MODELOS DE ENCRIPTACIÓN EN BASE DE DATOS MS-SQL SERVER

ING. WILLIAM TORRES ACERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACION EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C., CUNDINAMARCA
2018

MODELOS DE ENCRIPTACIÓN EN BASE DE DATOS MS-SQL SERVER

ING. WILLIAM TORRES ACERO

Monografía presentada como requisito para optar al título de:
Especialista en Seguridad Informática

PhD(c). Gabriel Mauricio Ramírez Villegas
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C., CUNDINAMARCA
2018

Nota de aceptación:

Firma del presidente del jurado

Firma del presidente del jurado

Firma del presidente del jurado

Bogotá D.C., fecha (2, noviembre, 2018)

Cuando se lucha por lo que quieres, obtienes lo que mereces

Dedicado a mis Padres por sus buenos consejos, a mi esposa por su ayuda incondicional y a mis hijos porque ellos son la razón por la cual toda la lucha que he desarrollado a lo largo de este proceso académico tiene sentido.

"Nunca consideres el estudio como una obligación, sino como una oportunidad para penetrar en el bello y maravilloso mundo del saber."

Albert Einstein

CONTENIDO

pág.

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

INTRODUCCIÓN

Las empresas en Colombia necesitan evolucionar en el manejo de la información, principalmente el almacenamiento de las bases de datos, mejorando la protección de los datos, ya que es uno de sus activos más importantes; por este motivo se han generado en Colombia iniciativas y Leyes con el fin de procurar la protección de datos personales, viendo a la información como algo fundamental para el desarrollo de intercambio de datos.

Dentro de este nuevo esquema de intercambio de datos y el manejo de grandes volúmenes de información, es indispensable pensar en la seguridad y la protección de la misma, lo que hace necesario evolucionar la manera en que se exhiben los datos por medio de métodos de encriptación.

Se podrán determinar los mejores mecanismos de protección, con el fin de almacenar los datos de forma segura por medio de criptografía asimétrica, simétrica e hibrida, de forma que pueden ser aplicados dentro de las empresas en Colombia, tanto públicas como privadas, ofreciendo la aplicación de buenas prácticas que no están siendo totalmente aprovechadas por los DBA (Administrador de Bases de Datos – en inglés DataBase Administrator).

En la presente monografía, se quiere presentar una opción clara y posible de implementar, la cual permitirá encontrar modelos específicos de seguridad mediante encriptación de las bases de datos MS-SQL SERVER, teniendo en cuenta que en Colombia se tiene un gran campo de acción, ya que existen en la actualidad gran cantidad de clientes (empresas) con este tipo de motor de bases de datos, tanto a nivel público como privado.

Los modelos de encriptación que se van a presentar, han sido desarrollados y certificados tanto por su fabricante “Microsoft”, como verificados y avalados por expertos DBA que han tenido la experiencia en este tipo de metodologías de encriptación, tanto en Colombia como en el mundo.

1. FORMULACIÓN DEL PROBLEMA

Las bases de datos hoy en día corresponden a uno de los activos de mayor interés para las compañías, siendo de vital importancia preservarlas, protegerlas y respaldarlas[1], esto puede ser un dolor de cabeza para los DBA (Administrador de Bases de Datos) de las organizaciones que tiene que buscar permanentemente la forma de proteger su integridad y su consistencia, garantizando en todo tiempo que sean seguras[2].

Los modelos de encriptación en base de datos MS-SQL Server versiones 2008 en adelante, visto desde el punto de vista de las organizaciones (empresas), se fundamentan con el fin de proteger las bases de datos lo cual es algo muy importante y de alto impacto para las organizaciones[3], la custodia de la información hoy en día no solo es una necesidad, sino una obligación.

Dentro de la investigación se denotarán las problemáticas en que puede incurrir cualquier empresa que descuide la protección de sus datos al no contar con modelos de encriptación en las mismos, un ejemplo de alto impacto lo sufrió Yahoo (en 2014), donde se presentó un robo de 500 millones de cuentas, este tipo de ataque, develó datos robados, donde se encontraban preguntas y respuestas de seguridad sin cifrar[4].

Estos problemas de seguridad los cuales también afectan las bases de datos MS-SQL Server, deberán ser mitigados tomando medidas de protección que claramente se conocerán dentro del presente documento, la problemática actual para el manejo de Bases de Datos y que ha generado grandes tropiezos como el mencionado anteriormente hace que los DBA concentren sus objetivos en la protección a través del cifrado de la información basado en métodos que se mostrarán dentro del desarrollo de la presente monografía.

A través del tiempo la preocupación en proteger las BD, junto con los modelos que se deben implementar, han ido evolucionando drásticamente, sin embargo, no hay un conocimiento muy profundo sobre el tema en las empresas colombianas, ni un modelo estándar que indique la mejor manera de efectuar la aplicabilidad de

[1] Agustín Saiz Martínez. Datacentric. ¿Qué importancia tienen las bases de datos a nivel empresarial? [En Línea]. Disponible en: http://www.datacentric.es/blog/bases-datos/importancia-bases-de-datos-2/

[2] PowerData. Especialistas en gestión de datos. [En Línea]. Disponible en: https://www.powerdata.es/seguridad-de-datos

[3] Ruyt Soriano. Licencias Online. La importancia de la protección a las bases de datos. [En Línea]. Disponible en: https://www.licenciasonline.com/mx/es/noticias/la-importancia-de-la-proteccion-a-las-bases-de-datos

[4] Manel Manchón. ED economía digital. Los diez mayores ataques informáticos de 2016. Barcelona. [En Línea]. Disponible en: https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

métodos seguros y conocidos de seguridad en las bases de datos a través de la encriptación.

El problema específico que tienen hoy las empresas sobre la protección de sus bases de datos, se encuentra en los modelos de protección que deben tener de forma clara y precisa, para lo cual por medio del presente documento se presentarán los modelos susceptibles de ser utilizados e implementados.

Pregunta de Investigación

¿Cuál es el nivel de seguridad y los modelos de encriptación aplicables a las Bases de Datos MS SQL Server versiones 2008 en adelante, de las empresas colombianas?

2. JUSTIFICACIÓN

Es posible inferir que la protección criptográfica dentro de las bases de datos MS-SQL Server, deberían ser un fundamento básico dentro de la construcción de soluciones basados en este motor de base de datos, siendo pertinente indicar que en todo el mundo la protección de la información allí consignada es de vital importancia, ya que los datos son lo más vital para proteger en las organizaciones tales como; bancos, universidades, empresas industriales, entre otros[5].

Es por este motivo que se debe exaltar lo fundamental de la encriptación dentro de las bases de datos, principalmente en motores MS-SQL Server, como lo demuestra el estudio donde se evidencia que dicha seguridad criptográfica genera gran confianza, estudio denominado "El cifrado y las bases de datos" realizado por la Universidad Autónoma de México[6], con el cual se puede inferir con claridad los múltiples beneficios a nivel de seguridad y la forma en que se puede aplicar sin perder su rendimiento ideal.

De otra parte, la presente monografía permitirá adquirir conocimiento más avanzado en materia de criptografía, ya que hoy en día pese a que se menciona mucho el tema, aún no se tiene una idea precisa de la forma de operación de este modelo de seguridad, por lo tanto, se va a esbozar de forma un poco más profunda los algoritmos basados en criptografía simétrica, asimétrica e hibrida[7].

El gran problema que resolverá el presente documento, corresponde en mostrar un modelo ya estudiado y efectivo de encriptación de BD, garantizando a las empresas colombianas; niveles de seguridad apropiados, cumplimiento de legislación sobre protección de datos y mecanismos efectivos de seguridad para los DBA.

Este tipo de procesos de mejora en materia de seguridad para las Bases de Datos, se convierte en una necesidad imperativa en esta era tecnológica donde al mismo ritmo que avanzan las mejoras en rendimiento, performance y seguridad, también avanza los métodos de ataque y de intento de penetración, esto hace que gran cantidad de esfuerzos de las empresas se centren en mejorar y proteger sus sistemas de información, cuyo eje principal son sus datos.

De la misma manera, la presente monografía, pretende presentar de manera

[5] Quintana Zavala Rosinela. Gestiopolis. Bases de datos y su importancia dentro de una Organización. [En Línea]. Disponible en: https://www.gestiopolis.com/bases-datos-importancia-dentro-una-organizacion/

[6] Johnny Villalobos Murillo. Universidad Nacional Autónoma de México. Consideraciones para el uso de Cifrado en las Bases De Datos. México. [En Línea]. Disponible en: https://revista.seguridad.unam.mx/numero22/consideraciones-para-el-uso-de-cifrado-en-las-bases-de-datos

[7] Yuri Tatiana Medina Vargas, Haider Andrés Miranda Mendez. Revista Mundo Fesc. Edición 9. Op. cit., p. 14-20.

efectiva métodos de encriptación existentes que se puede implementar en las BD MS SQL SERVER en las empresas colombianas, el cual exhibe ventajas en la protección de datos, y recoge las mejores prácticas en materia de criptografía simétrica, asimétrica e hibrida mostrando de manera específica el uso de adecuado de las mismas.

La presente monografía va a permitir evidenciar esta característica de protección dentro de un contexto probado y verificado tanto por el fabricante como por las diferentes empresas que participan en comunidades organizadas, la empresa Microsoft®[8] cuenta con modelos de base de datos PYME (Pequeñas y Medianas Empresas), y se centra en el soporte y calidad para este tipo de sector.

Basado en la experiencia que tiene el fabricante (Microsoft ®) y sus comunidades PYME, cuenta con una serie de buenas prácticas y modelos de mejoramiento, los cuales denotan un sin número de oportunidades de mejora sobre aplicación de criptografía eje central de la presente monografía.

Aunque no se puede precisar la escala más rigurosa e infalible sobre protección y prevención, sí se demostrará que el uso de herramientas como lo es la encriptación simétrica, asimétrica e hibrida ayudará a blindar de forma eficiente las Bases de Datos SQL Server corporativas, teniendo en cuenta que existen a lo largo de años una serie de experiencias tanto del fabricante, de su grupo de investigación, así como, las comunidades de DBA que contribuyen con su experiencia en posibles mejoras y soluciones.

Igualmente se va a evidenciar, que al realizar este proyecto de investigación las empresas en Colombia que tengan este motor de base de datos, podrán tener la capacidad de implementar de forma sencilla y efectiva otro nivel de seguridad garantizando protección integral de los datos y ejerciendo control efectivo sobre la información.

[8] Micosoft Español. {2018}. {En línea}. Disponible en: https://www.microsoft.com/es-co

3. OBJETIVOS

3.1. GENERAL

Analizar las técnicas de encriptación en las bases de datos MS-SQL Server versión 2008 en adelante, para uso en las empresas que cuenten con este motor de base de datos en Colombia.

3.2. ESPECÍFICOS

3.2.1 Identificar modelos de encriptación para las bases de datos MS-SQL Server, y establecer su funcionamiento

3.2.2 Determinar las mejoras de seguridad mediante encriptación aplicable a las bases de datos MS-SQL Server

3.2.3 Interpretar los beneficios obtenidos mediante modelos de seguridad sobre las bases de datos de forma clara y precisa

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Dentro de los aspectos más importantes respecto a la protección de los datos, se encuentra el manejo de las BD, en el entendido que la protección de la información es el eje fundamental de los DBA (Administradores de Base de Datos)[9], en tal sentido siempre se trata de brindar mayor seguridad a la transaccionalidad de la información, procurando en todo momento determinar estrategias de prevención de: robo de información, ataques informáticos, denegación de servicio, entre otros[10].

Es por esto, que uno de los problemas fundamentales, es que los datos pueden quedar expuestos para que sean capturados, copiados y modificados, y una de las formas de mitigar esta problemática es la encriptación de los datos contenidos dentro de las BD principalmente MS-SQL Server, por medio de modelos de encriptación.

En razón a lo anterior se puede ver la necesidad de presentar estudios y análisis de pertinencia sobre la encriptación de bases de datos MS-SQL Server[11], algo que puede brindar a los DBA ejemplos sobre la administración de los motores de bases de datos que hoy en día tienen un crecimiento exponencial, es el que posee: "World Data Centre for Climate El WDCC (Centro Mundial de datos para el clima) quien almacena la BD más inmensa del mundo, la misma contiene cerca de 220 terabytes de data y 6 petabytes en datos adicional, conteniendo información sobre el clima, pronósticos y simulaciones."[12].

Dicha base de datos puede incurrir en una pérdida de información sino manejara encriptación, lo que podría ser catastrófico y casi irrecuperable debido a su magnitud y tamaño, este es uno de los factores que hace que la protección de la información tenida en las BD sea algo indiscutible, y una de las mejores maneras de garantizar su consistencia y seguridad es la encriptación la cual a través de la presente

[9] M.I.D. Norma Laura Salazar Viveros. Universidad Autónoma del estado de Hidalgo. Administración de Bases de Datos. México. [En Línea]. Disponible en: http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro21/12_definicin_de_administrador_de_base_de_datos_dba.html

[10] AcensTechnologies. Bases de datos y sus vulnerabilidades más comunes. España. [En Línea] Disponible en: https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

[11] Carlos Galindo González. Gestiopolis. Almacenes de datos y sistemas de información en Microsoft sql server 2008. (2009). [En Línea]. Disponible en: https://www.gestiopolis.com/almacenes-datos-sistemas-informacion-microsoft-sql-server-2008/

[12] 20 MINUTOS EDITORA, S.L. Las 10 bases de datos más grandes del mundo. (2007) [En Línea]. Disponible en: http://www.20minutos.es/noticia/203609/0/bases/datos/grandes/

monografía va a ser evidenciada.

Ahora bien, en Colombia también se ha evidenciado la importancia de las bases de datos para las empresas tanto públicas como privadas, deben conservar, administrar y proteger la información de sus bases de datos, lo cual puso en jaque a casi todo el sector empresarial, ya que en Colombia no estaban muy preparados para este proceso[13].

Las autoridades gubernamentales y las empresas del sector privado han promovido la protección de la información de todos los ciudadanos, al punto de crear una ley que protege el tratamiento de datos personales que es almacenado por las mismas empresas y deben garantizar su seguridad e integridad, como lo indica Colombia Legal Corporation:

"El Derecho de Habeas Data fue creado en Colombia con el fin de permitir a todos los ciudadanos saber, renovar y modificar la totalidad de la información que puedan contener en las distintas entidades y bases de datos del país. Nació como eje principal de los artículos 15 y 20 de la Constitución Política de Colombia. Seguidamente, fue creado como derecho independiente, del que gozan todos los ciudadanos."[14]

Por lo cual se generó la ley que reconoce los datos de las personas como un derecho que debe ser protegido por todas las empresas que puedan tener acceso a ellas o que las contengan dentro de sus plataformas tecnológicas, garantizando los derechos constitucionales de los colombianos, así:

"La Superintendencia de Industria y Comercio, indica, que la Ley de Protección de Datos Personales hace reconocimiento y protección del derecho que poseen todas y cada una de las personas a conocer, actualizar y rectificar toda la información que hayan sido recogida sobre ellas dentro de bases de datos las cuales sean susceptibles de procesamiento por cualquier tipo de entidad pública o privada"[15].

Dentro de los análisis de uso de las bases de datos a nivel global se encuentra que MS SQL Server es una de las más reconocidas en el cuadrante de Gartner a noviembre de 2017, lo que hace que su uso a nivel mundial sea uno de los más altos:

---

[13] Dinero.com. Las nuevas normativas que pusieron a los empresarios contra la pared. (2016) [En Línea]. Disponible en: http://www.dinero.com/edicion-impresa/pais/articulo/nuevas-normas-sobre-manejo-de-bases-de-datos-y-de-archivos-documentales-en-colombia/221913

[14] Asesores Legales Especialistas. Colombia Legal Corporation. (2016). [En Línea]. Disponible en: http://www.colombialegalcorp.com/derecho-de-habeas-data/

[15] Superintendencia de Industria y Comercio. Sobre la protección de datos personales. (2016) [En Línea]. Disponible en: http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

Figura 1. Distribución sistemas de administración de bases de datos operativas

Fuente: Microsoft Inc. 2017. [En Línea]. Disponible en Internet: https://info.microsoft.com/gartner-odbms-magic-quadrant-register.es-es.1.html?ls=website

Se hace necesario que los esfuerzos estén encaminados a blindar a través de diferentes modelos la información y protegerla, como se dijo anteriormente, ya no solo las organizaciones privadas están preocupadas en este sentido, sino también los gobiernos, en Colombia la Superintendencia de Industria y Comercio está muy al tanto en este sentido procurando la protección de la información de todos los usuarios de cualquier tipo de empresa en el territorio nacional[16].

Por las razones descritos anteriormente se vio la necesidad a través de este proyecto de investigación y se van a mostrar las ventajas de la criptografía, claro con sus posibles desventajas (si las hay), con el fin de entregar a cualquier empresa que esté interesada en mejorar la seguridad de sus BD (Bases de Datos) MS-SQL Server con las mejores condiciones técnicas.

Las mismas están previamente probadas y validadas tanto por expertos como por un sinnúmero de empresas a todo nivel que también son clientes de este tipo de tecnología, es importante destacar que los escenarios de seguridad para las BD hoy en día nos permiten hacer simulaciones muy completas y precisas, lo que puede ayudar a garantizar que la salida a producción tenga casi igualdad de condiciones que el ambiente real de operación.

[16] Superintendencia de Industria y Comercio. (2018). [En Línea]. Disponible en: http://www.sic.gov.co/proteccion-de-datos-personales

Se debe tener en cuenta, que lo importante de este proyecto y lo que se busca, es presentar basado en una gran cantidad de antecedentes reales y casos de éxito la importancia en la protección de la información contenida en las BD[17], la forma en que se debe garantizar a todo nivel la integridad de la información, así como la certeza que lo que viaja a través de cualquier medio de comunicación es seguro y confiable, con base en lo indicado por SAIZ MARTÍNEZ.

La importancia de las bases de datos en las empresas permite replantearse muchas mejoras y mecanismos en materia de seguridad, ya que la información (datos) se ha vuelto en uno de los activos más importantes sobre todo a nivel empresarial, la protección de podríamos decir que es lo principal para los DBA, ya que la esencia de una DB el salvaguardar los datos conservando en todo momento su integridad, aspecto que es de vital importancia en todo lo concerniente a manejo y administración de BD.

En su gran mayoría, los datos sensibles en todo el mundo se encuentran almacenados dentro de sistemas de BD comerciales principalmente Oracle, Microsoft SQL Server entre otros, lo cual genera que efectuar un ataque en una base de datos se ha convertido en una de las metas favoritas para los delincuentes informáticos, lo que puede darnos un indicio el porqué de las agresiones externas sobre las BD, unos de los más comunes pueden ser la inyección de SQL.

Se pude evidenciar que los hackers se han dedicado a encontrar este tipo de vulnerabilidades de las páginas WEB con el fin de desarrollar su explotación, del mismo modo y como un referente de la problemática que se tiene, según estudio efectuado en febrero de 2009 por The Independent Oracle Users Group (IOUG), se puede afirmar que cerca del cincuenta por ciento de todos los usuarios que usan Oracle en sus BD no cuentan con los lo menos dos parches que no han sido aplicados, para brindar mayor seguridad[18]

A lo largo del tiempo las empresas, han enfocado su atención principalmente en el aseguramiento de los perímetros de las redes a través de cortafuegos (firewall), IPS/IDS, antivirus, entre otros lo que nos demuestra que cada vez las empresas se están orientando en la seguridad sobre las BD, principalmente aquellas críticas para la organización con información sensible, salvaguardándolos de penetraciones y de modificaciones no permitidas. Uno de ellos y funcionalmente uno de los más importantes es la encriptación de la base de datos a través de llaves asimétricas,

[17] SORIANO, Ruyt. La importancia de la protección a las bases de datos. [En Línea]. Licencias Online. (2016). Disponible en: https://www.licenciasonline.com/mx/es/noticias/la-importancia-de-la-proteccion-a-las-bases-de-datos

[18] ISO/IEC 27001:2005 - Information technology -- Security techniques [en]. (2013) [En Línea]. Disponible en: http://www.iso.org/iso/catalogue_detail?Csnumber=42103

siendo el eje principal de este proyecto de monografía[19].

Ahora bien, partiendo de que el cifrado informático con el cual se opera en la actualidad, se basa en la ciencia de la criptografía, la cual se ha utilizado desde tiempos inmemorables por los seres humanos con el fin de preservar información sensible de forma secreta mucho antes de la era digital (actual), los que se preocupaban por este tipo de tecnología eran los gobiernos, fundamentalmente con fines militares, un ejemplo de ello, fueron los generales militares espartanos, quienes mandaban información muy sensible a través del uso de cilindros de madera.

Dicha codificación era de mucho interés, la misma consistía básicamente en plegar pergamino en torno a una escítala donde se escribía la información en la parte extensa, una vez que llegaba a su destino, necesitaba de otra escítala la cual era de un tamaño similar y así se descifraba la información, porque si se quería leer sin este aparato simplemente se veían letras sin ningún orden ni sentido[20].

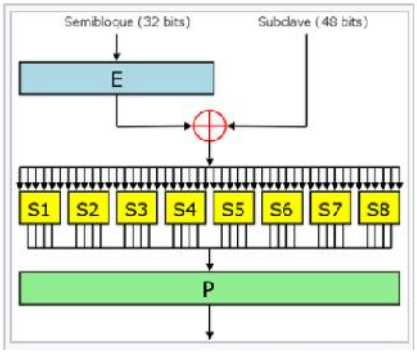
De tal manera, se puede evidenciar, que los seres humanos persistentemente han tratado por todos los medios de proteger la información, también llamados datos, hoy en día, en lugar de usar una escítala se puede contar con ordenadores los cuales logran efectuar un cifrado mucho más complejo, llegando a ser imposible de ser descifrado por el ser humano normal, actualmente el cifrado cuenta con una serie de algoritmos que revisten mucha complejidad y robustos los cuales actúan como una orientación para cifrar y descifrar cualquier tipo de mensaje cuando sea necesario.

Alguno de los primeros cifrados desarrollados tecnológicamente corresponde al modelo de cifrado de datos (Data Encryption Standar o DES) el cual apareció en el año 1970 por la compañía IBM con el fin de proteger información importante del gobierno, ya para el año 1977 se logró crear una versión levemente modificada la cual se convirtió en un estándar en Estados los Unidos la cual fue expandida a todo el mundo posteriormente.

Figura 2. La función Feistel (Función-F) de DES

[19] Microsoft. SQL Server y claves de cifrado de base de datos (motor de base de datos). (2017). [En Línea]. Disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine?view=sql-server-2017

[20] La necesidad de ocultar: desde la escítala a la criptografía cuántica. (2010). [En Línea] Disponible en: http://www.teknoplof.com/2010/07/05/la-necesidad-de-ocultar-desde-la-escitala-a-la-criptografia-cuantica/



Fuente: Herramientas Web para la enseñanza de protocolos de comunicación. [En Línea]. Disponible en Internet: http://neo.lcc.uma.es/evirtual/cdd/tutorial/presentacion/des.html

De otra parte, es importante indicar, que la encriptación basada en llaves simétricas basa su funcionamiento para la encriptación y desencriptación en la necesidad de usar la misma llave, por este motivo, si se llegase al caso que la llave fuera pública y asequible a cualquier usuario, se podría ver la información que está protegida y encriptada en la base de datos.

Desde luego, no es necesario preocuparse por esto, ya que este tipo de encriptación es sin lugar a dudas una de las más comunes. Es así, que, con el fin de establecer una llave simétrica, la misma tiene que estar encriptada mediante un certificado correspondiente a una llave asimétrica, sin embargo, en algunos momentos de otra llave simétrica, esto hace que se brinde mayor seguridad ya que el usuario deberá utilizar los diferentes mecanismos de encriptación si necesita contar con la llave que le dará la posibilidad de encriptar o desencriptar los datos requeridos.

Dentro de los modelos de encriptación que se pueden manejar para las bases de datos SQL SERVER, se debe buscar la eficiencia que puede ofrecer la criptografía simétrica como asimétrica aprovechando las ventajas de cada una o ha visto de otra forma, pero con el mismo resultado evitando las vulnerabilidades que representan las mismas, en este sentido el simétrico no es muy seguro y el asimétrico es lento.[21]

4.2. MARCO CONCEPTUAL

Teniendo en cuenta aspectos basados en seguridad, no se puede afirmar que todo está escrito, ya que algo muy cierto es que cada vez que se crean mecanismos de seguridad, del mismo modo los denominamos hackers dedican todo su tiempo en poder descubrir, vulnerar y penetrar los sistemas de seguridad, entre ellas una de las finalidades más codiciadas en la obtención de información para ser aprovechada de alguna manera.

[21] GenBeta. Tipos de criptografía: simétrica, asimétrica e hibrida. (2017). (En Línea). Disponible en: https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Sin embargo, en ocasiones lo único que persiguen es causar daño y tratar de demostrar que son mejores que los sistemas de seguridad, efectivamente hasta los mejores protocolos de seguridad han sido vulnerados, la amenaza siempre va estar presente, por ello, justamente lo más importante es tomar todas las medidas de precaución principalmente sobre las BD.

Según Verizon indica que el 96% de los datos vulnerados en el transcurso del año 2012 tenían su fuente en las BD, dentro de su informe entre otras cosas se pudo constatar que más de 242 millones de registros aparecieron latentemente envueltos en accesos no autorizados, según indicaciones de la Open Security Foundation[22], lo cual demuestra la vitalidad de las BD.

En el informe anteriormente mencionado, se constata que el ataque a las bases de datos cada día va en crecimiento, siempre la protección de la información es algo que el ser humano necesita resguardar, ahora bien, existen muchas recomendaciones de seguridad que deberían ser implementadas como: control de privilegios, prevención en la programación para evitar la inyección de código, malware, denegación de servicio (DoS), entre otros, la monografía se va a centrar en la protección mediante criptografía.

Una de las más grandes ventajas de la criptografía asimétrica, consiste en que la utilización de sus contraseñas es mucho más simple y segura, en razón a que la contraseña que es utilizada y distribuida es pública conservándose la privada solo para uso exclusivo de su propietario, lo cual permite convivir también con claves simétricas para manejar dos niveles de protección.

Del mismo modo, existen métodos que han sido mejorados con el tiempo, un ejemplo; en una semejante longitud de contraseña y mensaje se hace necesario mucho más tiempo de procesamiento, en razón a que las contraseñas tienen ser de un mayor tamaño que las contraseñas simétricas (usualmente poseen cinco o más veces que el tamaño de las claves simétricas), el mensaje una vez es cifrado contiene más espacio que el original. Por este motivo los nuevos mecanismos con clave asimétrica se fundamentan en curvas elípticas, cuentan con características menos dispendiosas haciendo que la consulta sobre la base de datos sea más eficiente y efectiva.

Efectivamente hablando en términos de protección, luego de analizar y revisar varias líneas de investigación en materia de criptografía para bases de datos, la mejor opción conocida hasta ahora buscando la protección de los datos es la criptografía asimétrica, principalmente porque nos puede ayudar a garantizar protección en la integridad de la información, basado en la estructura que usa donde decodificar o desencriptar necesita de un algoritmo específico que tiene intervención

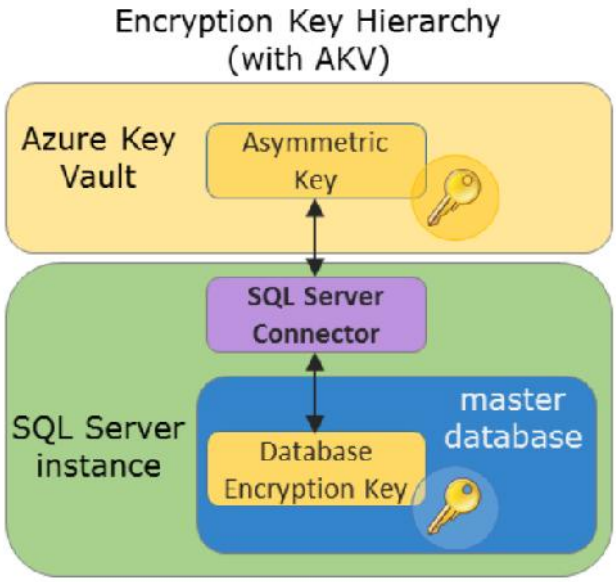
[22] Las 10 grandes amenazas de seguridad en las bases de datos. (2013). [En línea]. Disponible en: http://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad-bases-datos/

de un validador que da fe que la llave es la correcta.

Lo anterior hace que la posible vulnerabilidad que se pueda presentar se reduzca drásticamente, ya que esta metodología de protección aún no ha sido superada en su esencia, lo que han hecho hoy en día los distintos fabricantes (SQL, Oracle, MySQL, entre otros) es adicionar niveles de control o métodos más complejos, pero la esencia de su funcionamiento no deja de ser la misma.

Recordemos que se fundamenta en el manejo de un par de contraseñas; una pública (la cual se envía sin que genere contratiempos a cualquier persona que quiera enviar algo cifrado) y otra privada (la cual no es conocida y justamente es la que protege la integridad de la información), con base en lo anterior, en el caso que se quiera, que tres personas manden un archivo cifrado, lo que hace es enviarles la clave pública (la misma está vinculada a la llave privada) así podrán enviar de forma confidencial, teniendo la clave privada de ese archivo que solo el destinatario puede descifrar.

Figura 3. Usar el conector de SQL Server con características de cifrado de SQL



Fuente: Microsoft Inc. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Esto puede aparentar que el sistema es un poco incompleto, puesto que se puede inferir que conociendo la contraseña pública fácilmente se deducir la contraseña privada, sin embargo, estas metodologías de técnicas criptográficas hacen uso de algoritmos con una complejidad muy avanzada, en razón a que la contraseña privada y pública podrían llegar a tener 2048bits de tamaño (se diría que es casi imposible de decodificar).

De acuerdo a lo indicado por IBM; “Todos los sistemas de cifrado están basados en

el concepto de contraseña. Una contraseña es la fuente de una transformación, normalmente matemática, de un mensaje ordinario en un mensaje ilegible. Durante siglos, la mayoría de los sistemas de cifrado se basaban en un cifrado de clave privada. El cifrado de clave pública es el único reto al cifrado de clave privada que ha aparecido en los últimos 30 años"[23]

Esto quiere decir, que hasta la fecha en materia de seguridad de información enfocada hacia bases de datos la protección más efectiva es la criptografía asimétrica, sin lugar a dudas es un concepto muy trabajado y mejorado a lo largo del tiempo, se puede decir que es la evolución de aprendizaje múltiple en prevención de vulnerabilidades, ya que hoy en día es usado por bancos, grandes empresas, compañías de comercio electrónico, es decir todos aquellos que buscan la defensa de su información se ven abocados al uso de este método de protección.

1&1 Digital Guide, indica: "Los datos almacenados en las BD son, por lo general, de vital relevancia para el buen funcionamiento de la estructura interna o externa de muchas empresas, además de alojar datos sensibles como direcciones, accesos a cuentas bancarias o información de contacto de clientes y de proveedores. En el mundo online, los servidores web acceden a ellas para obtener la información necesaria para que una web funcione y se visualice correctamente"[24].

Se puede inferir, sobre los modelos de encriptación de la base de datos MS-SQL Server, que existe bastantes casos de éxito, así como documentación que nos puede ayudar a la implementación de este mecanismo para cualquier empresa o individuo, toda vez que sus componentes no son complejos de implementar, pero si es complejo de vulnerar.

4.2.1. Tipos de cifrado existentes hoy en día

Hoy en día existen los cifrados de llave simétrica, los cuales usan una llave equivalente tanto para el proceso de cifrado como para el proceso de descifrado de la información, un ejemplo símil ilustrativo sería, cuando una persona X envía una caja con un cerrojo que solo abre con una llave a una persona Y, la persona Y recibe dicha caja y la abre con otra llave igual que la que tiene la persona X, esto se puede definir como un tipo de cifrado simétrico.

Por otro lado, el cifrado asimétrico posee una mayor complejidad, de forma

[23]Criptografía de clave pública. (2014). [En Línea]. Recuperado de: https://www.ibm.com/support/knowledgecenter/es/SSMKHH_9.0.0/com.ibm.etools.mft.doc/ac55940_.htm

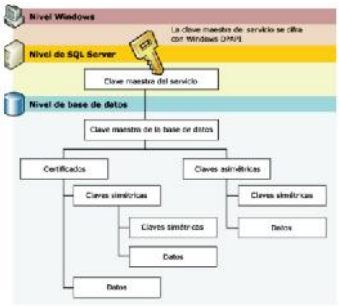
[24] Bases de datos: la importancia de asegurar tu información. (2017). [En línea]. Recuperado de: https://www.1and1.es/digitalguide/servidores/seguridad/bases-de-datos-la-importancia-de-asegurar-tu-informacion/

ilustrativa se puede decir que la misma persona X envía la misma caja, pero previamente le pide a la persona Y que le envie el cerrojo abierto pero que no envie la llave, la persona X cierra la caja y la asegura, pero sin tener la llave que lo abre, al recibirlo la persona Y puede abrirlo ya que tiene la llave, ahora bien, si la persona Y quiere devolverle la caja segura a la persona X debe hacer el mismo proceso.

Es así como, únicamente un usuario poseería la llave para abrir el cerrojo, claro está que el proceso que efectúa un ordenador a través de un algoritmo es mucho más complejo y es bastante más sensitivo, ya que la llave jamás es transportada a ningún lugar ni es copiada, con el fin de evitar que una tercera persona logre obtenerla mientras está en su tránsito.

Justamente este tipo de encriptación es la que se va a visualizar a lo largo de este proyecto de investigación denotando sus múltiples ventajas y beneficios enfocado principalmente en las Bases de Datos SQL-Server, a pesar que los procesos de encriptación poseen unos orígenes muy antiguos su evolución a nivel de complejidad ha sido inconmensurable, y debe ser así para prevenir que pueda ser detectado con facilidad.

Figura 4. Cifrando datos con SQL Server



Fuente: Microsoft Inc. [En Línea]. Disponible en Internet: https://msdn.microsoft.com/es-es/library/bb972194.aspx

Ahora bien, dentro del contexto de seguridad de las bases de datos podemos encontrar tres tipos de métodos que son aplicables para protección criptográfica en SQL SERVER, los cuales permiten un funcionamiento tanto de forma individual, sin depender el uno del otro, como de forma conjunta, aplicando dichos mecanismos en una parte para un tipo de esquema y el otro para afianzarse de forma que genere un tipo de doble protección.

Las claves asimétricas se componen de una clave de tipo privado y su proporcionada clave pública, cada una tiene la facultad de descifrar los datos que cifra la otra, sin embargo, el proceso de cifrado y descifrado asimétricos efectúan un consumo elevado relativamente alto de recursos, sin embargo, proporcionan un grado de seguridad superior al que hace el cifrado simétrico. Hay que saber que, las claves de tipo asimétrico pueden ser utilizadas para cifrar claves simétricas con el fin de ser almacenadas en una base de datos.

Figura 5. Criptografía asimétrica

Fuente: El autor

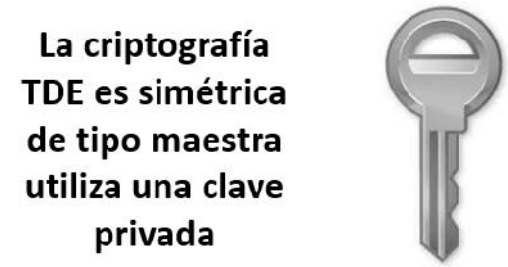
Las claves simétricas, son claves que se utilizan para cifrar y descifrar de forma más rápida y eficiente, lo que le permite que sean más adecuadas para uso de forma acostumbrada para datos confidenciales dentro de una base de datos, en este orden de ideas son las más usadas comúnmente a nivel de bases de datos ya que no necesita de una entidad certificadora que las valide.

Figura 6. Criptografía simétrica

Fuente: El autor

El cifrado de datos transparente (TDE), corresponde a un caso excepcional de cifrado que hace uso de una clave simétrica. TDE efectúa el cifrado a una base de datos completa por medio de una clave simétrica la cual se denomina “clave de cifrado de base de datos”, es decir corresponde a una clave de tipo maestra que puede convivir con una clave de tipo asimétrica que esté almacenada en un módulo EKM y así protegen la clave de cifrado de base de datos.

Figura 7. Criptografía TDE



Fuente: El autor

Teniendo en cuenta, como se ha mencionado, es de vital importancia la protección de los datos siendo una acción que no debe descuidarse, con el fin de resguardar la información cuando es almacenada en las tablas, ciertos datos no deben ser fácilmente accesibles y en el caso que se deba acceder a ellos, deben ser presentados de manera encriptada.

Ahora bien, una de las formas en que pueden estar los datos encriptados dentro de la BD, se puede crear a través del uso de complejas funciones que encripten la información aplicando un algoritmo complejo, sin embargo, ese método no sería eficiente, en razón que el tiempo que le llevaría crear dicha función es considerablemente alto, generando bugs. SQL Server, desde a partir de la versión 2005, brinda formas de encriptación de la data directamente sobre la base de datos, como se puede observar en el Anexo B. Ejercicio encriptación y desencriptación MS-SQL Server.

4.3. MARCO CONTEXTUAL

SQL Server y claves de cifrado de base de datos (motor de base de datos)[25]

A través de este enlace se puede encontrar como el grupo de ingenieros de Microsoft, nos presentan la manera en que se debe efectuar de mejor manera la encriptación de claves asimétricas para bases de datos MS SQL SERVER, del mismo modo nos muestra la aplicación para las contraseñas de MS SQL Server y las contraseñas de las BD, lo cual permite efectuar los niveles de seguridad sugeridos para este tipo de encriptación. Siendo un beneficio para los DBA de las Pymes en Colombia.

Cifrado de base de datos SQL Server por TDE[26]

Josep Ma Solanes, indica a través de este artículo una manera en que se puede efectuar la codificación sobre una BD con MS SQL Server a través del Transparent Data Encryption (TDE) de Microsoft, se detalla el paso a paso de su aplicabilidad y la forma adecuada de efectuar dicho proceso, este sirve para versiones de SQL

[25] SQL Server y claves de cifrado de base de datos (motor de base de datos). (2017). [En línea]. Recuperado de: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine?view=sql-server-2017

[26] Cifrado de base de datos SQL Server por TDE. (2017). [En línea]. https://www.jmsolanes.net/es/cifrado-base-datos-sql-server-tde/

Server 2008 hasta 2016, claro está únicamente de tipo Enterprise, Datacenter de 2008 R2 o Developers las cuales deben ser de tipo producción.

Datos Abiertos – Gobierno Digital Colombia[27]

El gobierno colombiano, promueve el uso de datos abiertos en las organizaciones tanto públicas como privadas con el fin de compartir información de interés público, la cual se debe hacer con las medidas de seguridad necesarias que pueden brindarle a la ciudadanía en general acceso a la información, pero con mecanismos de protección de los datos. Siendo un beneficio para las empresas colombianas que buscan integrarse entre ellas y, entre ellas y el estado

Registro Nacional de Bases de Datos Colombia[28]

El Registro Nacional de Bases de Datos (RNBD), incorpora el directorio de tipo público de las BD que deben sujetarse a tratamiento en Colombia, estas bases de datos son administradas por la Superintendencia de Industria y Comercio, las cuales son para consultar libremente por los ciudadanos, el Gobierno generó reglamentación sobre la información mínima que debe estar contenida dentro del RNBD, así como, los términos, condiciones y especificaciones que debe tener para ser registradas.

Empresas colombianas se preocupan por su seguridad informática[29]

Dentro de lo presentado por la revista Dinero, en Colombia las empresas se están preocupando el un alto nivel por la seguridad y la protección de su información, lo que lo ha puesto en un nivel muy alto en América Latina, ya que el nivel de protección en materia de seguridad es superior al 77% mientras que en la región está por el orden del 74%, lo que evidencia que Colombia está cada vez más preocupado por la protección. Cifras que alertan a las PYMES para adoptar modelos de protección mediante criptografía.

---

[27] Proyecto Datos Abiertos. (2017). [En Línea]. Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/w3-article-9407.html

[28] Superintendencia de Industria y Comercio. Registro Nacional de Bases de Datos. (2018). [En Línea]. Recuperado de: http://www.sic.gov.co/registro-nacional-de-bases-de-datos

[29] Revista Dinero. Empresas colombianas se preocupan por su seguridad informática. (2018). [En Línea]. Recuperado de: https://www.dinero.com/empresas/articulo/noticias-empresariales-en-podcast-de-tercera-semana-de-junio-2018/259598

4.4. MARCO LEGAL

4.4.1. En Colombia

Constitución Política de Colombia de 1991, Artículo 15. Donde presenta el derecho fundamental de salvaguarda de datos, así: *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."*[30]

La Ley Estatutaria 1266 de 2008, en esta se incorporan las disposiciones generales para hábeas data, así mismo se normaliza el control de los datos contenidos en BD de tipo personal, centrado especialmente sobre la información financiera, bancaria, productiva, de bienes y servicios que puedan provenir de otros países, así mismo se decretan otras disposiciones afines.[31]

Ley 1581 de 2012 donde se reglamenta en todo el territorio nacional el procedimiento sobre los datos contenidos en las BD, cuyo ámbito de aplicación se encuentra dentro de los elementos y disposiciones contenidos en la mencionada ley las cuales podrán ajustarse al uso de los datos personales que se encuentren inscritos en cualquier BD, donde deban ser tratados por las entidades tanto públicas o privadas.

Dentro de la misma Ley en el literal *"g) Principio de seguridad"*, menciona: *"…La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;"* (subrayado fuera de texto)[32]

Decreto 1727 de 2009, en el que es reglamentada la forma en la que los entes Bancarios manejan la información de tipo Financiera, Crediticia, Comercial, de Servicios y la que venga de otros países, la cual debe mostrar todos los datos de los titulares de la información.[33]

---

[30] Constitución Política de Colombia. [En Línea]. Recuperado de: https://wsr.registraduria.gov.co/IMG/pdf/constitucio-politica-colombia-1991.pdf

[31] Ley Estatutaria 1266 de 2008. [En Línea]. Recuperado de: http://wp.presidencia.gov.co/sitios/normativa/leyes/Documents/Juridica/Ley%201266%20de%2031%20de%20diciembre%202008.pdf

[32] Ley 1581 2012. (2012). [En Línea]. Recuperado de : http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[33] Decreto 1727 de 2009. [En Línea]. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36251

Resolución 76434 de 2012, en esta, es anulado lo comprendido por el Título V en la Circular Única emitida por la SIC, que habla de Acreditación impartiendo condiciones referentes sobre la protección de Datos Personales, especialmente, lo que tiene que ver en el acatamiento de la Ley 1266 de 2008, la cual habla de reportes de información financiera, crediticia, comercial, de servicios y la originada de otros países.[34]

En este sentido, aunque no existen unas características técnicas específicas de protección de los datos contenidos en una base de datos, sólo en términos generales, se debe garantizar la seguridad y el acceso hacia la información que en ellas esté contenida, teniendo en cuenta esto se puede aseverar que una de las medidas que se tiene a través de este documento de investigación es la encriptación asimétrica de las bases de datos SQL SERVER.

4.4.2. En América Latina

Según indica la OEA (Organización de los Estados Americanos), las bases de datos son parte del programa que lidera el Departamento de Derecho Internacional (DDI) referente al acceso de la información pública. Del mismo modo, es también una contribución para el análisis del tema que efectúa la Comisión de Asuntos Jurídicos y Políticos de la OEA, los cuales se presentan en los mandatos y las resoluciones que desarrolla la Asamblea General de la OEA.[35]

Se indica que el concepto de privacidad se encuentra directamente relacionado con la intimidad lo cual es un derecho garantizado dentro de los principales documentos interamericanos y universales sobre derechos humanos, trayendo consigo el reto de nivelar el balance entre el derecho a la intimidad de cada persona, versus el crecimiento de la tecnología y el mundo de las Tecnologías de Información y las Comunicaciones.

Es por este motivo de los países de América Latina, muestra el avance en la incorporación del derecho proteger los datos personales en sus políticas y respectivas constituciones generando normas específicas, en cada uno de los países de acuerdo al ejercicio de sus normales legales aplicables.

4.4.3. En el Mundo

[34] Resolución 76434 de 2012. [En Línea]. Recuperado de: https://normativa.colpensiones.gov.co/colpens/docs/resolucion_superindustria_76434_2012.htm
[35] OEA. (2018) [En Línea]. Recuperado de: http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

La Unión Europea, bajo la Directiva 95/46 establece prohibición para la transferencia de información hacia países que no posean algún tipo de defensa de sus datos, así mismo determina procedimientos con el fin de establecer en nivel de un país en cuanto a protección. Para la aplicabilidad de esta Directiva, el Grupo de Autoridades del Artículo 29 estableció y aplicó un concepto para desarrollar las medidas de adopción.[36]

El mayor beneficio que obtiene el país, al ser considerado conveniente para transferir datos es que logra intercambiar información de los demás países miembros de la Unión Europea sin el requerimiento de un trámite o condición técnica adicional. De acuerdo a lo indicado por la Agencia Española de Protección de Datos, hasta 2014, los países considerados que ofrecen protección adecuada, son:

Tabla 1. Países con protección de datos adecuados, según la Agencia Española de Protección de Datos

País	País
• Andorra	• Israel
• Argentina	• Isla de Man
• Canadá (Sector privado)	• Jersey
• Suiza	• Nueva Zelanda
• Islas Feroe	• Uruguay
• Guernsey	• Entidades que ofrecen garantías adecuadas para la protección de datos (Escudo de Privacidad – "Privacy Shield")

Fuente: El Autor

[36] Agencia Española de Protección de Datos. Protección de datos en el mundo. (2014). [En Línea]. Recuperado de: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

5. DISEÑO METODOLÓGICO PRELIMINAR

Teniendo en cuenta el problema que se ha trazado, para el desarrollo de la monografía, y alcanzar los objetivos planteados, se han definido los componentes descritos a continuación con un enfoque cuantitativo, para que se desarrollen a través de las siguientes actividades:

5.1. TIPO DE INVESTIGACIÓN

Corresponde a una monografía de investigación exploratoria, ya que el objetivo principal del estudio es realizar investigación en torno a un tema poco conocido, para profundizar más sobre él, encontrar diferentes contextos a través de la investigación y mostrarlos dentro del desarrollo del presente documento.

5.2. POBLACIÓN

La población es de tipo delimitada, puesto que aplica únicamente para empresas que cuenten con motor de BD MS SQL SERVER de Microsoft en Colombia, tanto para versiones Estándar como Empresariales, dicha población estará en la capacidad técnica de poder implementar la encriptación objeto de estudio.

5.3. MUESTRA

Dentro del desarrollo de esta investigación, se ha seleccionado una muestra de tipo discrecional o intencional, la cual muestra intencionalmente o por juicio el lugar donde se selecciona de acuerdo al discernimiento de un grupo o intención objeto de estudio. En el caso de la presente monografía se van a tomar empresas que cuenten con el motor de BD MS SQL SERVER activo y funcionando, en este caso, se utiliza una muestra intencional porque los entrevistados cumplen con una descripción o propósito específico que es necesario para realizar la investigación.

5.4. TÉCNICAS PARA LA RECOLECCIÓN DE DATOS

Dentro de la técnica de recolección en esta monografía, se ha seleccionado una muestra de tipo discrecional o intencional, se toma de una parte deliberadamente o por criterio donde se escoge basado en el conocimiento de un grupo o intención objeto de estudio. En el caso de este proyecto de investigación se van a tomar empresas que trabajen con el motor de BD MS SQL SERVER activo y funcionando, en este caso, se utiliza una muestra intencional porque los entrevistados cumplen con una descripción o propósito específico que es necesario para realizar la

investigación.

5.4.1. Técnicas de recolección de información

En la presente monografía, para permitir su desarrollo, se determinan efectuar los siguientes aspectos:

- Documentos en medios electrónicos, videos en línea sobre encriptación asimétrica en SLQ SERVER.
- Investigación sobre metodologías de implementación de claves asimétricas aplicadas a SQL SERVER
- Resultado de las entrevistas a DBA (Administradores de Bases de Datos) sobre aplicabilidad y métodos de encriptación para BD MS SQL SERVER

5.4.2. Fuentes de información

5.4.2.1. Fuentes primarias

Las fuentes de información primarias se obtienen mediante búsqueda bibliográfica, artículos técnicos especializados, monografías, tesis, libros o artículos de revistas de informática referentes a la encriptación y la seguridad en los motores de BD MS SQL SERVER.

5.4.2.2. Fuentes secundarias

Basado en las fuentes primarias se utilizan resúmenes, listados de referencias y compilaciones sobre encriptación de BD MS SQL SERVER, dichas fuentes se documentan a través de bibliografía, con el fin de soportar el estudio de investigación desarrollado.

5.4.3. Técnicas de procesamiento y análisis de datos

En el desarrollo del procesamiento de datos basado en las diferentes fuentes obtenidas, se efectúa análisis de la información documental, verificación de los modelos de encriptación sugeridos en el motor de bases de datos SQL SERVER, con el fin de presentar un análisis crítico de los resultados obtenidos en la recolección de datos.

5.5. ACTIVIDADES

Para el desarrollo de la monografía como elemento de investigación se efectúan las siguientes etapas:

5.5.1. Etapa 1. Levantamiento de Información

Procedemos con el proceso de documentar y analizar de la información referente al tema objeto de investigación, a través de las fuentes primarias y secundarias teniendo en cuenta las técnicas de recolección de información planteadas anteriormente con el fin de construir la base documental necesaria para demostrar de forma argumentativa la investigación desarrollada sobre la seguridad en las bases de datos SQL SERVER en cuanto a la protección a través de la encriptación. Para ello las actividades realzadas fueron:

- Análisis y verificación del proceso de encriptación a través de llaves asimétricas en el motor de BD MS SQL SERVER.
- Identificar los beneficios y características favorables al aplicar este tipo de seguridad en las BD.
- Verificar por medio de ejercicios prácticos la defensa sobre las BD al momento de utilizar la protección por medio de encriptación simétrica y asimétrica.

5.5.2. Etapa 2. Interpretación y análisis de información

Una vez es obtenida la documentación que permitirá implementar un método de protección a través de encriptación asimétricas en las bases de datos SQL SERVER, se puede proceder de manera efectiva a desarrollar las siguientes actividades:

- Estudiar ejemplos prácticos y probados sobre ambiente de pruebas de la seguridad de encriptación asimétrica en la base de datos SQL SERVER.
- Analizar las pruebas hacia los motores de base de datos para determinar si el mecanismo de encriptación satisface la investigación objeto la presente monografía donde se puede demostrar la hipótesis planteada.
- Construcción del informe de evaluación final que nos permite inferir el beneficio de contar con este tipo de seguridad en la base de datos.
- Elaboración del documento final para la monografía de acuerdo al tema de investigación.

5.5.3. Etapa 3. Entrega documento final

Presentación de análisis final de resultados obtenidos a manera de conclusiones, presentación del informe de evaluación de las aplicaciones de seguridad criptográfica y presentación formal del documento final de la investigación.

6. MODELOS DE ENCRIPTACIÓN BASES DE DATOS

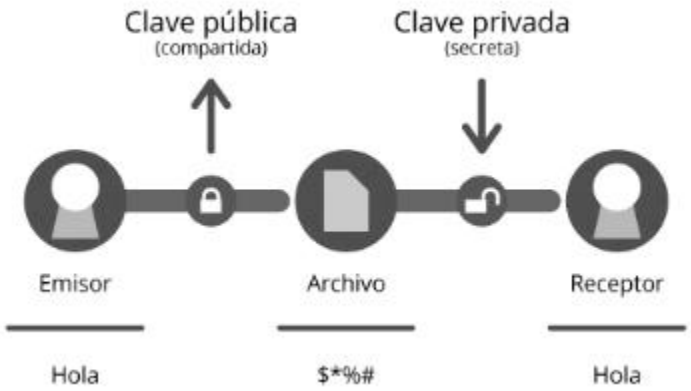
6.1. TIPOS DE MODELOS DE ENCRIPTACIÓN

6.1.1. Modelo de encriptación de claves asimétricas bases de datos SQL SERVER

Uno de los modelos de encriptación para la BD MS SQL Server, son las contraseñas de cifrado la cual incluye composición de claves públicas, privadas y simétricas las cuales son usadas para salvaguardar los datos más relevantes. En este sentido la contraseña simétrica es creada al momento de hacer la instalación de SQL Server cuando se inicia la instancia por primera vez.[37]

En el momento que se hace la instalación del motor de BD MS SQL Server, el sistema operativo hace la creación de las claves públicas y privadas, éstas mismas son utilizadas con el fin de salvaguardar la contraseña simétrica. Así las cosas, para cada instancia que se crea de MS-SQL Server en donde se hace el almacenamiento de datos confidenciales son creadas un par de claves pública y privada.

Figura 8. Criptografía asimétrica base de datos SQL SERVER



Fuente: Genbeta. Pedro Gutierrez. (2013). [En Línea]. Disponible en Internet: https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

Teniendo en cuenta lo planteado en el sitio oficial de Microsoft, donde se indica:

> *"SQL Server tiene dos aplicaciones principales para las claves: una clave maestra de servicio (SMK) generada en y para una instancia de SQL*

[37] Certificados y claves asimétricas de SQL Server. (2017). [En Línea]. Disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/sql-server-certificates-and-asymmetric-keys?view=sql-server-2017

Server, y una clave maestra de base de datos (DMK) usada para una base de datos.

La clave maestra de servicio se genera automáticamente la primera vez que se inicia la instancia de SQL Server y se utiliza para cifrar una contraseña de servidor vinculado, las credenciales y la clave maestra de base de datos. La SMK se cifra mediante la clave del equipo local y la API de protección de datos de Windows (DPAPI). La DPAPI utiliza una clave derivada de las credenciales de Windows de la cuenta de servicio de SQL Server y de las credenciales del equipo. La clave maestra de servicio solo puede descifrarse con la cuenta de servicio en la que se creó o con una entidad de seguridad que tenga acceso a las credenciales del equipo."[38]

Es importante tener en cuenta que la protección sobre las claves de la base de datos SQL Server se encuentra directamente relacionada con el sistema operativo donde está contenida, como se indicó anteriormente genera que su seguridad esté directamente relacionada con su servidor.[39]

Se debe tener en cuenta que, para tener acceso a las bases de datos protegidas con una contraseña maestra, se hace necesaria la misma cuenta de servicio de MS-SQL Server con la que fue creada la contraseña o la cuenta de la maquina o servidor al momento de su instalación. Ahora bien, es posible hacer el cambio de la cuenta de servicio de MS-SQL Server o si lo prefiere la cuenta del equipo, sin que esto genere la perdida de acceso a la clave, pero, si se llega a hacer el cambio de las dos, no podrá tener acceso a la clave maestra de servicio.[40]

En el caso que se llegue a perder la contraseña maestra de servicio y no se tenga ninguno de los dos elementos de acceso, prácticamente será imposible decodificar la información y los elementos codificados a través de la clave original, en este sentido la conservación (recordación) de la clave es fundamental ya que si se pierde o se olvida no hay forma de ingresar a los datos.

6.1.2. Modelo de encriptación de claves simétricas bases de datos SQL SERVER

Ahora se va a tratar la forma en que se puede crear una clave simétrica, para lo cual se debe utilizar alguno de los siguientes métodos: certificado, contraseña, clave

[38] Microsoft. Tecnología, SQL Server y claves de cifrado de base de datos (motor de base de datos). {En Línea}. {12 de marzo de 2018}. disponible en: (https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine)

[39] Licencias Online. La importancia de la protección a las bases de datos. {En Línea}. {20 de mayo de 2018}. Disponible en: https://www.licenciasonline.com/mx/es/noticias/la-importancia-de-la-proteccion-a-las-bases-de-datos

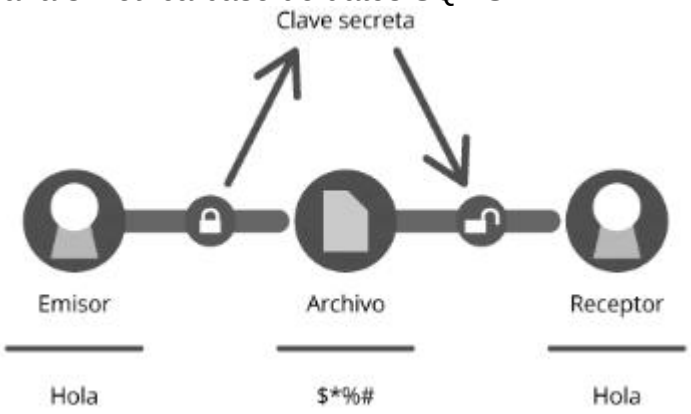
[40] Microsoft. Claves asimétricas. (2017). [En Línea]. Disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/sql-server-certificates-and-asymmetric-keys?view=sql-server-2017

simétrica, clave asimétrica o PROVIDER. Una clave tiene la posibilidad de contar con más de un cifrado de cada tipo, es decir, la misma clave simétrica tiene la posibilidad de cifrarse con varios certificados, contraseñas, claves simétricas e incluso claves asimétricas todas a la vez.

> "*Si se utiliza una contraseña para cifrar una clave simétrica, en lugar de la clave pública de la clave maestra de base de datos, se utiliza el algoritmo de cifrado TRIPLE DES. Por ello, las claves creadas con un algoritmo de cifrado seguro, como AES, se protegen mediante un algoritmo menos seguro*"[41]

Las claves simétricas son las más comunes dentro del proceso de cifrado, sin embargo, no son las más seguras para prevenir ataques, ya que pese a que existen varias opciones de cifrado las mismas pueden ser detectadas mediante modelos de ataques conocidos para SQL Server tales como; ataques de inyección de código, preferencia de privilegios de usuario por privilegios de grupo, control de acceso y gestión de derechos sin clave segura, entre otros.

Figura 9. Criptografía simétrica base de datos SQL SERVER



Fuente: Genbeta. Pedro Gutierrez. (2013). [En Línea]. Disponible en Internet: https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

6.2. ANÁLISIS DE PRUEBAS ENCRIPTACIÓN SQL SERVER

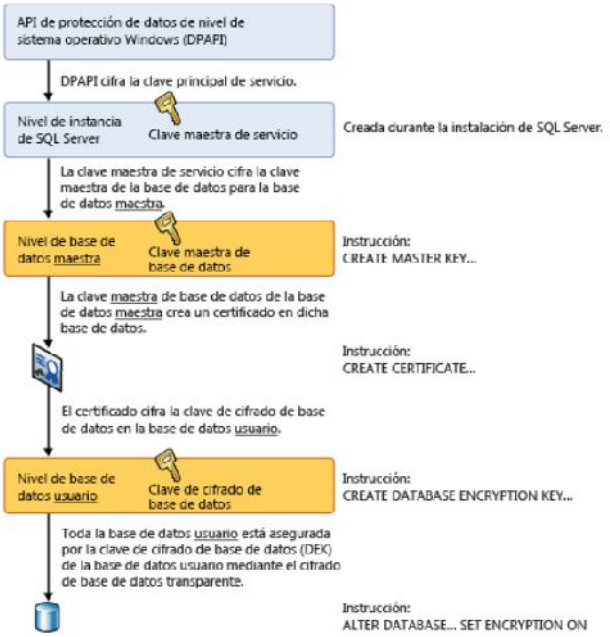
Teniendo en cuenta los modelos presentados por Microsoft Ltd, se puede proceder a efectuar análisis sobre pruebas de encriptación asimétrica y simétrica en bases de datos SQL SERVER por medio de la utilización de TDE

[41] Microsoft. Crear claves simétricas idénticas en dos servidores. {En Línea}. {15 de marzo de 2018}. disponible en: (https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/create-identical-symmetric-keys-on-two-servers)

(Transparent Data Encryption)[42], los pasos se encuentran en el Anexo A- Análisis de Pruebas con la descripción de cada uno de los pasos.

Con este procedimiento práctico se pudo verificar que dentro de la base de datos quedó activado el cifrado asimétrico, este tipo de esquema en modo gráfico, se puede ver la figura donde muestra la arquitectura del cifrado TDE:

Figura 10. Cifrado TDE



Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2012/bb934049%28v%3dsql.110%29

6.3. HERRAMIENTA PARA EFECTUAR LAS PRUEBAS

Teniendo en cuenta que estamos hablando de SQL SERVER, la herramienta que se utilizó para hacer las pruebas es SQL Server Management Studio (SSMS), en el cual como se pudo evidenciar en el punto anterior, a través de ella se pudo configurar y activar el proceso de encriptación asimétrica a la base de datos.

Una vez activada la encriptación procedemos a efectuar intentos de penetración con las herramientas de Kali Linux, una de ellas sqlmap, efectuando inyección de código

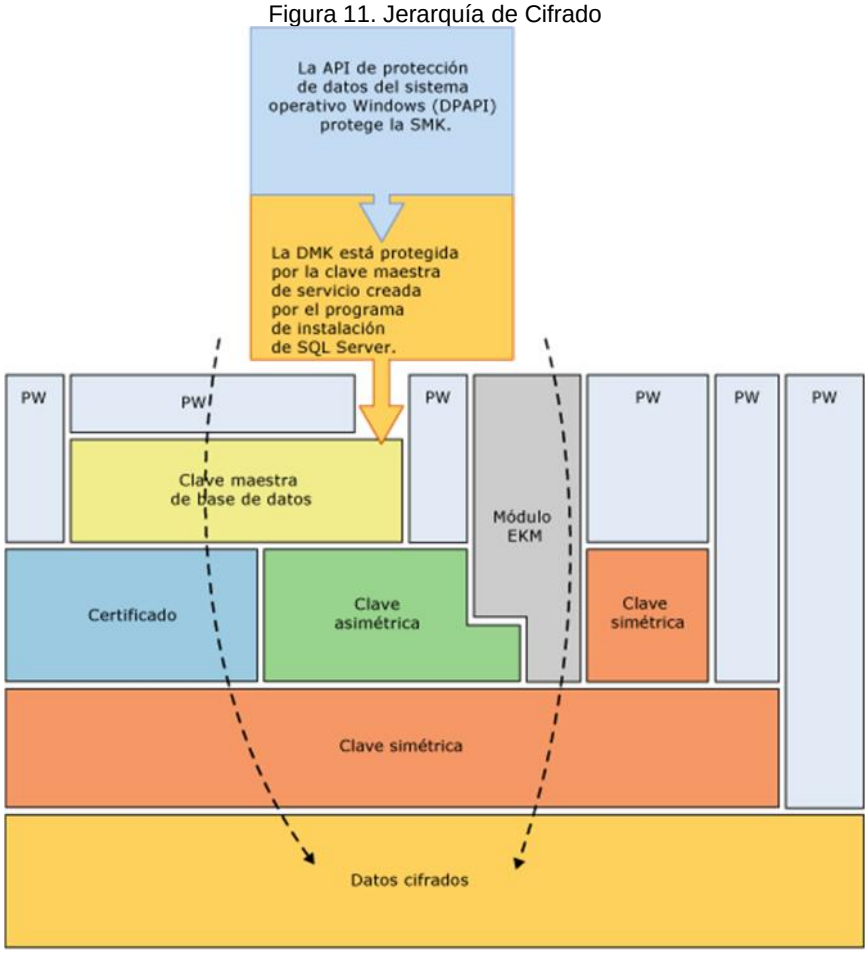
[42] Microsoft. Usar el conector de SQL Server con características de cifrado de SQL. {En Línea}. {5 de mayo de 2018}. disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

con el fin de verificar que la protección criptográfica es efectiva, lo mismo se puede evidenciar dentro del Anexo D – Pruebas de penetración Kali Linux de la presente monografía.

6.4. PROCESO DE CIFRADO SQL SERVER

Para MS SQL SERVER el proceso de codificación de la data cuenta con una infraestructura de cifrado jerárquico con administración de claves. En este caso cada una de las capas efectúa cifrado la capa inferior mediante combinación de certificados, claves asimétricas y claves simétricas. Dichas claves tanto asimétricas como simétricas tienen la posibilidad de estar almacenadas fuera de SQL SERVER bajo un módulo de Administración extensible de claves (EKM).[43]

Figura 11. Jerarquía de Cifrado



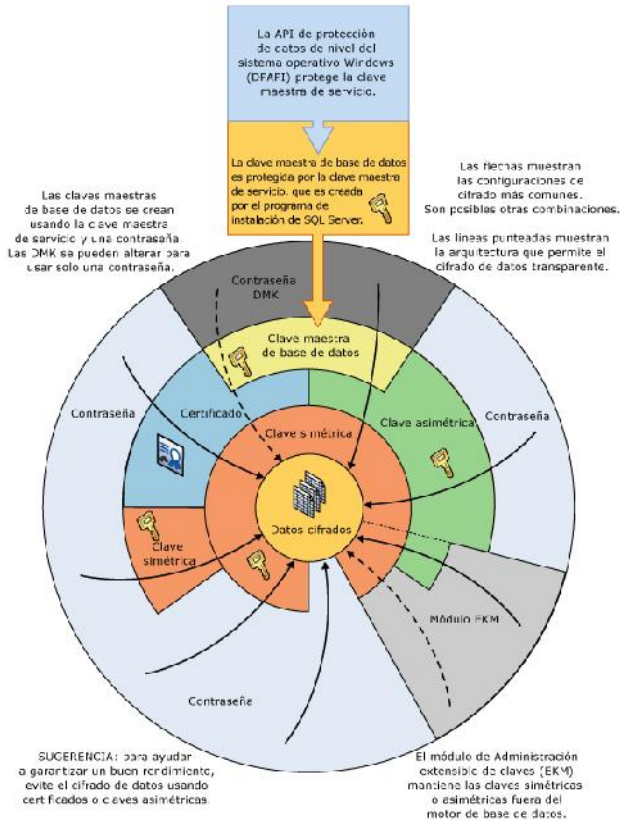
Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2012/ms189586%28v%3dsql.110%29

[43] Microsoft. Jerarquía de cifrado. {En Línea}. {5 de mayo de 2018}. disponible en: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2012/ms189586%28v%3dsql.110%29

Se deben tener en cuenta algunos conceptos esenciales para identificar el mejor método de cifrado:

- Con el fin de contar con el mejor rendimiento, se cifran los datos utilizando claves simétricas en lugar de certificados o claves asimétricas.
- En cuanto a las claves maestras de base de datos, éstas se protegen mediante la clave maestra de servicio al momento de hacer la instalación del motor de base de datos
- Existen otras jerarquías de cifrado que apilan niveles adicionales.
- Es importante conocer que el módulo de Administración extensible de claves (EKM) puede mantener claves simétricas o asimétricas por fuera del motor de base de datos SQL SERVER.
- No se debe olvidar que la clave maestra de servicio, así como las claves maestras de base de datos corresponden a claves simétricas.

Figura 12. Encriptación alternativa de base de datos SQL SERVER de forma mixta



Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2012/ms189586%28v%3dsql.110%29

En la Figura 12, muestra los conceptos adicionales siguientes:

- Las flechas indican las jerarquías de cifrado comunes.

- Las claves simétricas y asimétricas de EKM pueden proteger el acceso a las claves simétricas y asimétricas almacenadas en SQL Server. La línea de puntos asociada a la EKM indica que las claves de la EKM podrían reemplazar a las claves simétricas y asimétricas que se almacenan en SQL Server.[44]

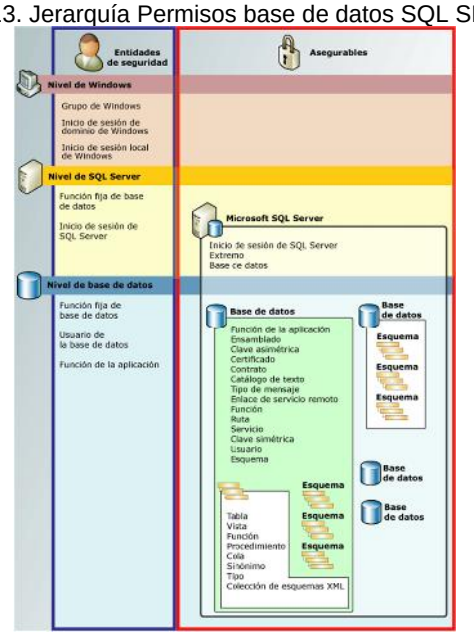
[44] Microsoft. Jerarquía de cifrado. {En Línea}. {5 de mayo de 2018}. disponible en: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2012/ms189586%28v%3dsql.110%29

7. EVIDENCIA PRÁCTICA ECRIPTACIÓN SQL SERVER

7.1. ENCRIPTAR Y DESENCRIPTAR EN SQL SERVER

A través de la siguiente figura se explica el proceso de encriptación y desencriptación de bases de datos MS-SQL Server, mediante el gráfico de la figura 13, se puede observar el nivel la jerarquía de los permisos de SQL-SERVER, en este sentido muestra la lógica aplicable de la encriptación tanto simétrica como asimétrica de las bases de datos.

Figura 13. Jerarquía Permisos base de datos SQL SERVER



Fuente: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2008-r2/ms191465(v=sql.105)

Para el proceso de encriptación, las sentencias de MS-SQL Server se encuentran detalladas en el Anexo B. Ejercicio encriptación y desencriptación MS-SQL Server de la presente Monografía, en la figura anterior se representan los niveles que se deben cumplir para que el usuario pueda llegar a la consulta de la información contenida en la base de datos.

Del mismo modo, se realiza otra prueba de encriptación a través del Anexo C. Ejercicio encriptación MS-SQL Server, en el cual se puede demostrar el uso de encriptación asimétrica para bases de datos SQL Server 2008 en adelante, permitiendo de forma simple su aplicabilidad.

7.2. VENTAJAS Y DESVENTAJAS ENCRIPTACIÓN SQL SERVER

Al momento de aplicar seguridad de encriptación asimétrica y simétrica en las bases de datos SQL SERVER, existen ciertos tipos de riesgos, ventajas y desventajas que hay que tener en cuenta al momento de aplicarlas en las bases de datos, para ello se presentan en el siguiente cuadro comparativo:

Tabla 2. Ventajas y desventajas criptografía

Tipo	Ventajas	Desventajas
Llave simétrica	⟆ El cifrado que efectúa hace que sea muy sencillo de utilizar. ⟆ Es bastante útil para cifrar archivos que contengan datos de tipo personal. ⟆ Solamente necesita una única clave ⟆ Es muy veloz, además usa mucha menor cantidad de recursos informáticos que otros modelos de cifrado ⟆ Es bastante usada con el fin de ayudar a la prevención de riesgos de seguridad ⟆ En el caso que se utilicen varias claves compartidas con varios usuarios, y una de estas claves se encuentra en peligro, afecta únicamente a un usuario y no se ven afectados todos.	⟆ Se hace necesario comunicar la clave privada. ⟆ Al momento de manejar una gran cantidad de claves, la gestión se hace muy difícil. ⟆ El tipo de criptografía basada en clave simétrica es vulnerable a posibles ataques por fuerza bruta o ataques de diccionario.
Llave asimétrica	⟆ Intercambia claves por firma digital ⟆ La contraseña privada solo es conocida por un usuario y la contraseña pública la conocen todos ⟆ Mucho más segura 1024 bits en adelante ⟆ Confidencialidad, integridad y no repudio	⟆ Es lenta en su funcionamiento ⟆ Solo permite menos de 50 claves ⟆ Presenta costo para su funcionamiento ⟆ Depende de un tercero

Fuente: El autor

En cuanto a la criptografía hibrida recoge las mejores prácticas de los dos métodos, lo que hace es hacer que los métodos coexistan de una manera sinérgica haciendo

que sus bondades conformen una estructura de defensa suficiente que garantice protección de los datos.

La encriptación hibrida incluye las bondades que representan la unión de los dos modelos de encriptación asimétrica y simétrica, nos ofrece el uso de los dos modelos de manera que la protección sobre la información contenida en las bases de datos cuente con mayores niveles de protección, trayendo beneficios tales como:

- Permite la generación de una clave pública y de otra de tipo privado (del lado del receptor).
- Facilita el cifrado de un archivo de manera síncrona.
- El receptor puede hacer el envío de su clave pública.
- Hace que la clave se pueda cifrar usando la misma que encripto el archivo utilizando la clave pública del receptor.
- Permite efectuar el envío del archivo cifrado (síncronamente), así mismo permite que la clave del archivo cifrado (asíncronamente), solo puede ser vista por el receptor

7.3. ANÁLISIS DE RESULTADOS

Al efectuar un análisis basado en la información investigada, se puede determinar que, como las dos maneras de efectuar cifrado: asimétrico y simétrico, se poseen ventajas y desventajas, lo más sugerible es aprovechar los beneficios de los dos modelos de encriptación y disminuir los fallos que posee cada uno, el mejor modo es encontrar un equilibrio al hacer uso de los modelos, donde se aprovechan los beneficios de cada tipo de cifrado.

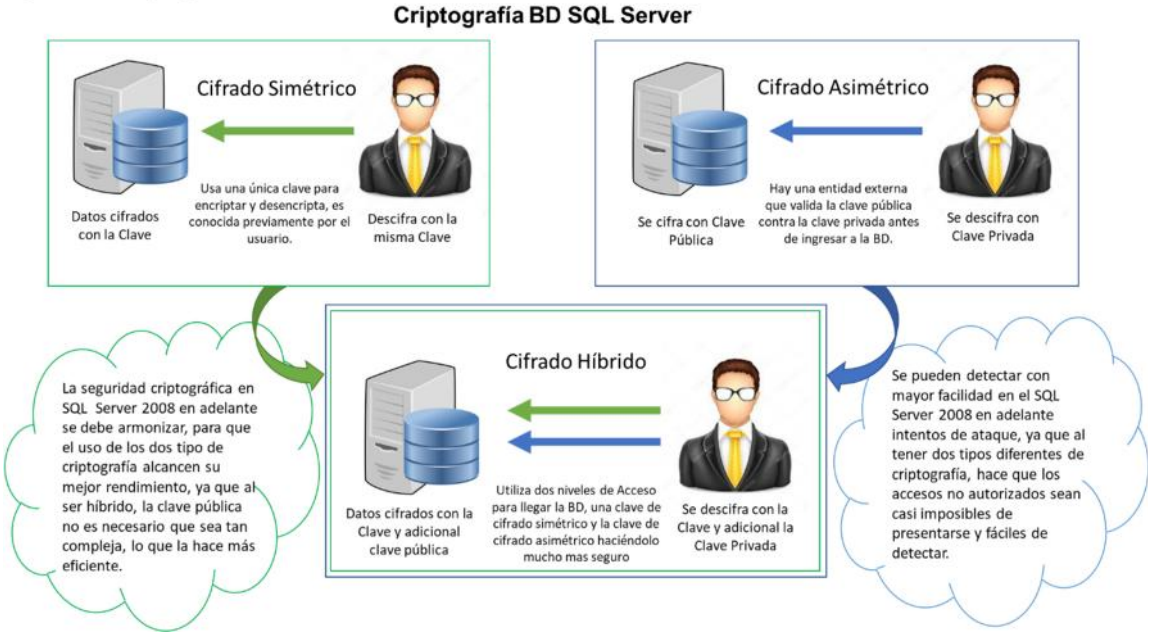
De otra parte, se puede inferir que la mejor manera de contar con seguridad criptográfica, y a su vez un rendimiento óptimo, es a través de la combinación de los dos modelos, es decir un tipo de seguridad hibrida (simétrica y asimétrica), la cual encuentra un equilibrio entre una muy buena seguridad y a su vez un rendimiento razonable, capaz de soportar con eficiencia las necesidades de cualquier DBA en una de las empresas colombianas, que cuenten con el motor de BD MS-SQL Server.

Además de todos beneficios meramente técnicos presentados a lo largo de la presente Monografía, sobre la encriptación hibrida (simétrica y asimétrica) existe un aspecto de protección de datos que ahora es una política gubernamental el Colombia de obligatorio cumplimiento, tanto para empresas públicas como privadas, lo que hace no solo aconsejable sino necesaria su aplicabilidad en un mundo en constante evolución y mejoramiento continuo.

Dentro de los anexos de la presente monografía, se pudo visualizar el uso de los métodos de encriptación simétrica y asimétricas e hibrida de las bases de datos MS-SQL Server la cual sirve desde la versión 2008 en adelante, muestra de una manera muy sencilla el proceso de encriptación de las bases de datos, que puede ser usado por las empresas en Colombia que cuenten con este tipo de motor y versión de base de datos, lo cual hace que se puede hacer una protección de forma rápida y efectiva sin que se altere su estructura.

En la siguiente infografía, se muestra el beneficio de aplicación de la criptografía simétrica y asimétrica (híbrida) dentro del motor de base de datos MS SQL Server 2008 en adelante, en razón a que una la criptografía simétrica es bastante usada con el fin de ayudar a la prevención de riesgos de seguridad y la criptografía asimétrica hace uso de intercambia claves por firma digital, lo que hace que la contraseña privada solo es conocida por un único usuario, así la publica la conozcan todos.

Figura 14. Criptografía híbrida



Fuente: El Autor

Esta combinación híbrida de los dos modelos de encriptación, hace que su robustez se duplique, y que las PYMES en Colombia, pueden adoptar mecanismos más seguros y de simple aplicación, uno nativo del motor de BD MS SQL Server y el otro a través de una entidad certificadora externa.

8. CONCLUSIONES

A través de la presente monografía, se pudo demostrar los beneficios que tiene la inclusión de cifrado simétrico, asimétrico e híbrido dentro de las BD SQL SERVER, permitiendo a los DBA contar con una herramienta probada y certificada para proteger la información sensible.

Es posible evidenciar por medio del contexto visto durante el desarrollo de la monografía que no se puede hablar de seguridad sin tener en cuenta la criptografía en las bases de datos, de otra parte, se pudo evidenciar los mecanismos de protección a través de ejemplos prácticos y precisos donde se aplicaba esta seguridad.

Se pudo dar cumplimiento a los objetivos propuestos dentro de la presente monografía de manera clara y precisa, demostrando las características favorables que se pueden obtener en para la protección de la información, uno de los principales objetivos es poder aplicar estos modelos a las empresas en Colombia que manejen el motor de BD SQL SERVER.

No es posible dejar a un lado que hoy en día la seguridad informática es una prioridad a todo nivel, y que la protección de los datos ya es una obligación de las empresas tanto públicas como privadas velar por la protección de acceso a datos sensibles, finalmente es posible establecer que la encriptación hibrida es la mejor manera para salvaguardar las BD de una manera totalmente efectiva.

Ya que la encriptación hibrida hace que se utilicen claves simétricas y asimétricas generando que las mismas coexistan de manera efectiva y precisa, previo análisis de su aplicabilidad, disminuyendo los factores de error y lentitud sobre los motores de bases de datos SQL SERVER, haciendo más efectivo y seguro el manejo de la información contenida.

Se logró identificar la manera en la que los DBA, cuentan con herramientas mejoradas a través de las diferentes versiones del motor de bases de datos, y los beneficios de contar con comunidad de expertos en seguridad especialmente en criptografía, no obstante, es claro que en materia de seguridad no todo está escrito y se cuenta con una constante evolución que hace que se debe estar muy al tanto de los cambios y mejoras que publica el fabricante Microsoft.

Puede determinarse que, a través de la presente monografía, se cumplieron los objetivos propuestos ya que los modelos de encriptación asimétrica y simétrica e hibrida, son un complemento ideal para que las empresas en Colombia puedan contar de manera efectiva con la protección sobre los datos eje fundamental de las

organizaciones principalmente el respeto de las políticas gubernamentales sobre la protección de la información personal.

El nivel de seguridad y los modelos de encriptación aplicables a las BD MS SQL Server de las empresas colombianas, está en el modo híbrido (simétrica y asimétrica) teniendo en cuenta los presentado dentro de la presenta monografía, del mismo modo se pudo determinar que la protección basada en seguridad asimétrica ha funcionado en varios esquemas de bases de datos que el fabricante Microsoft aplica a las denominadas PYMES (Pequeñas y Medianas Empresas), lo cual es totalmente aplicable a las empresas colombianas.

A futuro se puede inferir, que los modelos de encriptación tanto simétrica como asimétrica en un contexto híbrido, ofrecen un esquema más completo de protección, basado en las mejores características que ofrece cada una de ellas, blindando de una manera efectiva los procesos transaccionales aplicable a las bases de datos MS SQL Server versión 2008 en adelante.

9. BIBLIOGRAFÍA

Bases de datos y sus vulnerabilidades más comunes. AcensTechnologies. {En Línea}. {11 de diciembre de 2017} disponible en: (https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf)

Escenarios de seguridad de aplicaciones en SQL Server. Microsoft. {En Línea}. {9 de diciembre de 2017} disponible en: (https://msdn.microsoft.com/es-es/library/bb669057(v=vs.110).aspx)

Especialistas en gestión de datos. PowerData. {En Línea}. {9 de diciembre de 2017} disponible en: (https://www.powerdata.es/seguridad-de-datos)

Microsoft. Tecnología, certificados y claves asimétricas de SQL Server. {En Línea}. {7 de diciembre de 2017}. disponible en: (https://docs.microsoft.com/es-es/sql/relational-databases/security/sql-server-certificates-and-asymmetric-keys)

PASTORINO, Cecilia. Noticias, opiniones y análisis de la comunidad de seguridad de ESET. WELIVESECURITY. {En Línea}. {9 de diciembre 2017} disponible en: (https://www.welivesecurity.com/la-es/2017/09/05/consejos-bases-de-datos-seguras/)

SAIZ MARTÍNEZ, Agustín. ¿Qué importancia tienen las bases de datos a nivel empresarial? Datacentric. {En Línea}. {9 de diciembre de 2017} disponible en: (http://www.datacentric.es/blog/bases-datos/importancia-bases-de-datos-2/)

SORIANO, Ruyt. La importancia de la protección a las bases de datos. Licencias Online. {En Línea}. {9 de diciembre de 2017} disponible en: (https://www.licenciasonline.com/mx/es/noticias/la-importancia-de-la-proteccion-a-las-bases-de-datos)

MANCHÓN, Manel. Los diez mayores ataques informáticos de 2016. ED economía digital. {En Línea}. {9 de diciembre de 2017} disponible en: (https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html)

QUINTANA ZAVALA, Rosinela. Bases de datos y su importancia dentro de una Organización. Gestiopolis. {En Línea}. {11 de diciembre de 2017} disponible en: (https://www.gestiopolis.com/bases-datos-importancia-dentro-una-organizacion/)

MEDINA VARGAS, Yuri, MIRANDA MENDEZ, Haider. Comparación de Algoritmos Basados en la Criptografía Simétrica DES, AES y 3DES. En: Revista Mundo Fesc. Edición 9. p. 14-20.

SALAZAR VIVEROS, Norma. Administración de Bases de Datos. Universidad Autónoma del estado de Hidalgo. {En Línea}. {11 de diciembre de 2017} disponible en: (http://cidecame.uaeh.edu.mx/lcc/mapa/PROYECTO/libro21/12_definicin_de_administrador_de_base_de_datos_dba.html)

GALINDO GONZÁLEZ, Carlos. Almacenes de datos y sistemas de información en Microsoft sql server 2008. Gestiopolis. {En Línea}. {11 de diciembre de 2017} disponible en: (https://www.gestiopolis.com/almacenes-datos-sistemas-informacion-microsoft-sql-server-2008/)

Las 10 bases de datos más grandes del mundo. 20 MINUTOS EDITORA, S.L. {En Línea}. {11 de diciembre de 2017} disponible en: (http://www.20minutos.es/noticia/203609/0/bases/datos/grandes/)

Las nuevas normativas que pusieron a los empresarios contra la pared. Dinero.com. {En Línea}. {11 de diciembre 2017} disponible en: (http://www.dinero.com/edicion-impresa/pais/articulo/nuevas-normas-sobre-manejo-de-bases-de-datos-y-de-archivos-documentales-en-colombia/221913)

Sobre la protección de datos personales. Superintendencia de Industria y Comercio. {En Línea}. {11 de diciembre 2017} disponible en: (http://www.sic.gov.co/sobre-la-proteccion-de-datos-personales)

Microsoft. Tecnología, SQL Server y claves de cifrado de base de datos (motor de base de datos). {En Línea}. {12 de marzo de 2018}. disponible en: (https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine)

Ventajas y desventajas de la criptografía. w3ii.com. {En Línea} {7 de diciembre de 2017} disponible en: (http://www.w3ii.com/es/cryptography/benefits_and_drawbacks.html)

VILLALOBOS MURILLO, Johnny. Consideraciones para el uso de Cifrado en las Bases De Datos. Universidad Nacional Autónoma de México. {En Línea}. {11 de diciembre de 2017} disponible en: (https://revista.seguridad.unam.mx/numero22/consideraciones-para-el-uso-de-cifrado-en-las-bases-de-datos)

SQL Server y claves de cifrado de base de datos (motor de base de datos). (2017). [En línea]. Recuperado de: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine?view=sql-server-2017

Cifrado de base de datos SQL Server por TDE. (2017). [En línea].

https://www.jmsolanes.net/es/cifrado-base-datos-sql-server-tde/

Ley 1581 2012. {2012}. {En Línea}. {11 de marzo de 2018}. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

Microsoft. Tecnología, SQL Server y claves de cifrado de base de datos (motor de base de datos). {En Línea}. {12 de marzo de 2018}. disponible en: (https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/sql-server-and-database-encryption-keys-database-engine)

Microsoft. Crear claves simétricas idénticas en dos servidores. {En Línea}. {15 de marzo de 2018}. disponible en: (https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/create-identical-symmetric-keys-on-two-servers)

Microsoft. Usar el conector de SQL Server con características de cifrado de SQL. {En Línea}. {5 de mayo de 2018}. disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Microsoft. Jerarquía de cifrado. {En Línea}. {5 de mayo de 2018}. disponible en: https://docs.microsoft.com/es-es/previous-versions/sql/sql-server-2012/ms189586%28v%3dsql.110%29

Memorias de un DBA. Encriptación de datos en SQL Server. {En Línea}. {9 de mayo de 2018}. Disponible en: https://dbamemories.wordpress.com/category/sql-server-database/encriptacion/

OEA. Departamento de Derecho Internacional (DDI). {En Línea}. {9 de mayo de 2018}. Disponible en: http://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp

Agencia Española de Protección de Datos. Protección de datos en el mundo. {En Línea}. {10 de mayo de 2018}. Disponible de: http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

Trainer SQL. Manual SQL Server. {En Línea}. {10 de mayo de 2018}. Disponible en: http://www.manualsqlserver.com/?p=1081

Docs Microsoft. Cifrar una columna de datos. {En Línea}. {10 de mayo de 2018}. Disponible en: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/encrypt-a-column-of-data?view=sql-server-2017

Microsoft. Centro de seguridad para el motor de base de datos SQL Server y la base de datos SQL Azure. {En Línea}. {10 de mayo de 2018}. Disponible en:

https://msdn.microsoft.com/es-co/library/bb510589(v=sql.120).aspx

Technet Microsoft. Seguridad de SQL Server. {En Línea}. {11 de mayo de 2018}. Disponible en: https://technet.microsoft.com/es-es/library/ms172399(v=sql.105).aspx

ApexSQL. Microsoft. Auditoría de seguridad de bases de datos SQL Server. {En Línea}. {11 de mayo de 2018}. Disponible en: https://solutioncenter.apexsql.com/es/auditoria-de-seguridad-de-bases-de-datos-sql-server/

Stucom Centro de Estudios Tecnología Barcelona. Encriptación en Bases de Datos. {En Línea}. {11 de mayo de 2018}. Disponible en: https://espai.stucom.com/tecnologia/encriptacion-en-bases-de-datos/

DJK devjoker. Como encriptar cadenas y campos en SQL server 2005. {En Línea}. {11 de mayo de 2018}. Disponible en: http://www.devjoker.com/contenidos/articulos/82/Como-encriptar-o-cifrar-cadenas-y-campos-en-SQL-server-2005-ENCRYPTBYPASSPHRASE-y-DECRYPTBYPASSPHRASE.aspx

Corobori WebDesign. Como encriptar una columna en una base de datos SQL Server. {En Línea}. {11 de mayo de 2018}. Disponible en: https://www.corobori.com/Corobori_Como_encriptar_una_columna_en_una_base_de_datos_SQL_Server-MTI=.aspx

Just another Microsoft MVPs site. La Visión de un Ingeniero de Campo. Encriptación Simétrica. {En Línea}. {11 de mayo de 2018}. https://blogs.msmvps.com/pmackay/2004/11/27/encriptaci-n-sim-trica/

Genbeta. Pedro Gutierrez. {En Línea}. {11 de mayo de 2018}. Disponible en Internet: https://www.genbetadev.com/seguridad-informatica/tipos-de-criptografia-simetrica-asimetrica-e-hibrida

ApexSQL. Encriptación de copias de seguridad SQL Server. {En Línea}. {11 de mayo de 2018}. Disponible en Internet: https://solutioncenter.apexsql.com/es/encriptacion-de-copias-de-seguridad-sql-server/

Eduardo N. Castillo Caballero. Encriptación de datos con SQL SERVER. {En Línea}. {11 de mayo de 2018}. Disponible en Internet: https://encdesarrollo.wordpress.com/2015/02/11/encriptacion-de-datos-con-sql-server/

Encriptación a nivel de columna (Always Encrypted) en SQL Server 2016 Express

SP1. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://geeks.ms/jorge/2017/10/19/encriptacion-a-nivel-de-columna-always-encrypted-en-sql-server-2016-express-sp1/

IBM Knowledge Center. Habilitación de cifrado de datos transparente en bases de datos de SQL Server. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://www.ibm.com/support/knowledgecenter/es/SSW2NF_9.0.0/com.ibm.ase.help.doc/topics/t_enable_tde.html

Sothis. Explorando SQL Server 2016: siempre encriptado. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://www.gruposothis.com/explorando-sql-server-2016-siempre-encriptado/

AACOSTA. Opciones de encriptación para tablas/base de datos/datos en SQL 2014. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: http://aacosta.com.mx/2017/04/18/opciones-encriptacion-tablasbase-datosdatos-sql-2014/

SQL Shield. Qué entendemos por encriptación de base de datos?. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: http://www.sql-shield.com/es

Michael Villegas. Encriptación de datos en SQL Server. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://dbamemories.wordpress.com/2011/09/28/encriptacion-de-datos-en-sql-server-parte-1/

ARCGIS. Cifrado transparente de datos (TDE) para el espacio de trabajo de revisor en SQL Server. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://desktop.arcgis.com/es/arcmap/latest/extensions/data-reviewer-guide/admin-dr-sql-server/transparent-data-encryption-tde-for-the-reviewer-workspace-in-sql-server.htm

Microsoft. Información general sobre la seguridad de SQL Server. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://docs.microsoft.com/es-es/dotnet/framework/data/adonet/sql/overview-of-sql-server-security

Ahmad Yaseen. SQLShackIr. Nuevas características y mejoras en SQL Server 2016 SP1. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://www.sqlshack.com/es/nuevas-caracteristicas-y-mejoras-en-sql-server-2016-sp1/

Sql Server 2008. Usuarios, Roles, Encriptación y Back Up de la base de datos. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: http://leonelmartinez.udem.edu.ni/wp-content/uploads/2015/01/SQL-SEGURIDAD-Y-PROTECCION.pdf

Power Data. Los inconvenientes de la encriptación. {En Línea}. {12 de mayo de 2018}. Disponible en Internet: https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/cinco-inconvenientes-del-encriptado-de-datos

Anexo A. Análisis de Pruebas

Paso 1.

Crear una credencial de SQL Server para el motor de BD que se usará para TDE

El motor de BD usa la credencial para acceder a Key Vault durante la activación de la BD. Se recomienda crear otro id. de cliente y secreto de Azure Active Directory en la parte I para Motor de base de datoscon el fin de limitar los permisos del Almacén de claves que se conceden.

Modifique el script de Transact-SQL siguiente como se indica a continuación:

Edite el argumento IDENTITY (ContosoDevKeyVault) para dirigirlo a Azure Key Vault.
Si usa Azure público, reemplace el argumento IDENTITY por el nombre de su Azure Key Vault de la parte II. Reemplazar la primera parte del argumento SECRET con el id. de cliente de Azure de la parte I. En este ejemplo, el id. de cliente es EF5C8E094D2A4A769998D93440D8115D.

Se completa la segunda parte del argumento SECRET con el secreto de cliente de la parte I. En este ejemplo, el secreto de cliente de la parte I es Replace-With-AAD-Client-Secret. La cadena final para el argumento SECRET será una secuencia larga de letras y números, sin guiones.

Figura 15. Ejemplo práctico creación credenciales

```
SQL                                                                    Copiar

USE master;
CREATE CREDENTIAL Azure_EKM_TDE_cred
    WITH IDENTITY = 'ContosoDevKeyVault', -- for public Azure
    -- WITH IDENTITY = 'ContosoDevKeyVault.vault.usgovcloudapi.net', -- for Azure Government
    -- WITH IDENTITY = 'ContosoDevKeyVault.vault.azure.cn', -- for Azure China
    -- WITH IDENTITY = 'ContosoDevKeyVault.vault.microsoftazure.de', -- for Azure Germany
    SECRET = 'EF5C8E094D2A4A7G9998D93440D8115DReplace-With-AAD-Client-Secret'
FOR CRYPTOGRAPHIC PROVIDER AzureKeyVault_EKM_Prov;
```

Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Paso 2.

Se crea un inicio de sesión de SQL Server para Motor de base de datos para TDE, este un inicio de sesión de SQL Server se agrega la credencial del Paso 1. De este modo es posible evidenciar para el caso del ejemplo, de “Transact-SQL” donde se usa la misma clave que se importó anteriormente.

Figura 16. Creación inicio de cesión

```sql
USE master;
-- Create a SQL Server login associated with the asymmetric key
-- for the Database engine to use when it loads a database
-- encrypted by TDE.
CREATE LOGIN TDE_Login
FROM ASYMMETRIC KEY CONTOSO_KEY;
GO

-- Alter the TDE Login to add the credential for use by the
-- Database Engine to access the key vault
ALTER LOGIN TDE_Login
ADD CREDENTIAL Azure_EKM_TDE_cred ;
GO
```

Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Paso 3.

Crear la contraseña de encriptación de la BD (DEK)

La DEK cifrará los archivos de registros y datos en la instancia de la BD y se cifrará con la clave asimétrica del Almacén de claves de Azure. La DEK tiene la posibilidad de crearse con cualquier algoritmo compatible con SQL Server y cualquier longitud de clave que sea necesaria.

Figura 17. Crear la clave de cifrado de base de datos (DEK)

```sql
USE ContosoDatabase;
GO

CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER ASYMMETRIC KEY CONTOSO_KEY;
GO
```

Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Paso 4.

Activar TDE

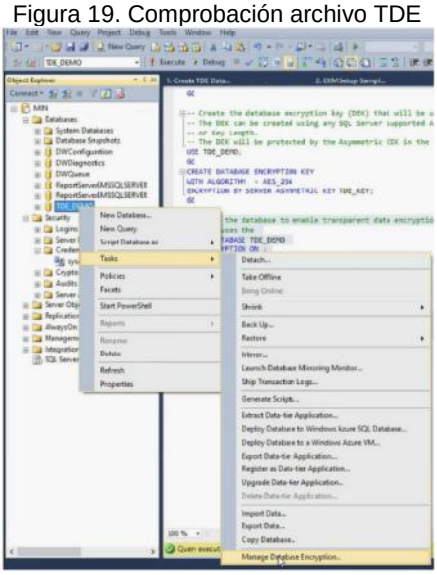
Figura 18. Activar TDE

```sql
-- Alter the database to enable transparent data encryption.
ALTER DATABASE ContosoDatabase
SET ENCRYPTION ON;
GO
```

Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Con la utilización de Management Studio, es posible comprobar que se ha activado TDE conectándose a la base de datos con el Explorador de objetos. Luego haciendo clic con el botón derecho en la base de datos, al seleccionar Tareas y dar clic en Administrar cifrado de base de datos.

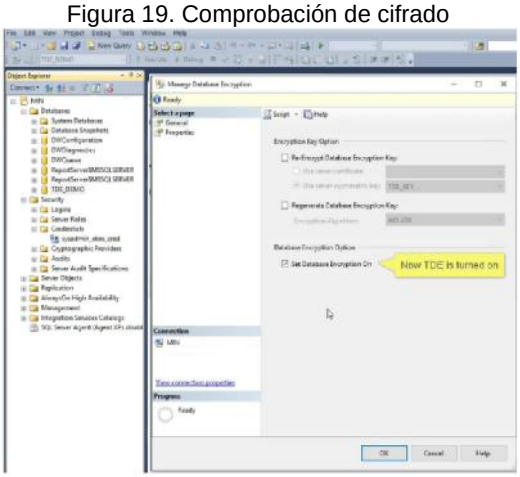
Figura 19. Comprobación archivo TDE



Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Ahora bien, en el cuadro de diálogo “Administrar cifrado de base de datos”, se confirmará que TDE está activado y qué clave asimétrica estará cifrando la DEK, esto se puede evidenciar claramente dentro de la Figura siguiente que muestra esta operación de manera gráfica:

Figura 19. Comprobación de cifrado



Fuente: Docs Microsoft. [En Línea]. Disponible en Internet: https://docs.microsoft.com/es-es/sql/relational-databases/security/encryption/use-sql-server-connector-with-sql-encryption-features?view=azuresqldb-current&viewFallbackFrom=sql-server-2017

Anexo B. Ejercicio encriptación y desencriptación MS-SQL Server

- Passphrase:

Este tipo de cifrado muestra la forma más sencilla y básica de encriptar los datos con SQL Server, a través de su mecanismo, se hace la encriptación de algún tipo de palabra o contraseña “asegurada” sin nada más, uno de los problemas es que no existe seguridad en la contraseña no exige mecanismos de contraseña segura, si la contraseña es expuesta se pierde toda la seguridad. Existe otra posibilidad de problema con esta metodología, es que puede que no todos los datos de una columna sean encriptados con la misma clave, éste es el problema que trae este mecanismo con lo cual la información quedaría irrecuperable, ejemplo:

```
-- Primero se limpia todo el ambiente
IF (DATABASEPROPERTY('DBSegura','version') > 0)
BEGIN
USE MASTER
ALTER DATABASE DBSegura SET single_user WITH ROLLBACK IMMEDIATE
DROP DATABASE DBSegura
END

— Luego se crea la base de datos de prueba con el nombre que se quiera
USE MASTER
GO
CREATE DATABASE DBSegura
GO
—  Se usa la base de datos recién creada
USE DBSegura
GO

— Se crea tabla Cliente con una columna denominada TC que sea de tipo varbinary
con el fin que contenga la información encriptada
CREATE TABLE dbo.Cliente
(CodCliene INT NOT NULL IDENTITY(1,1)
,Nombres VARCHAR(100) NOT NULL
,TC VARBINARY(150))
GO

— Ahora se hace la inclusión de un valor
INSERT INTO dbo.Cliente (Nombres, TC)
VALUES (‘WilliamTorres’, ENCRYPTBYPASSPHRASE(‘FraseSecreta’,‘4444-
4444-4444-4444’))
GO
```

```
— Procedemos a hacer un select convencional
SELECT CodCliente, Nombres, TC
FROM dbo.Cliente

/*
CodCliente Nombres       TC
———————- ————— ——————————
1          William Torres  0x01000000F2994AC0...
*/

— Se hace un select con una frase incorrecta
SELECT CodCliente, Nombres, CONVERT(VARCHAR(50),
DECRYPTBYPASSPHRASE('NoFraseSecreta',TC))
FROM dbo.Cliente

/*
CodCliente Nombres       TC
———————- ————— ——————————
1          William Torres NULL
*/

— Ahora se hace select con la frase correcta
SELECT CodCliente, Nombres, CONVERT(VARCHAR(50), DECRYPTBYPASSP
HRASE('FraseSecreta',TC))
FROM dbo.Cliente

/*
CodCliente Nombres       TC
———————- ————— ——————————
1          William Torres  4444-4444-4444-4444
*/

— Se hace un select con una frase incorrecta
SELECT CodCliente, Nombres, CONVERT(VARCHAR(50),
DECRYPTBYPASSPHRASE('NoFraseSecreta',TC))
FROM dbo.Cliente

/*
CodCliente Nombres       TC
———————- ————— ——————————
1          William Torres NULL
*/
```

```
— Ahora hacemos un select con la frase correcta
SELECT CodCliente, Nombres, CONVERT(VARCHAR(50), DECRYPTBYPASSP
HRASE('FraseSecreta',TC))
FROM dbo.Cliente

/*
CodCliente Nombres      TC
———————- ———— ———————
1          William Torres  4444-4444-4444-4444
*/

— Ahora se hace un select con una frase incorrecta
SELECT CodCliente, Nombres, CONVERT(VARCHAR(50),
DECRYPTBYPASSPHRASE('NoFraseSecreta',TC))
FROM dbo.Cliente

/*
CodCliente Nombres      TC
———————- ———— ———————
1          William Torres  NULL
*/

— Ahora se hace un select con la frase correcta
SELECT CodCliente, Nombres, CONVERT(VARCHAR(50), DECRYPTBYPASSP
HRASE('FraseSecreta',TC))
FROM dbo.Cliente

/*
CodCliente Nombres      TC
———————- ———— ———————
1          William Torres  4444-4444-4444-4444
*/
```

- Symmetric Key

Como se ha descrito, el proceso de encriptación mediante llaves simétricas tiene como principio de funcionamiento la encriptación y desencriptación de la información a través del uso de una misma llave. Es decir que, se debe proteger la llave para que no sea publicada o accesible a todos los usuarios, ya que todo el que tenga la llave podrá visualizar los datos importantes que se encuentran encriptados dentro de la BD.

Ahora, la creación de una llave simétrica, tiene que ser encriptada mediante un certificado, bien sea por medio de una llave de tipo asimétrica o a través de otra

llave simétrica, haciendo que se brinde mayor seguridad puesto que el usuario deberá intentar sobrepasar los mencionados métodos de encriptación y llegar a la llave que le dará el permiso de encriptar o desencriptar el contenido que este en la BD, así:

```
-- se hace la limpieza del ambiente
IF (DATABASEPROPERTY('DBSegura','version') > 0)
BEGIN
USE MASTER
ALTER DATABASE DBSegura SET single_user WITH ROLLBACK IMMEDIATE
DROP DATABASE DBSegura
END

— Se crea la base de datos para hacer las pruebas
USE MASTER
GO
CREATE DATABASE DBSegura
GO

—  Se usa la base de datos recién creada
USE DBSegura
GO

— Ahora se crea una tabla con una columna DocNum de tipo varbinary que
contenga la información encriptada
CREATE TABLE dbo.SymetricKeyEncription
(Nombres VARCHAR(100)
,DocNum VARBINARY(128))
GO

— Se crea una Database Master Key
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'ClaveSegura'
GO

— Se crea el certificado necesario
CREATE CERTIFICATE PrimerCertificado WITH SUBJECT='DBAMemories
Certificate',
EXPIRY_DATE = '12/31/2018'
GO

— Se hace la creación de la llave simétrica
CREATE SYMMETRIC KEY LlaveSimetrica
WITH
KEY_SOURCE = 'MyKeySource',
IDENTITY_VALUE = 'MyIdentityValue',
ALGORITHM = AES_256
```

```
ENCRYPTION BY CERTIFICATE PrimerCertificado;
GO

— Se hace una consulta y se visualiza las llaves simétricas de la base de datos, para este ejercicio tenemos dos la DMK y la llave simétrica creada a partir del certificado.
SELECT name, algorithm_desc, create_date
FROM sys.symmetric_keys

/*
name                 algorithm_desc create_date
____________________ ______________ ____________________
##MS_DatabaseMasterKey## TRIPLE_DES     2018-05-12 11:34:10.121
LlaveSimetrica       AES_256        2018-05-12 11:34:17.600
*/
```

Anexo C. Encriptación Asimétrica MS-SQL Server

Sintaxis[45]

```
CREATE ASYMMETRIC KEY Asym_Key_Name
  [ AUTHORIZATION database_principal_name ]
  [ FROM <Asym_Key_Source> ]
  [ WITH <key_option> ]
  [ ENCRYPTION BY <encrypting_mechanism> ]
  [ ; ]

<Asym_Key_Source>::=
    FILE = 'path_to_strong-name_file'
  | EXECUTABLE FILE = 'path_to_executable_file'
  | ASSEMBLY Assembly_Name
  | PROVIDER Provider_Name

<key_option> ::=
  ALGORITHM = <algorithm>
    |
  PROVIDER_KEY_NAME = 'key_name_in_provider'
    |
    CREATION_DISPOSITION = { CREATE_NEW | OPEN_EXISTING }

<algorithm> ::=
    { RSA_4096 | RSA_3072 | RSA_2048 | RSA_1024 | RSA_512 }

<encrypting_mechanism> ::=
   PASSWORD = 'password'
```

Argumentos

FROM Asym_Key_Source
Especifica el origen desde el que se carga el par de claves asimétricas.

AUTHORIZATION database_principal_name
Especifica el propietario de la clave asimétrica. El propietario no puede ser un rol ni un grupo. Si se omite esta opción, el propietario será el usuario actual.

FILE =’path_to_strong-name_file’

[45] Creación de Clave Asimétrica (Transact-SQL). {En Línea}. {05 de junio de 2018}. disponible en: https://docs.microsoft.com/es-es/sql/t-sql/statements/create-asymmetric-key-transact-sql?view=sql-server-2017

Especifica la ruta de acceso a un archivo de nombre seguro desde el que se carga el par de claves.

Esta opción no está disponible en las bases de datos independientes.

EXECUTABLE FILE =’path_to_executable_file’
Especifica un archivo de ensamblado desde el que se carga la clave pública. Limitado a 260 caracteres por MAX_PATH de la API de Windows.

Esta opción no está disponible en las bases de datos independientes.

ASSEMBLY Assembly_Name
Especifica el nombre de un ensamblado desde el que se carga la clave pública.

ENCRYPTION BY <key_name_in_provider> Especifica cómo se cifra la clave. Puede ser un certificado, una contraseña o una clave asimétrica.

KEY_NAME =’key_name_in_provider’
Especifica el nombre de la clave del proveedor externo. Para obtener más información sobre la Administración extensible de claves, vea Administración extensible de claves (EKM).

CREATION_DISPOSITION = CREATE_NEW
Crea una nueva clave en el dispositivo de Administración extensible de claves. Debe utilizarse PROV_KEY_NAME para especificar el nombre de clave en el dispositivo. Si ya existe una clave en el dispositivo, se producirá un error en la instrucción.

CREATION_DISPOSITION = OPEN_EXISTING
Asigna una clave asimétrica de SQL Server a una clave de Administración extensible de claves. Debe utilizarse PROV_KEY_NAME para especificar el nombre de clave en el dispositivo. Si no se proporciona CREATION_DISPOSITION = OPEN_EXISTING, el valor predeterminado es CREATE_NEW.

ALGORITHM = <algorithm>
Se pueden proporcionar cinco algoritmos: RSA_4096, RSA_3072, RSA_2048, RSA_1024 y RSA_512.

RSA_1024 y RSA_512 están en desuso. Para usar los algoritmos RSA_1024 o RSA_512 (no se recomienda), debe establecer la base de datos en el nivel de compatibilidad de base de datos 120 o inferior.

PASSWORD = ’password’
Especifica la contraseña con la que se cifra la clave privada. Si no está presente esta cláusula, la clave privada se cifrará con la clave maestra de la base de datos. password tiene un máximo de 128 caracteres. password debe cumplir los requisitos

de la directiva de contraseñas de Windows del equipo que ejecuta la instancia de SQL Server.

Permisos

Se hace necesario el acceso CREATE ASYMMETRIC KEY dentro de la BD. Solo si se usa la declaración AUTHORIZATION, es necesario el acceso IMPERSONATE en la entidad de seguridad de la BD o el permiso ALTER en el rol de aplicación. Solo los inicios de sesión de Windows, únicamente iniciar la sesión de MS SQL Server y las relaciones sobre la aplicación contienen contraseñas asimétricas. En cambio, grupos y roles son incapaces de contar con contraseñas asimétricas.

Ejemplos

A. Crear una clave asimétrica

En el siguiente ejemplo se crea una clave asimétrica con el nombre PacificSales09 mediante el algoritmo RSA_2048 y se protege la clave privada con una contraseña.

```
CREATE ASYMMETRIC KEY PacificSales09
   WITH ALGORITHM = RSA_2048
   ENCRYPTION BY PASSWORD = '<enterStrongPasswordHere>';
GO
```

B. Crear una clave asimétrica desde un archivo, concediendo autorización a un usuario

En el siguiente ejemplo se crea la clave asimétrica PacificSales19 a partir de un par de claves almacenadas en un archivo y, a continuación, se autoriza al usuario Christina a utilizar la clave asimétrica.

```
CREATE ASYMMETRIC KEY PacificSales19 AUTHORIZATION Christina
   FROM FILE = 'c:\PacSales\Managers\ChristinaCerts.tmp'
   ENCRYPTION BY PASSWORD = '<enterStrongPasswordHere>';
GO
```

C. Crear una clave asimétrica de un proveedor de EKM

En el ejemplo siguiente se crea la clave asimétrica EKM_askey1 a partir de un par de claves almacenadas en un archivo. A continuación, lo cifra mediante un proveedor de Administración extensible de claves llamado EKMProvider1 y una clave en dicho proveedor llamada key10_user1.

```
CREATE ASYMMETRIC KEY EKM_askey1
   FROM PROVIDER EKM_Provider1
   WITH
      ALGORITHM = RSA_2048,
      CREATION_DISPOSITION = CREATE_NEW
      , PROVIDER_KEY_NAME  = 'key10_user1' ;
GO
```

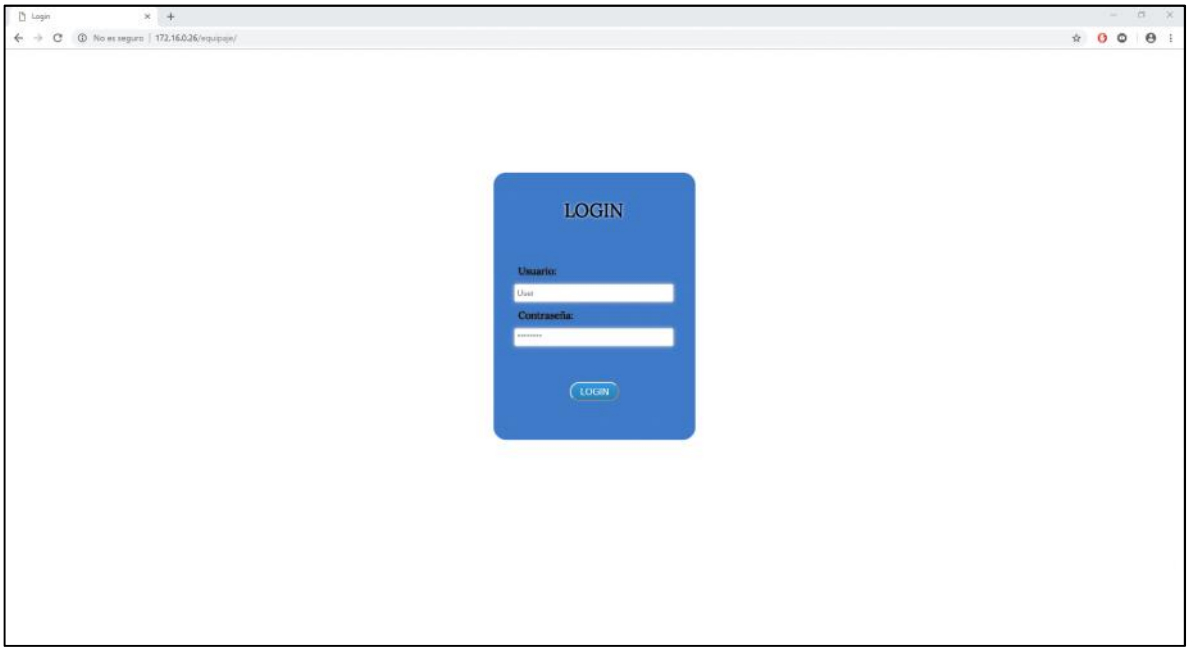
Anexo D. Pruebas de Penetración Kali Linux

Ataque a través de inyección de código por SQLMAP

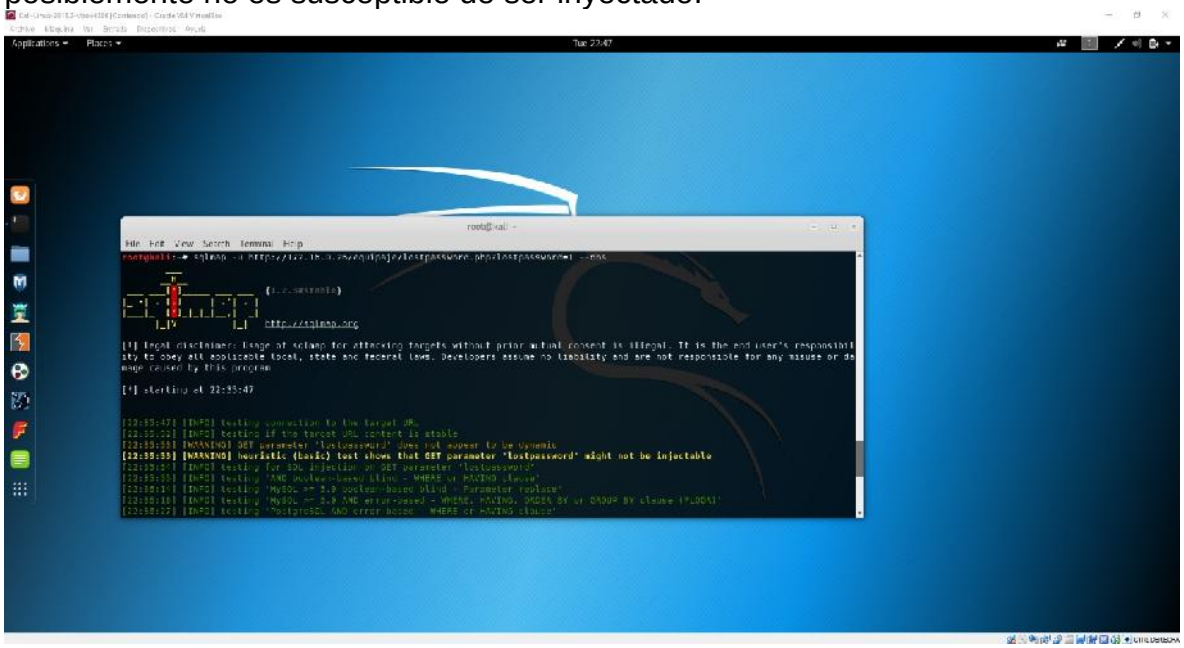
Una vez se tiene el sitio WEB publicado y funcionando, se procede a verificar la seguridad criptográfica, efectuando un intento de penetración por inyección de código, a través de la herramienta **SQLMAP de Kali Linux**, para lo cual se ingresa el comando:

"sqlmap -u http://172.16.0.26/woperweb/front/lostpassword.php?lostpassword=1 --dbs",

allí se pueden evidenciar los resultados de aplicar la seguridad criptográfica e identificar las vulnerabilidades que puede tener.



Al momento de hacer en intento de inyección de código nos advierte que posiblemente no es susceptible de ser inyectado.



Luego de hacer el proceso de inyección al sitio, nos muestra que la base de datos que queremos atacar no puede ser inyectada, lo cual nos muestra que la criptografía utilizada ha sido efectiva.