Universidad CENFOTEC

Maestría en Tecnologías Bases de Datos

Documento final de Proyecto de Investigación Aplicada 2

Diseño de una metodología de control de accesos en bases de datos relacionales para estandarizar la correcta administración del manejo de identidades.

Antony Calderón Vega

Mayo, 2022

Universidad Cenfotec
Carrera de Postgrado
Maestría en Tecnología de Bases de Datos

DECLARACIÓN JURADA

Yo, **Calderón Vega Antony,** número de identificación: **304700140**, estudiante de la Universidad Cenfotec, de la carrera Maestría en Tecnología de Bases de Datos, declaro bajo fe de juramento y consciente de las responsabilidades penales de este acto, que soy el autor intelectual del Proyecto de Investigación Aplicada 2 titulado: **"Diseño de una metodología de control de accesos en bases de datos relacionales para estandarizar la correcta administración del manejo de identidades",** por lo que libero a la Universidad Cenfotec, de cualquier responsabilidad en caso de que mi declaración sea falsa.

Firmado en San Pedro, Montes de Oca, San José-Costa Rica, el día 3 de junio de 2022.

Firma estudiante

Agradecimientos

Primeramente, deseo brindar agradecimiento a mi persona, pues ante toda la espera, ante todas las barreras que se me han interpuesto, la disciplina y perseverancia siempre han estado de mi lado; todas esas horas de desvelo, todas esos días, semanas y años de constancia han dado fruto y finalmente pude concluir el proyecto final de graduación para obtener el título de Maestría en Bases de Datos, estoy sumamente orgulloso de todo el sacrificio realizado para lograrlo.

Por otro lado, quiero dar las gracias a todas esas personas que estuvieron de mi lado académico, tanto compañeros, profesores, directores académicos y, por supuesto, todas aquellas personas que están detrás de ellos, sin ellos nunca hubiese podido terminar este trabajo de investigación. Además, quiero darle las gracias rotundas a Western Union por apoyarme desde el inicio y siempre darme la oportunidad de continuar en el desarrollo académico.

Finalmente, quiero darle las gracias a mi esposa Ariel por estar siempre a mi lado en todos estos años de conclusión de posgrado. También a mi padre Leonel por todo el esfuerzo realizado laboralmente para apoyarme en mis proyectos de estudio, a mi madre Lorena por siempre estar ahí inspirándome en estudiar y lograr mis sueños y metas académicas, también a mis amigos, y todos aquellos que hayan colaborado y fueron parte fundamental del desarrollo de esta investigación, gracias a todos.

Dedicatoria

Este trabajo de investigación está dedicado a Federico del Valle Monge (q. e. p. d.), pues fue de las primeras personas que influyó positivamente en mí en el ambiente profesional y me brindó las guías necesarias para continuar mi carrera universitaria. Lastimosamente nunca pude demostrarle mi afecto y de esta forma intento demostrar mi aprecio hacia lo buen amigo y compañero que fue mientras compartimos el mismo espacio de trabajo.

Universidad Cenfotec
Carrera de Postgrado
Maestría en Tecnología de Bases de Datos

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría en Tecnología de Bases de Datos,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Calderón Vega Antony.**

JOSE ALBERTO CABEZAS JAIKEL (FIRMA) Digitally signed by JOSE ALBERTO CABEZAS JAIKEL (FIRMA) Date: 2022.06.08 14:01:00 -06'00'

MBD. José Cabezas Jaikel
Tutor

MIS. Luis Sanabria Rodríguez
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA) Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA) Fecha: 2022.06.08 15:38:39 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 3 de junio de 2022

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Tabla de Contenido

Tabla de Figuras

Abstract

Las bases de datos son el activo empresarial más importante, ya que en ella se almacenan, estratégicamente, los elementos que dan vida a las compañías. De ahí, se origina la necesidad de fortalecer los procedimientos de seguridad de control de accesos en las bases de datos. Al no haber una documentación formal sobre los correctos procedimientos que se siguen, hay diferentes maneras de manejar los accesos de usuarios dentro de los motores. Por lo tanto, en este trabajo de investigación se plantea una propuesta para controlar las acciones que brinden, remuevan, modifiquen o certifiquen usuarios en las bases de datos relacionales.

Para este fin, se aplicaron diferentes funcionalidades adaptadas a los motores de bases de datos seleccionados para seguir una sola estrategia, la cual consiste en seguir los estándares de reconciliación, aprovisionamiento y deprovisionamiento de cuentas en estas bases de datos. Por consiguiente, se seleccionaron los productos de MySQL, Oracle y SQL Server; en los cuales se brindan casos de uso donde se puede comprender cómo debería ser implementado y los filtros necesarios.

Palabras Clave: bases de datos relacionales, control de accesos, Oracle, MySQL, Microsoft SQL Server, estándar, reconciliación, aprovisionamiento, deprovisionamiento.

Capítulo 1. Introducción

1.1 Generalidades

Actualmente, la complejidad de los sistemas y la diversidad de productos, así como las modalidades y estrategias que se utilizan en la selección de versiones para los diseños en las infraestructuras utilizadas, han colocado el control de accesos a los diversos sistemas o recursos de las organizaciones como un tema de interés, ya que es indispensable conocer quiénes tienen acceso a la información y qué tipo de datos son los que se utilizan en cada uno de los sistemas.

Ahora bien, dentro de estos sistemas y aplicaciones requieren la utilizar un dominio de los accesos, los cuales también incluyen las bases de datos, que se constituyen como sistemas de gobernanza que controlan y almacenan el flujo de información. Por lo tanto, se le debe prestar atención especial a la forma en que se está auditando la información dentro de estas, para evitar a toda costa riesgos ligados al mal uso de los datos y filtraciones que pueden provocar desastres empresariales si no se maneja de la manera correcta.

1.2 Antecedentes del problema

El problema que se expone en esta investigación es la ausencia de un proceso estandarizado y documentado, que brinde información sobre el manejo del control de accesos en las bases de datos relaciones. Por su naturaleza, las bases de datos están constituidas por muchos elementos documentados debido a la complejidad que existe alrededor de los diferentes diseños, desarrollos e infraestructuras. Son estos elementos previamente mencionados los cuales se pretenden recopilar en esta investigación. Es importante señalar que el control de accesos no cuenta con una documentación basta que defina los procesos de manejo de identidades.

La información disponible no es suficiente para solucionar el problema propuesto, ya que es necesario buscar fuentes de información específicas que procuren resolver el dilema del control estandarizado de accesos en bases de datos. Hay diversas soluciones que se pueden extrapolar, ya que los detalles concuerdan en cuanto a la estandarización que se debe seguir en las certificaciones que se encuentran en el mercado.

Ahora bien, estos problemas han sido resueltos de diversas formas en las compañías que utilizan bases de datos relacionales, debido a que estas deben seguir leyes de protección de datos y son auditadas regularmente por entes especializados en el control de accesos. Sin embargo, la mayoría de estas compañías no proveen la información a la comunidad interesada de cómo el problema fue resuelto, debido a la información que integra las bases de datos.

Es por esto que, después de buscar información de cómo se ha tratado el control de accesos específicamente en las bases de datos, no se obtuvieron resultados significativos que puedan corroborar la existencia de una forma estandarizada de auditoría en las bases de datos relacionales. Por lo tanto, es necesario iniciar el proceso de documentación, para construir un registro de los detalles que rodean este proceso, de esta forma, propiciar más investigaciones que puedan fortalecer la seguridad informática dentro de las compañías.

1.3 Definición y descripción del problema

En la actualidad existen muchos tipos de software para el manejo de sistemas de bases de datos, que van desde tipo relacionales hasta NoSQL. Entre los tipos relaciones cabe destacar que la forma en que se maneja la información de accesos está definida adecuadamente, esto se debe a sus principios estructurales, los cuales promueven el manejo de datos de forma específica. Para tener una visión más clara

de los principios que se persiguen en esta investigación se utilizará el ranking generado por DB-Engines (2021)[1], el cual es potenciado por la empresa SOLIT IT. Este ranking emplea diversos métodos para otorgar puntajes a cada una de las bases de datos relaciones que se encuentran en el mercado. A continuación, se exponen los criterios utilizados:

- Número de menciones del sistema en sitios web, medido como número de resultados en las consultas de los motores de búsqueda. Los buscadores utilizados fueron Google y Bing para esta medición. Para contar solo los resultados relevantes, se buscó “nombre del sistema” junto con el término “base de datos”, por ejemplo: "Oracle" y "base de datos".
- Interés general en el sistema. Para esta medición, se utilizó la frecuencia de las búsquedas en Google Trends.
- Frecuencia de los debates técnicos sobre el sistema. En este caso, se utilizó el número de preguntas relacionadas y el número de usuarios interesados en los sitios de preguntas y respuestas más populares relacionados con informática Stack Overflow y DBA Stack Exchange.
- Número de ofertas de empleo en las que se menciona el sistema. Se utilizó el número de ofertas en los principales buscadores de empleo Indeed y Simply Hired.z
- Número de perfiles en redes profesionales en los que se menciona el sistema. Para lo cual, se utilizó la red profesional más popular a nivel internacional, LinkedIn.
- Relevancia en las redes sociales. Se contabilizaron el número de publicaciones en Twitter en los cuales se menciona el sistema.

[1] Contenido original de los puntos definidos a continuación disponible en el enlace correspondiente de la sección de Referencias.

El resultado final al realizar el estudio a partir de los factores mencionados anteriormente, y dando a conocer únicamente los 10 productos relacionales con más puntajes según los cálculos realizados al mes de setiembre de 2021 queda de la siguiente manera:

Tabla 1

Motores de bases de datos y sus puntajes respectivos

Nombre del producto	Puntaje calculado	Tipo del producto
Oracle	1271.55	Relational, Document store, Graph, RDF store, Spatial
MySQL	1212.52	Relational, Document store, Spatial
Microsoft SQL Server	970.85	Relational, Document store, Graph, Spatial
PostgreSQL	577.5	Relational, Document store, Spatial
IBM Db2	166.56	Relational, Document store, RDF store, Spatial
SQLite	128.65	Relational
Microsoft Access	116.94	Relational
MariaDB	100.7	Relational, Document store, Graph, Spatial
Hive	85.58	Relational

Fuente: elaboración propia a partir de solit IT (2021)

A partir de la información presentada en la tabla 1, el puntaje sumado de los motores más relevantes da como resultado 4630.85**,** por lo tanto, si se toma como referencia la suma de los primeros 3 productos con la puntuación más alta, en el cual el resultado de ellos es de 3454.92, se podría concluir que, invirtiendo tiempo de investigación en ellos se podría abarcar al menos un 74.60% de las herramientas que se están utilizando en el mercado actual.

1.4 Justificación

Ante los elementos estadísticos brindados anteriormente, se puede observar que hay una gran variedad de productos para el manejo de bases de datos. Naturalmente, no todos tienen el mismo público meta, unos cuentan con más popularidad y recursos para robustecerse, sin embargo, tienen un mismo objetivo: brindar un sistema que se adapte a las necesidades de resguardo de la información de una forma ordenada y concisa. Empero, no se tiene un sistema estandarizado el cual garantice que los usuarios que tienen acceso a ellas están siendo correctamente monitoreados y se asegure que estos cuenten con el permiso exclusivo para cumplir con las responsabilidades laborales por las que fue contratado por la empresa.

Debido a las particularidades encontradas en las soluciones formuladas se puede afirmar que se ha realizado en diferentes escenarios. Por una parte, los productos cuentan con elementos que los desarrolladores crearon con este objetivo. Por otra parte, las bases de datos son los activos empresariales más importantes ya que contienen la información que mantiene viva a las compañías.

Por lo tanto, cada compañía debe de construir su propio sistema para que responda a la situación concreta en la que se encuentren, la cual varía según sus necesidades, la información que manejan y los objetivos planteados para la herramienta. Debido a las dificultades en la forma en la cual se ha venido subsanando las necesidades de las compañías, en cuanto al sistema de control de acceso, esta investigación realizará una documentación formal sobre el proceso correcto que debería llevarse a cabo en cuanto al control de accesos en las bases de datos y, además, determinar cuáles estrategias deberían utilizarse para poder tener un sistema limpio de intrusos y con la mínima cantidad de actividades que puedan generar corrupción en los datos, así como tener un control que permita asegurar que

la información dentro de las bases de datos no vaya a tener un uso indebido y la interacción de los usuarios con estas bien vigilada.

1.5 Viabilidad

Sobre el control de accesos en las bases de datos relacionales hay escasas referencias documentales, las cuales demuestran los sistemas que se están implementando en las empresas que requieren constantemente auditar las identidades. Estas soluciones o estrategias probablemente fueron elaboradas de forma empírica para satisfacer requerimientos de cumplimiento.

Debido a esta situación se crea la necesidad de contar con una metodología estructurada y siguiendo una línea estandarizada. Es precisamente este el objetivo del presente trabajo. Para poder realizar dicha consigna será necesario recopilar toda la información.

Es posible que el escenario que se pueda encontrar vaya a ser complicado e incluya muchas aristas que, al avanzar en la investigación, tengan que tomarse en cuenta para que el diseño pueda ser polarizado a muchos ambientes empresariales. Existe suficiente documentación la cual puede ser de ayuda para poder guiar la investigación hacia un diseño que sea viable para su correcta implementación y que también pueda considerar todas las variables que se encontrarán.

1.5.1 Punto de vista técnico.

Para realizar esta investigación se requieren ciertas características específicas las cuales son elementales para llevar a cabo la investigación y la construcción de la herramienta metodológica. Además, es menester mencionar que se requieren tanto habilidades blandas como técnicas, ya que, de esta forma será más fácil la labor de diseño del trabajo propuesto. Los elementos necesarios son los siguientes:

Tabla 2

Habilidades requeridas

Habilidad	Tipo	Descripción
Investigador	Blanda	Esta es la habilidad más importante, ya que constantemente se necesitará buscar referencias sobre diversos temas. Esta exploración requiere que se busquen fuentes confiables y que se adapten a los escenarios que se presentarán.
Bases de datos	Técnica	La elección del motor, estudio de los requisitos y el diseño son características requeridas para poder evaluar el escenario al que se expondrá este proyecto.
Infraestructura	Técnica	Parte de la investigación requerirá esfuerzos por establecer reglas de qué tipo de infraestructura debe implementarse, cuáles son las características del servidor o el recurso que se vaya a utilizar para instalar la base de datos, cuáles puertos deben estar habilitados para realizar la conexión y otros requisitos fundamentales para una implementación exitosa.
Comunicación efectiva	Blanda	Una adecuada comunicación es indispensable, ya que se estará en constante comunicación con usuarios técnicos y no técnicos, por lo tanto, se debe adecuar el mensaje, según el destinatario.

Fuente**:** Elaboración propia (2021)

A partir de los elementos compartidos en la tabla anterior se puede hacer una descripción del investigador para conocer si tiene las habilidades necesarias para implementar este proyecto:

Tabla 3

Habilidades del investigador

Habilidad	Nivel de conocimiento	Tipo de experiencia	Años de experiencia
Investigación	Intermedio-Avanzado	Académica-Profesional	7
Base de datos	Avanzado	Profesional	2
Infraestructura	Intermedio	Profesional	2
Comunicación	Intermedio	Académica-Profesional	2

Fuente: Elaboración propia (2021)

Como se puede observar, el investigador cuenta con las habilidades requeridas para realizar este proyecto. Es preciso señalar que, para esta clase de investigaciones no es requerido que el perfil sea experto, sino que cuente con ciertas habilidades que puedan probar que el trabajo se podrá llevar a cabo exitosamente. Por lo tanto, se puede afirmar que técnicamente es viable continuar con la investigación.

1.5.2 Punto de vista operativo.

El propósito de este trabajo se ha señalado anteriormente es diseñar una metodología de control de accesos en bases de datos relacionales. Para llevar a cabo esta consigna, no se requiere un patrocinador para realizar pruebas en sus sistemas de producción, ya que se generarán diversas herramientas las cuales se desarrollarán en sistemas aislados y validados de forma independiente.

Además, si alguna empresa desea utilizar las metodologías que se dictan en esta investigación, se recomienda aplicar las estrategias de ciclo de vida del software donde, previamente, se hagan las pruebas respectivas en los sistemas de desarrollo y también se validen en sistemas de calidad antes de proceder con los sistemas de producción.

1.5.3 Punto de vista económico.

Luego de haber analizado las habilidades que se requieren para el desarrollo de esta investigación en los puntos previos se utiliza como referencia la descripción del puesto de Ingeniero en Seguridad de la Información según el sitio desarrollado por Sokanu, (s.f) en donde menciona que “son responsables de la aplicación y administración del hardware y el software de seguridad de la red, de la aplicación de la política de seguridad y del cumplimiento de los requisitos de las auditorías y

recomendaciones de seguridad”[2]. Debido a que el perfil profesional cumple con los requisitos de esta investigación, se calculará el salario equivalente al puesto de Ingeniero en Seguridad de la Información.

Para realizar la proyección salarial se utilizará como referencia el salario promedio de los Ingenieros en Seguridad de la Información según el sitio especializado SalaryExpert del ERI Economic Research Institute (2020) y actualizado el 25 de octubre de 2020:

Tabla 4

Información salarial promedio del Ingeniero en Seguridad de la Información en Costa Rica

Posición	Salario anual	Salario mensual	Tarifa por hora
Ingeniero en Seguridad de la Información	₡ 18 269 197	₡ 1 522 433	₡ 8 783,27

Fuente: Elaboración propia (2021)

Por lo tanto, para el desarrollo de este proyecto se puede concluir que la inversión económica sería de:

Tabla 5

Costo total de la investigación

Investigador	Horas semanales de ingeniería	Meses de investigación	Costo total
Antony Calderón	35	8	₡11,066,920.2

Fuente: Elaboración propia (2021)

Al tipo de cambio actual utilizando al Banco Central de Costa Rica (2021) como punto de referencia, para el día 11 de octubre del 2021 la investigación tendría un costo de **$**17,521.48.

[2] They are responsible for the implementation and administration of network security hardware and software, enforcing the security policy and complying with requirements of security audits and recommendations

Por otro lado, las compañías desarrolladoras de motores de bases de datos comparten licencias exclusivas para desarrolladores las cuales no tienen ningún costo, por lo que no habrá una inversión en este rubro. También, se utilizarán ambientes virtuales que requieren sistemas operativos, sin embargo, la universidad provee el licenciamiento correspondiente lo cual favorece que no se deba hacer una inversión extra por este requerimiento en específico.

1.6 Objetivos

Para establecer los objetivos de este estudio se utiliza como base la taxonomía Bloom de 1956. Se utilizará esta taxonomía debido a su estructura y versatilidad para emplearse en cualquier área de investigación.

1.6.1 Objetivo general

Diseñar una metodología de control de accesos en bases de datos relacionales para estandarizar la correcta administración del manejo de identidades.

1.6.2 Objetivos específicos

1. Definir las buenas prácticas utilizadas en el mercado en cuanto al manejo correcto de identidades para comprender los requisitos que se deben cumplir en la metodología.
2. Diferenciar los elementos de manejo de identidades que afectarán el control de accesos en las bases de datos relacionales para documentarlos y tomarlos en cuenta en el desarrollo de esta investigación.
3. Desarrollar una estrategia que satisfaga el modelo de manejo de identidades en bases de datos relacionales para utilizarlo como base en la estandarización de la metodología.

4. Analizar los resultados obtenidos en la comparación del estándar creado y los elementos que componen a las diferentes estrategias de manejo de identidades para comprobar su efectividad en el control de accesos en bases de datos.

1.7 Alcances y limitaciones

1.7.1 Alcances

- Se entregará una documentación del proceso que debe llevarse a cabo para el correcto manejo o aplicación de la metodología de control de accesos en bases de datos relacionales.
- Desarrollo de herramientas para motores de bases de datos Oracle, SQL Server y MySQL con la correspondiente documentación de uso.
- Análisis de casos en los cuales se pueda comprobar el resultado final y en el cual se puedan brindar recomendaciones en cómo se le puede sacar provecho a los elementos que ofrecen las herramientas.
- Se realizarán pruebas de funcionamiento en ambientes virtualizados y controlados por el investigador.
- Uso de la herramienta PowerShell para emular el comportamiento de un sistema gestor de gobernanza de control de accesos.

1.7.2 Limitaciones

- No se incluirán bases de datos fuera del ambiente relacional.
- No se aplicarán estas herramientas en ambientes de producción de ninguna empresa.
- No se contará con ningún patrocinador en esta investigación.

1.8 Estado de la cuestión

El control de accesos es un tema de investigación que ha tomado mayor relevancia desde que las leyes globales de protección de datos adquirieron mayor relevancia a razón de mejorar los procesos de seguridad en la información. Por esto, se hace necesario recolectar referencias bibliográficas sobre el tipo de investigaciones.

1.8.1 Planificación de la revisión

Para encontrar fuentes confiables que brinden una perspectiva similar a la que se plantea en este trabajo de investigación se utilizaron varias palabras claves para delimitar la búsqueda. Cabe mencionar que, para este apartado se utiliza como fuente de información Scholar Google como buscador primario, sin embargo, no se descarta utilizar más recursos en las futuras etapas de investigación.

Se realizaron diversas búsquedas para poder obtener artículos o trabajos de investigación pertinentes para la elaboración del estado de la cuestión del presente trabajo. Entre los resultados que se encuentran en el buscador de Google Scholar se puede apreciar que, a la hora de hacer una búsqueda con palabras determinantes para esta investigación como “Identity and Access management”, “access control”, se obtienen cientos de artículos relacionados con blockchain, IoT, Cloud, y otros temas no relevantes para los fines de este estudio. Por lo tanto, se tuvo que indagar en diversos enlaces dentro de los resultados para encontrar investigaciones que puedan ofrecer información complementaria para este proyecto.

Tabla 5

Palabras claves utilizadas en las cadenas de búsqueda

Palabra clave	**Palabra clave (español)**	**Descripción**
Access control	Control de accesos	Se refiere a la acción de controlar las identidades y sus accesos a los diferentes recursos.
Standard	Estándar	Se busca que haya alguna propuesta o seguimiento de algún estándar en la implementación.
Database	Base de datos	Se requiere que se incluyan o mencionan elementos relacionados a las bases de datos en la investigación.
Policy	Política	Complementando a la palabra “estándar” es necesaria para conocer si la investigación se basa en alguna política de control de accesos.
Identity Management/ access management	Manejo de identidad/manejo de accesos	Se refiere a la acción de administrar y controlar accesos con sus respectivas identidades correspondientes.

Fuente: Elaboración propia (2021)

Adicionalmente, en la siguiente tabla se muestran las palabras recurrentes en los resultados dentro de las cadenas de Google Scholar. Sin embargo, fueron filtradas para poder obtener investigaciones favorables para los objetivos que se persiguen en este trabajo:

Tabla 6

Palabras claves filtradas en las cadenas de búsqueda

Palabra clave	Palabra clave (español)	Razón por la que se filtra
Blockchain	Cadenas de bloques	Este término generaba fue recurrente en la búsqueda refiriéndose a elementos de Bitcoins
Health	Salud	Muchas investigaciones estaban dirigidas a elementos de salud; área que, para efectos de esta investigación no será tomada en cuenta.
Cloud	Nube	Hay gran cantidad de investigaciones enfocadas en ambientes de la nube.
IOT/Internet of Things	Internet de las cosas	Se encuentran investigaciones que se refieren a elementos físicos que se conectan a la red, los cuales no son parte de esta investigación.
Network	Red	Este término se enlaza a elementos como enrutadores, switches, VLAN, entre otros y no concuerdan con los propósitos de la investigación.

Fuente: Elaboración propia (2021)

1.8.2 Ejecución de la revisión

1.8.2.1 Criterios de inclusión

- Aquellos trabajos que contengan elementos teóricos sobre cómo implementar las características que se están proponiendo en este trabajo de investigación.

- Investigaciones relacionadas directamente con control de accesos en los cuales se haya implementado al menos un elemento de estudio (aplicación, base de datos, servidor).
- Las instituciones o universidades que hayan desarrollado el estudio y cumplan con una serie de requisitos a partir de los análisis planteados en las plataformas de scimagoir.com o topuniversities.com las cuales se explicarán más adelante.
- Fuentes tecnológicas confiables que desarrollen investigación con información relevante para el campo de estudio.
- Cualquier elemento visual que llame la atención del lector en los títulos de los resultados de las búsquedas.

1.8.2.2 Criterios de exclusión

- Aquellos trabajos en los cuales el título no incluya específicamente el tema relacionado al control de accesos.
- El trabajo contiene palabras que son atractivas para la investigación, pero que no se desea utilizar para no alargar los filtros y afectar directamente los resultados ya obtenidos.
- Soluciones enfocadas en bases de datos no relacionales (NoSQL), ya que no son de interés para este trabajo de investigación.

1.8.2.3 Instituciones de fuentes a utilizar

En este apartado se dará una breve descripción de las instituciones que se encontraron para poder desarrollar el Estado de la Cuestión de esta investigación.

Tabla 7

Instituciones y sus respectivas descripciones

Nombre de institución	**Descripción**
International Journal of Engineering and Technology (IJIERT)	Esta revista internacional está diseñada especialmente para la publicación de artículos en ingeniería, investigación y avances tecnológicos.[3]
University of Turku	Según resultados brindados por topuniversities.com esta universidad tiene altos resultados en generación de investigación, además, se encuentra entre las 300 mejores universidades del mundo.
International Journal of Engineering Research and Applications (IJERA)	Es una revista internacional de acceso abierto revisada por pares que publica artículos de investigación o revisión que aportan información novedosa en todas las áreas de la Ingeniería y la Tecnología. Además, es aprobada por la UGC.[4]

[3] The international journal provides the prospect to publish the original research papers with the author-friendly environment through its processes. This international journal is specially designed for paper publication in engineering, research, and technological advances.

[4] International Journal of Engineering Research and Applications (IJERA) is an open access online peer reviewed international journal that publishes research/review articles which contribute new theoretical results in all areas of Engineering & Technology. IJERA is UGC approved Journal.

GEINTEC Magazine	Esta revista tiene como objetivo difundir la producción científica nacional e internacional en las áreas de gestión, innovación y tecnologías. Además, funciona como un entorno que permite y promueve el intercambio de experiencias e ideas entre los investigadores nacionales y extranjeros que trabajan en estas áreas[5]

Fuente*:* Elaboración propia (2021)

1.8.2.4 Trabajos de investigación a utilizar

Basado en los criterios de inclusión y exclusión mencionados anteriormente, así como las tablas de resultados, se determinó que los trabajos utilizados para la evaluación del estado de la cuestión serán:

- El primero fue desarrollado por Mohammed, I. A. (2017) y se titula "SYSTEMATIC REVIEW OF IDENTITY ACCESS MANAGEMENT IN INFORMATION SECURITY" que se traduce al español como "REVISIÓN SISTEMÁTICA DE LA GESTIÓN DEL ACCESO A LA IDENTIDAD EN LA SEGURIDAD DE LA INFORMACIÓN". A continuación, se presente el propósito de la investigación:

  > El principal problema que este documento tratará de resolver es revisar cómo la gestión de la identidad y el acceso es importante en la

[5] The GEINTEC Magazine aims to disseminate national and international scientific production in the areas of management, innovation and technologies, also serving as an environment that allows the exchange of experiences and ideas between national and foreign researchers working in these areas

seguridad de la información. En la actualidad, la ciberdelincuencia va en aumento, y las violaciones de datos pueden ser muy costosas, así como dañar la imagen de su organización[6] (Mohammed, 2017).

- El segundo fue desarrollado por Toelen, O. (2008) y lleva como título “Identity and access management” que se traduce al español como “Gestión de identidades y accesos”. Seguidamente, se muestra un fragmento del resumen de la investigación:

  Esta tesis consiste principalmente en una investigación sobre la Gestión de Identidades y Accesos. Se discute la terminología relacionada con este tema y se sugiere una definición funcional formal. Se exploran los retos empresariales a los que se enfrenta la Gestión de Identidades y Accesos, las tecnologías que la componen y las soluciones que puede ofrecer[7] (Toelen, 2008).

- El tercero fue desarrollado por Al-Khouri, A. M. (2011) y lleva como título “Optimizing Identity and Access Management (IAM) Frameworks” que se traduce al español como “Optimización de los marcos de gestión de identidades y accesos (IAM)”. A continuación, se muestra un fragmento del resumen de la investigación:

  Este artículo ofrece una visión general de la literatura sobre gestión de identidades y accesos. En él se intenta analizar los impulsores del

[6] The main problem that this paper will try to solve is to review how identity and access management is important in information security. In this day and age, cybercrime is on the increase, and data breaches can be very costly as well as damaging to your organization's image

[7] This thesis majorly consists of a research on Identity and Access Management. Terminology related to this topic is discussed and a formal functional definition is suggested. It explores the business challenges Identity and Access Management addresses, the technologies it consists of and the solutions it can and may offer

> negocio, las tendencias, los problemas y los desafíos asociados a la implantación de dichos sistemas. Posteriormente, presenta un marco estratégico y un ecosistema global para la implantación de sistemas de acceso en diferentes contextos de aplicaciones.[8] (Al-Khouri, 2011)

- El cuarto fue desarrollado por Devlekar, S., & Ramteke, V. (2021) y se titula "Identity and Access Management: High-level Conceptual Framework" que se traduce al español como "Gestión de identidades y accesos: Marco conceptual de alto nivel". A continuación, se muestra una parte del resumen de la investigación:

  > Este documento identificará varios componentes de una solución IAM que son esenciales y deben ser considerados mientras se implementa y evalúa la solución IAM y proporciona un marco IAM de alto nivel que permitirá a los profesionales de la seguridad de la información determinar la postura de seguridad IAM de una organización.[9]

1.8.3 Resumen de los resultados

En esta sección se estarán analizando las lecturas que fueron seleccionadas para ser parte del estado de la cuestión de este trabajo de investigación, pues estos serán las bases teóricas de este proyecto. Además, demostrarán la efectividad de tener una documentación sólida sobre el control de accesos en las bases de datos relacionales.

---

[8] This article provides an overview of identity and access management literature. It attempts to analyze the business drivers, trends, issues and challenges associated with the implementation of such systems. It then presents a strategic framework and an overall ecosystem for the implementation of identity and access management system in different contexts of applications.

[9] This paper will identify various components of an IAM solution that are essential and should be considered while implementing and assessing the IAM solution and provides a high-level IAM framework that will allow information security professionals to assess the IAM security posture of an organization

1.8.3.1 Análisis Lectura 1

La primera lectura analizada consiste en el trabajo de investigación realizado por Ishaq Azhar Mohammed (2017) denominado “Systematic review of identity access management in information security” el cual se mencionó brevemente en la sección anterior donde se brinda información del resumen del trabajo.

En general el autor brinda una perspectiva sobre la importancia de implementar sistemas de manejo de identidades para tener un centro de gobernanza en el cual se pueda mantener un control sobre las identidades digitales que se utilizan en las organizaciones y las estrategias que fortalezcan los procesos internos. En la lectura se menciona que

> La gestión de acceso a la identidad se compone de tres áreas funcionales: seguridad de los datos, aprovisionamiento y cumplimiento (o cumplimiento normativo). Las soluciones de gestión de identidades y accesos basadas en la nube han ganado popularidad gracias al concepto de información sin fronteras. La solución tradicional de gestión de acceso IAM se ocupaba principalmente del aprovisionamiento de datos dentro de la organización (Mohammed, 2017).

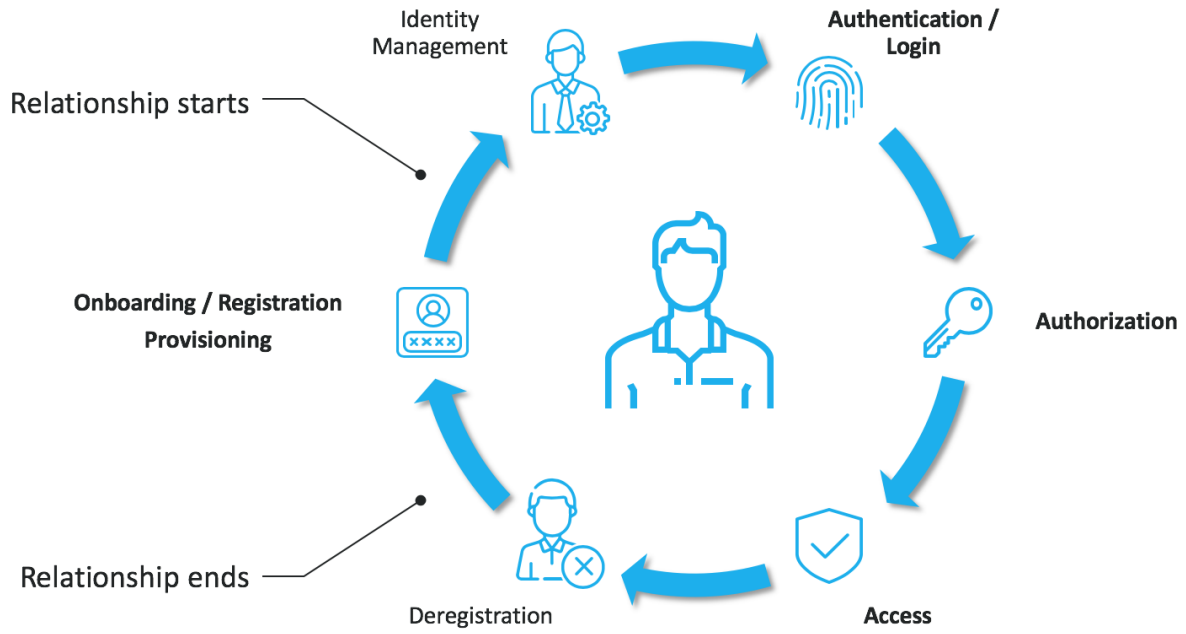
En esta referencia se brindan varios elementos interesantes como los son el aprovisionamiento que se refiere a aquella estrategia estructurada que brinda accesos de manera automática, semiautomática o manual estrictamente requeridos por los usuarios para cumplir sus funciones básicas dentro de las organizaciones. Aunado a lo anterior, existe el opuesto a aprovisionamiento que es el deprovisionamiento, que se refiere al hecho de cuando un usuario termina su relación con la compañía y se

inicia un proceso para eliminar todos los accesos a los recursos empresariales y así eliminar cualquier riesgo de filtración de información.

En la siguiente imagen se explica gráficamente lo que se llama el ciclo de manejo de identidades a grandes rasgos:

Figura 1

Ciclo de identidades



Fuente: Thomas Bröker (2019)

En esta imagen se puede observar el proceso de cada usuario cuando inician o terminan su relación en la compañía correspondiente. Este ciclo es fundamental para este trabajo ya que es importante visualizar y tener una idea general de la metodología que requiere el manejo y control de identidades en las compañías.

Este proceso se lleva a cabo utilizando distintas herramientas que permiten al usuario digital a acceder a su computadora dentro de un dominio con sus respectivas licencias requeridas para poder realizar el trabajo por el cual fue contratado. Sin

embargo, los accesos extras, por ejemplo, a bases de datos, deben ser solicitados de manera individual por los usuarios o por medio de reglas empresariales.

Finalmente, el autor concluye que la implementación de sistemas de manejo de identidades en las organizaciones de una empresa

> puede lograr un equilibrio saludable entre la seguridad, la reducción de riesgos, la educación de sus trabajadores (tanto a los clientes como a los empleados), y el uso de los servicios que necesitan siempre que los requieran mediante estableciendo un programa IAM confiable (Mohammed, 2017).

1.8.3.2 Análisis Lectura 2

El segundo trabajo analizado fue elaborado por Toelen (2008), la cual se titula “Gestión de identidades y accesos”. En la investigación el autor menciona varios de los temas que fueron abordados anteriormente desde una perspectiva bastante similar, pero brinda un apartado que es muy importante en el mundo de IAM que son los roles:

> El control de acceso basado en roles es un mecanismo de autorización que a menudo se asocia con IAM. (...) La mayoría de las veces, se denomina simplemente RBAC. (...) RBAC corresponde con un enfoque descendente del control de acceso. En lugar de agrupar acceso a ciertos recursos en un solo sistema y llamarlo rol, en RBAC, un rol comienza como una visión abstracta que forma parte de la semántica del negocio y no está relacionada con la tecnología (Toelen, 2008).

Este es un tema fundamental en la gestión efectiva de identidades y accesos, pero, especialmente en las bases de datos, debido a que en ellas se pueden abstraer los roles de modo que se cumplan las variables organizacionales y se mitiguen

muchos de los riesgos de pérdida de información los sistemas relacionales. En los siguientes apartados se retomarán los roles en las bases de datos.

De modo general el RBAC pretende tener un control de los accesos por medio de roles y, a partir de ahí, centralizar el acceso para que, cuando se requiera hacer una modificación de permisos, se realicen los cambios a un grupo específico de rol y no individualmente a los usuarios.

A excepción de este nuevo elemento del que hace mención el usuario, la mayoría del trabajo de investigación del autor se enfoca en temas como infraestructura, implementación y varios elementos alrededor del manejo de identidades que se podrían hacer referencia en capítulos posteriores.

1.8.3.3 Análisis Lectura 3

El siguiente estudio analizado fue desarrollado por Al-Khouri (2011) en su trabajo titulado “Optimizing Identity and Access Management (IAM) Frameworks”, el cual el autor enfoca su investigación en la teoría de la disciplina de la gestión de identidades y accesos, por lo tanto, brinda una perspectiva más brusca sobre la confiabilidad de los procesos que se llevan a cabo en las organizaciones para proveer los accesos requeridos por los usuarios para desarrollar su trabajo:

> Con el paso del tiempo, la gestión de identidades ha evolucionado como una disciplina independiente en consonancia con la creciente importancia que esta tecnología ha adquirido a lo largo de los años. Los investigadores y los profesionales han realizado un sinfín de intentos para construir sistemas de gestión de identidades conscientes de la comunidad y para establecer mayores niveles de confianza entre los usuarios de diferentes redes digitales. Sin embargo, el problema crítico radica en el hecho de que hay pocos sistemas

> implementados en la práctica que proporcionen sólidas capacidades de autenticación de usuarios y nuevos niveles de confianza en la forma en que se establecen y verifican las identidades (Al-Khouri, 2011).

Aunado a lo anterior, el autor muestra la necesidad de integrar la estrategia de IAM con otros sistemas para que se puedan fortalecer los procesos de control de accesos:

> La gestión de identidades y accesos, como muchas otras soluciones, no puede añadir valor de forma aislada. El valor global de la gestión de identidades y accesos depende totalmente depende del nivel y la facilidad con la que se integra con otros sistemas empresariales (Al-Khouri, 2011).

Estas integraciones que se mencionan son aquellas plataformas que proveen información actualizadas de empleados, contratistas, directorios activos (Active Directory), inicio único de sesión (Single Sign-On), VPN (Virtual Private Network), dispositivos de accesos físicos (Badge), entre otros. Para efectos de esta investigación muchos de estos elementos no serán tomados en consideración, ya que el objetivo es estandarizar el control de accesos en las bases de datos y no implementar una estrategia completa de la gestión de accesos.

Además, en esta investigación Al-Khouri (2011) enfoca su trabajo en la implementación de una estrategia a nivel gubernamental, sin descartar que muchos de sus puntos sean aplicables a niveles empresariales, ya que la metodología sigue un patrón de uso que puede extrapolarse a diferentes ambientes, de hecho, en una de sus conclusiones menciona lo siguiente:

> Con las crecientes necesidades de identificación y el rápido crecimiento de la tecnología de la información, la forma de satisfacer los requisitos de acceso

> físico y de acceso lógico muestran un alto grado de convergencia. Una identidad digital emitida a una persona sirve para proporcionar control de acceso a áreas físicas controladas para el acceso seguro, así como el acceso a la información lógica segura (Al-Khouri, 2011).

Aunque lo que este trabajo de investigación persigue es un control de acceso de identidades digitales, la parte física es un elemento fundamental en la estrategia de IAM que debería ser parte de cualquier sistema de gobernanza organizacional.

1.8.3.4 Análisis Lectura 4

Finalmente, se seleccionó el estudio de Devlekar y Ramteke (2021) titulada “Identity and Access Management: High-level Conceptual Framework”, en la cual se realiza un recorrido general sobre la terminología alrededor de la estrategia de IAM. Así mismo, la investigación se ocupa de definir términos técnicos propios de la disciplina.

En primer lugar, los autores brindan la definición de lo que consideran “identidad digital”, que también se podría considerar como “identidad virtual” señalando que:

> La identidad digital es la representación de cualquier individuo o entidad en un formato electrónico. Puede ser una persona, un proceso, un servicio o un recurso en un sistema informático. Se refiere a los identificadores únicos y al conjunto de atributos asociados.

Como se menciona en el fragmento anterior un servicio puede ser una identidad que tenga acceso a recursos empresariales. Sin embargo, a partir de esta afirmación surgen varias interrogantes, a saber: ¿quién es el dueño de ese servicio? ¿digitalmente hablando, quién debería ser responsable de esa cuenta de servicio?

¿debería asignarse la cuenta a un usuario activo de la compañía o se deberían crear cuentas abstractas que puedan contener esas cuentas de servicio que no son “humanas”?

Estas preguntas podrían responderse en este trabajo de investigación, o bien, al menos esbozar algunas recomendaciones. No obstante, existen muchas dependencias empresariales a tomar en cuenta antes de proponer una respuesta.

La propuesta realizada por los autores contiene muchos elementos de alto nivel que podrían utilizarse en una estrategia como tal de IAM donde se implemente un sistema completo. Además, brinda elementos de auditoría que, eventualmente, podrían considerarse en esta investigación. Los autores, entre otras cosas, concluyen en la investigación que:

> Es posible investigar más sobre la elaboración de un marco a nivel de implementación basado en tecnologías IAM particulares con los controles de seguridad necesarios, que puede servir como herramienta para IAM y consultores de seguridad de la información.

Lo anterior, confirma que uno de los propósitos de investigación era brindar más y mejores herramientas auditables para establecer fuertes controles sobre los procesos de aprovisionamiento de identidades.

1.8.4 Conclusiones estado de la cuestión

Basado en los análisis realizados en la sección anterior se puede concluir que:

- La documentación que existe actualmente hace mención a la implementación de sistemas estructurales para la correcta gestión de identidades y accesos desde una óptica general.

- No existe documentación específica que señale la metodología correcta para la administración de accesos en bases de datos.
- Las lecturas seleccionadas brindan diversos elementos que pueden ser utilizados a lo largo de esta investigación, como apoyo para fortalecer teóricamente los elementos que se estarán utilizando.
- Dentro de la documentación se encontraron múltiples referencias a IAM en la nube, sin embargo, no es del interés de esta investigación.

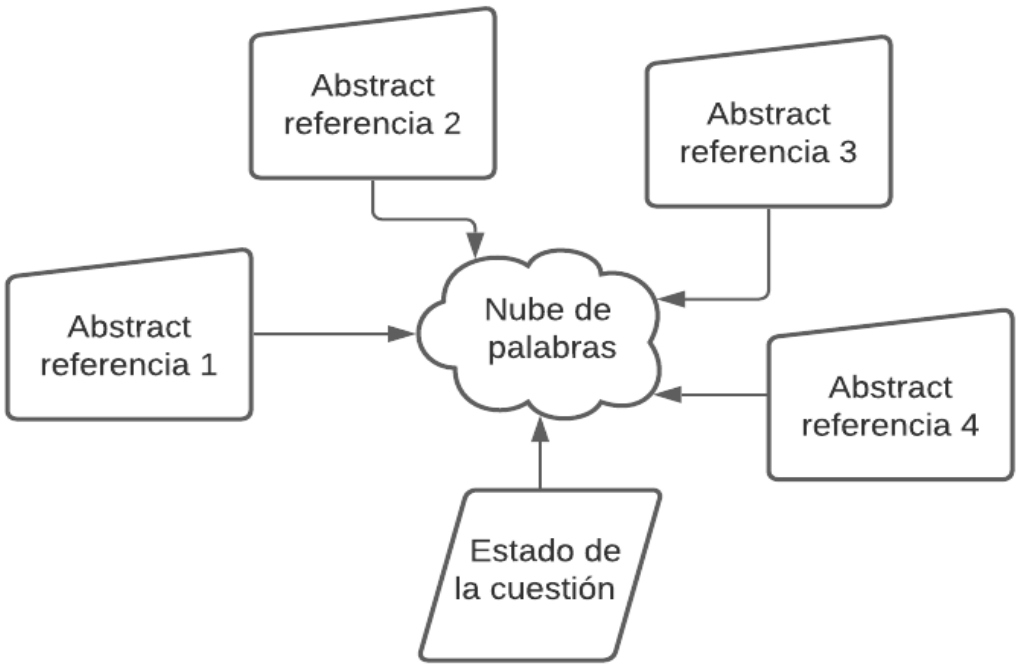
Capítulo 2. Marco Teórico o Conceptual

En este apartado se utiliza una estrategia de conteo de palabras que frecuentemente aparecen en el apartado del estado de la cuestión, presentado anteriormente. Además, se le agregan los resúmenes de los trabajos que se referencian en el mismo, con el fin de dar mayor énfasis a los conceptos que se definirán en el marco conceptual.

Para ello se ilustra la metodología utilizada para generar la “nube” que se desarrolla a partir del conteo de palabras:

Figura 2

Generación de la nube de palabras



Fuente: Elaboración propia (2021)

La imagen anterior se construye a partir de la información presentada en el estado de la cuestión (sección 1.9). La lectura de estos artículos académicos fue

traducida y utilizada como ejercicio para generar la nube de palabras junto al estado de la cuestión, y estas tienen como título:

Abstract referencia 1: Systematic Review of Identity Access Management in Information Security.

Abstract referencia 2: Identity and Access Management.

Abstract referencia 3: Optimizing Identity and Access Management (IAM) Frameworks.

Abstract referencia 4: Identity and Access Management: High-level Conceptual Framework.

Ahora bien, el resultado final de la estrategia utilizada fue la siguiente nube de palabras generada en el sitio: https://www.nubedepalabras.es/

Figura 3

Nube de palabras generada

Fuente: Elaboración propia (2021)

De este resultado se utilizaron varios filtros en donde aparecen monosílabos que no son relevantes, también palabras en inglés que ya aparecen en la nube, y algunas preposiciones que tampoco agregan valor al resultado. Finalmente, se procede a la elección de 10 palabras que son relevantes en este trabajo y necesitan tomar forma mediante una decisión para delimitar su uso en este trabajo de investigación. Cabe destacar que hay palabras que por sí solas no generan el impacto deseado, pero al unirse con otra se logra dar el contexto apropiado:

Tabla 8

Palabras por definir

Concepto por definir	Motivo de la inclusión
Control de accesos	Palabras centrales y esenciales de la investigación.
Bases de datos	Parte fundamental del trabajo a desarrollar.
Gobernanza	Elemento clave para el desenvolvimiento del control de accesos.
Integridad	Palabra que evita la corrupción de los datos.
Seguridad de la información	Estrategia de uso que estandariza las metodologías utilizadas para el control de accesos.
Sistema	Identificador de los diferentes recursos gubernamentales a tomar en cuenta en el modelo.
Iso	Estándar que sirve como guía para la evaluación de los modelos a crear.
Recursos	Definición que complementa a la palabra sistema en la descripción de las fuentes de datos.
Entidad gubernamental	Esclarece qué elementos son los que componen el aparato estatal.
Políticas	Definición que delimita las acciones y procesos a llevar a cabo siguiendo códigos y leyes gubernamentales.

Fuente**:** Elaboración propia (2021)

2.1 Definición de conceptos

A partir fuentes de información distintas y confiables, en este apartado se conceptualizarán las palabras seleccionadas en la tabla 8 para delimitar su función

en este trabajo de investigación con el objetivo de evitar confusiones o malversación de la información generada en los demás apartados que integran este trabajo.

2.1.1 Definición de control de accesos

El control de accesos es un término bastante amplio en ambientes de seguridad de la información. En este caso se utilizará como referencia la definición brindada por Benantar (2005) donde menciona que “la necesidad de divulgar el acceso a la información y a los recursos y servicios informáticos disponibles sólo a las entidades autorizadas”. Por lo tanto, se puede comprender que el control de accesos tiene como objetivo ser un punto desde el cual se pueda visualizar quiénes tienen acceso a la información.

Así mismo, Benantar propone la definición de entidad como “(…)un término genérico que se refiere a un agente activo capaz de iniciar y realizar un proceso de algún tipo” , lo cual hace referencia a la necesidad de brindarle una identidad al agente activo que se menciona en la definición. Por lo tanto, se puede concluir en este apartado que el control de accesos es un proceso centralizado que busca administrar el acceso a la información por medio del manejo de entidades por parte de parte de los individuos.

2.1.2 Definición de bases de datos

El término base de datos en esta investigación está relacionado con aspectos de infraestructura, pues la evaluación que se estará realizando será por medio de diferentes modelos y diseños que estarán involucrando las bases de datos. Basado en la definición Morley y Parker (2009) una base de datos es “una colección de datos relacionados que se almacenan de manera que permitan recuperar la información según sea necesario”, por supuesto esta es una definición general, indica que las

bases de datos son elementos que guardan datos y ayuda a las aplicaciones a interactuar con la información que se encuentra dentro de ella y, de esta forma, agregar valor a las diversas necesidades de los involucrados.

2.1.3 Definición de gobernanza

Esta palabra ampliamente utilizada en distintas áreas del saber y especialmente extendida, en entornos políticos. Sin embargo, en esta ocasión la palabra gobernanza en el contexto informático y ambientes de seguridad es definida por el International Bureau of Education & UNESCO. (s. f.) como aquellas "(…) estructuras y procesos diseñados para garantizar la rendición de cuentas, la transparencia, la capacidad de respuesta, el estado de derecho, la estabilidad, la equidad y la inclusión, el empoderamiento y una base amplia".

A nivel de sistemas informáticos estos elementos que se incluyen en la definición se siguen. Además, a ellos se unen principios que García-Morales (2011) menciona en su investigación sobre "Gobernanza de la Información" como lo son:

- Accountability (Rendición de cuentas).
- Transparencia.
- Integridad.
- Protección.
- Cumplimiento.
- Disponibilidad.
- Retención.
- Disposición.

Al avanzar en esta investigación, cada uno de estos será utilizados para describir las diferentes situaciones que se encontrarán en los sistemas donde se realizará la evaluación de este trabajo.

2.1.4 Definición de integridad

En este caso, Nguyen (2003) define integridad como “(…) como la protección contra la modificación o destrucción no autorizada de la información”. Por lo tanto, la integridad es un elemento que complementa a la gobernanza en cuanto a su utilidad de conservar la información tal y como se recibe, sin tener que recurrir a estrategias para modificar el contexto y que esta pierda su relevancia.

De esta forma, la integridad es un elemento fundamental para esta, puesto que en la evaluación de los sistemas gubernamentales se estará vigilando los procesos de los controles de acceso y así como el adecuado cumplimiento de la integridad de las entradas y salidas de información para que los datos no sean descontextualizados.

2.1.5 Definición de seguridad de la información

Este elemento de la investigación será el que define el propósito principal de realizar el diseño de control de accesos en los sistemas de bases de datos, pues se desea tener un control centralizado de accesos a los diferentes sistemas para cumplir con medidas de seguridad de la información.

Para este término, Zapata (2020) menciona que la seguridad de la información se define como “(…) la aplicación y gestión de medidas de seguridad apropiadas mismas que permiten resguardar y proteger la información, cumpliendo con tres dimensiones principales: la confidencialidad, disponibilidad e integridad”. A partir de lo anterior, se puede observar que la seguridad de la información entreteje otros términos definidos o mencionados.

2.1.6 Definición de sistema

El contexto de sistemas en esta investigación tiene un significado similar al que podría entenderse con aplicación, pero se debe añadir elementos que puedan ser requeridos para hacer la evaluación como lo son las bases de datos y servidores. En términos generales un sistema se refiere a un elemento al que un usuario pueda tener acceso y se necesite evaluar el control de accesos en él y poder monitorearlos por medio de comportamientos en el tiempo y configuraciones de roles.

2.1.7 Definición de ISO

A partir de la International Organization for Standardization (s. f.), el cual es un organismo internacional independiente, formado en los años 60, para crear estándares y un consenso internacional sobre diferentes elementos, entre ellos la seguridad informática.

El ISO es un organismo fundamental y tiene que ser una referencia directa para poder completar los objetivos que se persiguen.

2.1.8 Definición de recursos

Los recursos se refieren a las características con las que cuentan los sistemas, podría ser igualmente utilizado en el contexto de sistemas o aplicaciones, pero principalmente serán referidos como elementos particulares que podrían utilizarse para generar los reportes de usuarios activos en las aplicaciones. Estos recursos pueden ser conexiones por medio de API, interfaces web, conexiones a bases de datos, generación de reportes en líneas de comandos, entre otros, que podrían aparecer una vez se avance en este trabajo de investigación.

2.1.9 Definición de IAM

Las siglas a las que hacen referencia IAM vienen dadas por “Identity and Access Management” las cuales se pueden traducir como Manejo de Accesos e Identidades. Gunter et al. (2011) lo conceptualiza como “la gestión de identidades y accesos (IAM) consiste en nombrar y autenticar a los titulares y asignar y actualizar sus derechos de autorización para los sistemas informáticos y de red de una empresa.” Como se puede observar, este término hace referencia a la acción de poder gestionar correctamente las identidades y sus respectivos accesos en los diferentes recursos organizacionales.

Por lo tanto, se puede concluir que IAM es aquella estrategia que brinda diversos elementos a las compañías para poder gestionar correctamente los accesos de sus usuarios, con el objetivo de corroborar que sus accesos sean únicamente los requeridos para cumplir sus funciones y de esta forma formular planes para evitar que usuarios indebidos utilicen información que no requieran.

2.1.10 Definición de políticas

La palabra política, al igual que gobernanza, es ampliamente utilizada en diversas disciplinas y áreas del saber. Para esta investigación se delimitarán únicamente su uso en relación a las políticas públicas donde se utilizará como base para evaluar si el control de accesos en los recursos gubernamentales está alineado con los códigos y leyes reglamentarias existentes.

Basado en la definición de Lahera (2002) las políticas públicas se definen como “programa de acción de una autoridad pública o al resultado de la actividad de una autoridad investida de poder público y de legitimidad gubernamental”. Precisamente el término “legitimidad gubernamental” son de especial interés para este apartado,

pues es uno de los principios que sigue esta investigación, el cual es dar a conocer el grado de legitimidad de un proceso que se está utilizando para el control de acceso (quiénes tienen información a cuál información y cuál es su rol en las aplicaciones).

Capítulo 3. Marco Metodológico

3.1 Tipo de Investigación

Esta investigación se enmarca en las investigaciones aplicadas, ya que como señala Lozana (2014):

> La investigación aplicada tiene por objetivo la generación de conocimiento con aplicación directa y a mediano plazo en la sociedad o en el sector productivo. Este tipo de estudios presenta un gran valor agregado por la utilización del conocimiento que proviene de la investigación básica (p.35).

Esta definición coincide con los fines de la presente investigación, ya que su objetivo es resolver una problemática productiva que se encuentra en un caso específico. Por lo tanto, se puede decir que el proceso tiene por objetivo crear conocimiento base, al contrario, pretende servirse de conocimiento base creado por otras investigaciones y utilizarlo para generar una solución en concreto.

Esto confirma que, principalmente se está utilizando conocimiento heredado de investigaciones puras para poder cumplir con el objetivo general de este trabajo. Los dos tipos más comunes de investigación en la literatura son la pura (o básica) y la aplicada, además de la investigación evaluativa. Cada tipo tiene características bien definidas. Por último, se puede descartar que esta investigación será evaluativa, ya que, aunque no se tiene un cliente definido, se estaría generando conocimiento que puede ser utilizado por diferentes clientes con características muy particulares.

3.2 Alcance Investigativo

El alcance de esta investigación es de tipo descriptivo, debido a la necesidad de conceptualizar muchas definiciones que se relacionan con otros campos, pero se han adaptado al ámbito del control de accesos que se está evaluando en este trabajo.

Si bien existe mucha información al respecto, esta no se encuentra sistematizada. Por otro lado, no hay mucha información de la implementación, es por ello que se requiere utilizar estructuras empleadas en otras áreas y adaptarlas al control de accesos en bases de datos relacionales.

Baptista et al. (2014) señalan que el alcance descriptivo consiste en:

> (…) buscar especificar las propiedades, las características, y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar cómo se relacionan éstas (p. 92).

Es decir, el objetivo de la investigación no es explicar por qué los elementos están compuestos en el orden o forma actual, sino que se concentrará en describir las bases que se utilizarán y cómo se hará la evaluación respectiva a partir de esto.

3.3 Enfoque

El enfoque de esta investigación tendrá un carácter alternativo, ya que como señala Naranjo (2020) “el enfoque alternativo es enteramente compatible con propuestas en boga, como la ciencia de diseño, que también están orientadas a facilitar la investigación en informática y en otras ingenierías” (p. 9).

Es necesario mencionar que esta investigación no tiene un enfoque cuantitativo, pues existen muchas variables las cuales pueden afectar el sistema y no habría una forma de extraerlas y analizarlas de forma aislada sin tener certeza de que no existen otras, las cuales también se deban considerar. De igual modo, no se puede clasificar como enfoque cualitativo, pues el objetivo no es encontrar los elementos

subjetivos, sino que también se busca una aplicación directa, la cual necesita obtener más que la interpretación para poder desarrollar la evaluación respectiva de las necesidades a exponer.

Debido a lo señalado anteriormente sobre el enfoque cuantitativo, no es posible abordar el método mixto. Ante esta situación nace la necesidad de utilizar un enfoque distinto que se adapte a la especificidad de esta investigación y es precisamente el enfoque alternativo el que cumple con estas necesidades particulares.

Para poder desarrollar un enfoque alternativo es “necesario definir lo que la literatura explica en cuanto al encuadre epistemológico, ontológico y axiológico de la investigación” (Naranjo, 2020, p. 9); lo cual conduce a esta investigación a definir las dimensiones propuestas para poder cumplir con la necesidad de abordarlas individualmente para correlacionarse entre sí.

3.3.1 Dimensión epistemológica

La epistemología es definida por Esquivel et al (2011) como la “(…) área de la ciencia que se ocupa de establecer los criterios básicos para determinar el carácter científico o no de los enunciados y las teorías.” (p. 20). Además, la epistemología puede estar basada en elementos de autoridad, razón y experiencia basándose en teorías epistemológicas pluralistas como la que menciona Marisol Facuse (2003). A partir de lo anterior, se hace fundamental utilizar esta dimensión en la presente investigación para poder generar un diseño adecuado a la situación expuesta y de esta forma poder validar el uso del nuevo conocimiento con las necesidades de negocio actuales.

Por otro lado, se estarían utilizando los elementos de autoridad, para poder referirse a conocimiento de fuentes que han estudiado casos similares y que son

considerados expertos, se puede utilizar la razón como elemento en donde se puede validar qué está bien y qué se puede mejorar, así como la experiencia como punto fundamental para identificar diferentes escenarios que se interpongan en el camino.

3.3.2 Dimensión ontológica

La ontología es un elemento que en principio viene dado por una fuerte influencia filosófica, pero luego del desarrollo tecnológico, este se pudo incluir en investigación donde se incluye los sistemas informáticos sin perder su esencia teórica. Barchini et al. (2007) mencionan que el estudio ontológico es utilizado para "especificar y comunicar el conocimiento del dominio de una manera genérica y son muy útiles para estructurar y definir el significado de los términos" (p. 2), también añaden tres puntos importantes en la resolución de problemas:

- Entender cómo diferentes sistemas comparten información.
- Descubrir ciertas distorsiones presentes en los procesos cognitivos de aprendizaje en un mismo contexto.
- Formar patrones para el desarrollo de SI.

A partir de lo anterior, en el contexto de esta investigación, la ontología es una dimensión necesaria, pues se necesita tener claro todos los puntos y aristas dentro del caso para poder estructurar y diseñar exitosamente un diseño por medio del aprendizaje continuo donde se documentan los patrones que se encuentren en los recursos de las organizaciones actualmente.

3.3.3 Dimensión axiológica

Naranjo (2020) define la axiología como la encargada de "estudiar los valores, es decir, clasificar cuáles cosas son buenas y qué tan buenas son" (p. 6), además, es la que "permite formalizar escalas de valores para no utilizar conceptos cuya definición o medición de su valor intrínseco resulta muy vaga" (Naranjo, 2020, p. 6).

Debido a lo expuesto anteriormente, la dimensión axiológica se plantea como idónea para la investigación en cuestión, ya que permitirá diseñar el sistema de control de accesos en bases de datos relacionales, para ello se debe clasificar los elementos y verificar la idoneidad de cada uno de ellos, así como las recomendaciones respectivas sobre las metodologías que se están utilizando actualmente.

3.4 Diseño

La naturaleza de este trabajo está planteada a partir de un diseño enfocado en investigación evaluativa. Esta investigación requiere estandarizar un proceso de control de accesos en bases de datos que sigan los mismos parámetros. Por consiguiente, todos los casos donde se requiera utilizar esta metodología podrán seguir los mismos patrones de uso.

Así mismo, la investigación según señalan Cook y Reichardt (1986) tiene la particularidad de ser flexible ya que está compuesta por elementos cualitativos y cuantitativos, lo cual describe a la perfección el enfoque alternativo. Además, los autores mencionan que:

> (…) un investigador no tiene por qué adherirse ciegamente a uno de los paradigmas polarizados que han recibido las denominaciones de “cualitativo” y “cuantitativo”, sino que puede elegir libremente una mezcla de atributos de ambos paradigmas para atender mejor a las exigencias del problema de la investigación con que se enfrenta (p. 10).

A partir de lo anterior es necesario definir lo que se debe entender por evaluación, para lo cual Gómez et al. (1996) señalan que:

> (…) la evaluación es un esfuerzo por reconocer qué cambios se presentan durante y después de un programa de acción y qué parte de dichos cambios pueden atribuirse al programa (p. 27).

Hay que mencionar, además que Gómez et al. (1996) sugieren cuatro principios a seguir alrededor de la evaluación, a saber:

1. Propósito: El propósito de evaluar es mejorar el funcionamiento del sistema. En el sistema educativo, esto significa mejorar su enclave en la sociedad y, por tanto, garantizar la calidad de los programas en sus diferentes niveles y modalidades.

2. Función: La evaluación tiene como patrón de funcionamiento la conciencia social. Si se carece de esta condición, la evaluación será restringida, unilateral y logrará mejorar la institución o el programa.

3. Uso: Los resultados de la evaluación deben darse a conocer a todos los actores y ponerse a disposición del público.

4. Fin: La evaluación debe orientarse y organizarse teniendo en cuenta que el punto final de ésta es la toma de decisiones.

Finalmente, el tipo de evaluación que se realizará será una evaluación externa, la cual es realizada por un agente que se encuentra fuera de las organizaciones que pueden utilizar esta metodología (el investigador de este trabajo). El evaluador aplicará sus conocimientos académicos y profesionales en el área por analizar. Las habilidades y competencias del evaluador se explicaron en el apartado 1.5 Viabilidad.

3.5 Población y Muestreo

Esta investigación tiene el objetivo de diseñar un proceso estandarizado que se utiliza en el control de acceso en bases de datos relacionales. Por lo tanto, la

población está conformada por todas aquellas aplicaciones o sistemas que utilicen bases de datos de tipo SQL Server, MySQL y Oracle. Sin embargo, es probable que no todas las bases de datos sean aplicables para esta estrategia, debido a que existen gran variedad de políticas (internas y externas) que pueden aplicarse en los diversos modelos de negocios de las compañías.

En cuanto a las características de las bases de datos que podrían ser incluidas en la población de este trabajo de investigación se plantean:

- Sistemas de bases de datos productivos o de desarrollo relevantes para las empresas.
- Sistemas de datos de datos productivos o de desarrollo con un nivel relevante de solicitudes de accesos que ayuden a reducir la intervención manual de control de accesos.
- Sistemas de bases de datos productivos o de desarrollo identificados por auditores internos y externos para ser controlados de manera automática por esta metodología
- Sistemas de bases de datos relaciones tipo SQL Server, MySQL y Oracle en los cuales se puedan ejecutar exitosamente las funciones que se están diseñando en este trabajo de investigación.
- Aquellos sistemas de bases de datos que manejan información valiosa para la institución

Debido a que en cada compañía o empresa habrá gran cantidad de sistemas con las características requeridas se deberá realizar una valoración interna para poder identificar con cuáles recursos humanos y de infraestructura se cuentan para cumplir con los requerimientos.

En esta investigación no se trabajarán casos específicos empresariales, ya que se creará una metodología la cual podrá ser extrapolada a diversos sectores empresariales y se podrán realizar las modificaciones del método basado en las políticas internas.

Por otro lado, al realizar el muestreo pueden presentarse situaciones que modifiquen el comportamiento del muestreo, como lo son: la confidencialidad de la información, la disponibilidad de los involucrados en los procesos, entre otras. Existen muchos diversos escenarios que deberán ser documentados para enriquecer el trabajo de investigación, además, de esta forma futuras investigaciones interesadas tendrán esta información disponible.

3.6 Instrumentos de Recolección de Datos

El instrumento que se utilizará para la recolección de datos para este trabajo de investigación será la observación participativa estructurada enfocado en desarrollar de manera científica. Esto se hace basado en el método clínico de Díaz (2011) la cual señala que este instrumento consiste en “observar un objetivo claro, definido y preciso: el investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación” (p. 7) en donde la participación estructurada viene definida como

> (…) el investigador se incluye en el grupo, hecho o fenómeno observado para conseguir la información “desde adentro”. (…) La observación estructurada es en cambio la que se realiza con la ayuda de elementos técnicos apropiados, tales como: fichas, cuadros, tablas, etc, por lo cual se le denomina observación sistemática (p. 8).

Es necesario aclarar que no se utilizan otras estrategias de recolección de datos como las encuestas, debido a que no se cuenta con algún patrocinador que pueda aportar respuestas a las preguntas brindadas en la encuesta.

A partir de lo expuesto, se concluye que la observación es un método eficiente e idóneo para este trabajo, pues el investigador puede ajustar cada observación dependiendo de los resultados que se van logrando en el diseño de la estrategia.

3.7 Técnicas de Análisis de Información

Para esta sección se utilizarán diagramas de flujos de datos para poder brindar una herramienta gráfica que permita observar los resultados obtenidos en la sección 3.6 y cuál sería su diagrama como tal para poder visualizar los caminos que se estarían tomando en las decisiones lógicas que se implementen.

En esta sección se reunirán y sistematizarán técnicas para demostrar la funcionalidad de la metodología una vez que ya se haya puesto en marcha el proyecto y se puedan obtener datos confiables.

Es preciso aclarar que, en esta investigación no se utilizan otras técnicas de análisis de datos ya que estas son aplicables en casos específicos y este trabajo de investigación pretende conseguir estandarizar una metodología y no restringirse a un caso específico donde hay un patrocinador.

3.8 Estrategia de Desarrollo de la Propuesta

Como se ha explicado anteriormente, este trabajo de investigación pretende documentar y estandarizar el control de accesos en bases de datos relacionales. Para cumplir con estas consignas es necesario utilizar una herramienta de gobernanza de la información.

Para emular el funcionamiento de estas herramientas de gobernanza de la información se creará un conjunto de scripts en el lenguaje PowerShell para mostrar cuáles serían las entradas y las salidas esperadas en la estrategia propuesta. Además, estos scripts se utilizarán para visualizar mediante una consola el comportamiento de los datos recibidos y enviados.

Aunado a lo anterior, se crearán procedimientos almacenados en los productos seleccionados en el punto 1.3 Tipo de Investigación para poder brindar las opciones que se van a poder ejecutar en las estrategias de control de accesos, aprovisionamiento y deprovisionamiento de cuentas en las bases de datos.

Capítulo 4. Análisis del Diagnóstico

Esta sección se ocupará de recopilar estudios que han utilizado estrategias similares a la que se plantea en esta investigación. De esta forma, se visualizarán distintas perspectivas y soluciones que se han utilizado para construir un control de accesos más seguro.

En la sección 1.3 se mencionó que la solución propuesta en esta investigación responde a diversas necesidades que existen en las empresas. Sin embargo, no hay una documentación sobre la implementación de estas metodologías, por diversas razones, por ejemplo, la protección de sus procesos internos o confidencialidad de la información. Existe, empero un método que utiliza procesos de seguridad muy robustos y que se desean explicar en este apartado.

Esta estrategia se denomina Endpoint Security Platform (Plataforma de seguridad para terminales) o algunas veces también llamada Endpoint Protection Platform (Plataforma de protección para terminales o EPP por sus siglas en inglés). McAfree (s.f) define esta técnica como “la práctica de salvaguardar los datos y los flujos de trabajo asociados a los dispositivos individuales que se conectan a su red”[10] (McAfree, s.f). El autor señala un elemento trascendental que debe ser tomado en cuenta en esta investigación: los dispositivos individuales. Estos pueden categorizarse como terminales que pueden lograr conectarse a una red interna o externa, por ende, el elemento de red es de suma importancia para poder explicar cómo va a ser utilizado en este trabajo.

Así mismo, es importante agregar que, como señala Forcepoint (2021):

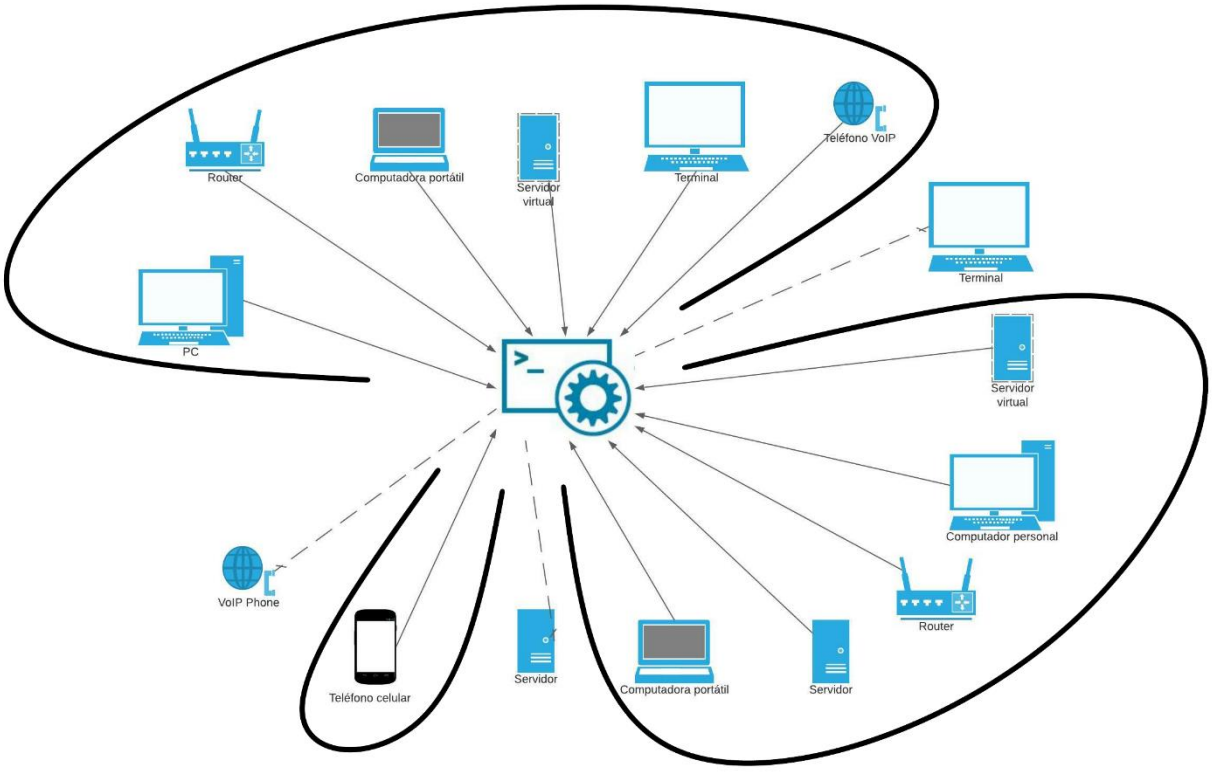
[10] is the practice of safeguarding the data and workflows associated with the individual devices that connect to your network

Las soluciones de seguridad para puntos finales suelen utilizar un modelo de protección cliente-servidor, empleando tanto una solución de seguridad gestionada centralmente para proteger la red como un software cliente instalado localmente en cada punto final utilizado para acceder a esa red.

A partir de lo anterior se puede inferir que estas plataformas de seguridad para terminales instalan un cliente en los dispositivos que tengan acceso a una red en específica y a su vez estos tienen comunicación directa con una base de datos centralizada, en la cual se monitorean diferentes comportamientos de datos. Por lo tanto, el esquema de lo mencionado anteriormente se puede interpretar de la siguiente forma:

Figura 4

Esquema de Endpoint Protection Platform



Fuente: Elaboración propia (2022)

Como se puede observar la estrategia de EPP tiene como norte la centralización del control de múltiples funciones dentro de todos los dispositivos que tengan el cliente instalado y, que, al mismo tiempo, estén conectados a la red empresarial. EPP tiene múltiples funcionalidades para proteger los dispositivos de diversos riesgos asociados a la vulnerabilidad de la información. Sin embargo, este apartado explicará, principalmente, la centralización de control de accesos en el que se brinda una visualización en tiempo real de los usuarios con accesos a las terminales.

Además, es importante mencionar que, esta funcionalidad de control de accesos en los activos empresariales se encuentra dentro de una red de interés para la compañía se realiza únicamente a nivel del dispositivo. Sin embargo, es claro que no hay funcionalidades que controlen el acceso dentro de las aplicaciones que se albergan en los dispositivos, este es, precisamente, el objetivo de esta investigación: tener una funcionalidad que controle los accesos a las bases de datos a nivel de la aplicación.

Ahora bien, basado en las comparaciones entre empresas, que realizó la compañía Gartner entre productos o estrategias similares de mercado que utilizan la metodología EPP en 2021 se observaron los siguientes resultados:

Figura 5

Cuadrante mágico para Endpoint Protection Platform (2021)

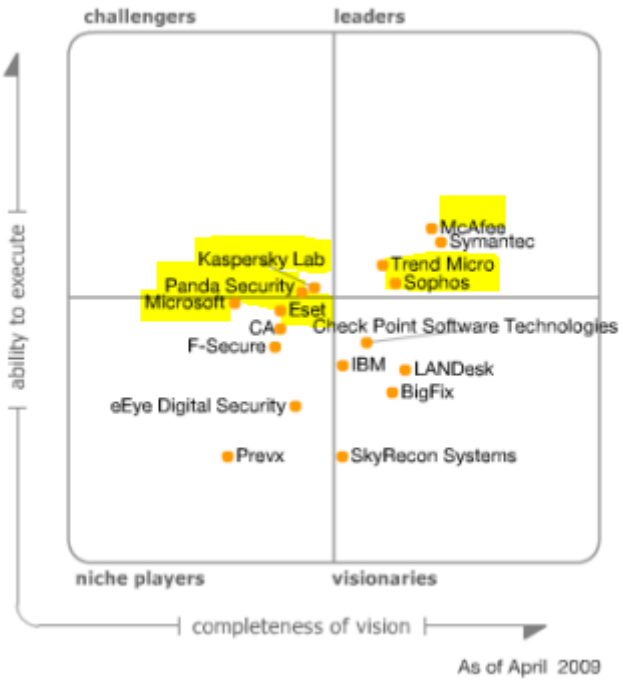
Fuente: Gartner (May, 2021)

En la imagen anterior se muestran compañías que desarrollan productos para implementar estrategias de EPP. Por lo tanto, hay diversas formas en las que el control de accesos en dispositivos disponibles en una red se ha aplicado. A pesar de esto, ninguna ha desarrollado o ha añadido alguna funcionalidad que permita, además de tener los usuarios con acceso por dispositivo, tener la opción de usuarios con acceso a bases de datos. De ahí la importancia de desarrollar esta funcionalidad la cual brindaría más seguridad y control sobre los accesos que se otorgan en las bases de datos.

A continuación, se muestra el cuadrante de 2009 en esa misma categoría:

Figura 6

Cuadrante mágico para Endpoint Protection Platform (2009)



Fuente: Gartner (2009)

Como se puede observar, en el cuadrante de 2022 ilustra una diferencia significativa respecto al cuadrante de 2009, con lo cual se muestra un incremento que ha sufrido la tecnología alrededor de la estrategia de EPP. En la imagen anterior se muestra que, muchas de las compañías líderes o precursoras quedaron desplazadas en el último informe del 2021, esto se debe a que las compañías requieren soluciones rápidas y eficaces, que se adapten fácilmente a las necesidades que emergen constantemente.

Como se mencionó anteriormente, desarrollar un EPP no es el objetivo de esta investigación, empero las estrategias que se utilizan son similares a las que se desean diseñar en este trabajo la cual consiste en fortalecer los procedimientos de control de accesos en las bases de datos. La herramienta elaborada puede adentrarse en un mercado que crece rápidamente y tiene un impacto positivo para las compañías.

En el siguiente capítulo se explicará la metodología para implementar la estandarización, así como las características con las que deben cumplir los dispositivos para implementar la metodología.

Capítulo 5. Propuesta de Solución

En el desarrollo de este capítulo, se mostrarán las propuestas para estandarizar el control de accesos en las bases de datos relacionales para los tres productos que se eligieron en la sección 1.3 Definición y Descripción del Problema en base a la popularidad de estos mismos. Se mostrarán mediante gráficas los objetivos planteados, así mismo, se brindarán los códigos correspondientes según las cualidades de los productos.

El objetivo de este capítulo es mostrar tres alternativas para tres acciones fundamentales del ciclo de vida de manejo de identidades. Estas son:

1) La reconciliación de usuarios (RECON): A partir de lo propuesto por Sath Inc (2022), la reconciliación consiste en

   > un proceso de auditoría del gobierno de la identidad que compara el acceso de los usuarios, los derechos de acceso y las cuentas privilegiadas con la fuente de identidad autorizada acordada. Este proceso se utiliza para confirmar qué datos están presentes en una aplicación, y sincronizar esos datos con un sistema de gestión de identidades existente para garantizar el acceso correcto a los sistemas para las personas adecuadas (Sath Inc., 2022).[11]

2) Aprovisionamiento y deprovisionamiento de cuentas: Este proceso, según OneLogin (s. f.) implica la creación, actualización y eliminación de las cuentas de los usuarios en distintas aplicaciones y sistemas. Aunado a lo anterior, OneLogin (s.f) indica que “esta práctica de gestión de accesos puede incluir a

[11] Reconciliation is an Identity Governance audit process, which compares User access, access rights, and privileged accounts, against the agreed-upon authoritative identity source of truth. This process is used to confirm what data is present in an application and sync that data with an existing Identity Management System to ensure the right access to systems for the right people.

veces información asociada, como los derechos de los usuarios, la pertenencia a grupos e incluso los propios grupos”[12] (OneLogin, s. f.)

A partir de lo señalado previamente, se brindan estrategias para aplicar las acciones, de RECON, aprovisionamiento y deprovisionamiento de cuentas, en las bases de datos MySQL, SQL Server y Oracle. Las versiones utilizadas de los productos mencionados son:

Tabla 9

Versiones de los productos utilizados

Producto	**Versión**
Oracle SQL Developer	21.4.2.018.1706
Java (TM) Platform	1.8.0_311
Oracle	19.0.0.0.0
MySQL	8.0.27
MySQL Workbench	8.0
Microsoft SQL Server 2019 (RTM)	15.0.2000.5 (X64)
SQL Server Management Studio	15.0.18390.0
Windows 10 Education 10.0 (Cliente)	10.0.19043 N/A Build 19043
Windows Server 2022	10.0.20348 N/A Build 20348

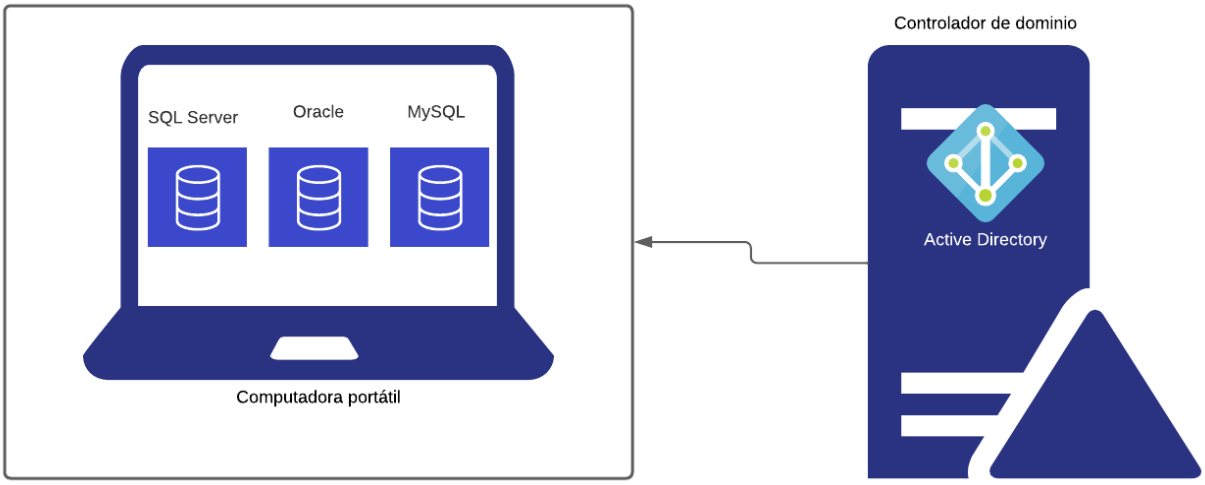
Fuente: Elaboración propia (2022)

La infraestructura que se utilizó para el desarrollo de esta solución consiste en dos máquinas virtuales. La primera, se comporta como cliente-servidor en el que se instalan todas las instancias de bases de datos. La segunda, consiste en un servidor de control de dominio para ingresar a la máquina dentro de él y, de esta forma, controlar los usuarios y los grupos de Active Directory con los que se brindan los accesos correspondientes a las cuentas en sus respectivos productos. Lo anterior se muestra en el siguiente diagrama:

[12] User provisioning and deprovisioning involves the process of creating, updating, and deleting user accounts in multiple applications and systems. This access management practice can sometimes include associated information, such as user entitlements, group memberships and even the groups themselves

Figura 7

Diagrama de la infraestructura utilizada



Fuente: Elaboración propia (2022)

A continuación, se describen los casos a los que se les dará una solución con cada uno de los productos.

Caso 1 (Creación de cuenta y aprovisionamiento)

- Usuario recién contratado.
- Usuario con nuevos roles dentro de la compañía.
- Se necesita una cuenta no humana o robótica para ejecutar diferentes procedimientos dentro de los esquemas.
- Primera vez que el usuario solicita el acceso.
- El usuario requiere un acceso limitado de lectura en un esquema.

Caso 2 (Aprovisionamiento a cuenta existente)

- El usuario ya existe en el esquema y necesita añadir un privilegio extra en su perfil.
- Las funciones del usuario cambiaron y se le brinda un acceso diferente.

- Hubo un cambio en los roles de la organización y este usuario tendrá que realizar más actividades.

Caso 3 (Deprovisionamiento de privilegio a cuenta existente)

- En este caso el usuario ya existe en el esquema y requiere remover uno o varios privilegios de su perfil sin borrar la cuenta.
- Se le removieron responsabilidades al usuario y no es requerido que tenga el privilegio.
- Se realizó una auditoría y se encontró que el usuario tiene un acceso que no requiere.
- El usuario cambió de posición y ya no necesita tener el privilegio.

Caso 4 (Deprovisionamiento completo de una cuenta existente)

- El usuario termina la relación con la compañía.
- El usuario cambió de departamento y no necesita este acceso.

5.1 MySQL

Este producto presenta una particularidad; por defecto no contiene la opción de crear o dar acceso a usuarios Windows o de tipo objeto en Active Directory, únicamente se pueden crear usuarios locales. Otra peculiaridad es que los accesos se manejan por medio de acciones y no por roles. Por lo tanto, se debe brindar a cada usuario acceso a la acción que requiera desarrollar.

5.1.1 Reconciliación de usuarios en MySQL

5.1.1.1 Creación del procedimiento almacenado

El script propuesto para poder desarrollar esta acción de RECON es el siguiente:

```
DELIMITER //
-- CREACIÓN DEL PROCEDIMIENTO ALMACENADO
CREATE PROCEDURE GET_USERS_WITH_ACCESS_TO_MYSQL_SCHEMA()
BEGIN
    -- SELECCIÓN DE TODAS LAS COLUMNAS DE LA TABLA DB
    -- SELECCIÓN DE LAS COLUMNAS ÚLTIMA ACTUALIZACIÓN DE LA CONTRASEÑA,
CUENTA BLOQUEADA Y CONTRASEÑA EXPIRADA DE LA TABLA DE USERS
    SELECT
DB.*,US.password_last_changed,US.account_locked,US.password_expired
    FROM mysql.db DB
    LEFT JOIN mysql.user US ON DB.User = US.User
    LEFT JOIN sys.user_summary SUM ON DB.User = SUM.user;
END //
-- FINALIZACIÓN DEL PROCEDIMIENTO ALMACENADO
DELIMITER ;
```

5.1.1.2 Ejecución del procedimiento almacenado

La llamada de este procedimiento almacenado es el siguiente:

```
CALL GET_USERS_WITH_ACCESS_TO_MYSQL_SCHEMA()
```

Este comando brindaría un resultado como el siguiente:

Figura 8

Resultado ejecución del RECON en MySQL

# Host	Db	User	Select_priv	Insert_priv	Update_priv	Delete_priv	Create_priv	Drop_priv	Grant_priv	References_	Index_priv	Alter_priv	Create_tmp	Lock_tables	Create_view	Show_view_	Create_rout	Alter_routir	Execute_pri	Event_priv	Trigger_priv	password_l	account_loc	password_e
localhost	new_schem	newuser	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	2022-02-20 (	N	N
localhost	new_schem	user	Y	Y	Y	N	N	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	2022-02-21 (	N	N
localhost	performanc	mysql.sessi	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	2022-02-20 (	Y	N
localhost	sys	mysql.sys	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	2022-02-20 (	Y	N

Fuente: Elaboración propia (2022)

Este es un procedimiento almacenado sencillo, sin embargo, tiene todos los elementos esenciales que se pueden utilizar en una acción de RECON en una base de datos. Como se observa en la imagen anterior, el resultado brinda muchas columnas debido a que cada una representa una acción que el usuario puede ejecutar en el esquema.

Así mismo, se puede observar que con este resultado se capturan todos los usuarios de los esquemas dentro de la instancia, lo cual le otorga habilidad a la herramienta de gobernanza de datos para procesarlos y ejecutar acciones de acuerdo con las políticas organizacionales.

5.1.2 Aprovisionamiento de cuentas en MySQL

La propuesta para la estandarización del aprovisionamiento de cuentas en MySQL es la siguiente:

```
DELIMITER //
-- CREACIÓN DEL PROCEDIMIENTO ALMACENADO
CREATE PROCEDURE AccountManagement ( hostname varchar(10), p_login varchar(30),
p_schema varchar(20), p_password varchar(30),schema_privilege varchar(30),p_action
varchar(30))
BEGIN
-- ESTE COMANDO ES EXCLUSIVO CUANDO LA ACCIÓN ES "ADD"
    IF p_action = 'ADD'
    THEN
-- ESTOS COMANDOS SON PARA CREAR UN OBJETO DE USUARIO EN EL HOST/SERVIDOR SI ESTE
NO EXISTE
        SET @create_user = CONCAT('CREATE USER IF NOT EXISTS
',p_login,'@',hostname,' IDENTIFIED BY ','\'',p_password,'\'');
        PREPARE stmt_create FROM @create_user;
        EXECUTE stmt_create;
        DEALLOCATE PREPARE stmt_create;

-- ESTOS COMANDOS SON PARA CONCEDER UN SOLO ACCESO DE PRIVILEGIO AL USUARIO EN EL
ESQUEMA
        SET @grant_access = CONCAT('GRANT ',schema_privilege,' ON ',p_schema,'.* TO
',p_login,'@',hostname);
        PREPARE stmt_grant FROM @grant_access;
        EXECUTE stmt_grant;
        DEALLOCATE PREPARE stmt_grant;
    END IF;

-- ESTE COMANDO ES EXCLUSIVO CUANDO LA ACCIÓN ES 'DROP'
    IF p_action = 'DROP'
    THEN
-- ESTOS COMANDOS SON PARA ELIMINAR COMPLETAMENTE EL OBJETO DEL USUARIO EN EL
HOST/SERVIDOR
        SET @drop_user = CONCAT('DROP USER ',p_login,'@',hostname);
        PREPARE stmt_drop FROM @drop_user;
        EXECUTE stmt_drop;
        DEALLOCATE PREPARE stmt_drop;
    END IF;

-- ESTE COMANDO ES EXCLUSIVAMENTE CUANDO LA ACCIÓN ES 'DELETE'
    IF p_action = 'DELETE'
    THEN
-- ESTOS COMANDOS SON PARA ELIMINAR UN SOLO PRIVILEGIO PARA EL USUARIO EN EL
ESQUEMA
        SET @delete_access = CONCAT('REVOKE ',schema_privilege,' ON ',p_schema,'.*
FROM ',p_login,'@',hostname);
        PREPARE stmt_delete FROM @delete_access;
        EXECUTE stmt_delete;
        DEALLOCATE PREPARE stmt_delete;
    END IF;
END //
-- FINALIZACIÓN DEL PROCEDIMIENTO ALMACENADO
DELIMITER ;
```

En el procedimiento almacenado mostrado previamente se puede observar más lógica aplicada a la estrategia de control de acceso, ya que existen acciones concretas de ADD (Añadir), DELETE (Borrar), DROP (Eliminar). En múltiples

panoramas se podría utilizar este procedimiento almacenado. El cual se explica en la siguiente sección.

5.1.2.1 Aplicación Caso 1 MySQL

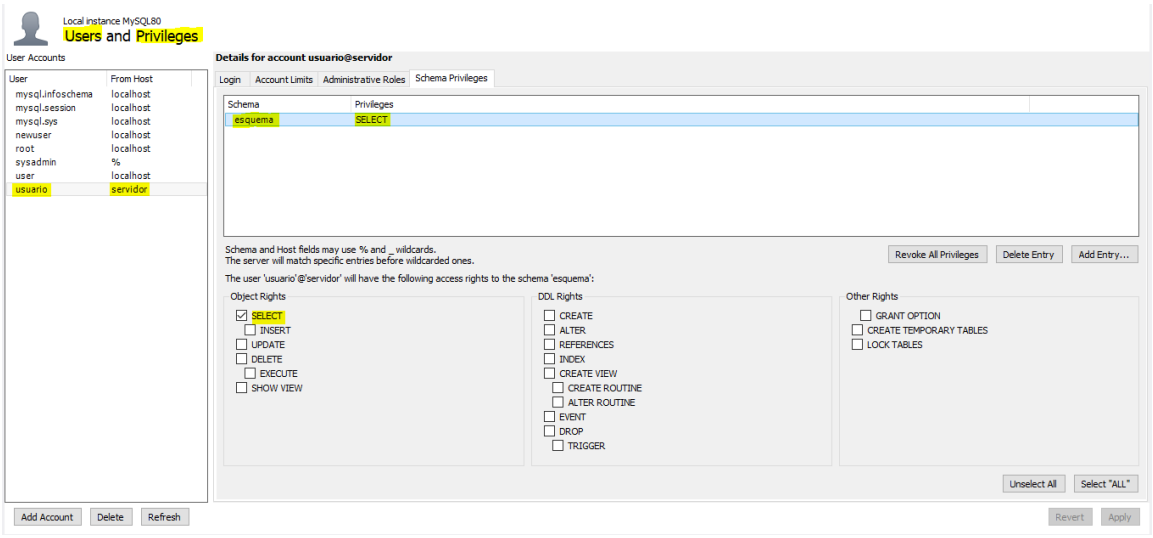
Para resolver este caso se ejecutará el siguiente comando:

```
CALL AccountManagement('servidor','usuario','esquema','contraseña','SELECT','ADD');
```

Este comando creará un usuario en el servidor sin ningún privilegio y añadirá este usuario al esquema seleccionado con la acción “SELECT”. En la siguiente imagen se muestra el resultado del procedimiento almacenado:

Figura 9

Usuario creado en el esquema correspondiente



Fuente: Elaboración propia (2022)

5.1.2.2 Aplicación Caso 2 MySQL

Para resolver este caso se ejecutarán los siguientes comandos:

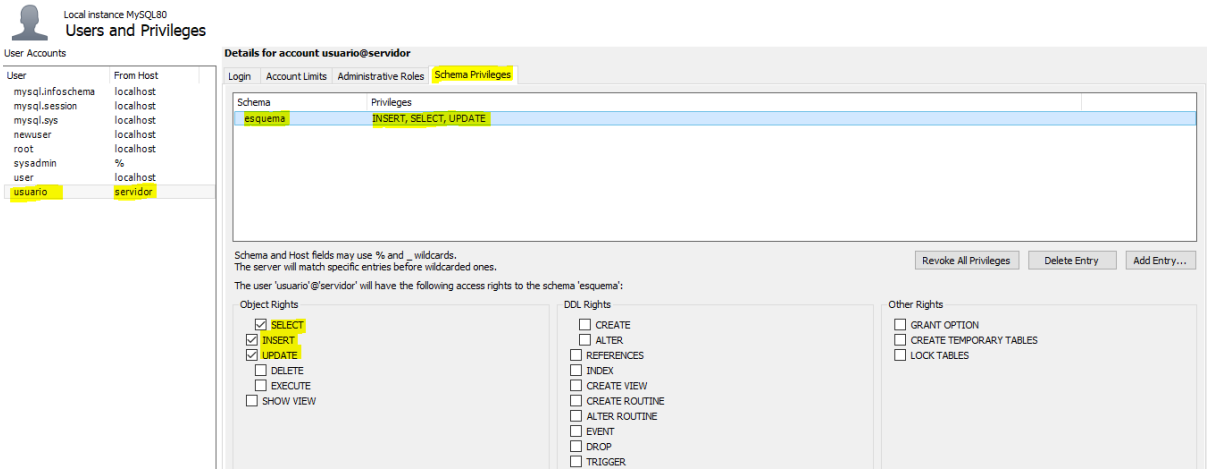
```
CALL AccountManagement('servidor','usuario','esquema','','INSERT','ADD');
CALL AccountManagement('servidor','usuario','esquema','','UPDATE','ADD');
```

Como se puede observar, son dos acciones diferentes, ya que el procedimiento almacenado otorga los privilegios individualmente. También, se puede advertir que el

campo asignado para la contraseña debe estar vacío, debido a que el usuario ya existe en el servidor. A continuación, se muestra el resultado del procedimiento almacenado:

Figura 10

Aprovisionamiento de accesos extras



Fuente: Elaboración propia (2022)

5.1.2.3 Aplicación Caso 3 MySQL

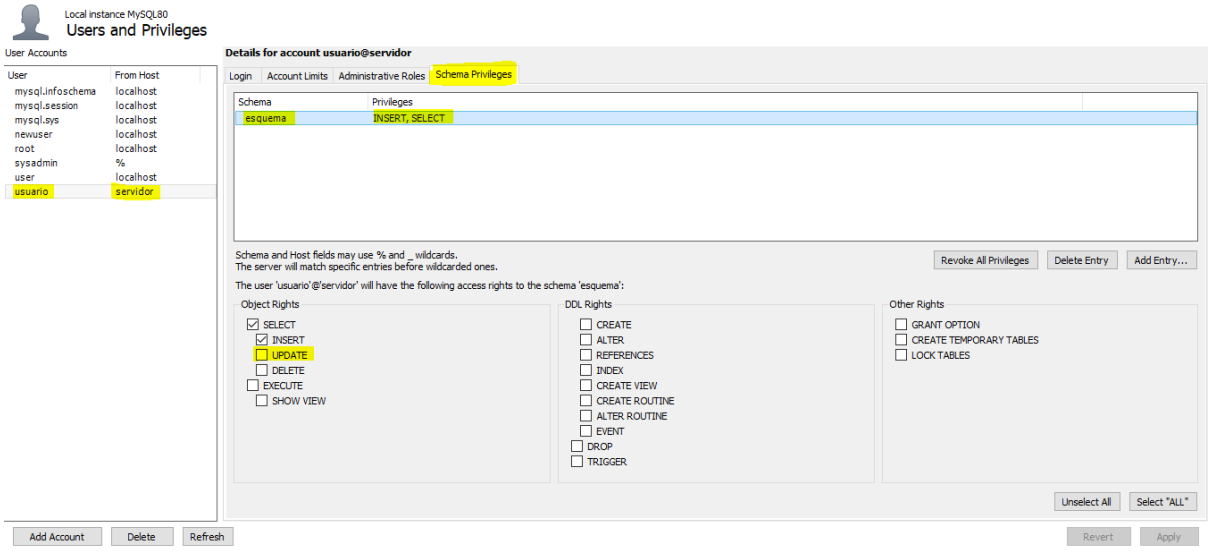
Para resolver este caso se ejecutarán los siguientes comandos:

```
CALL AccountManagement('servidor','usuario','esquema','','UPDATE','DELETE');
```

Nuevamente, se observa que la contraseña está vacía porque el usuario ya existe y ahora se utiliza el parámetro de DELETE para borrar un privilegio adquirido por el usuario en el esquema.

Figura 11

Deprovisionamiento de privilegios



Fuente: Elaboración propia (2022)

5.1.2.4 Aplicación Caso 4 MySQL

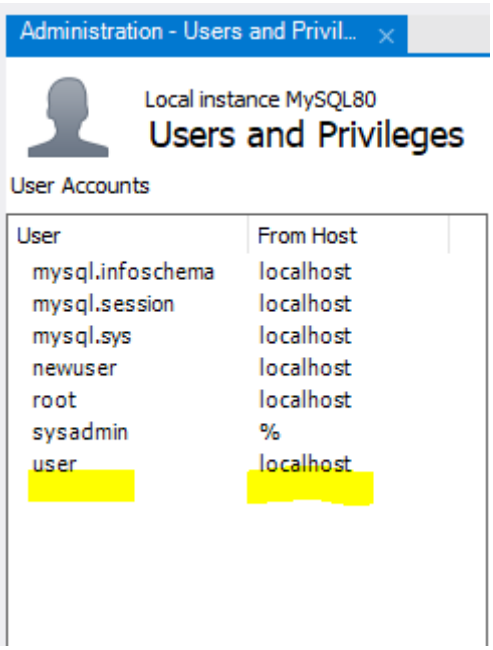
Para resolver este caso se ejecutarán los siguientes comandos:

```
CALL AccountManagement('servidor','usuario','esquema','','','DROP');
```

Aquí se observa que además de la contraseña,el espacio del privilegio está vacío, ya que se eliminará absolutamente todo privilegio del usuario dentro del esquema y del servidor.

Figura 12

Eliminación completa del usuario



Fuente: Elaboración propia (2022)

5.2 Microsoft SQL Server

A diferencia de MySQL este producto tiene más funcionalidades para brindar accesos por medio de roles, el cual es el método utilizado para automatizar los procesos de RECON y aprovisionamiento de cuentas. También, cuenta con la opción de manejar objetos externos del controlador de dominio, tanto individuales como grupales. Así mismo, Microsoft SQL Server tiene la posibilidad de brindar acceso mediante acciones en las tablas, sin embargo, dificulta más la aplicación de este estándar, por lo tanto, esa opción no será utilizada en esta solución.

En la lógica implementada en esta solución se incluyen, exclusivamente, opciones para otorgar acceso al usuario, por ejemplo, LOGIN en cual consiste en un acceso superficial al servidor donde se estará hospedando el objeto creado y a partir de ese LOGIN, se crea un usuario dentro de la base de datos para que pueda tener

el rol correspondiente. Finalmente, dentro de SQL Server existen usuarios locales, la diferencia de estos respecto a los del controlador de dominio es que, a la hora de crearlos, se debe de otorgar una contraseña de forma local, en cambio en el caso de los mencionados anteriormente, las contraseñas son manejadas de forma externa.

5.2.1 Reconciliación de usuarios en SQL Server

5.2.1.1 Creación del procedimiento almacenado

El script propuesto para poder desarrollar esta acción de RECON es el siguiente:

```
ALTER PROCEDURE GET_USERS_WITH_ACCESS_TO_SQLSERVER_SCHEMA
AS
BEGIN
--EN ESTE APARTADO SE REALIZA LA DECLARACIÓN DE LAS VARIABLES
--QUE SE EXTRAERÁN PARA CAPTURAR LA INFORMACIÓN DE LOS USUARIOS
DECLARE @DB_USers TABLE(DATABASE_NAME sysname,
                        USERNAME sysname null,
                        LOGIN_NAME sysname null,
                        TYPE sysname null,
                        DB_LOGIN_TYPE sysname null,
                        SERVER_LOGIN_TYPE sysname null,
                        DEFAULT_SCHEMA sysname null,
                        ROLE_ASSOCIATED varchar(max),
                        CREATED_DATE datetime,
                        MODIFY_DATE datetime,
                        HOSTNAME sysname)

--SE UTILIZA EL PROCEDIMIENTO ALMACENADO SP_MSFOREACHDB PARA
--RECORRER CADA UNA DE LAS BASES DE DATOS EN EL SISTEMA Y SE
--ALMACENAN EN LA VARIABLE QUE SE CREÓ ANTERIORMENTE
INSERT @DB_USers EXEC sp_MSforeachdb
                'use [?]
                SELECT ''?'' AS DATABASE_NAME
                ,DBP.name AS USERNAME
                ,SP.name AS LOGIN_NAME
                ,DBP.type AS TYPE
                ,DBP.type_desc AS DB_LOGIN_TYPE
                ,SP.type_desc AS SERVER_LOGIN_TYPE
                ,DBP.default_schema_name as DEFAULT_SCHEMA
                ,USER_NAME(DRM.role_principal_id) AS ROLE_ASSOCIATED
                ,DBP.create_date as CREATED_DATE
                ,DBP.modify_date as MODIFY_DATE
                ,(SELECT TOP 1 name
                    FROM [master].[sys].[servers]) HOSTNAME
                FROM sys.database_principals DBP
                LEFT OUTER JOIN sys.server_principals SP
                    ON SP.sid=DBP.sid
                LEFT OUTER JOIN sys.database_role_members DRM
                    ON DBP.principal_id=DRM.member_principal_id '

--COMANDO PARA TENER LA LECTURA DE LOS VALORES QUE SE RECOLECTARON EN LA EJECUCIÓN
ANTERIOR.
SELECT  USERS.*,last_log.last_logged_in
FROM @DB_USers USERS
--ESTA CORRELACIÓN FUE REALIZADA PARA OBTENER LA ÚLTIMA CONEXIÓN DEL USUARIO
LEFT JOIN (SELECT login_name, max(login_time) as last_logged_in
            FROM sys.dm_exec_sessions
            GROUP BY login_name) last_log ON last_log.login_name = USERS.LOGIN_NAME
WHERE USERS.DB_LOGIN_TYPE NOT IN ('DATABASE_ROLE','CERTIFICATE_MAPPED_USER','')
AND USERS.USERNAME NOT LIKE '##%'
END
GO
```

5.2.1.2 Ejecución del procedimiento almacenado

La llamada de este procedimiento almacenado es el siguiente:

```
EXEC GET_USERS_WITH_ACCESS_TO_SQLSERVER_SCHEMA
```

Este comando brindaría un resultado como el que se muestra a continuación:

Figura 13

Resultado ejecución del RECON en SQL Server

Results | Messages

	DATABASE_NAME	USERNAME	LOGIN_NAME	TYPE	DB_LOGIN_TYPE	SERVER_LOGIN_TYPE	DEFAULT_SCHEMA	ROLE_ASSOCIATED	CREATED_DATE	MODIFY_DATE	HOSTNAME	last_logged_in
21	msdb	MS_DataCollectorIntern...	NULL	S	SQL_USER	NULL	dbo	dc_admin	2019-09-24 14:21:49.847	2019-09-24 14:21:49.847	COMPUTER	NULL
22	test_db	dbo	LAB\helpdesk	U	WINDOWS_US...	WINDOWS_LOGIN	dbo	db_owner	2003-04-08 09:10:42.287	2022-02-08 23:08:37.143	COMPUTER	2022-02-24 22:07:47.893
23	test_db	guest	NULL	S	SQL_USER	NULL	guest	NULL	2003-04-08 09:10:42.317	2003-04-08 09:10:42.317	COMPUTER	NULL
24	test_db	INFORMATION_SCHEMA	NULL	S	SQL_USER	NULL	NULL	NULL	2009-04-13 12:59:11.717	2009-04-13 12:59:11.717	COMPUTER	NULL
25	test_db	sys	NULL	S	SQL_USER	NULL	NULL	NULL	2009-04-13 12:59:11.717	2009-04-13 12:59:11.717	COMPUTER	NULL
26	test_db	test_account	NULL	S	SQL_USER	NULL	dbo	NULL	2022-02-09 00:46:36.947	2022-02-09 00:46:36.947	COMPUTER	NULL
27	lablocal	dbo	LAB\helpdesk	U	WINDOWS_US...	WINDOWS_LOGIN	dbo	db_owner	2003-04-08 09:10:42.287	2022-02-09 00:30:16.423	COMPUTER	2022-02-24 22:07:47.893
28	lablocal	guest	NULL	S	SQL_USER	NULL	guest	NULL	2003-04-08 09:10:42.317	2003-04-08 09:10:42.317	COMPUTER	NULL
29	lablocal	INFORMATION_SCHEMA	NULL	S	SQL_USER	NULL	NULL	NULL	2009-04-13 12:59:11.717	2009-04-13 12:59:11.717	COMPUTER	NULL
30	lablocal	sys	NULL	S	SQL_USER	NULL	NULL	NULL	2009-04-13 12:59:11.717	2009-04-13 12:59:11.717	COMPUTER	NULL
31	lablocal	LAB\LABuser1	NULL	U	WINDOWS_US...	NULL	guest	NULL	2022-02-09 22:59:49.103	2022-02-09 22:59:49.103	COMPUTER	NULL
32	lablocal	LAB\ad_db	LAB\ad_db	G	WINDOWS_GR...	WINDOWS_GROUP	db_datawriter	db_datawriter	2022-02-15 19:52:20.163	2022-02-15 19:52:20.163	COMPUTER	NULL
33	AdventureWorks2...	dbo	NULL	U	WINDOWS_US...	NULL	dbo	db_owner	2003-04-08 09:10:42.287	2017-10-27 14:33:01.273	COMPUTER	NULL
34	AdventureWorks2...	guest	NULL	S	SQL_USER	NULL	guest	NULL	2003-04-08 09:10:42.317	2003-04-08 09:10:42.317	COMPUTER	NULL

Fuente: Elaboración propia (2022)

La ejecución del procedimiento almacenado creado para este producto y para desarrollar el proceso de RECON brinda información muy valiosa en su resultado, ya que, puede utilizarse para implementar una gobernanza más compacta del control de accesos en este producto de base de datos. Como se puede observar, el procedimiento almacenado extrae dinámicamente todos los usuarios de todas las bases de datos que existen en el servidor con su respectivo tipo de usuario, lo cual es necesario para identificar si la cuenta es de un individuo o grupo de Active Directory, Local o bien un rol establecido.

También, se puede observar en las diferentes columnas qué tipo de rol se tiene asignado, cuándo fue creada y la ubicación física de la base de datos. Con toda esta información se puede desarrollar una lógica dentro de la herramienta de control de accesos en la cual se verifique si la persona tiene el rol correcto dentro de la base de datos.

5.2.2 Aprovisionamiento de cuentas en SQL Server

La propuesta para la estandarización del aprovisionamiento de cuentas en SQL Server es la siguiente:

```
CREATE PROCEDURE AccountManagement @Type varchar(10), @login varchar(30), @database
varchar(20), @password varchar(30),@role varchar(30),@action varchar(30)
AS
BEGIN
    --ESTE COMANDO ES EXCLUSIVAMENTE CUANDO LA ACCIÓN ES 'CREAR'
    IF @action = 'CREATE'
        BEGIN
         --ELEGIR SI EL USUARIO A CREAR ES UN USUARIO DEL
         --DIRECTORIO ACTIVO O UN USUARIO LOCAL
            --LA LÓGICA DEL USUARIO DE AD INICIA
            IF @Type='Windows'
            BEGIN
                DECLARE @cmd_windows varchar(200)
                --COMANDO DE CREACIÓN DE LA SESIÓN (PRIMER PASO)
                 SET @cmd_windows = 'CREATE LOGIN ['+@login +']
                                     FROM WINDOWS WITH
                                     DEFAULT_DATABASE=[master]'
                --TRY LOOP
                BEGIN TRY
                    --CREAR LA EJECUCIÓN DEL COMANDO DE INICIO DE SESIÓN
                    IF NOT EXISTS(SELECT * FROM SYS.server_principals
                        WHERE name = @login)
                        BEGIN
                            EXEC (@cmd_windows)
                        END
                END TRY
                --CATCH ERROR
                BEGIN CATCH
                       SELECT
                        ERROR_MESSAGE() AS ErrorMessage;
                END CATCH
            END
            --LA LÓGICA DEL USUARIO DE AD INICIA FINALIZA
            ELSE
                --AUTENTICACIÓN SQL SERVER AUTHENTICATION/USUARIO LOCAL
                 --/CUENTA DE SERVICIO LÓGICA INICIAL
                IF @Type='Local'
                BEGIN
                    DECLARE @cmd_local varchar(200)
                    --COMANDO DE CREACIÓN DE LA SESIÓN (PRIMER PASO)
                    set @cmd_local = '
                        CREATE LOGIN ['+@login+']
                        WITH PASSWORD = '''+@password+''',
                        DEFAULT_DATABASE = [master],
                        CHECK_POLICY = OFF,
                        CHECK_EXPIRATION = OFF ; '
                        --TRY LOOP
                        BEGIN TRY
                            EXEC (@cmd_local)
                        END TRY
                           --CATCH ERROR
                        BEGIN CATCH
                            PRINT ERROR_MESSAGE()
                        END CATCH
                END
                --AUTENTICACIÓN SQL SERVER AUTHENTICATION/USUARIO LOCAL
                 --/CUENTA DE SERVICIO LÓGICA FINALIZA
```

```
                    DECLARE @create_user varchar(500)
                    SET @create_user = ('USE '+@database+';
                                        CREATE USER ['+@login+']
                                        FOR LOGIN ['+@login+'];
                                        USE '+@database+';
                                        ALTER USER ['+@login+']
                                        WITH DEFAULT_SCHEMA='+@role+';
                                        ALTER ROLE ['+@role+']
                                        ADD MEMBER ['+@login+']')
                    EXEC (@create_user)
        END

    --ESTE COMANDO ES EXCLUSIVO CUANDO LA ACCIÓN ES 'MODIFICAR'
    --'MODIFICAR' ES NECESARIO CUANDO LA CUENTA YA EXISTE Y SE REQUIERE AÑADIR UN
NUEVO ROL EN EL PERFIL DE LA CUENTA
    IF @action = 'MODIFY'
    BEGIN
        DECLARE @modify_user varchar(500)
        SET @modify_user = ('USE '+@database+';
                            ALTER ROLE ['+@role+']
                            ADD MEMBER ['+@login+']')
        EXEC (@modify_user)
    END
    --ESTE COMANDO ES EXCLUSIVAMENTE CUANDO LA ACCIÓN ES 'DELETE'
    --'DELETE' ES LA ACCIÓN PARA BORRAR EXCLUSIVAMENTE UN ROL DEL PERFIL DEL
USUARIO, NO BORRARÁ LA CUENTA DE LA BASE DE DATOS O EL LOGIN
    IF @action = 'DELETE'
    BEGIN
        DECLARE @delete_role varchar(500)
        SET @delete_role = ('USE '+@database+'; ALTER ROLE ['+@role+'] DROP MEMBER
['+@login+']')
        EXEC (@delete_role)
    END
    --ESTE COMANDO ES, EXCLUSIVAMENTE, CUANDO LA ACCIÓN ES 'DROP'
    --'DROP' BORRARA COMPLETAMENTE EL USUARIO Y LA SESIÓN DE LA BASE DE DATOS
    IF @action = 'DROP'
    BEGIN
        DECLARE @drop_user varchar(500)
        --ELIMINAR LOS ROLES Y LA CUENTA DE USUARIO DE LA BASE DE DATOS
        SET @drop_user = ('USE '+@database+'; DROP USER ['+@login+']')
        EXEC (@drop_user)
        --ELIMINAR LA CUENTA DE ACCESO DEL PROPIO SERVIDOR
        SET @drop_user = ('USE [master];


                          IF EXISTS (SELECT name
                           FROM master.sys.server_principals
                           WHERE name = '''+@login+''')
                          BEGIN
                           DROP LOGIN ['+@login+']
                          END')

        EXEC (@drop_user)
    END
END
```

Como se puede observar este procedimiento almacenado contiene más elementos de los que existen en la sección anterior sobre MySQL, aunque, se pueden observar las acciones ADD (Añadir), DELETE (Borrar), DROP (Eliminar), se deben incluir más comandos para la creación del objeto “login” dentro del servidor y así otorgarle un acceso y finalmente crear el usuario dentro de la base de datos.

En el comando anterior se aprecia que existen usuarios que pertenecen a un dominio lo cual extiende la lógica que se debe implementar en el código. A continuación, se explicarán los casos en los que se pueden utilizar estos procedimientos almacenados para el correcto control de accesos en este tipo de bases de datos.

5.2.2.1 Aplicación Caso 1 SQL Server

5.2.2.1.1 Acceso a usuario con objeto de Active Directory

Para las situaciones enlistadas en el apartado anterior la solución sería ejecutar el siguiente comando:

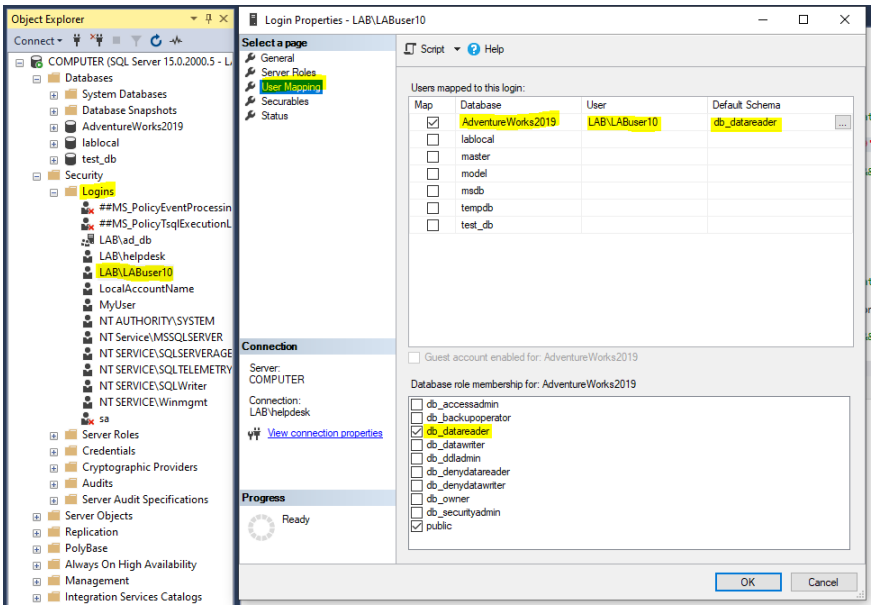
```
EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\LABuser10'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_datareader'
      ,@action = 'CREATE'
```

Este comando creará un login en el servidor y añadirá, además, un usuario homónimo con acceso a la base de datos y con el rol de 'db_datareader'. No obstante, se debe tomar en cuenta que en el @login debe añadirse el dominio (Dominio\Usuario) y, además se debe enviar la opción de @password vacía ya que la contraseña se maneja mediante Active Directory.

Por último, 'db_datareader' es un rol definido por defecto en el producto de Microsoft y se debe específicar el tipo como “Windows” para mostrarle al procedimiento almacenado que el usuario pertenece al dominio. Seguidamente, se muestra la sesión creada en el servidor y el usuario en la base de datos:

Figura 14

Sesión creada en el servidor

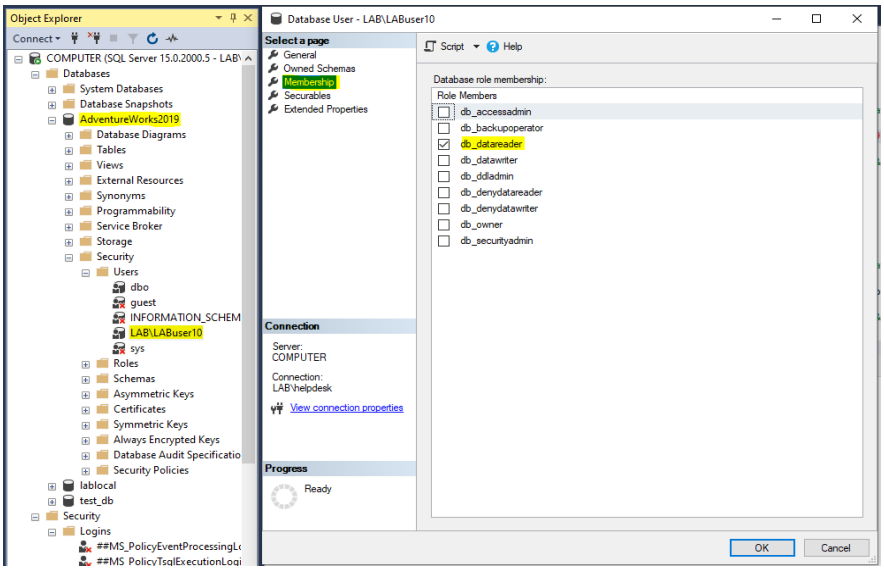


Fuente: Elaboración propia (2022)

La imagen anterior muestra cómo el comando que se ejecutó en este caso crea o exporta un usuario del Active Directory y le brinda accesos con sus respectivos roles.

Figura 15

Usuario creado en la base de datos



Fuente: Elaboración propia (2022)

Como se aprecia en la imagen anterior, a partir de la sesión creada en el servidor se genera un usuario dentro de la base de datos, en el cual se brinda el acceso correspondiente. Otro detalle para tomar en cuenta es que, este proceso no brinda acceso a todas las bases de datos, con el propósito de mejorar el control de accesos y otorgar, solamente, los privilegios que el usuario necesita para desarrollar sus actividades diarias.

5.2.2.1.2 Acceso a usuario local o cuenta de servicio

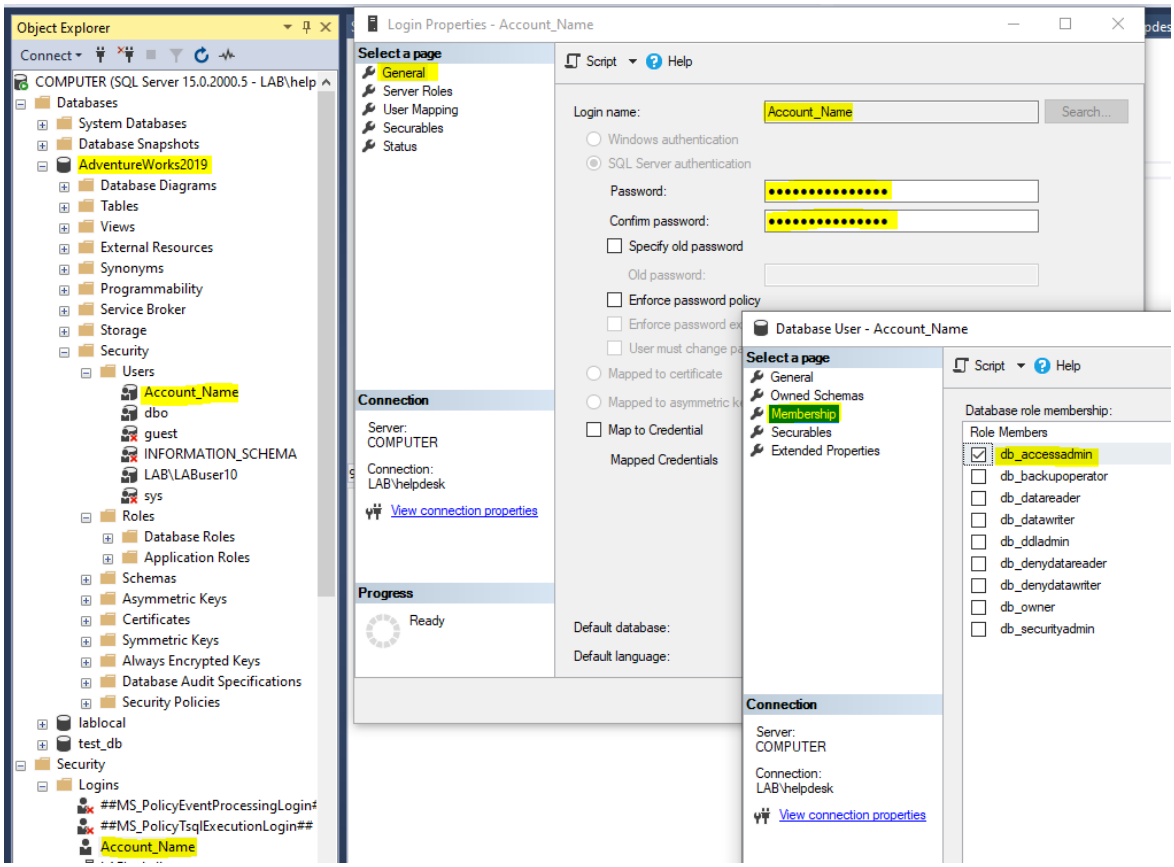
En este apartado se muestra cómo se otorgaría acceso a un usuario que no tiene un objeto en el Active Directory, estas cuentas suelen emplearse para usuarios externos, contratistas, cuentas de servicio o robots. La ejecución se desarrollaría de la siguiente manera:

```
EXEC AccountManagement
      @Type = 'Local'
      ,@login = 'Account_Name'
      ,@database = 'AdventureWorks2019'
      ,@password = 'StrongPassword123!'
      ,@role = ' db_accessadmin'
      ,@action = 'CREATE'
```

Las principales diferencias de este comando y que se presentó en la sección anterior es que el @Type debe ser representado como “Local”, esto para darle a conocer al procedimiento almacenado que el usuario no es parte del dominio, también el @login tiene un nombre completamente personalizado, no es necesario que lleve el dominio al inicio, y por último debe llevar una contraseña para otorgársela al usuario creado. El resultado es el siguiente:

Figura 16

Sesión creada en el servidor y usuario en la base datos



Fuente: Elaboración propia (2022)

El usuario local tiene el mismo comportamiento en la creación que el usuario con un objeto en el Active Directory, la única diferencia es que la contraseña se maneja por medio de la base de datos y no configurada de forma externa.

5.2.2.2 Aplicación Caso 2 SQL Server

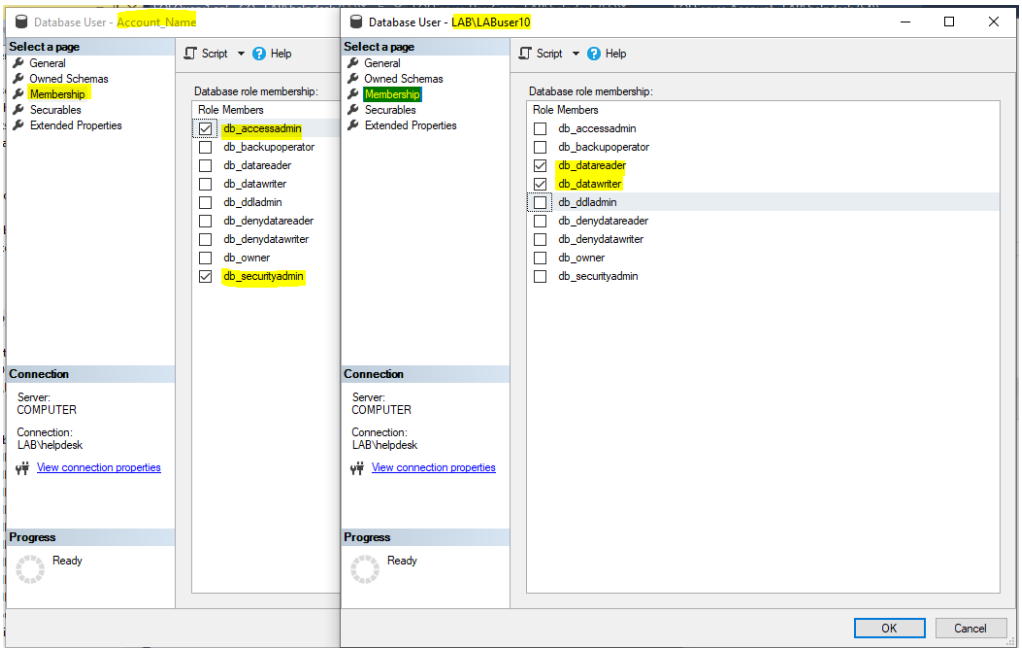
Para resolver este caso se ejecutará el siguiente comando:

```
EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\LABuser10'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_datawriter'
      ,@action = 'MODIFY'

EXEC AccountManagement
      @Type = 'Local'
      ,@login = 'Account_Name'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_securityadmin'
      ,@action = 'MODIFY'
```

Como se puede observar, la estrategia es la misma para ambos casos, ya sea una cuenta local o un usuario de Active Directory. En ninguno de los casos se agrega la contraseña, con lo cual el rol seleccionado se añade a su perfil de cuenta en la base de datos respectiva. Además, cabe mencionar que la sesión que ya existía no sufriría ninguna modificación, ya que la asignación del rol se realiza en la base de datos.

Figura 17

Modificación de los usuarios creados anteriormente



Fuente: Elaboración propia (2022)

5.2.2.3 Aplicación Caso 3 SQL Server

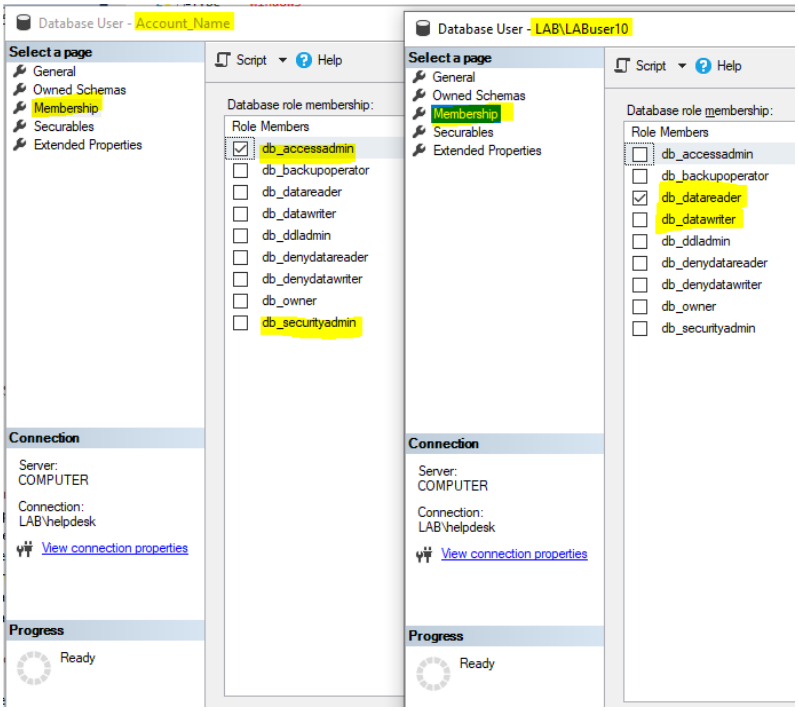
Para resolver este caso se ejecutará el siguiente comando:

```
EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\LABuser10'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_datawriter'
      ,@action = 'DELETE'

EXEC AccountManagement
      @Type = 'Local'
      ,@login = 'Account_Name'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_securityadmin'
      ,@action = 'DELETE'
```

Similar a lo observado en el caso anterior, en este ejercicio solamente se está removiendo el acceso que se otorgó anteriormente, sin modificar la sesión, simplemente se está borrando uno de los roles que se solicitaron anteriormente. Al igual que el caso anterior, no es necesario agregar la contraseña.

Figura 18

Eliminación de privilegios en usuarios de bases de datos



Fuente: Elaboración propia (2022)

5.2.2.4 Aplicación Caso 4 SQL Server

Para resolver este caso se ejecutará el siguiente comando:

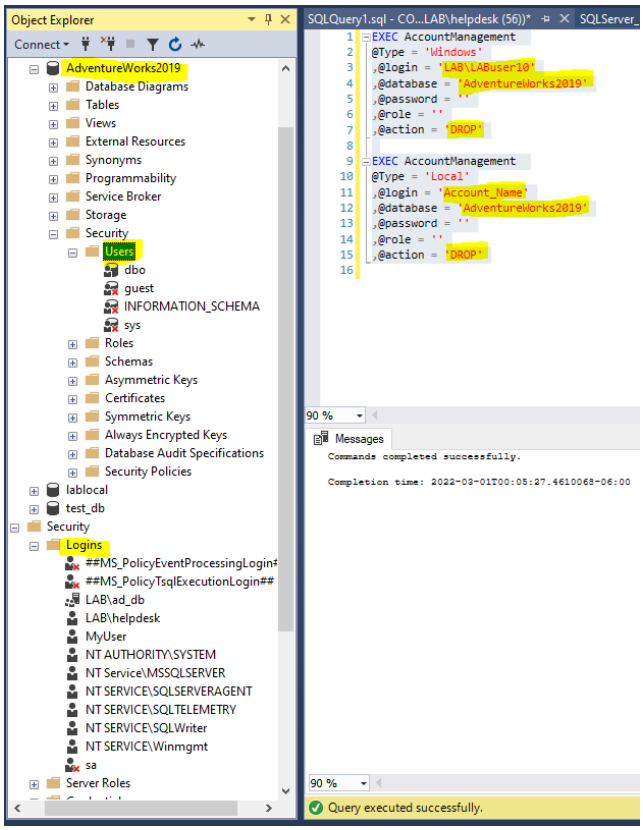
```
EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\LABuser10'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = ''
      ,@action = 'DROP'

EXEC AccountManagement
      @Type = 'Local'
      ,@login = 'Account_Name'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = ''
      ,@action = 'DROP'
```

En ambos casos el comportamiento es el mismo, ninguno requiere enviar parámetros de contraseñas ni roles seleccionados anteriormente, ya que este comando remueve todo el registro de estos usuarios, tanto a nivel de base de datos

como de servidor. Es importante mencionar que, para el caso del usuario de Active Directory, no se elimina el objeto del dominio, únicamente se remueve la sesión del servidor y la cuenta de la base de datos.

Figura 19

Remoción completa de los usuarios de la base de datos y la sesión



Fuente: Elaboración propia (2022)

5.2.2.5 Bonus track

En los casos mencionados previamente se observa cómo se podían controlar los accesos por medio de objetos en el Active Directory. Si bien, la demostración se realizó en usuarios individuales, también se puede utilizar la misma metodología aplicada a control de grupos de Active Directory, según los requerimientos de la empresa.

Además, se pueden crear sesiones y usuarios en la base de datos, modificar el acceso del grupo. También, se pueden remover privilegios y, por último, se puede eliminar completamente la sesión y el acceso a la base de datos a un grupo de Active Directory. Para las tareas anteriores los comandos serían los mismos presentados anteriormente, la única modificación consiste en colocar el nombre del grupo:

```
EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\ad_db'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_datareader'
      ,@action = 'CREATE'

EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\ad_db'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_datawriter'
      ,@action = 'MODIFY'

EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\ad_db'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = 'db_datawriter'
      ,@action = 'DELETE'

EXEC AccountManagement
      @Type = 'Windows'
      ,@login = 'LAB\ad_db'
      ,@database = 'AdventureWorks2019'
      ,@password = ''
      ,@role = ''
      ,@action = 'DROP'
```

Con esta característica implementada también se puede satisfacer o adaptar la solución propuesta a las diversas variables organizacionales, según las necesidades de la compañía.

5.3 Oracle

Esta herramienta se puede utilizar como una combinación de las soluciones implementadas en MySQL y SQL Server, pues en Oracle también se encuentran esquemas definidos y se pueden otorgar accesos locales como en MySQL. Además, se puede asignar roles y brindar accesos mediante objetos de Active Directory como en SQL Server.

Ahora bien, el tipo de escritura en los procedimientos almacenados tiene similitud con ambas plataformas, no obstante, se debe tomar en cuenta que existen muchos aspectos lógicos que se deben modificar a la hora de implementar el código en este producto.

5.3.1 Reconciliación de usuarios en Oracle

5.3.1.1 Creación del procedimiento almacenado

El script propuesto para poder desarrollar esta acción de RECON es el siguiente:

```
CREATE OR REPLACE PROCEDURE GET_USERS_WITH_ACCESS_TO_ORACLE_SCHEMA AS
q SYS_REFCURSOR;
 BEGIN
    OPEN q FOR
            SELECT *
            FROM (
            -- ESTE APARTADO MUESTRA LOS USUARIOS Y SUS
            -- ROLES DENTRO DEL ESQUEMA
                SELECT DRP.GRANTEE AS USERNAME,
                    DRP.GRANTED_ROLE AS ROLE,
                    DRP.ADMIN_OPTION,
                    DU.ACCOUNT_STATUS,
                    DU.EXPIRY_DATE,
                    DU.DEFAULT_TABLESPACE,
                    DU.CREATED,
                    DU.AUTHENTICATION_TYPE,
                    DU.LAST_LOGIN,
                    DU.PASSWORD_CHANGE_DATE,
                    (SELECT SYS_CONTEXT('USERENV','IP_ADDRESS')
                        FROM dual) AS IP_ADDRESS
                FROM DBA_ROLE_PRIVS DRP
                LEFT JOIN DBA_USERS DU
                    ON DRP.GRANTEE = DU.USERNAME
                UNION
            -- ESTE APARTADO MUESTRA LOS USUARIOS Y SUS
            -- PRIVILEGIOS DENTRO DEL SISTEMA
                SELECT DRP.GRANTEE AS USERNAME,
                    DRP.PRIVILEGE AS ROLE,
                    DRP.ADMIN_OPTION,
                    DU.ACCOUNT_STATUS,
                    DU.EXPIRY_DATE,
                    DU.DEFAULT_TABLESPACE,
                    DU.CREATED,
                    DU.AUTHENTICATION_TYPE,
                    DU.LAST_LOGIN,
                    DU.PASSWORD_CHANGE_DATE,
                    (SELECT SYS_CONTEXT('USERENV','IP_ADDRESS')
                        FROM dual) AS IP_ADDRESS
                FROM DBA_SYS_PRIVS DRP
                LEFT JOIN DBA_USERS DU
                    ON DRP.GRANTEE = DU.USERNAME
                )
                ORDER BY USERNAME;
     DBMS_SQL.return_result (q);
END;
```

5.3.1.2 Ejecución del procedimiento almacenado

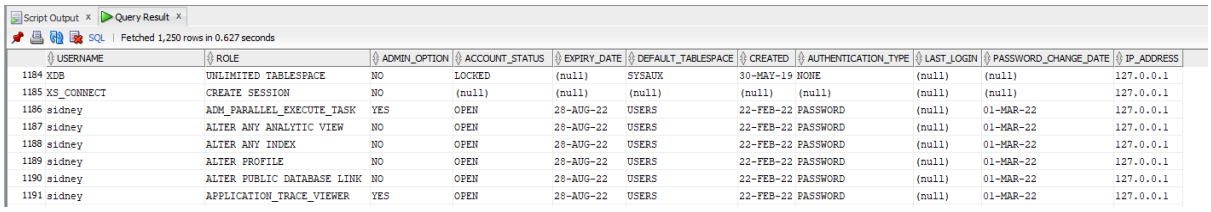
La llamada de este procedimiento almacenado es la siguiente:

```
EXECUTE GET_USERS_WITH_ACCESS_TO_ORACLE_SCHEMA();
```

Este comando brindaría un resultado como el siguiente:

Figura 20

Resultado ejecución del RECON en Oracle



Script Output | Query Result

Fetched 1,250 rows in 0.627 seconds

	USERNAME	ROLE	ADMIN_OPTION	ACCOUNT_STATUS	EXPIRY_DATE	DEFAULT_TABLESPACE	CREATED	AUTHENTICATION_TYPE	LAST_LOGIN	PASSWORD_CHANGE_DATE	IP_ADDRESS
1184	XDB	UNLIMITED TABLESPACE	NO	LOCKED	(null)	SYSAUX	30-MAY-19	NONE	(null)	(null)	127.0.0.1
1185	XS_CONNECT	CREATE SESSION	NO	(null)	(null)	(null)	(null)	(null)	(null)	(null)	127.0.0.1
1186	sidney	ADM_PARALLEL_EXECUTE_TASK	YES	OPEN	28-AUG-22	USERS	22-FEB-22	PASSWORD	(null)	01-MAR-22	127.0.0.1
1187	sidney	ALTER ANY ANALYTIC VIEW	NO	OPEN	28-AUG-22	USERS	22-FEB-22	PASSWORD	(null)	01-MAR-22	127.0.0.1
1188	sidney	ALTER ANY INDEX	NO	OPEN	28-AUG-22	USERS	22-FEB-22	PASSWORD	(null)	01-MAR-22	127.0.0.1
1189	sidney	ALTER PROFILE	NO	OPEN	28-AUG-22	USERS	22-FEB-22	PASSWORD	(null)	01-MAR-22	127.0.0.1
1190	sidney	ALTER PUBLIC DATABASE LINK	NO	OPEN	28-AUG-22	USERS	22-FEB-22	PASSWORD	(null)	01-MAR-22	127.0.0.1
1191	sidney	APPLICATION_TRACE_VIEWER	YES	OPEN	28-AUG-22	USERS	22-FEB-22	PASSWORD	(null)	01-MAR-22	127.0.0.1

Fuente: Elaboración propia (2022)

El desarrollo de esta solución para el proceso de RECON en el producto de Oracle está basado en los principios que definen los accesos dentro de los esquemas los cuales son roles otorgados y privilegios del sistema, es por esto que, se puede ver la función UNION dentro de los comandos, pues la tabla de DBA_ROLE_PRIVS contiene la información de los usuarios y sus roles. Por otro lado, se consulta la tabla DBA_SYS_PRIVS DRP que contiene los usuarios y sus distintos privilegios dentro del sistema.

Adicionalmente, se establecen correlaciones con la tabla de usuarios que contiene información general de los mismos y, a partir de ahí, se pueden encontrar datos como: cuándo fueron creados, cuándo fue la última vez que la contraseña expiró, cuándo expira la cuenta y cuál es la IP del servidor donde está localizado el producto de Oracle.

Con toda esta información se puede crear una lógica en la cual se puedan correlacionar las cuentas con identidades dentro del sistema de gobernanza de la información y generar alertas al usuario para que cambie su contraseña, si es

necesario, o se podrían integrar funciones para identificar usuarios que no deberían tener un acceso de administrador.

5.3.2 Aprovisionamiento de cuentas en Oracle

La propuesta para la estandarización del aprovisionamiento de cuentas en Oracle es la siguiente:

```
CREATE OR REPLACE PROCEDURE AccountManagement (p_type varchar2,
p_windows_login varchar2, admin_option varchar2, p_login varchar2,
p_password varchar2, schema_privilege varchar2, p_action varchar2)
AS
l_count NUMBER;
BEGIN
--ESTE COMANDO ES EXCLUSIVAMENTE CUANDO LA ACCIÓN ES 'CREAR'
IF p_action = 'ADD'
THEN
    --ESTE PASO ES NECESARIO PARA VERIFICAR SI EL USUARIO EXISTE O NO

    select count(*) INTO l_count from dba_users where
username=UPPER(p_login);
    IF (l_count=0)
    THEN
        IF p_type = 'Local'
        THEN
       --SI EL USUARIO NO EXISTE ESTOS COMANDOS SON NECESARIOS PARA CREARLO

            EXECUTE IMMEDIATE ('alter session set "_ORACLE_SCRIPT"=true');
            EXECUTE IMMEDIATE ('CREATE USER '||p_login||' IDENTIFIED BY
'||p_password);
            EXECUTE IMMEDIATE ('GRANT CONNECT TO '||p_login);
        END IF;
        IF p_type = 'Windows'
        THEN
       --SI EL USUARIO NO EXISTE ESTOS COMANDOS SON NECESARIOS PARA CREARLO

            EXECUTE IMMEDIATE ('alter session set "_ORACLE_SCRIPT"=true');
            EXECUTE IMMEDIATE ('CREATE USER '||p_login||' IDENTIFIED
EXTERNALLY AS '''||p_windows_login||''''');
            EXECUTE IMMEDIATE ('GRANT CONNECT TO '||p_login);
        END IF;
    END IF;
    --ESTA LÓGICA SE APLICA SI EL ACCESO REQUIERE EL NIVEL DE OPCIÓN ADMIN

    IF (admin_option = 'true')
    THEN
        EXECUTE IMMEDIATE ('GRANT '||schema_privilege||' TO '||p_login||'
WITH ADMIN OPTION');
    END IF;
    IF (admin_option = 'false')
    THEN
        EXECUTE IMMEDIATE ('GRANT '||schema_privilege||' TO '||p_login);
    END IF;

END IF;
```

```
-- ESTE COMANDO ES EXCLUSIVAMENTE CUANDO LA ACCIÓN ES 'DELETE'

IF p_action = 'DELETE'
THEN
    --ESTA ACCIÓN ELIMINA EL ACCESO SELECCIONADO PARA EL USUARIO
    --PERO NO ELIMINA LA CUENTA DEL ESQUEMA

    EXECUTE IMMEDIATE ('REVOKE '||schema_privilege||' FROM '||p_login);
END IF;

-- ESTE COMANDO ES EXCLUSIVO CUANDO LA ACCIÓN ES 'DROP'

IF p_action = 'DROP'
THEN
    --ESTE COMANDO ES EXCLUSIVAMENTE CUANDO LA ACCIÓN ES 'DROP'
    --'DROP' BORRARÁ COMPLETAMENTE EL USUARIO Y LA SESIÓN DE LA BASE DE DATOS

    EXECUTE IMMEDIATE ('DROP USER '||p_login||' CASCADE');
END IF;

END AccountManagement;
/
```

Este procedimiento almacenado es similar al que se utilizó para SQL Server, ya que esencialmente tiene la misma estructura. Sin embargo, existen diferencias sustanciales en la sintaxis del código. A continuación, se precisan las dos diferencias más pronunciadas:

1) **p_windows_login:** este nuevo parámetro debe contener el nombre del objeto en el Active Directory si es un usuario externo de Oracle. La estructura debe ser: **usuario@dominio**.

2) **admin_option:** este parámetro tiene dos valores: ‘true’ o ‘false’. Los cuales hacen referencia a los valores booleanos (verdadero o falso), estos serán seleccionados si el usuario necesita, o no, que el rol o acceso que se está seleccionando requiere permisos elevados.

Es importante mencionar que, en el parámetro schema_privilege se puede seleccionar un acceso a nivel de GRANTED_ROLE o de SYSTEM_PRIVILEGE. La lista completa de estos niveles se puede encontrar en (Oracle, s. f.)

5.3.2.1 Aplicación Caso 1 Oracle

Para resolver este caso se ejecutará el siguiente comando:

Para los casos anteriores el usuario requiere GRANTED_ROLES sin opción de administrador y adicionalmente necesita SYSTEM_PRIVILEGE con opción de administrador.

5.3.2.1.1 Acceso a usuario con objeto de Active Directory

Para los casos planteados anteriormente, la solución sería ejecutar el siguiente comando:

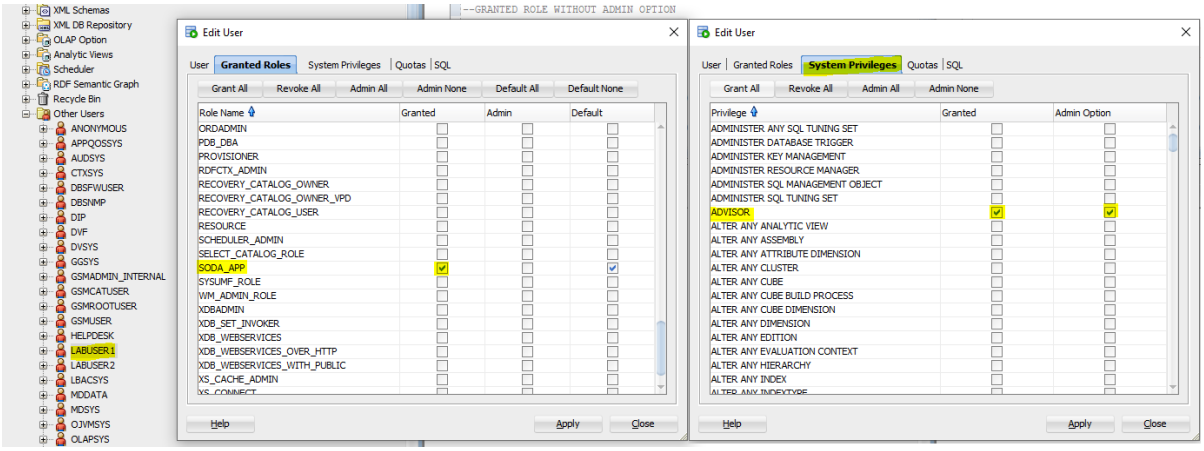
```
EXECUTE AccountManagement (/*p_type=*/'Windows',
/*p_windows_login =*/'LABuser1@lab.local',
/*admin_option =*/'false',
/*p_login =*/'LABuser1',
/*p_password =*/'',
/*schema_privilege =*/'SODA_APP',
/*p_action =*/'ADD');

EXECUTE AccountManagement (/*p_type=*/'Windows',
/*p_windows_login =*/'LABuser1@lab.local',
/*admin_option =*/'true',
/*p_login =*/'LABuser1',
/*p_password =*/'',
/*schema_privilege =*/'ADVISOR',
/*p_action =*/'ADD');
```

Para esta demostración se observa que la variación de la ejecución se da en los parámetros de **schema_privilege** y **admin_option** los cuales definen los accesos del usuario y sus niveles. También, se puede observar que, como es un usuario de Active Directory, no es necesario configurar una contraseña, pues esta se maneja de forma externa.

El resultado de esta ejecución es el siguiente:

Figura 21

Sesión creada en el servidor



Fuente: Elaboración propia (2022)

5.3.2.1.2 Acceso a usuario local o cuenta de servicio

En este apartado se muestra cómo se otorgaría acceso a un usuario que no tiene un objeto en el Active Directory, mayoritariamente estas cuentas son para usuarios externos, contratistas, cuentas de servicio o robots. La ejecución se del siguiente comando sería la propuesta para este tipo de usuario:

```
EXECUTE AccountManagement (/*p_type=*/'Local',
/*p_windows_login =*/'',
/*admin_option =*/'false',
/*p_login =*/'Local_Account_1',
/*p_password =*/'StrongPassword123',
/*schema_privilege =*/'BDSQL_USER',
/*p_action =*/'ADD');

EXECUTE AccountManagement (/*p_type=*/'Local ',
/*p_windows_login =*/'',
/*admin_option =*/'true',
/*p_login =*/'Local_Account_1',
/*p_password =*/'StrongPassword123',
/*schema_privilege =*/'ALTER SESSION',
/*p_action =*/'ADD');
```

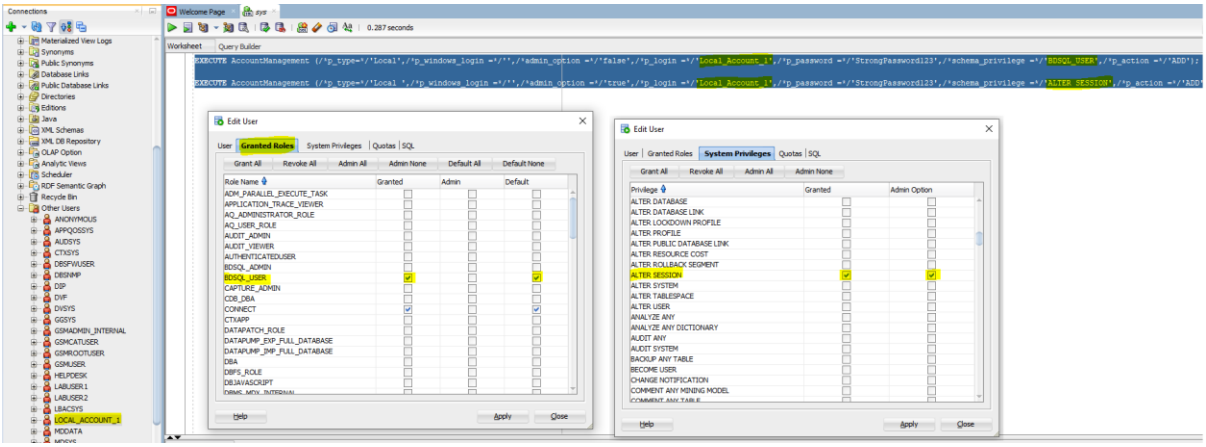
Si se comparan las principales características de esta ejecución con la anterior se puede observar que el **p_type** ahora es ***Local***, además, no se requiere el **p_windows_login** ya que en este apartado se insertaba el usuario de Active Directory. También, en esta solución se observa que se debe enviar una contraseña,

por limitaciones del sistema y complejidad de la implementación se recomienda que la contraseña sea alfanumérica. Los demás elementos son similares a los de la sección anterior.

El resultado de esta ejecución es el siguiente:

Figura 22

Sesión creada en el servidor



Fuente: Elaboración propia (2022)

5.3.2.2 Aplicación Caso 2 Oracle

Para resolver este caso se ejecutará el siguiente comando:

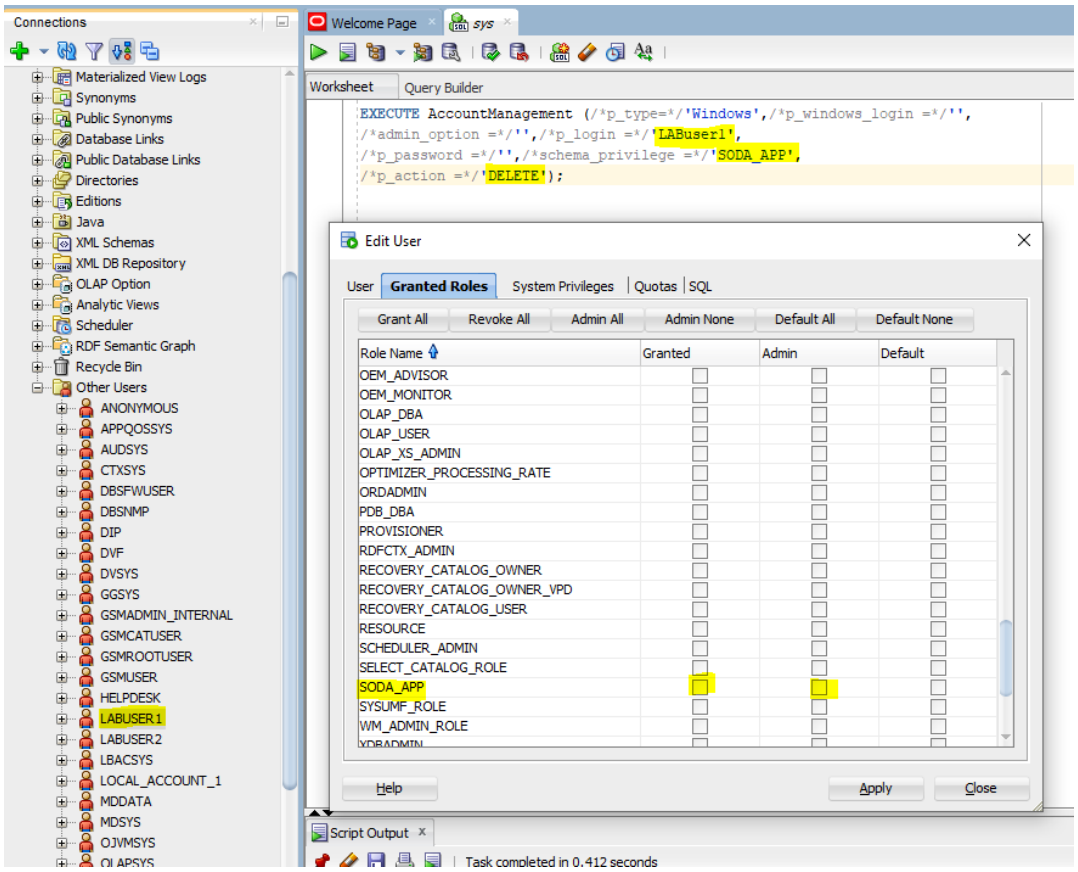
```
EXECUTE AccountManagement (/*p_type=*/'Windows',
/*p_windows_login =*/'',
/*admin_option =*/'',
/*p_login =*/'LABuser1',
/*p_password =*/'',
/*schema_privilege =*/'SODA_APP',
/*p_action =*/'DELETE');
```

Lo que se puede observar en este comando es que para el usuario de Active Directory, la eliminación del acceso es bastante sencillo, pues no se requiere el p_windows_login no es necesario mencionarlo nuevamente, ya que se estaría apuntando a la sesión ya existente.

Después de esta ejecución, el resultado se muestra a continuación:

Figura 23

Eliminación de privilegios en usuarios de bases de datos



Fuente: Elaboración propia (2022)

5.3.2.3 Aplicación Caso 3 Oracle

Para resolver este caso se ejecutará el siguiente comando:

- Usuario de Active Directory:

```
EXECUTE AccountManagement (/*p_type=*/'Windows',
/*p_windows_login =*/'LABuser1@lab.local',
/*admin_option =*/'',
/*p_login =*/'LABuser1',
/*p_password =*/'',
/*schema_privilege =*/'',
/*p_action =*/'DROP');
```

- Usuario Local:

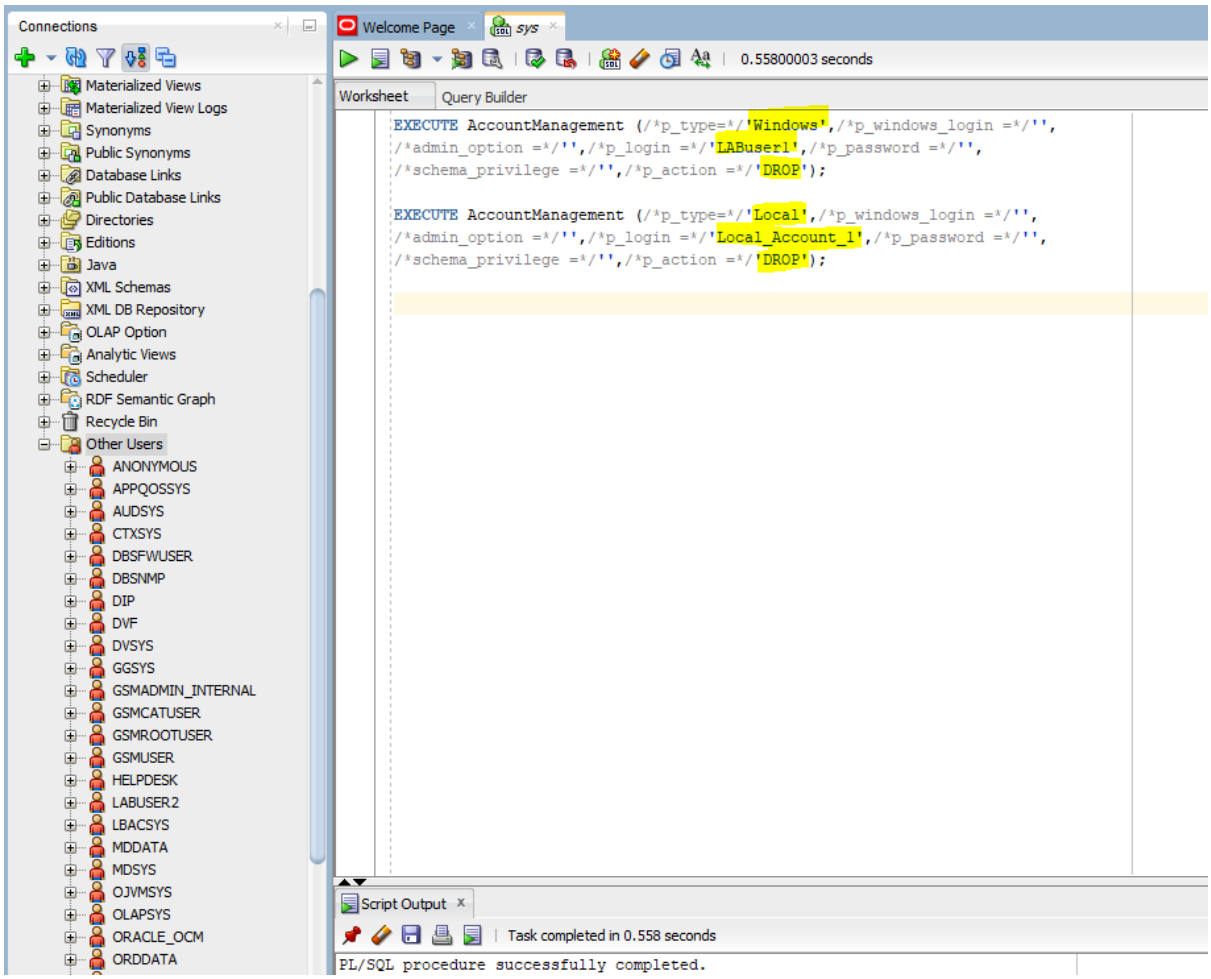
```
EXECUTE AccountManagement (/*p_type=*/'Local',
/*p_windows_login =*/'',
/*admin_option =*/'',
/*p_login =*/'Local_Account_1',
/*p_password =*/'',
/*schema_privilege =*/'',
/*p_action =*/'DROP');
```

Para ambos casos es similares, simplemente se deben llenar 3 espacios que serían el p_type, p_login y p_action los cuales van a remover completamente la cuenta de del esquema y el usuario no podrá conectarse en ninguna circunstancia ya que se elimina de raíz.

La ejecución provee el siguiente resultado:

Figura 24

Eliminación de privilegios en usuarios de bases de datos



Fuente: Elaboración propia (2022)

Capítulo 6. Conclusiones y Recomendaciones

6.1 Conclusiones

- A partir de la investigación realizada se puede concluir que, en el mercado actual, se aplican buenas prácticas para el control de accesos en los sistemas empresariales. Las cuales vienen dados por la reconciliación de cuentas (estrategia encargada de certificar periódicamente los usuarios y sus respectivas cuentas que existen en las diferentes aplicaciones y sistemas), el aprovisionamiento de cuentas (encargada de crear, modificar o eliminar cuentas). Estos elementos cierran el ciclo de vida de los accesos en las compañías la cual comienza al momento de con la primer relación entre un humano, robot o servicio con la empresa y finaliza cuando el usuario concluye la relación con la compañía.
- El correcto control o procedimiento que se debe llevar a cabo para brindar acceso a una cuenta fue el elemento principal de manejo de identidades que afectó positivamente el desarrollo de esta investigación. A partir de lo anterior, es importante conocer en la estructura y las funcionalidades que se habilitarán en los sistemas para entender cuál es el proceso para automáticamente brindar acceso a una base de datos y que el rol otorgado represente el mínimo acceso que la cuenta necesita para poder desarrollar el trabajo para el que fue asignado, de esta manera se sigue el principio del mínimo privilegio: conceder a los usuarios sólo los privilegios esenciales para realizar su trabajo (Edgerton, 2016)
- Si bien, se registra poca información sobre el control de accesos en bases de datos relacionales a nivel empresarial, por otro lado, existe vasta documentación (creada por parte de las compañías que soportan estos

productos y las diferentes comunidades de desarrolladores), sobre las diversas funcionalidades en los motores y sus respectivos lenguajes. Esto contribuyó a que la construcción de la herramienta se adaptara adecuadamente a la creación del estándar, el cual se ejecutó sin ningún inconveniente en los escenarios creados y facilitó el desarrollo de los casos expuestos.

- La comparación y la comprobación de la efectividad del estándar creado se desarrolló implícitamente, ya que esta investigación no utiliza ninguna institución en donde se pudiera extraer información de la forma en que se estaba implementando este control internamente, por lo tanto se utilizaron fuentes de información las cuales proveyeron los elementos teóricos necesarios para llevar a la práctica en ambientes controlados el desarrollo de scripts los cuales siguen los más minuciosos controles de accesos en los estándares de seguridad que existen hoy en día. Por lo tanto, la efectividad de esta metodología tiene un nivel abstracto significativo en el mercado de bases de datos relaciones ya que, de los motores que se seleccionaron en esta investigación, representan un 74 % del mercado actual y este estándar puede brindar una mayor agilidad y mayores elementos de seguridad a los componentes que se encuentran dentro de ellas.

6.2 Recomendaciones

- Cada empresa, compañía u organización tiene políticas que pueden afectar positiva o negativamente la implementación de esta estrategia, por lo que es necesario tener una comunicación efectiva con los líderes y, de esta forma, partir de la especificidad de cada empresa.
- Dentro de las infraestructuras físicas existen limitantes de cortafuegos (firewalls) que afectan la comunicación entre el servidor donde se encuentre el

producto de control de accesos y la base de datos donde se instalará la metodología, por lo tanto, es requerido conocer los procesos para habilitar los puertos de comunicación con el equipo de redes.

- El estándar elaborado fue desarrollado en las versiones mencionadas en la Tabla 9, por lo tanto, la implementación de esta herramienta en versiones anteriores puede tener un resultado diferente al mostrado en esta investigación.
- Es importante conocer la estructura de la compañía, en cuanto al manejo de dominios, pues se debe tener claro cuáles de ellos brindarán acceso a las bases de datos y cuáles reglas se deberán implementar en la política de control de accesos.

6.3 Trabajos a futuro

A partir del proceso de investigación, así como la construcción del instrumento de control de accesos en bases de datos relacionales, se identificaron algunas herramientas y metodologías que requieren de mejoras, o bien, la búsqueda de alternativas a los procedimientos utilizados en la actualidad. Estas son:

- Investigar la correcta implementación de esta metodología en productos instalados en la nube. Para lo cual es necesario identificar las configuraciones de seguridad particulares que requiere esta implementación.
- Con el objetivo de expandir la cantidad de productos que pueden beneficiarse por este estándar, se pueden desarrollar nuevos scripts en otros motores de bases de datos relaciones, como los presentados en la Tabla 1 (PostgreSQL, IBM Db2, SQLite, Microsoft Access, MariaDB, Hive).

- Es necesario iniciar el desarrollo de estas metodologías en bases de datos NoSQL o no relacionales ya que, debido a sus características, pueden ser una herramienta medular para garantizar la seguridad de las compañías.
- Finalmente, se podría desarrollar un software que escanee la red empresarial, identifique agentes de bases de datos instalados y ejecute los comandos de manera automática. De esta forma, se podría conectar la herramienta de control de accesos al software y controlar los dispositivos de red y los accesos de usuarios en las diversas bases de datos empresariales.

6.4 Detalles finales

Todos los scripts que fueron creados en este trabajo de investigación están almacenados en Github, herramienta que se utiliza para la centralización de códigos y para tener un control histórico de los cambios que se han realizado. De esta manera, la comunidad puede acceder a esta información y brindar recomendaciones de nuevas funcionalidades que se puedan desarrollar. El repositorio está localizado en el siguiente URL: https://github.com/Thonessi/DatabaseAccessControl

Referencias

Al-Khouri, A. M. (2011). Optimizing identity and access management (IAM) frameworks. *International Journal of Engineering Research and Applications*, 1(3), 461-477.

Barchini, G., Álvarez, M., Herrera, S., & Trejo, M. (2007). *El rol de las ontologías en* los SI. Revista Ingeniería Informática, 14, 1-12.

Benantar, M. (2005). *Access control systems: security, identity management and trust models*. Springer Science & Business Media.

Bröker, T. (2019). *HOW TO SUPPORT AN EFFECTIVE DIGITAL IDENTITY LIFECYCLE?* Obtenido de: https://blog.onegini.com/digital-identity-lifecycle

Cook, T. D., & Reichardt, C. S. (1986). Métodos cualitativos y cuantitativos en investigación evaluativa. Madrid: Morata.

DB-Engines, (2021). *Method of calculating the scores of the DB-Engines Ranking*. Obtenido de: https://db-engines.com/en/ranking_definition

Díaz, L. (2011). Método clínico: La observación.

De la Concepción, M. Á. Á., Ramírez, A. J., Ballesteros, M. D. M. M., Gasca, R. M., Núñez, M. L. P., & Morillo, L. M. S. (2011). *Extensiones para el Ciclo de Mejora Continua en la enseñanza e investigación de Ingeniería Informática*. Revista de Enseñanza Universitaria, (38), 4-26.

Devlekar, S., & Ramteke, V. (2021). Identity and Access Management: High-level Conceptual Framework. *REVISTA GEINTEC-GESTAO INOVACAO E TECNOLOGIAS*, 11(4), 4885-4897.

Edgerton, T. (2016, 17 febrero). *Principles of Access Management Control - Avatier*. The Identity and Access Management Blog. Recuperado 29 de marzo de 2022, de https://www.avatier.com/blog/principles-of-access-management-control/

ERI Economic Research Institute. (s. f.). Salary Expert - Information Security Engineer Salary Costa Rica. Obtenido de: https://www.salaryexpert.com/salary/job/information-security-engineer/costa-rica

Esquivel, J. C., Carbonelli, M., & Gabriela, I. (2011). Introducción al conocimiento científico y metodología de la investigación social.

Facuse, M. (2003). Una epistemología pluralista. Cinta de Moebio. Revista de Epistemología de Ciencias Sociales, (17).

Forcepoint. (2021). *What is Endpoint Security?* Obtenido de: https://www.forcepoint.com/cyber-edu/endpoint-security

García-Morales, E. (2012). *Gobernanza de la Información*. Notas ThinkEPI, 6.

Gartner (2009). Magic Quadrant for Endpoint Protection Platforms. Gartner RAS Core Research Note G, 208912.

Gunter, C. A., Liebovitz, D., & Malin, B. (2011). Experience-based access management: A life-cycle framework for identity and access management systems. *IEEE security & privacy*, *9*(5), 48.

Hernández-Sampieri, R., Fernández-Collado, C., & Baptista-Lucio, P. (2017). *Alcance de la Investigación*.

IJERA, (2021). *International Journal of Engineering Research and Applications*. Obtenido de: https://www.ijera.com/

International Bureau of Education & UNESCO. (s. f.). *Concept of Governance*. Obtenido de: http://www.ibe.unesco.org/es/node/9784

Lefferts, R. (2021, 10 mayo). *Gartner names Microsoft a Leader in the 2021 Endpoint Protection Platforms Magic Quadrant*. Microsoft Security Blog.

https://www.microsoft.com/security/blog/2021/05/11/gartner-names-microsoft-a-leader-in-the-2021-endpoint-protection-platforms-magic-quadrant/

Lozada, J. (2014). *Investigación aplicada: Definición, propiedad intelectual e industria*. CienciAmérica: Revista de divulgación científica de la Universidad Tecnológica Indoamérica, 3(1), 47-50.

McAfee. (s. f.). *What Is Endpoint Security?* Obtenido de https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint.html

Mohammed, I. A. (2017). SYSTEMATIC REVIEW OF IDENTITY ACCESS MANAGEMENT IN INFORMATION SECURITY. *International Journal of Innovations in Engineering Research and Technology*, 4(7), 1-7.

Morley, D., & Parker, C. S. (2009). *Databases and database management systems. Understanding computers: Today and tomorrow*, 588-627.

Nguyen, B. Q. (2003). *Information Assurance Issues and Requirements for Distributed Electronic Records Archives*. ARMY RESEARCH LAB ADELPHI MD.

OneLogin. (s. f.). What is User Provisioning & Deprovisioning? https://www.onelogin.com/learn/what-is-user-provisioning-and-deprovisioning#:%7E:text=User%20provisioning%20and%20deprovisioning%20key%20benefits%20Automated%20user,different%20department%20or%20division%2C%20or%20exits%20a%20company.

Oracle. (s. f.). Configuring Privilege and Role Authorization. Oracle Help Center. https://docs.oracle.com/database/121/DBSEG/authorization.htm#DBSEG4414

Parada, E. L. (2002). *Introducción a las políticas públicas*. Fondo de cultura económica.

Sath Inc. (2022, 19 enero). Reconciliation In Identity And Access Management. Sath.Com. https://sath.com/idhub/reconciliation/

Sokanu, (s.f). *What does a security engineer do?* Obtenido de https://www.careerexplorer.com/careers/security-engineer

solid IT, (2021). *DB-Engines Ranking of Relational DBMS*. Obtenido de: https://db-engines.com/en/ranking/relational+dbms

Toelen, O. (2008). *Identity and access management* (Doctoral dissertation, PhD thesis, Master. thesis).

Uribe, S. C., Zapata, A. P., & Gómez, B. R. (1996). Investigación evaluativa. Especialización en teoría, métodos y técnicas de investigación social. Módulo, 6.

Zapata Chasiguasin, K. B. (2020). *Sistema de gestión de seguridad de la información basado en las Normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato* (Bachelor's thesis, Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera de Ingeniería en Sistemas Computacionales e Informáticos).

Zeledón, L. N. (2020). *Investigación en Informática: el enfoque alternativo*. Technology Inside by CPIC, 5, 1-15.