPracticas	Projects	specific_goal_pro	text	varchar(max)
dbPracticas	projects_medicine	description_pro_med	text	varchar(max)
dbTutorias	Questions	description_quest	text	varchar(max)
utamatico	BUZON	SUGERENCIA	text	varchar(max)
utamatico	ERPCONTRATOS	CONEXPLICACION	text	varchar(max)
utamatico	ERPCONTRATOSDOCENTES	CONDOCEXPLICACION	text	varchar(max)
utamatico	ERPCONTRATOS	CONDOCIMGHORARIO	image	varbinary(max)
utamatico	ERPCONTRATOS	CONDOCOBSERVACION	text	varchar(max)
utamatico	MATRIZESCUELA	ins_actividades	text	varchar(max)
utamatico	MATRIZESCUELA	ins_paginaweb	text	varchar(max)

Cuadro 23. Tipos de datos descontinuados
Elaborado por: Investigador

Malas prácticas en ejecución de sentencias

JOINS no calificados

Se detectaron vistas, funciones y procedimientos con JOINS no calificados, como el siguiente ejemplo:

```
SELECT *
FROM libro, biblioteca
where libro.codigoLibro = bliblioteca.codigoLibro
```

Según las recomendaciones de Microsoft, se optó por la utilización de sentencias: INNER JOIN, LEFT JOIN RIGHT JOIN.

En el cuadro 24, se puede observar los objetos encontrados:

Base de datos	Vista/Procedure/Función
utamatico	sp_load_by_seguimiento
utamatico	sp_load_by_seguimiento_all
utamatico	sp_load_cambio_paralelo
utamatico	sp_load_cupos
utamatico	sp_load_horario
utamatico	sp_load_horas
utamatico	sp_movilidadCarrera
utamatico	spAnularMatricula
utamatico	spAux3
utamatico	spCCreditosExtras
utamatico	spCDatosEst
utamatico	spCertificadoNota
utamatico	spCEstMatriModulos
utamatico	spCMatriNoLegalizadas
utamatico	spCModulosEstPerido
utamatico	spCPeriodoIngreso
utamatico	spDatosestudianteCarrera
utamatico	spDBancarios
utamatico	spDCapacitacion
utamatico	spDConyugue
utamatico	spDDeclaracion
utamatico	spDHijos
utamatico	spDHLaboral
utamatico	spDInstruccion
utamatico	spHVerifica
utamatico	spMHorario
utamatico	spMNotasActualesCarrera
utamatico	spObtenerMatPensum
utamatico	spOtrasFacultades
utamatico	spPHorariogeneral
utamatico	spProfesorEspecialidad
utamatico	spSemiFechasModulos
utamatico	spTipoSubAreaConEspecifico
utamatico	spWAnulacionDatos

Cuadro 24. JOINS NO CALIFICADOS
Elaborado por: Investigador

Base de datos	Vista/Procedure/Función
utamatico	spWAux3
utamatico	spWEstCarreras
utamatico	spWEstudianteEstado
utamatico	spWFactura
utamatico	spWGeneraOrden
utamatico	spWHorarios
utamatico	spWLegalizarMat
utamatico	spWMateriasMatricula
utamatico	spWMateriasPensum
utamatico	spWMatriculasAct25
utamatico	spWNotasActuales
utamatico	spWNotasPeriodo
utamatico	spWRegistroMatricula
utamatico	spWVerFechaMatricula
utamatico	fCAux1
utamatico	fCTotalCredEst
utamatico	FHVERHORACOMPLETA
utamatico	fWAux1
utamatico	fWtotalcreditos
utamatico	spWAux2

Cuadro 24. (cont.)

Clausula ORDER BY ordenada por número entero

Se detecto en procedimientos almacenados (ver cuadro 25) el uso de la cláusula ORDER BY, que especifica los números de columnas ordinales como columnas de clasificación (una columna de clasificación se puede especificar como un entero no negativo que representa la posición del nombre o alias en la lista de selección), pero esto no es recomendable porque una lista de selección es susceptible a cambios (inclusión y disminución de columnas) que alteren su orden y por ende cambie el resultado entregado.

Base de datos	Vista/Procedure/Función
Utamatico	sp_load_horario
Utamatico	sp_cargar_datos

Cuadro 25. Clausula Order By
Elaborado por: Investigador

c. Control de desastres

Se tomó las medidas sugeridas por la guía según se detalla a continuación:

1. Respaldos de base de datos

Se configuraron en modo “SINGLE_USER” todas las bases de datos del servidor origen (SQL Server 2005) antes de realizar el último respaldo (respaldos finales que serán trasladados al nuevo servidor).

2. Bases de datos origen y destino en funcionamiento

Las cadenas de conexión de las aplicaciones que consumen fueron actualizadas para que trabajen con el nuevo servidor (SQL Server 2016), y se bajó el servicio del anterior servidor (SQL Server 2005), nunca los dos servidores funcionaron al mismo tiempo.

Se detectó una cadena de conexión que no fue actualizada, la misma que fue corregida. Ver gráfico 38.

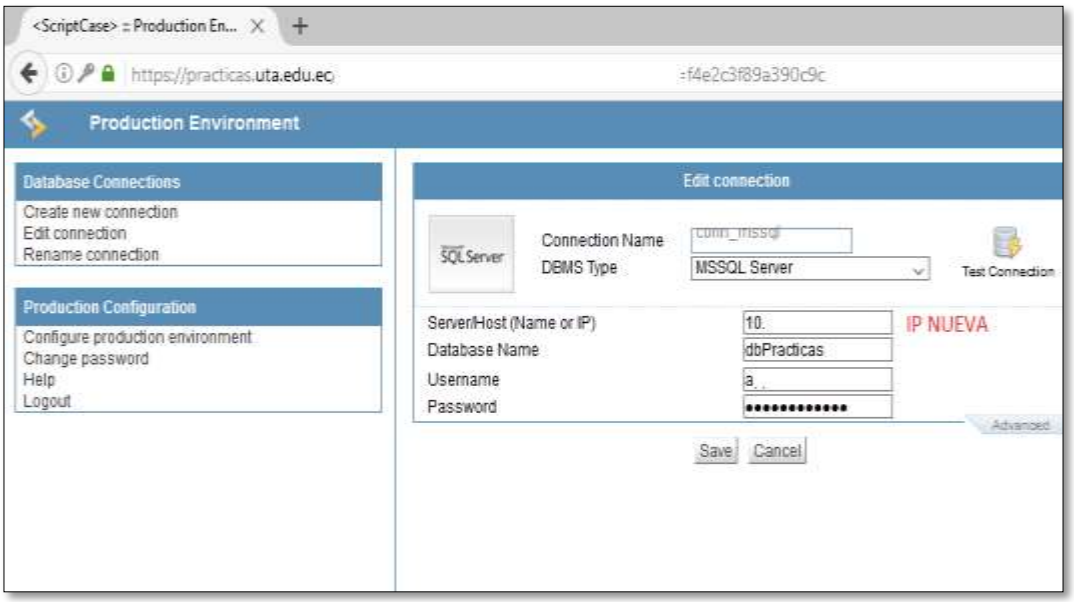


Gráfico 38. Cambio cadena conexión
Elaborado por: Investigador

3. Seguridad de respaldos

Se registro el responsable, la fecha de entrega y el motivo de cada uno de los respaldos realizados de las bases de datos en un documento para el efecto.

Se restringió el acceso no autorizado a los escenarios (máquinas virtuales) en donde se realizaron las respectivas pruebas del proceso de migración, a través de usuarios y contraseñas robustas.

Además, se optó por realizar todo el proceso de migración en la institución, más concretamente en la DITIC, y seguir estrictamente la medida recomendada en la guía, de no sacar información (respaldos de bases de datos) fuera del área de trabajo.

d. Extracción, transformación y carga

1. Instalar una copia separada de SQL Server 2016

A continuación, se describe los pasos más importantes realizados para la instalación de SQL Server 2016.
Ejecución del CD de instalación, en la opción instalación se seleccionó, “Realizar una nueva instalación de SQL Server”. Ver gráfico 39

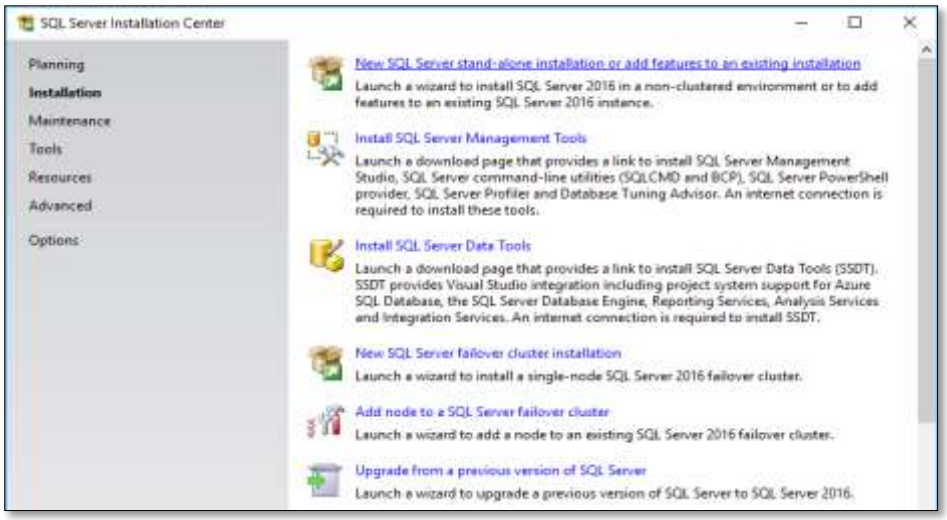


Gráfico 39. Nueva instalación - SQL Server 2016
Elaborado por: Investigador

A continuación, se seleccionó los componentes a instalar (Motor de Base de Datos, Analysis Services y otros). Para este caso se escogió, Motor de Base de Datos. Ver gráfico 40.

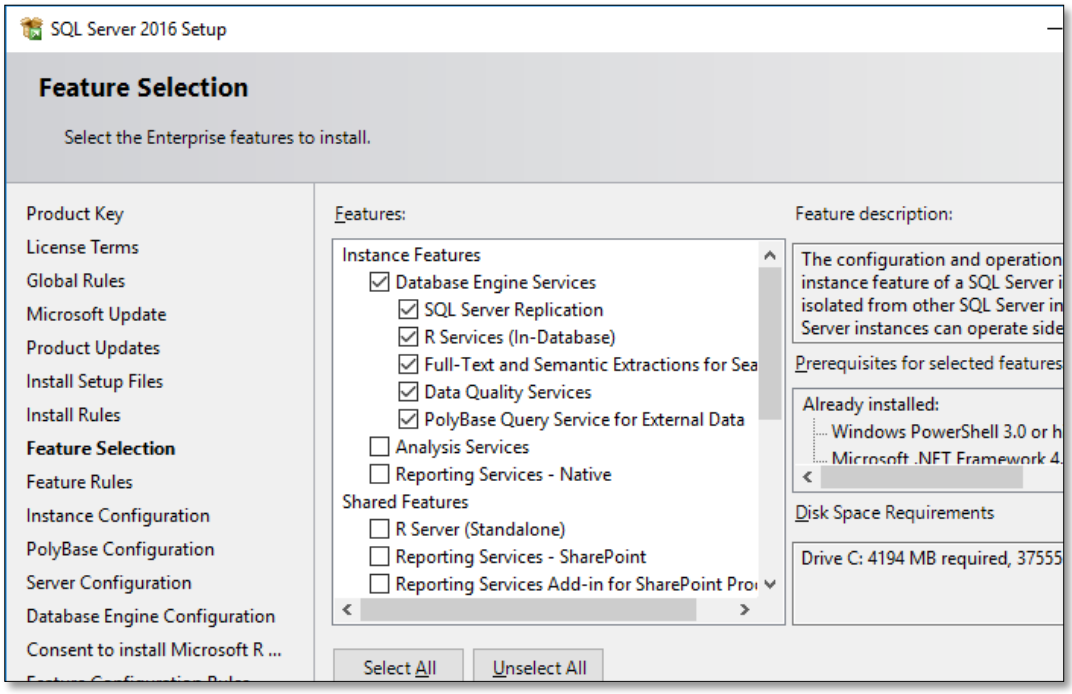


Gráfico 40. Selección de componentes - SQL Server 2016
Elaborado por: Investigador

En el siguiente paso se configuró las cuentas de usuario administrador, cuentas que permitirán administrar cada componente seleccionado en el paso anterior. Para este caso "Motor de base de Datos". Ver gráfico 41.

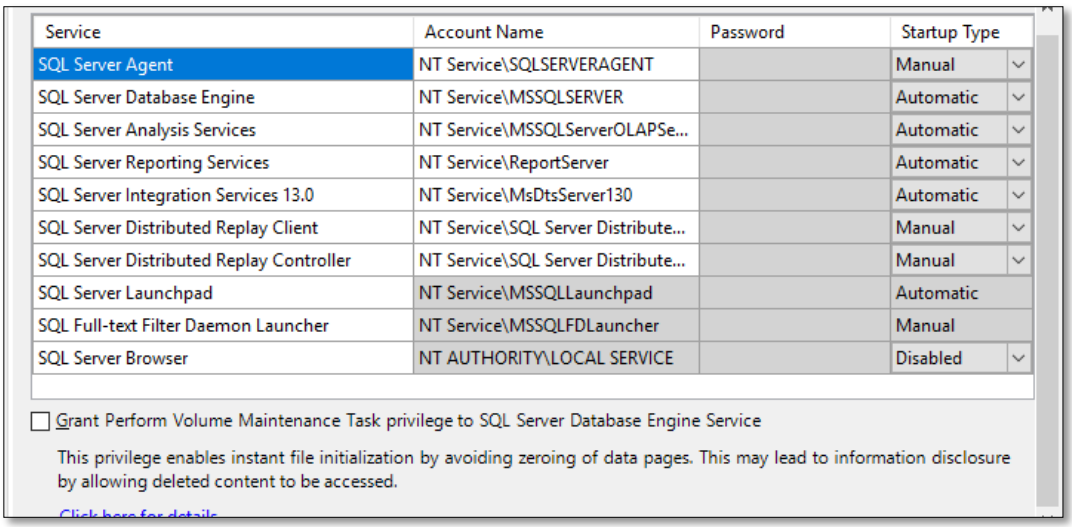


Gráfico 41. Cuentas de servicio - SQL Server 2016
Elaborado por: Investigador

Configurar la opción Collation, se especificó la mismas con respecto al servidor SQL Server 2005 (servidor origen). Ver gráfico 42.

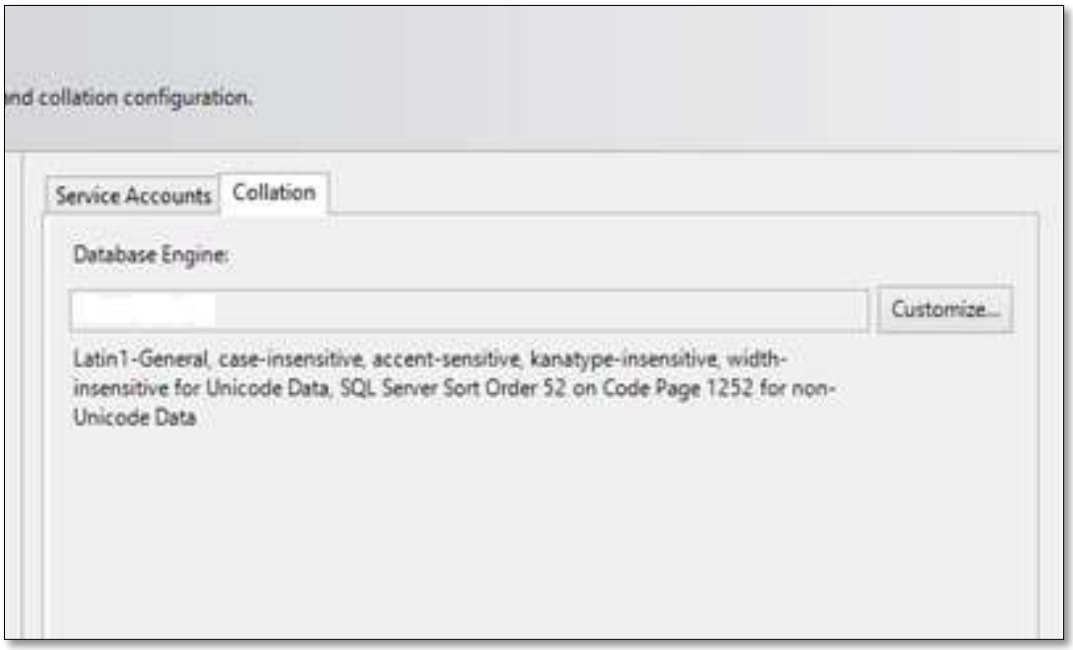


Gráfico 42. Configuración Collation - SQL Server 2016
Elaborado por: Investigador

La instalación culmina con un resumen de lo instalado. Ver gráfico 43.

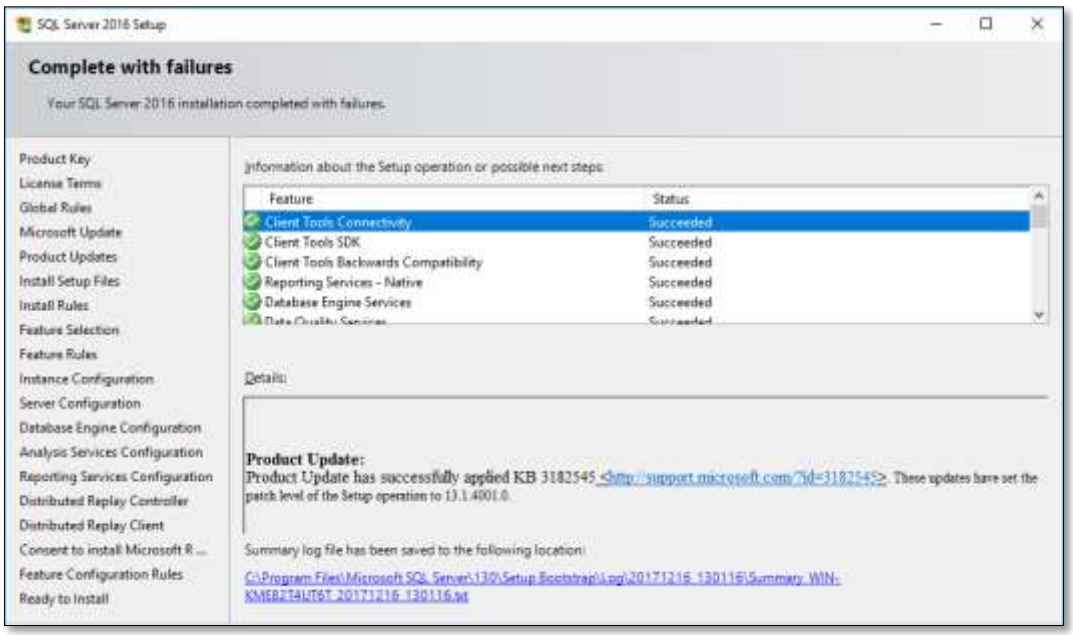


Gráfico 43. Finalización de instalación - SQL Server 2016
Elaborado por: Investigador

2. Asegurar que SQL Server 2005 está en el último Service Pack (Service Pack 4).

Con la ejecución del comando se comprobó que SQL Server 2005 cuenta con el Service Pack necesario para la migración. Ver gráfico 44.

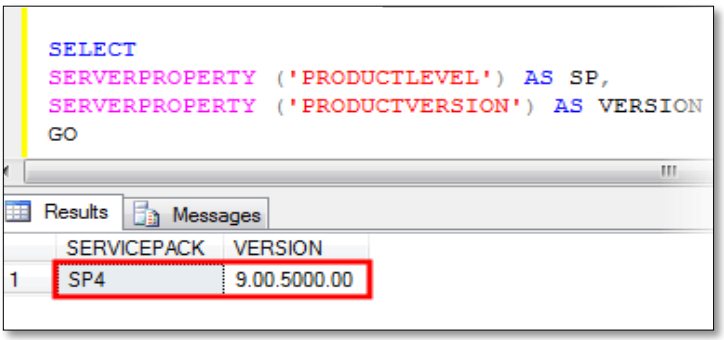


Gráfico 44 Comprobación de Service Pack - SQL Server 2005
Elaborado por: Investigador

3. Realizar una copia de seguridad de todas las bases de datos a ser migradas

Del listado de base de datos determinado en la especificación de requerimientos, se realizó las copias de seguridad respectivas, según lo indica la guía de migración. Cada una de las bases de datos se configuró en modo "SINGLE USER". Ver gráficos 45, 46 ,47 y 48.

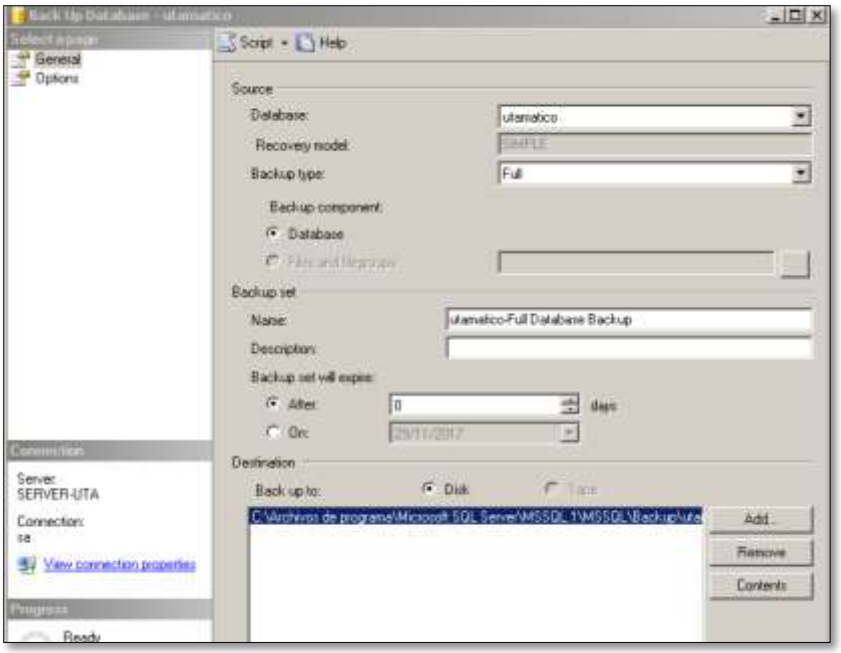


Gráfico 45. Respaldo utamatico - SQL Server 2005
Elaborado por investigador

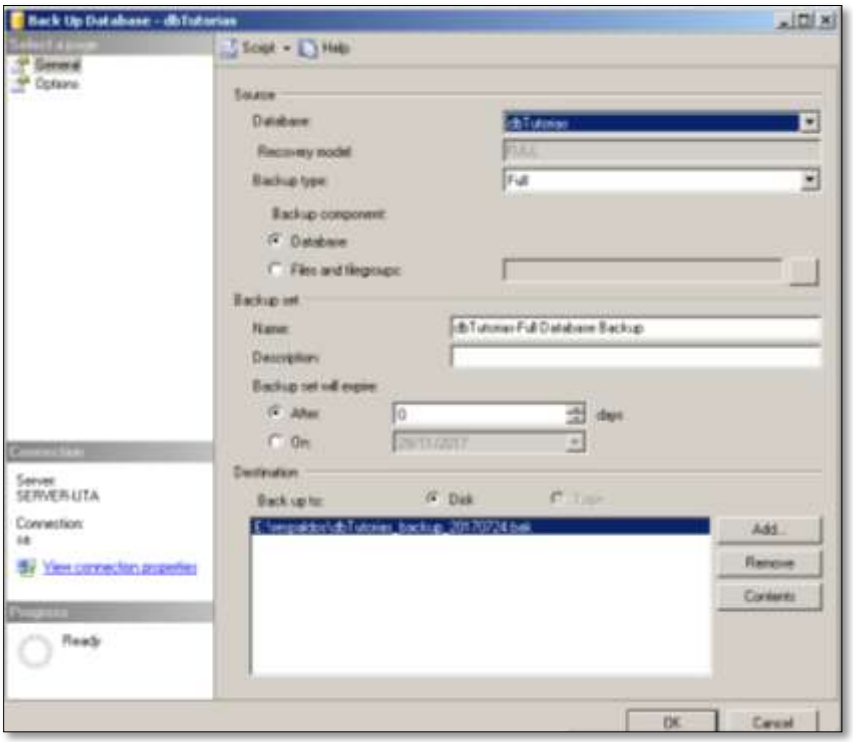


Gráfico 46. Respaldo dbTutorias - SQL Server 2005
Elaborado por: Investigador

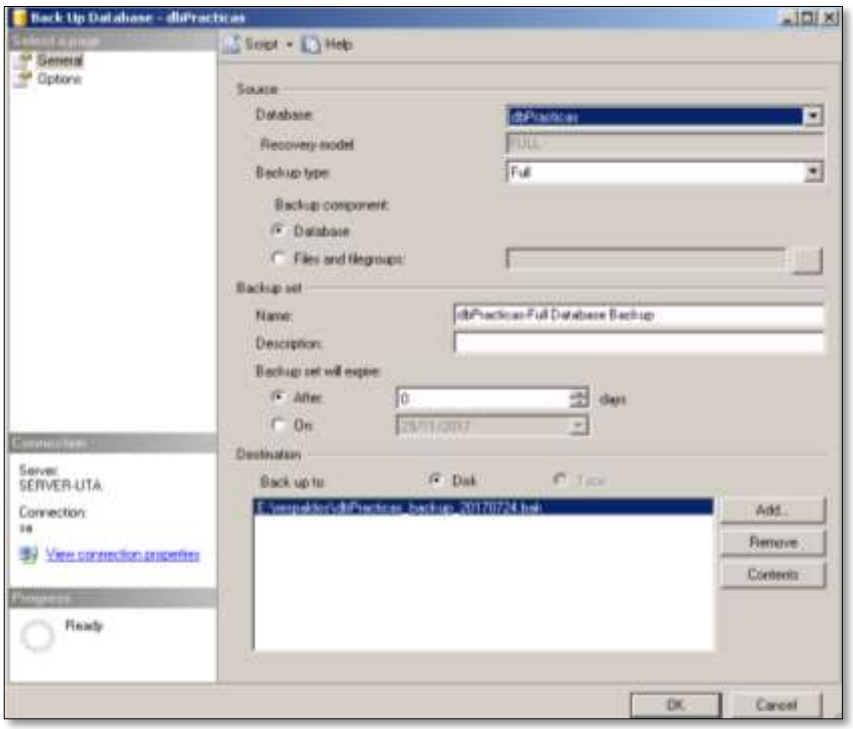


Gráfico 47. Respaldo dbPracticas - SQL Server 2005
Elaborado por: Investigador

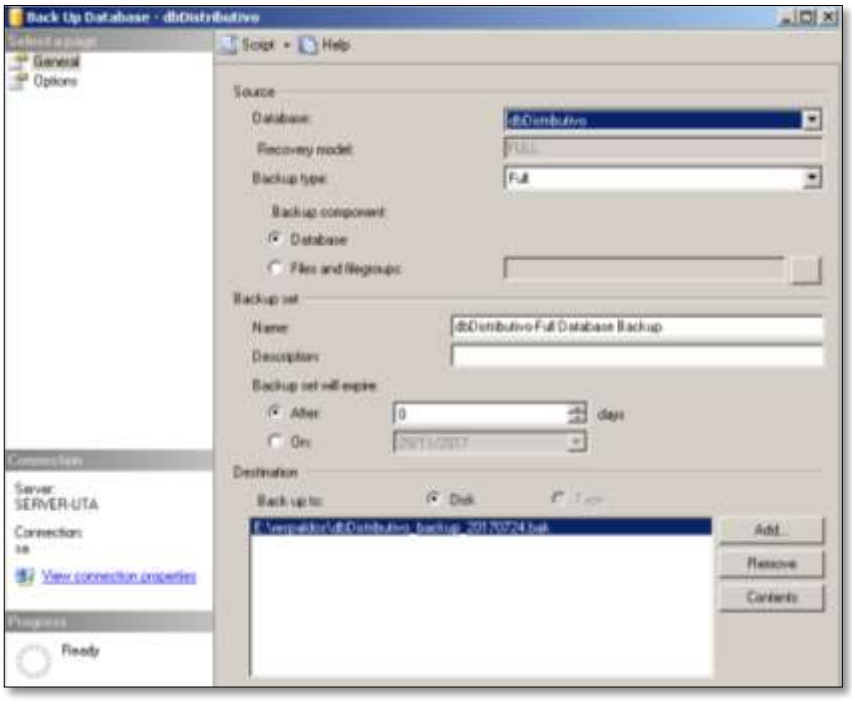


Gráfico 48. Respaldo dbDistributivo - SQL Server 2005
Elaborado por: Investigador

4. Instalar una copia intermedia de SQL Server 2008 R2. Ver las figuras 49, 50 y 51, que indican los pasos principales realizados para la instalación de SQL Server 2008 R2

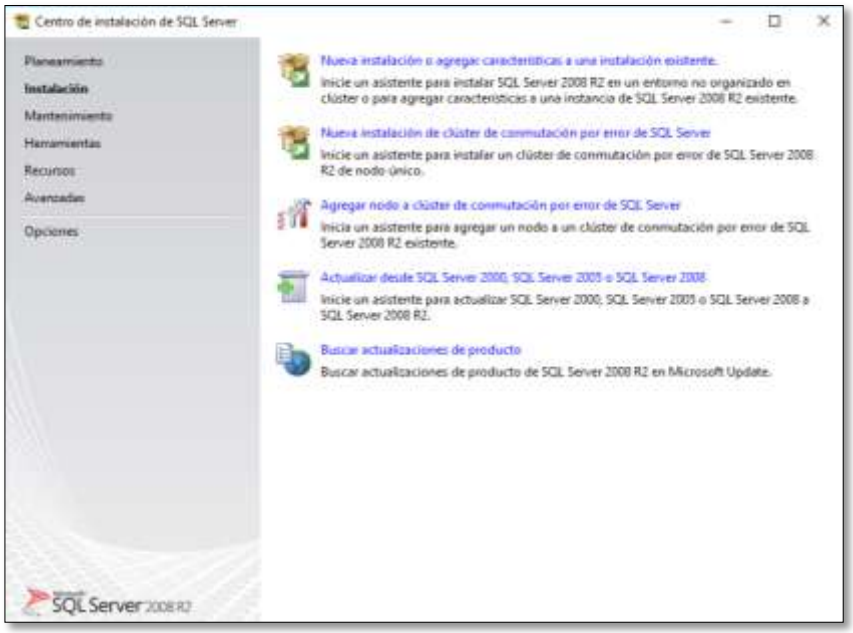


Gráfico 49. Instalación - SQL Server 2008 R2
Elaborado por: Investigador

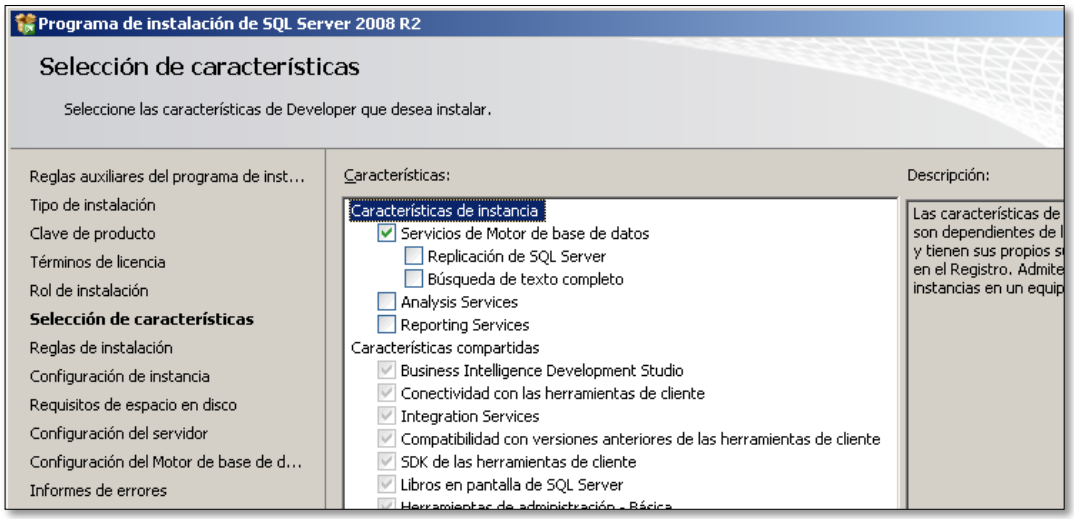


Gráfico 50. Selección de componentes - SQL Server 2008 R2
Elaborado por: Investigador

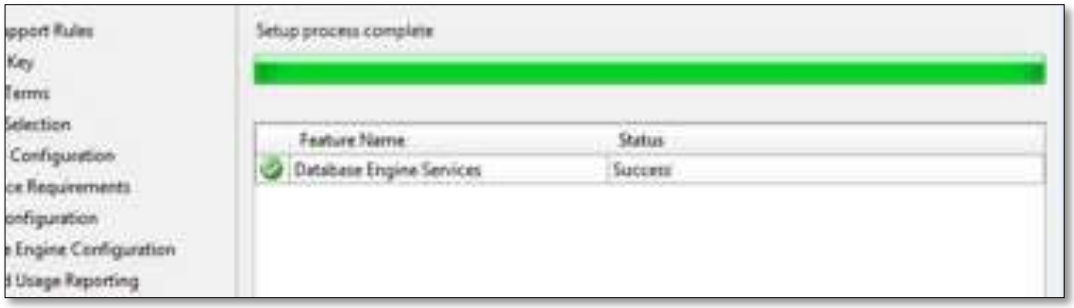


Gráfico 51. Finalización de instalación - SQL Server 2008 R2
Elaborado por: Investigador

5. Instalar el Service Pack adecuado en SQL Server 2008 R2 provisional.

Con la ejecución del siguiente comando se comprobó que SQL Server 2008 R2 cuenta con el Service Pack necesario para la migración. Ver gráfico 52.

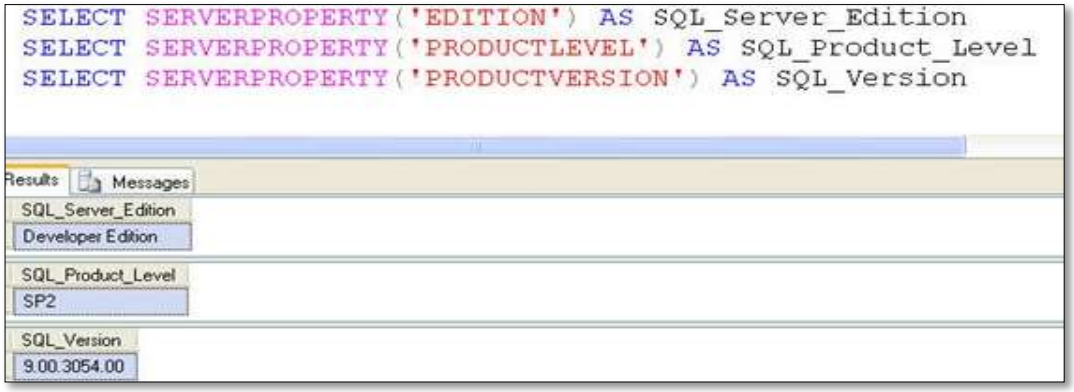


Gráfico 52. Comprobación de Service Pack - SQL Server 2008 R2
Elaborado por: Investigador

6. Restaurar la copia de seguridad de base de datos SQL Server 2005 en el sistema provisional SQL Server 2008/R2 que ha sido instalado provisionalmente.

Del listado de las bases de datos respaldadas en el servidor original (SQL Server 2005), se realizó las restauraciones respectivas de las bases de datos en SQL Server 2008 R2, como lo muestra el gráfico 53.

Las bases de datos restauradas fueron: utamatico, dbPracticas, dbTutorias, y dbDistributivo.

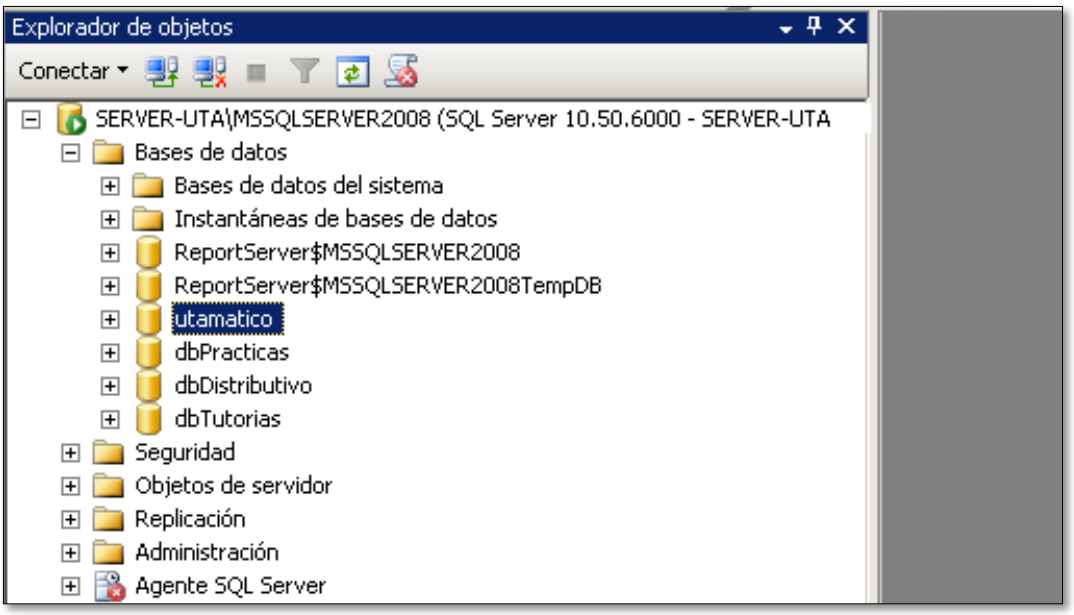


Gráfico 53. Bases de datos restauradas – SQL Server 2008 R
Elaborado por: Investigador

7. El siguiente paso fue realizar una copia de seguridad de estas bases de datos provisionales (SQL Server 2008 R2) para su posterior restauración en SQL Server 2016.

8. A continuación se tomó las copias de seguridad de las bases de datos provisionales (SQL Server 2008 R2) y se restauró en SQL Server 2016. Ver figuras 54, 55, 56 y 57.

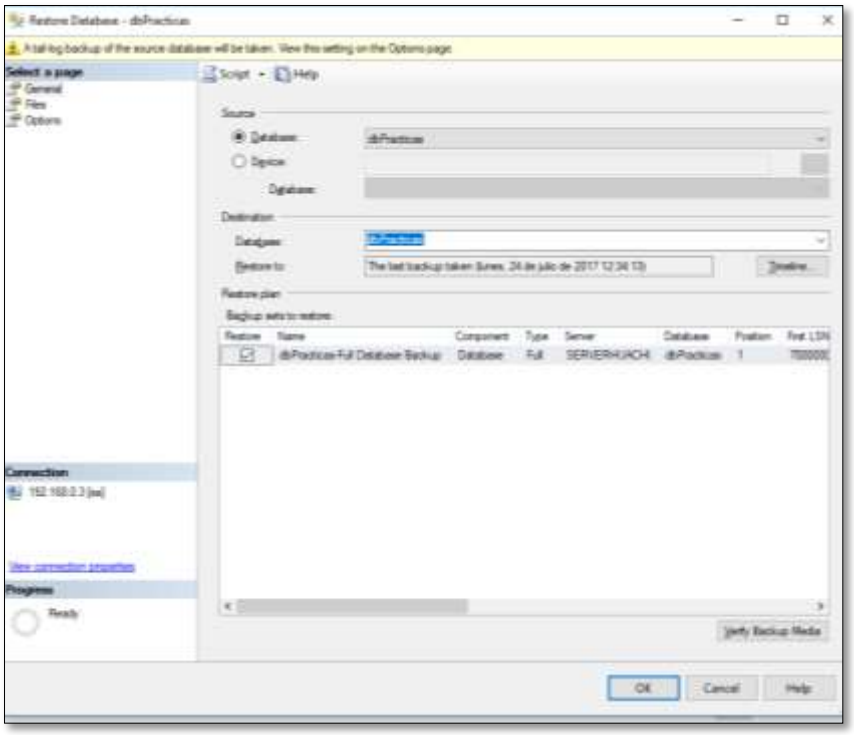


Gráfico 54. Restauración dbPracticas - SQL Server 2016
Elaborado por: Investigador

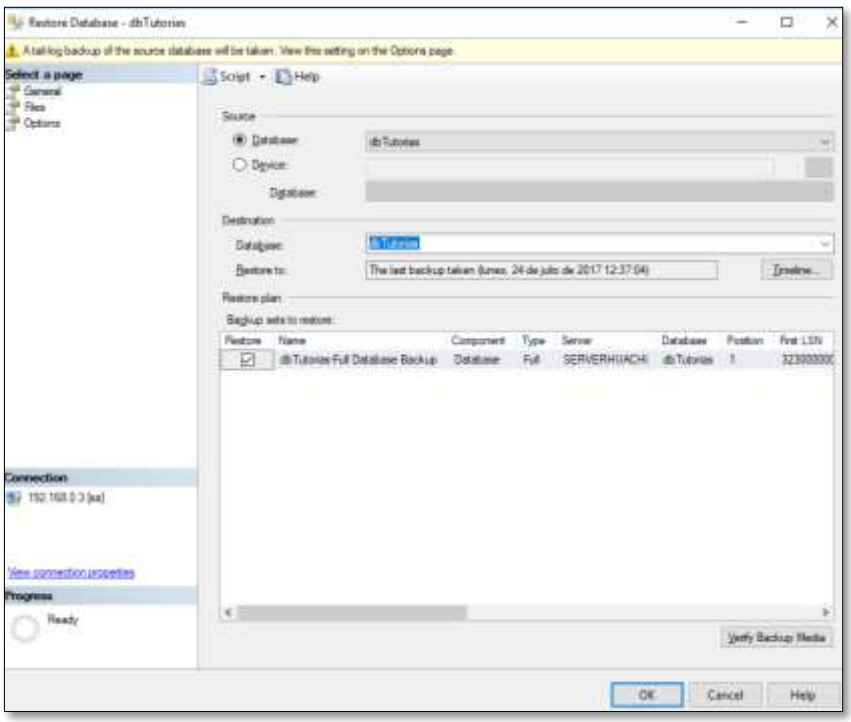


Gráfico 55. Restauración dbTutorias - SQL Server 2016
Elaborado por: Investigador

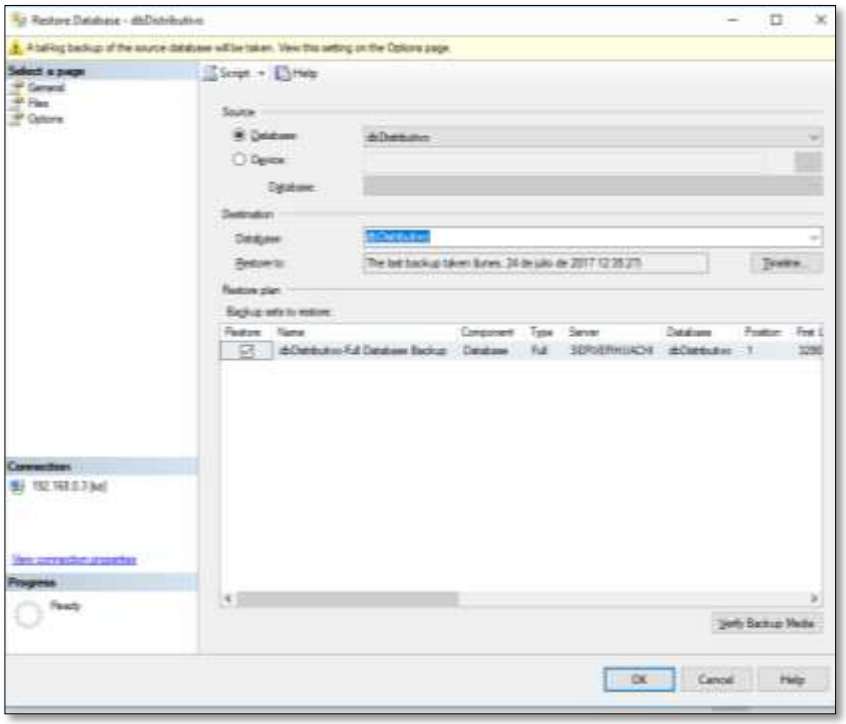


Gráfico 56. Restauración dbDistributivo - SQL Server 2016
Elaborado por: Investigador

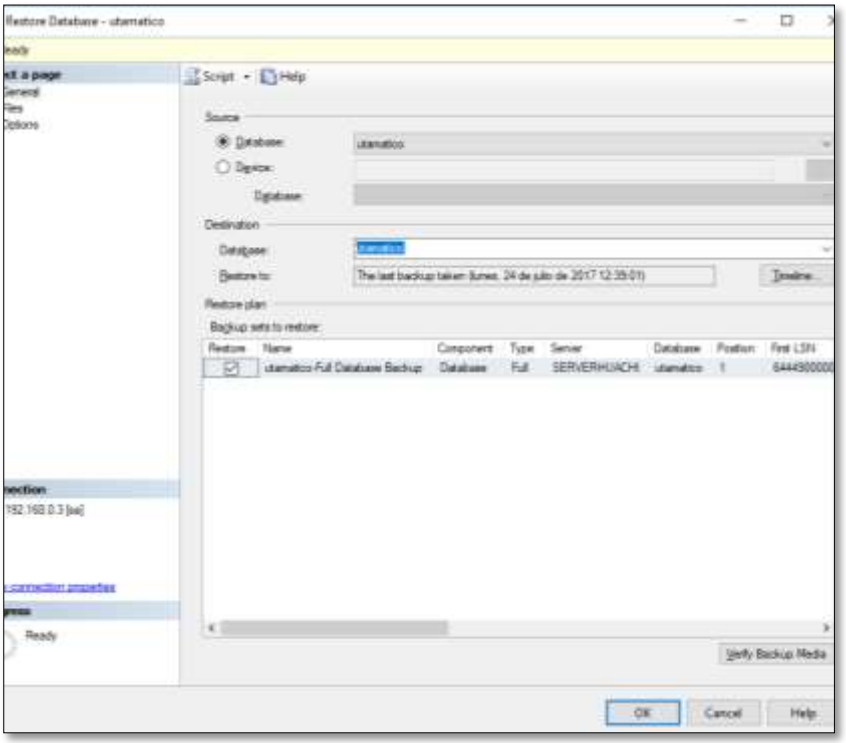


Gráfico 57. Restauración utamatico - SQL Server 2016
Elaborado por: Investigador

9. Trasladar los inicios de sesión

Una vez restauradas las bases de datos en SQL Server 2016, es necesario también trasladar los inicios de sesión con las respectivas contraseñas; con la finalidad de evitar usuarios huérfanos en el nuevo servidor. En el gráfico 58 se ilustra los usuarios huérfanos de la base de datos utamatico en SQL Server 2016.

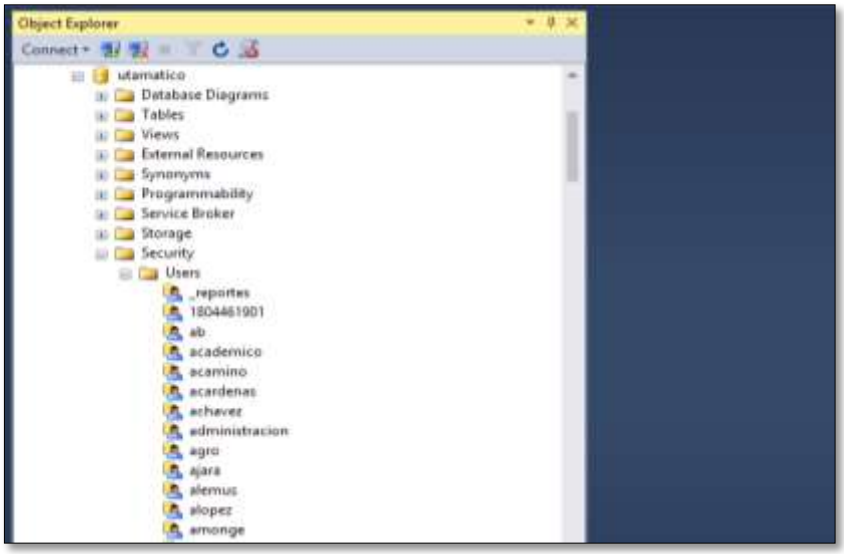


Gráfico 58. Usuarios huérfanos - SQL Server 2016
Elaborado por: Investigador

En el gráfico 59, se ilustra los inicios de sesión que fueron trasladados a SQL Server 2016.

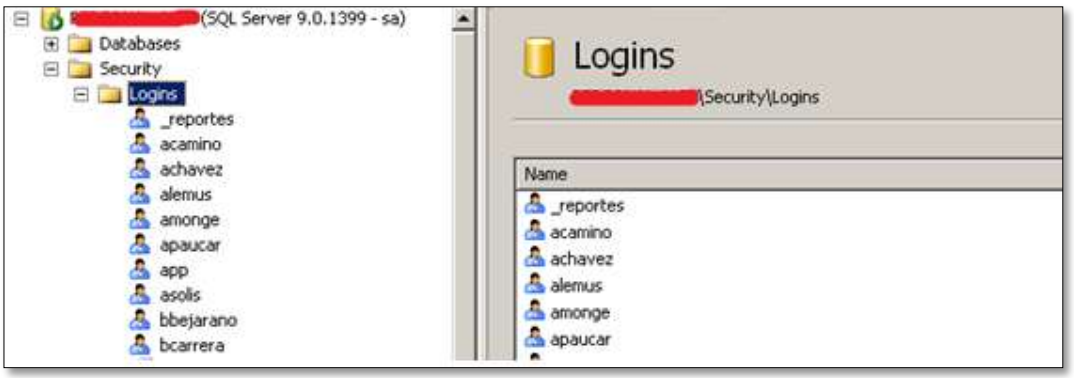


Gráfico 59. Inicios de sesión - SQL Server 2005
Elaborado por: Investigador

En el gráfico 60, se ilustra la ejecución en SQL Server 2005 del script que consta en la guía de migración, para la transferencia de logins.

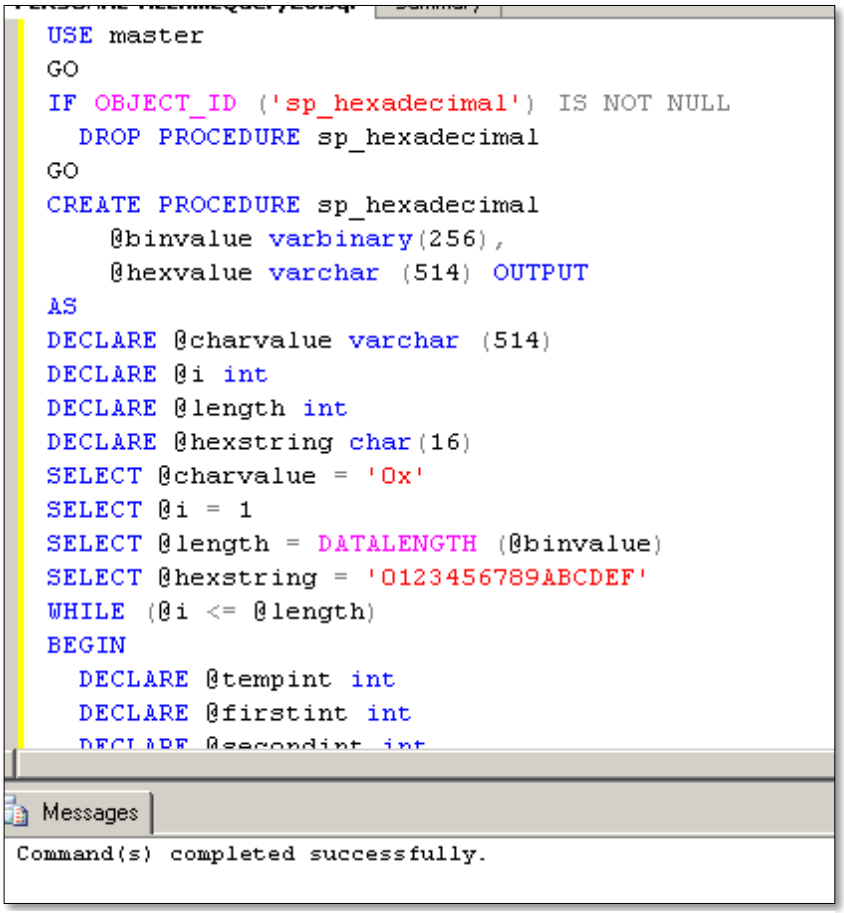


Gráfico 60. Ejecución script transferencia de logins
Elaborado por: Investigador

En el gráfico 61, se ilustra el resultado de la ejecución en SQL Server 2005 del procedimiento “master..sp_help_revlogin” generado en el paso anterior. El script resultante fue guardado para su posterior ejecución en el nuevo entorno.

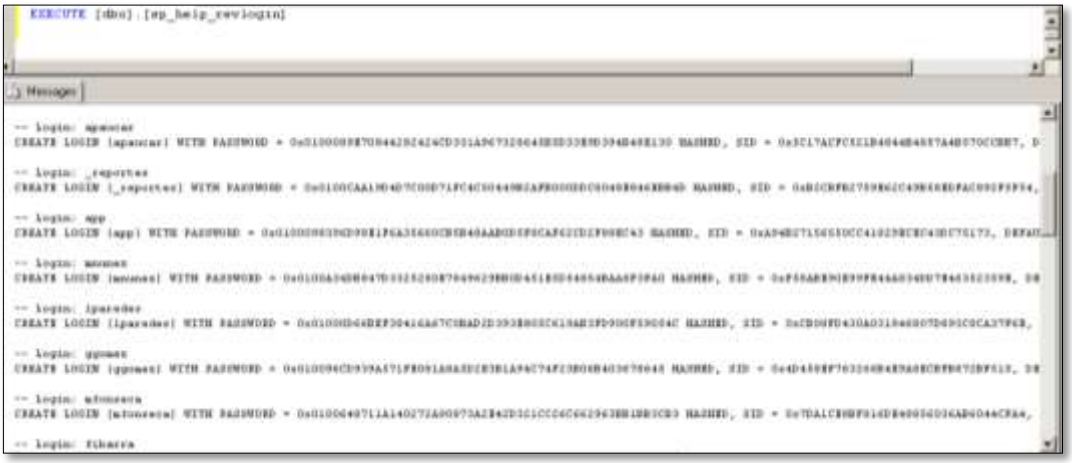


Gráfico 61. Script de logins
Elaborado por: Investigador

En el gráfico 62, se ilustra la ejecución en SQL Server 2016 del script de logins generado en el paso anterior y como resultado se asignó los inicios de sesión y contraseñas a todos los usuarios de las bases de datos migradas.

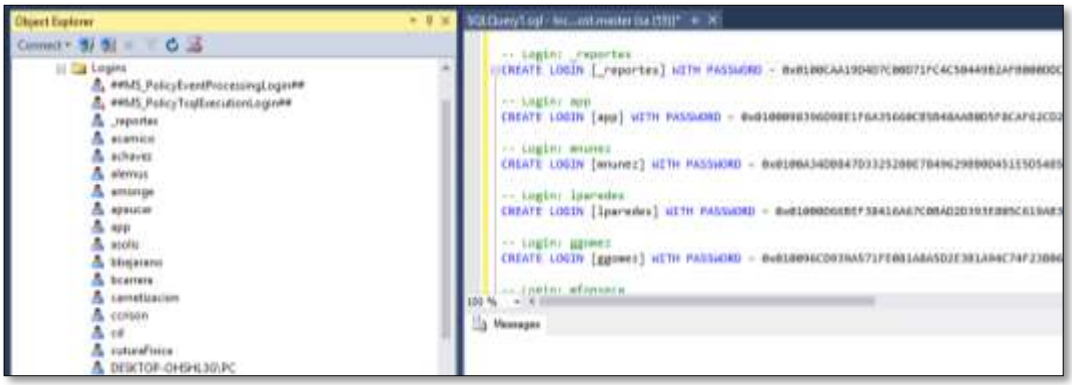


Gráfico 62. Asignación de usuarios huérfanos
Elaborado por: Investigador

10. Identificar y crear manualmente: servidores vinculados, trabajos, tablas maestras y otros componentes externos.

En el cuadro 26, se ilustra los servidores vinculados y trabajos, trasladados a SQL Server 2016

NOMBRE OBJETO	TIPO DE OBJETO
10.102.101.5	servidor vinculado
10.102.120.12	servidor vinculado
10.102.120.16	servidor vinculado
10.102.120.18	servidor vinculado
10.102.120.19	servidor vinculado
Respaldar	trabajo
Auditar	trabajo
enviarCorreo	trabajo

Cuadro 26. Objetos externos
Elaborado por: Investigador

11. Si se llegó a este punto significa que las bases de datos fueron migradas con éxito desde SQL Server 2005 a SQL Server 2016, las bases de datos funcionan en la nueva versión.

6.7.3 Vulnerabilidades en la DITIC y SQL Server 2016

Las vulnerabilidades detectadas en la DITIC por las características de SQL Server 2005, fueron probadas en el nuevo entorno (SQL Server 2016), dejando los siguientes resultados:

Vulnerabilidad del procedimiento extendido "xp_cmdshell"

Sistema operativo: Kali Linux
Software: Metasploit v4

Descripción de la vulnerabilidad

La vulnerabilidad permite la escala de privilegios a través del procedimiento extendido "xp_cmdshell", es decir, un usuario con privilegios "sysadmin" puede a través del procedimiento extendido "xp_cmdshell" apoderarse del sistema operativo donde reside el SGBD.

Explotación de la vulnerabilidad

Pasos

1. Utilizar el exploit "mssql_payload". Ver gráfico 63

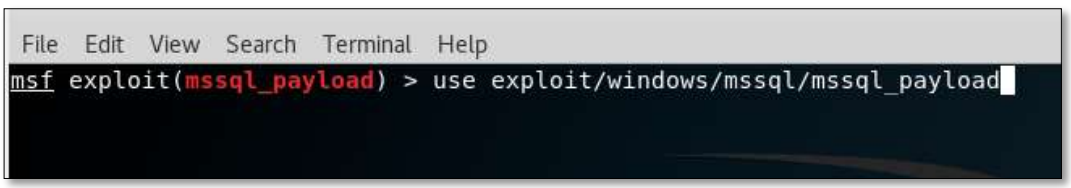


Gráfico 63. Utilización de exploit "mssql_payload" - SQL Server 2016
Elaborado por: Investigador

2. Parametrizar el exploit "mssql_payload" (ver gráficos 64 y 65), según los siguientes parámetros:

RHOSTS: IP del SGBD

USERNAME: Usuario del SGBD

PASSWORD: Password del SGBD (Puede ser obtenido por el atacante mediante ataques de fuerza bruta al SGBD)

LHOST: IP atacante

LPORT: Puerto atacante (los atacantes utilizan puertos conocidos para no causar sospechas).

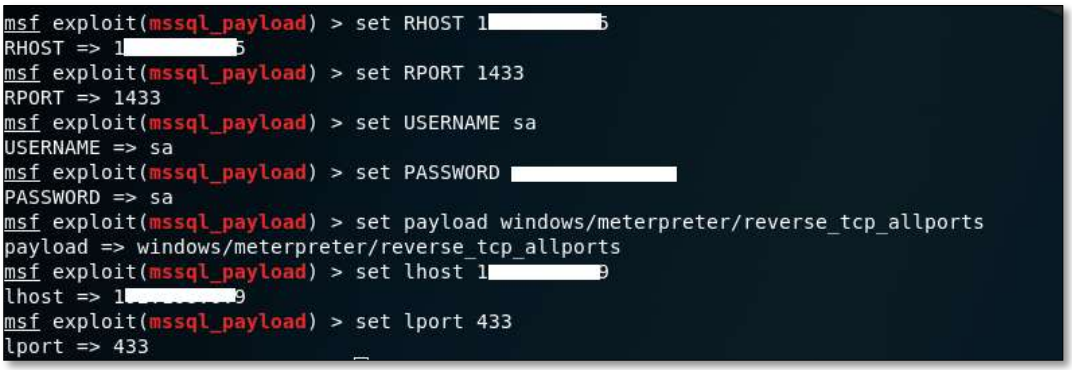


Gráfico 64. Parametrizar "mssql_payload" - SQL Server 2016
Elaborado por: Investigador

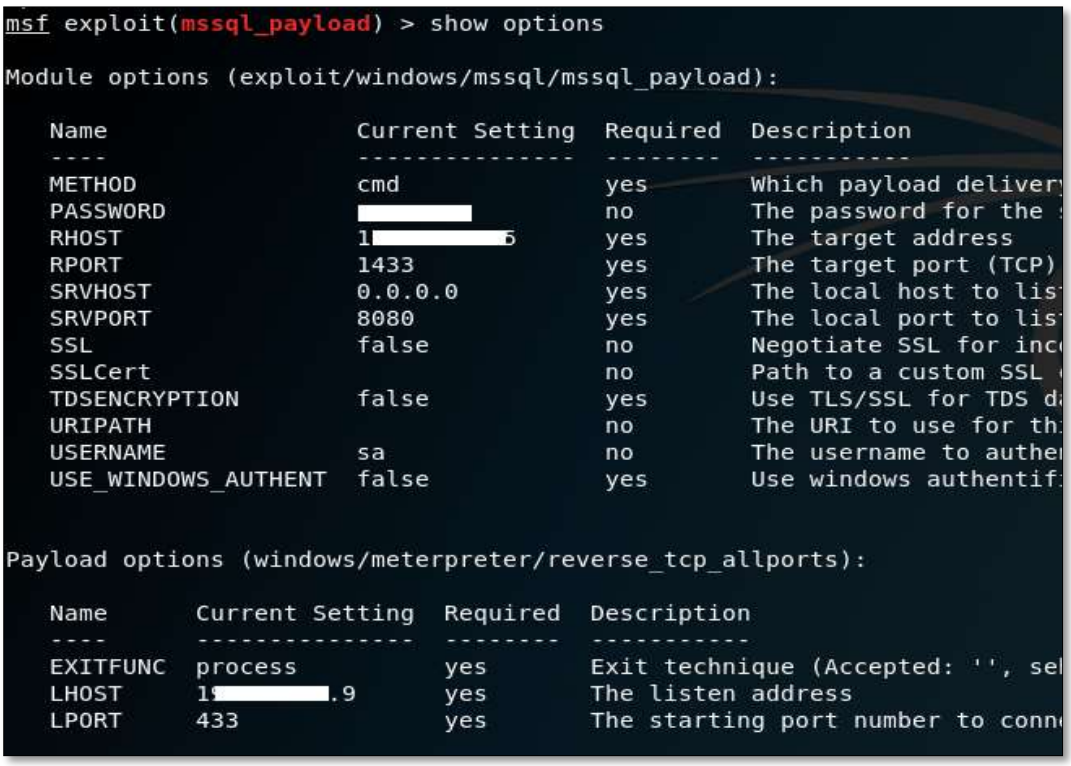


Gráfico 65. Opciones configuradas "mssql_payload" - SQL Server 2016
Elaborado por: Investigador

3. Ejecutar el exploit “mssql_payload”. Ver figura 66.

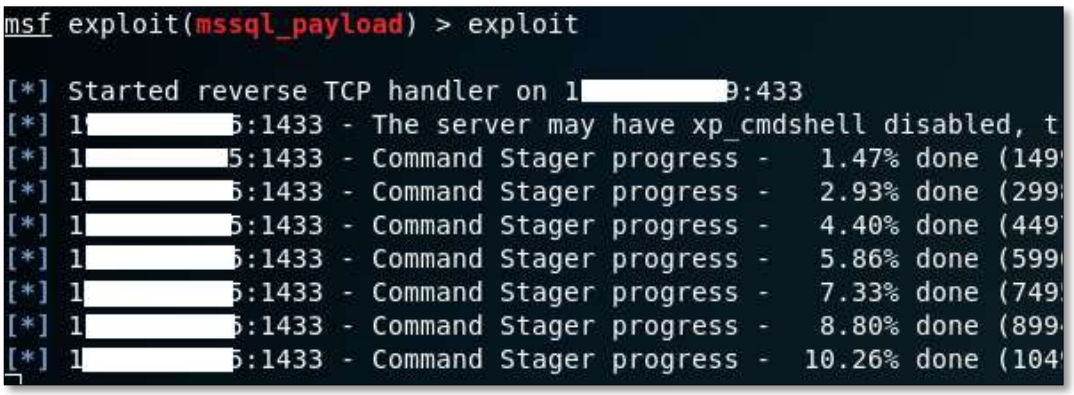


Gráfico 66. Ejecución de "mssql_payload" - SQL Server 2016
Elaborado por: Investigador

El resultado de la ejecución del exploit “mssql_payload” no fue exitoso, características de la versión permitieron evitar el ataque. Ver gráfico 67

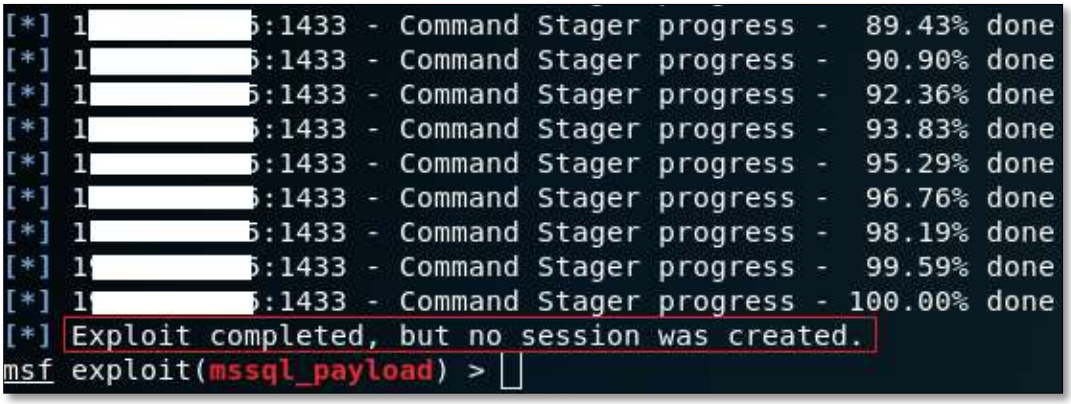


Gráfico 67. Resultado ejecución "mssql_payload" - SQL Server 2016
Elaborado por: Investigador

Vulnerabilidad del procedimiento extendido “sp_replwritetovarbin”

Herramientas utilizadas

Sistema operativo: Kali Linux

Software: Metasploit v4

Descripción de la vulnerabilidad

La vulnerabilidad permite el acceso remoto y escala de privilegios a través del procedimiento extendido “sp_replwritetovarbin”.

El procedimiento “sp_replwritetovarbin” puede ser ejecutado por cualquier usuario y nivel de privilegios del SGBD, el atacante puede aprovechar esta ventaja y combinando técnicas de inyección SQL puede obtener el acceso remoto al servidor que aloja el SGBD. Incluso funcionarios malintencionados con acceso al servidor (usuario y contraseña de ingreso) podrían explotar esta vulnerabilidad.

Explotación de la vulnerabilidad

Pasos

1. Utilizar el exploit “ms09_004_sp_replwritetovarbin”**.** Ver gráfico 68

Gráfico 68. Utilización de "ms09_004_sp_replwritetovarbin"
Elaborado por: Investigador

2. Parametrizar el exploit “ms09_004_sp_replwritetovarbin” (ver gráficos 69, 70 y 72), según los siguientes parámetros:

RHOSTS: IP del SGBD
USERNAME: Usuario del SGBD
PASSWORD: Password del SGBD
LHOST: IP atacante
LPORT: Puerto atacante (los atacantes utilizan puertos conocidos para no causar sospechas).

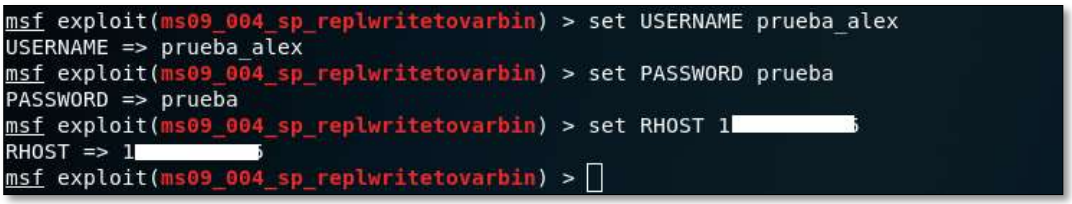


Gráfico 69. Seteo "ms09_004_sp_replwritetovarbin" (A)
Elaborado por: Investigador

Gráfico 70. Seteo "ms09_004_sp_replwritetovarbin" (B)
Elaborado por: Investigador

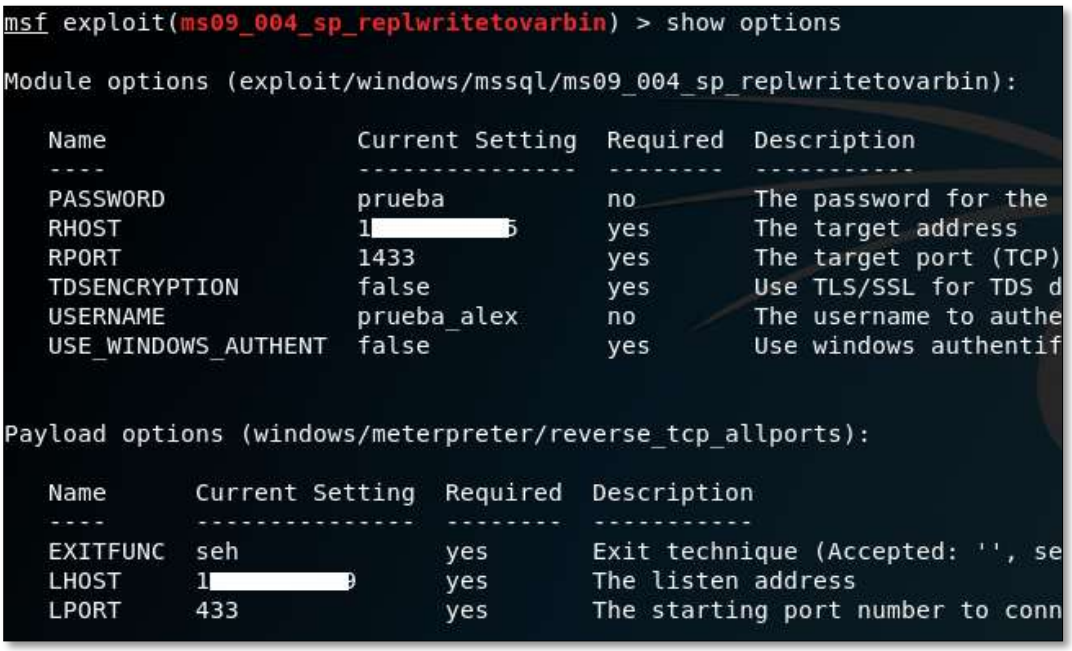


Gráfico 71. Parámetros seteados "ms09_004_sp_replwritetovarbin"
Elaborado por: Investigador

3. Ejecutar el exploit “ms_09_004_sp_replwritertovarbin”

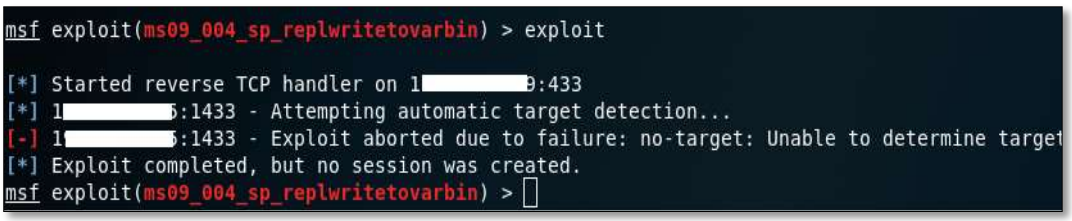


Gráfico 72. Ejecutar "ms09_004_sp_replwritetovarbin"
Elaborado por: Investigador

El resultado de la ejecución del exploit “ms_09_004_sp_replwritertovarbin” en SQL Server 2016 no fue exitoso, características de la versión resolvieron el hueco de seguridad.

En conclusión:

Con la ayuda de herramientas (Kali Linux y Metasploit), se comprobó que la utilización de SQL Server 2016 en la DITIC, permitió superar las 2 vulnerabilidades anteriormente detectadas en SQL Server 2005, vulnerabilidades que comprometían seriamente la seguridad en los datos. Cabe recalcar ante la aparición de nuevas amanezcas o errores en SQL Server 2016, éste cuenta con actualizaciones y parches de seguridad, los mismos que ayudaran a mejorar el resguardo de los datos en la DITIC.

Las copias de seguridad no cifradas de las bases de datos era otra vulnerabilidad detectada en la DITIC, la versión utilizada (SQL Server 2005) no permitía encriptación de los respaldos, la misma que fue superada a través de SQL Server 2016 y permite que en la DITIC las copias de seguridad puedan ser cifradas y por ende aumentar la seguridad de los datos.

Es importante utilizar la auditoría proporcionada por SQL Server 2016 (Server Audit) para el monitoreo de los datos en la DITIC, en lugar de la personalizada utilizada actualmente; con la finalidad de poseer una auditoria más robusta y menos proclive a errores u omisiones por parte del administrador de base de datos.

Además, es indispensable que en la DITIC se explote las mejoras en seguridad que brinda SQL Server 2016, como son la utilización de; mayor granularidad en los niveles de seguridad (seguridad a nivel de fila), cifrado permanente, administración extensible de claves (manejo de claves en fuentes externas), entre otras; que son unas claras mejoras en la gestión de la seguridad (ver cuadro 17).

En conclusión, las características proporcionadas por SQL Server 2016 inciden de manera positiva en la seguridad de los datos de la DITIC.

6.8 Conclusiones y recomendaciones

6.8.1 Conclusiones

- El enfoque migración a una nueva instalación es el más adecuado para la migración de bases de datos SQL Server 2005 a SQL Server 2016 por las características de mencionado enfoque de reducir al máximo el tiempo de inactividad.

- La guía para migración segura de datos desde SQL Server 2005 a SQL Server 2016 permite contar con una herramienta de apoyo que direcciona paso a paso todo proceso de migración entre estas versiones y asegura el traslado de datos.

- La aplicación de la guía de migración de datos desde SQL Server 2005 a SQL Server 2016 en la DITIC, permitió realizar el traslado de datos en forma segura entre estas dos versiones.

- Con la ayuda de SQL Server 2016, se logró superar vulnerabilidades que asechaban la anterior versión (SQL Server 2005) utilizada en la DITIC y como consecuencia se mejoró la seguridad de los datos en la Dirección.

6.8.2 Recomendaciones

- No esperar a que la versión de SQL Server utilizada en la DITIC pierda su soporte (actualizaciones y revisiones de seguridad) para realizar una migración o actualización de versión.

- Tomar medidas de seguridad con la información migrada (copias de seguridad), recuerde que en un proceso de migración es donde más expuesta se encuentra esta información a personas no autorizadas.

- Aplicar técnicas de encriptación o enmascaramiento a los datos críticos en la DITIC, con la finalidad de evitar que usuarios con acceso directo a la base de datos (incluido el administrador) puedan hacer mal uso éstos.

- Aprovechar las nuevas características de SQL Server 2016, con la finalidad de mejorar la seguridad de los datos en la DITIC.

Bibliografía

Avilés, G. G., & Academy, I. T. C. (2015). *Seguridad en Bases de Datos y Aplicaciones Web*: EISENBRAUNS.

Barcos, S. (2008). Reflexiones acerca de los sistemas de información universitarios ante los desafíos y cambios generados por los procesos de evaluación y acreditación. *Avaliação: Revista da Avaliação da Educação Superior, 13*(1), 209-244.

Carter, P. (2016). *Securing SQL Server: DBAs Defending the Database*. Botley.

Celis, A. (2014). Metodología para la migración deforma segura de Sistemas de Gestion de base de datos relacionales a sofware libre y estándares abiertos, 142. Retrieved from http://www.revistasbolivianas.org.bo/pdf/rpgi/n1/n1_a27.pdf

Cobo, A. *Diseño y programación de bases de datos*: Editorial Visión Libros.

Dueñas, P. (s.f.). *Cifrado de datos transparentes (TDE)*. Retrieved from http://www.danysoft.com /free/cifradoDatos.pdf

Fernández, C. (2010). *Análisis, desarrollo e implementación de auditoría en la base de datos Microsft SQL SERVER 2005.* Universidad Carlos III de Madrid, Retrieved from https://e-archivo.uc3m.es/bitstream/handle/10016/10588/pfc_memoriaV6_Clemente_Fernandez_Puerto.pdf?sequence=1

Fernández, V. (2006). *Desarrollo de sistemas de información*. In E. UPC (Ed.), *Una metodología basada en el modelado* (pp. 12). Retrieved from https://books.google.com.ec/books?id=Sqm7jNZS_L0C&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Garcia, A., Hurtado, C., & Alegre, M. (2011). *Seguridad Informática* (S. Ediciones Parainfo Ed. Primera ed.). Madrid.

Gonzalez, S. M. (2014). *UF1473 Salvaguarda y seguridad de los datos* (I. EDITORIAL Ed.).

Heredero, C. d. P., & López, J. (2004). *Informática y Comunicaciones en la Empresa* (E. EDITORIAL Ed.).

Jimenez, M. (2015). *UF 1471: Base de datos relacionales y modelado de datos*. Antequera.

Microsoft. (2006). Información General de copia de seguridad de SQL SERVER. Retrieved from https://technet.microsoft.com/es-es/library/ms175477(v=sql.90).aspx

Microsoft. (2016a). Copias de seguridad. Retrieved from https://docs.microsoft.com/es-es/sql/relational-databases/backup-restore/backup-overview-sql-server

Microsoft. (2016b). Enmascaramiento de datos dinámicos. Retrieved from https://docs.microsoft.com/es-es/sql/relational-databases/security/dynamic-data-masking

Microsoft. (2016c). Bases de datos independientes. Retrieved from https://docs.microsoft.com/es-es/sql/relational-databases/databases/contained-databases

Microsoft. (2016d). Cifrado de copias de seguridad de Microsoft. Retrieved from https://docs.microsoft.com/es-es/sql/relational-databases/backup-restore/backup-encryption

Microsoft. (2016e). Actualizaciones de ediciones y versiones admitidas. Retrieved from https://docs.microsoft.com/es-es/sql/database-engine/install-windows/supported-version-and-edition-upgrades

Microsoft. (2017a). Administración extensible de claves (EKM). Retrieved from https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/extensible-key-management-ekm

Microsoft. (2017b). Elegir un método de actualización del motor de base de datos. Retrieved from https://docs.microsoft.com/es-es/sql/database-engine/install-windows/choose-a-database-engine-upgrade-method

Microsoft. (s.f.-a). Introducción a las características de seguridad del motor relacional de SQL Server 2005.

Microsoft. (s.f.-b). Funciones de nivel de servidor. Retrieved from https://msdn.microsoft.com/es-es/library/ms188659(v=sql.90).aspx

Microsoft. (s.f.-c). Cómo transferir inicios de sesión y contraseñas entre instancias de SQL Server 2005 y 2008. Retrieved from https://support.microsoft.com/es-es/help/918992/how-to-transfer-logins-and-passwords-between-instances-of-sql-server

Morris, J. (2012). Practical Data Migration. In (Second ed., pp. 266): BCS Learning & Development Ltd. Retrieved from https://books.google.com.ec/books?id=AZKMrGyZGTcC&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

Paygude, P., & Devale, P. (2013). Automated Data Validation Testing Tool for Data Migration Quality Assurance. Retrieved from https://pdfs.semanticscholar.org/ea3f/a2d20e10cfc26ffe6f1b2ae54a0e7b8bccb7.pdf

Pérez, M. (2011). *SQL Server 2008 R2: motor de base de datos y administración*: RC Libros.

Silberschatz, A., Korth, H., & Sudarshan, S. (2002). FUNDAMENTOS DE BASES DE DATOS. In C. Fernández (Ed.), (Cuarta ed., pp. 53): Madrid. Retrieved from https://unefazuliasistemas.files.wordpress.com/2011/04/fundamentos-de-bases-de-datos-silberschatz-korth-sudarshan.pdf.

Snodgrass, A. (2014). Migrating from SQL Server 2005. In: Redmond Communications Inc.

Stacia, V., Cherry, D., & D'Anthony, J. (2016). *Introducing Microsoft SQL SERVER 2016* (M. Press Ed.). Washington.

Anexos

Anexo No. 1: Encuesta

Encuesta al Personal de la Dirección de Tecnología de Información y Comunicación de la Universidad Técnica de Ambato

Objetivo: Obtener información referente a las caracteristicas de SQL Server 2005 y su incidencia en la seguridad de los datos de la DITIC de la UTA.

Dirigido a:

- Administradores de BD
- Director DITIC
- Administradores de Seguridad Informática.

Instrucciones:

Marque una X en el casillero que corresponda

PREGUNTAS

1.- ¿Las características del SQL Server 2005 le permiten cumplir con los actuales estándares internacionales de seguridad de la información?

Si ( )

No ( )

2.- ¿En matriculación estudiantil, evaluación docente, registro de notas u otro escenario en el cual se requiera un nivel alto de seguridad. SQL Server 2005 está dotado para cumplir esos requerimientos?

Si ( )

No ( )

3.- ¿Al finalizar el contrato de soporte con SQL Server 2005, la desactualización de la herramienta generaría que los datos de la DITIC queden vulnerables para ataques informáticos exitosos?

Si ( )

No ( )

4.- ¿Las bases de datos en SQL Server 2005 de la UTA han sufrido algún tipo de ataque informático?

Si ( )

No ( )

5.- ¿Existe algún proceso de mantenimiento preventivo frente a nuevas vulnerabilidades que podría presentar SQL Server 2005?

Si ( )

No ( )

6.- ¿Las bases de datos en SQL Server 2005 de la DITIC cuentan con medidas de control de seguridad que permitan detectar nuevas amenazas a las que se expone sus datos?

Si ( )

No ( )

Anexo No. 2: Guía

Guía de explotación de vulnerabilidades de SQL Server

Las técnicas mostradas en la presente guía tienen la finalidad de mostrar como un atacante podría aprovechar las vulnerabilidades de SQL Server.

El objetivo de la guía no es enseñar técnicas para realizar ataques en contra de SQL Server.

- **Definiciones**

Exploit

Programa o código que se aprovecha de un agujero de seguridad (vulnerabilidad) en un sistema, de forma que un atacante podría usarla en su beneficio.

Metasploit

Herramienta de penetración de código libre, desarrollado para ejecutar exploits a un objetivo remoto.

Nmap

Nmap ("mapeador de redes") es una herramienta de código abierto para exploración de red y auditoría de seguridad. Se diseñó para analizar rápidamente grandes redes, aunque funciona muy bien contra equipos individuales.

Payload:

Es un programa que acompaña a un exploit para realizar funciones específicas una vez que el sistema objetivo es comprometido, la elección de un buen payload es una decisión muy importante a la hora de aprovechar y mantener el nivel de acceso obtenido en un sistema.

- **Herramientas utilizadas**

Sistema Operativo: Kali Linux
Software: Metasploit, NMAP

- **Desarrollo de la guía**

Escaneo

1. Ingresar a la consola de Kali Linux

2. Escanear la red con el objetivo de descubrir máquinas y servicios con SQL Server. Ejecutar el comando:

nmap -A -T4 192.168.50.0/24

La ejecución del comando mostrará información como: puertos abiertos, sistema operativo instalado, y si fuera el caso nos mostrará el nombre de la instancia, versión y puerto utilizado por SQL Server. Información de utilidad que permitirá redireccionar la búsqueda de vulnerabilidades a los equipos que proveen servicios de SQL Server. En el gráfico 1, se ilustra un ejemplo de los resultados que podría entregar la ejecución del comando.

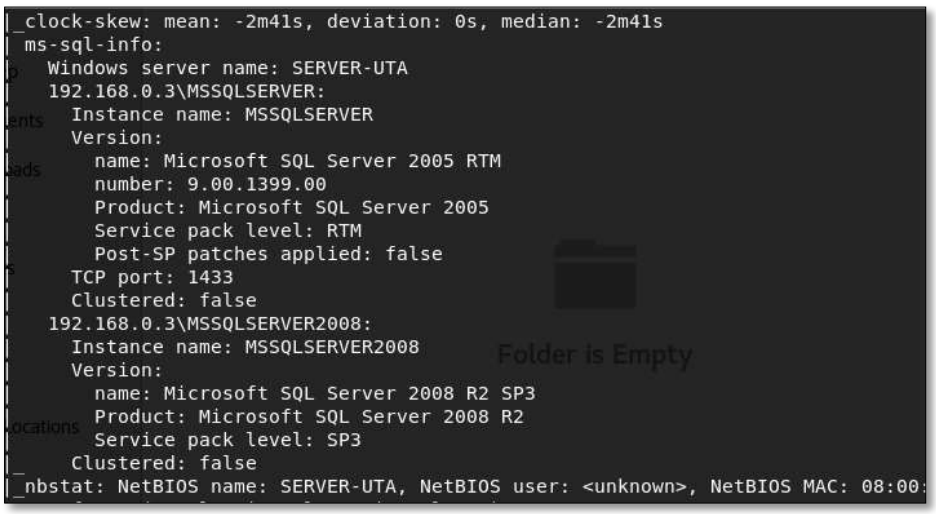


Gráfico 1. Ejecución de “NMAP”

Explotación de vulnerabilidades a través de Metasploit

3. Ejecutar el comando msfconsole (ver gráfico 2). Permite el ingreso a la consola de comandos de Metasploit.

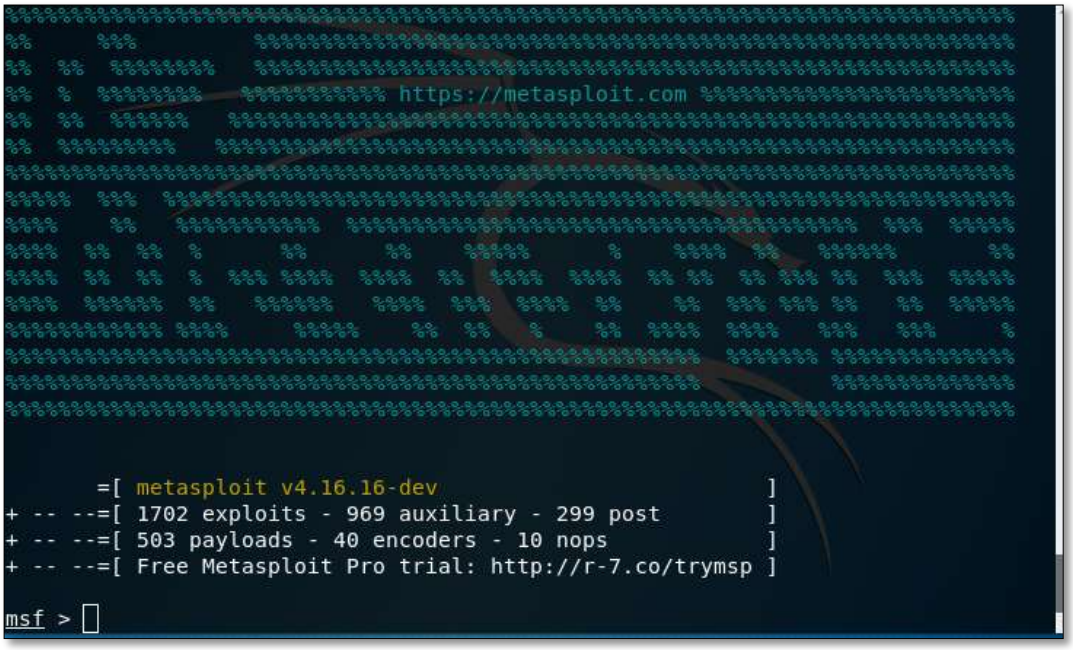


Gráfico 2. Metasploit

4. Ejecutar el comando search mssql (ver gráfico 3). Permite buscar en el repositorio de Metasploit todos los módulos de exploit relacionados con SQL Server.

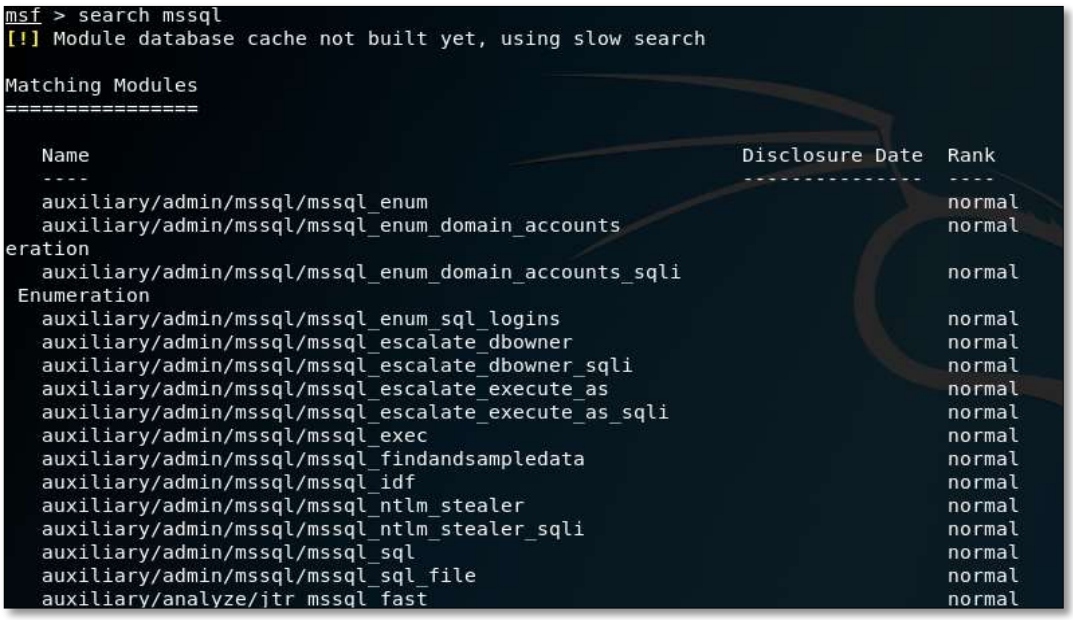


Gráfico 3. Búsqueda con “search”

5. Ejecutar el comando use “módulo de exploit” (ver gráfico 4). Permite seleccionar un módulo de exploit para su utilización. Se recomienda realizar pruebas con los módulos de exploits disponibles, con la finalidad de buscar posibles huecos de seguridad.

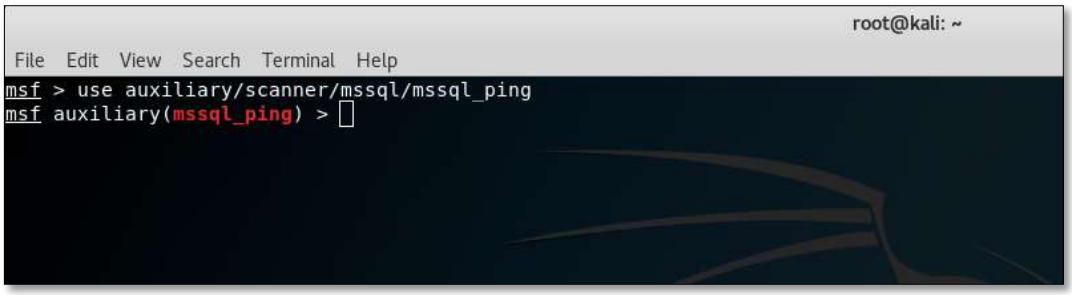


Gráfico 4. Comando “use”

6. Ejecutar el commando show options (ver gráfico 5). Una vez seleccionado el módulo de exploit, a través de show options podremos visualizar los parámetros necesarios para la ejecución del mismo.

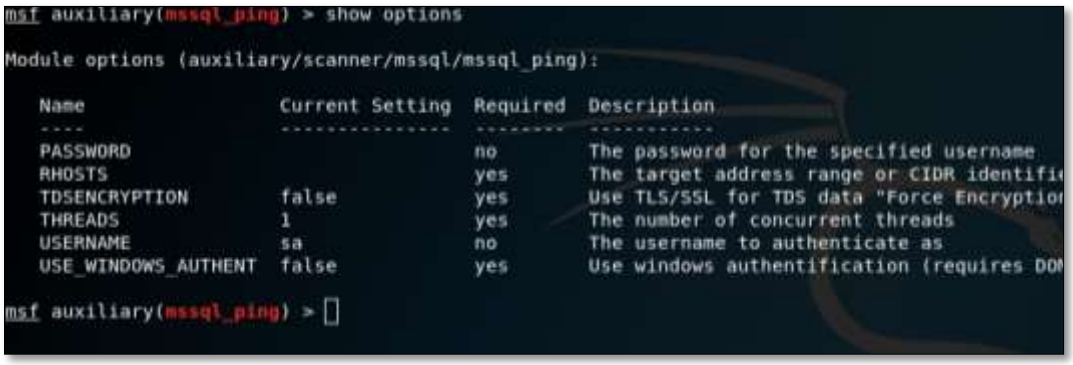


Gráfico 5. Ejecución “show options”

7. Ejecutar el comando set “parámetro” (ver gráfico 6). A través de la ejecución del comando set, podremos setear los parámetros necesarios para la ejecución del exploit.

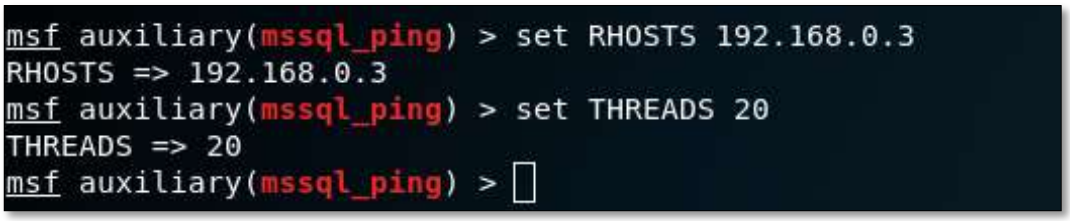


Gráfico 6. Seteo de parámetros

8. Ejecutar el comando exploit (ver gráfico 7). Permite la ejecución del módulo de exploit.

Gráfico 7. Ejecución de exploit

9. Si la ejecución del módulo del exploit se realizó con éxito, a través de payloads se puede aprovechar el acceso obtenido. A continuación, se detallan algunos comandos pertenecientes al payload meterpreter, utilizado en sistemas vulnerados:

help: Abrir uso ayuda meterpreter
sysinfo: Mostrar la información del sistema en el destino remoto.
ls: Lista de archivos y carpetas del objetivo.
ps: Mostrar todos los procesos en ejecución y que las cuentas estén asociadas con cada proceso.
shell: Crear un shell interactivo con todas las fichas disponibles.
execute -f cmd.exe -i: Ejecutar cmd.exe e interactuar con él.
execute -f cmd.exe -i -t: Ejecutar cmd.exe con todas las fichas disponibles.
execute -f cmd.exe -i -H -t: Ejecutar cmd.exe con todas las fichas disponibles y convertirlo en un proceso oculto.
upload file: Subir un archivo al objetivo.
download file: Descargar los archivos desde el objetivo.
reboot: Reinicie el equipo de destino.