Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 40-51
https://revistas.ulasalle.edu.pe/innosoft

Tipo de artículo: Artículos originales
Temática: Tecnologías de bases de datos
Recibido: 24/05/2022 | Aceptado: 02/07/2022 | Publicado: 30/09/2022

Identificadores persistentes:
ARK: ark:/42411/s9/a58
PURL: 42411/s9/a58

Trazabilidad de operaciones en base de datos para mitigar riesgos en los procesos de auditoría

Traceability of database operations to mitigate risks in audit processes

Cesar Mayta Avalos [1][0000-0002-5722-1854]*, **Fernando Rosales Castilla** [2][0000-0003-0668-2885], **Milca Gines Colana** [3][0000-0002-3596-2803]

[1] Universidad Nacional Jorge Basadre Grohmann de Tacna. cesar.mayta@unjbg.edu.pe
[2] Universidad Nacional Jorge Basadre Grohmann de Tacna. fernando.rosales@unjbg.edu.pe
[3] Universidad Nacional Jorge Basadre Grohmann de Tacna. milca.gines@unjbg.edu.pe

* Autor para correspondencia: fernando.rosales@unjbg.edu.pe

Resumen

En el ámbito de las bases de datos la falta de la trazabilidad de transacciones u operaciones es vital para responder a incidencias o hechos que pueden originarse dentro de ellas, como la alteración o acceso a información no autorizada. Este artículo busca proponer un modelo de auditoría a fin de mitigar el riesgo, utilizando el enfoque de auditoría de objetos aplicado a tablas y transacciones con Oracle. Finalmente se implementó un laboratorio en el cual se desplegó el modelo propuesto y que permitirá asegurar la confidencialidad, integridad y disponibilidad de la información.

Palabras clave: Auditoría, Bases de datos, Riesgos, Trazabilidad, Oracle.

Abstract

In the field of databases, the lack of traceability of transactions or operations in a database is vital to respond to incidents that may originate within them, such as the alteration of unauthorized information. This article proposes an auditing model to mitigate risk using Oracle's object and transaction auditing approach. Finally, a laboratory was implemented in which the proposed model was deployed, ensuring the information's confidentiality, integrity, and availability.

Keywords: *Audit, Databases, Risks, Traceability, Oracle.*

Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 40-51
https://revistas.ulasalle.edu.pe/innosoft

Introducción

Las bases de datos es la columna vertebral de todo sistema de información puesto que si esta fallara todo el sistema sería afectado, por lo que resulta importante que se esté siempre se encuentre disponible, asegurando la continuidad del negocio, por lo que el despliegue de planes y medidas permitirán brindarle la seguridad.

Concretamente en el caso del gestor de base de datos Oracle, vemos que se puede realizar una trazabilidad de operaciones sobre los objetos de esta misma, el cual sirva de control y mecanismo de protección; así durante el análisis y evaluación de riesgos en la aplicación de un proceso de auditoría de sistemas de información garantizara responder a la mitigación de las amenazas que puedan presentarse.

Conceptos previos

Sistema de Gestión de Seguridad de la Información:

El uso de la tecnología ha generado ciertos problemas a las organizaciones, que día tras día son más vulnerables a las amenazas que se presentan en el medio, las cuales pueden llegar a convertirse en un verdadero riesgo para la organización afectando el correcto funcionamiento de las actividades del negocio. Para contrarrestar dichas amenazas, las organizaciones deben generar un plan de acción frente a éstas. Este plan de acción es conocido como Sistema de Gestión de Seguridad de la Información (SGSI) y contiene los lineamientos que deben seguirse en la organización, los responsables y la documentación necesaria para garantizar que el SGSI sea aplicado y genere una retroalimentación.[1] La definición de SGSI se hace de manera formal en la norma ISO 27001, donde están los estándares y mejores prácticas de seguridad de la información.

Análisis de Riesgos:

El análisis de riesgos es la consideración del daño probable que puede causar en el negocio un fallo en la seguridad de la información, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información. En el ámbito de la seguridad informática, las metodologías de análisis de riesgos conforman una disciplina que se articula desde los Sistemas de Gestión de Seguridad de la Información SGSI en las organizaciones, realizando unos importantes escaneos de vulnerabilidades mediante el uso de una serie de modelos y procesos con el fin de proponer una forma más segura de cuidar la información y los recursos de TI [2]. Algunos de los objetivos de las

metodologías de análisis de riesgos corresponden a: Planificación de la reducción de riesgos, prevención de accidentes, visualización y detección de las debilidades existentes en los sistemas y ayuda en la toma de las mejores decisiones en materia de seguridad de la información [3].

Base de Datos:

Una base de datos es una colección de datos relacionados, se construyen siguiendo un diseño y se almacenan datos para realizar acciones específicas. Los datos que se almacenan en una base de datos tienen un origen y pertenecen o llevan relación con un evento en específico de la vida real, asimismo el contenido de las bases de datos es de interés de un grupo de usuarios activos. [4]

Auditoría de base de datos:

La auditoría de bases de datos consiste en un proceso de monitoreo continuo y riguroso de los controles que la administración ha establecido dentro de los sistemas de bases de datos y todos sus componentes para obtener una seguridad razonable de la utilización adecuada de los datos que son almacenados por los usuarios mediante los sistemas de información. El monitoreo y pruebas a los controles determinan la pertinencia y suficiencia de éstos, permitiendo entonces ajustar, eliminar o implementar nuevos controles para asegurar su adecuada utilización.[5]

Modelo propuesto para la Trazabilidad de operaciones mediante la aplicación de auditorías en Oracle

La información constituye uno de los pilares de gran valor de cualquier organización, por lo que resulta importante adoptar mecanismos que permitan asegurar la confidencialidad, seguridad e integridad y que permitan garantizar la continuidad del negocio o servicio.

Es conocimiento que en la actualidad toda organización almacena su información en repositorios y dentro de ellos podemos citar a los sistemas gestores de base de datos ya sean de tipo SQL o noSQL, alojados en una infraestructura de tipo física o en la nube.

Dentro de este contexto, el presente artículo de investigación trata de mostrar de forma descriptiva la importancia que toma el concepto de auditoria de base de datos, enmarcado en establecer controles que permitan minimizar los riesgos

de pérdida de datos, así como poder obtener una seguridad razonable y que permita responder a situaciones de incidencia presentados con la finalidad de explicar algún hecho de revisión y/o investigación.

Las bases de datos como activos de información y de misión crítica, requieren ser protegidas con mecanismos, políticas de seguridad, procedimientos, y controles debidamente verificados y que permitan asegurar la continuidad de los servicios que brinda cualquier organización.

La seguridad de las bases de datos estará garantizada por un modelo de auditoría, configurando el hecho de que, tiene una simbiosis entre estos dos conceptos: "No hay seguridad sin auditoría" [7].

Ubicación del Control:

El modelo propuesto consiste en desplegar el control dentro de la misma base de datos, lo cual será realizado en Oracle aprovechando su componente de auditoría, con la finalidad de establecer y desplegar un modelo auditor que permita asegurar la trazabilidad de las operaciones.

Aplicación de la Auditoría en Oracle:

Con la finalidad de desplegar nuestro modelo de auditoría a fin de garantizar la transparencia en la trazabilidad de las operaciones se realizará en la i) auditoria de objetos, estará centrada específicamente en las tablas del esquema principal de base de datos y que sirve de repositorio de la información; ii) auditoría de transacciones u operaciones de datos, en la cual se desplegará un control mediante disparadores que permita conocer el dato cuando es insertado en la tabla, así como las acciones de alteración y borrado de registros que puedan producirse ya sea desde alguna aplicación de la organización, software propietario de alguna compañía o dentro de la misma base de datos.

Desarrollo del Modelo de Auditoría:

En primera instancia hemos definido que para desarrollar el modelo propuesto de auditoría en Oracle, haremos uso del esquema HR [6], el cual corresponde a un grupo de tablas de ejemplo de Recursos Humanos que viene embebida dentro del sistema gestor de base de datos y adicionalmente viene con información (registros) que nos permitirá describir y aplicar las auditorías.

A continuación presentamos las tablas que este esquema define en la base de datos, así como una breve descripción de cada uno de ellos:

Tabla 1. Tablas del esquema de ejemplo HR

TABLA	DESCRIPCIÓN
REGIONS	Registros que describen la Región para un determinado país
COUNTRIES	Registros que describen un país
LOCATIONS	Registros de Direcciones para una determinada ciudad
DEPARTMENTS	Registros que muestra el Departamento o Área de una Organización
JOBS	Registros de los cargos en una organización así como el sueldo
EMPLOYEES	Registros de empleados asociados a determinado un salario y función
JOB_HISTORY	Registros histórico de una determinado cargo en una organización

a. Activando el componente auditor

La base de datos Oracle, hace uso un componente el cual en primera instancia deberá estar habilitado, esta tarea solo puede ser realizada por un DBA (Database Administrator o Administrador de Base de Datos) por tal motivo, si no se realiza este paso inicial no se podrá desplegar ningún modelo de auditoría que quiera desarrollarse.

```
SQL> show parameter audit_trail

NAME                                 TYPE        VALUE
------------------------------------ ----------- ------------
audit_trail                          string      NONE
```

En caso de encontrarse con el valor NONE, cambiaremos por la activación respectiva y posterior a ello debemos reiniciar los servicios de base de datos, con la finalidad de que el componente de auditoría quede preparado para su uso.

```
SQL> alter system set audit_trail='DB' scope=spfile;
```

b. Descripción del Registro de Auditoría de Objetos

La información que se plasma como auditoría es diversa, por lo que lectura e interpretación de dichos registros responde a datos como: Usuario conectado, identificador de sesión, computadora o servidor desde donde se esta conectando, qué tipo de operación de datos ha realizado como insert – delete – update, y hora/fecha en formato minucioso que trata de explicar dentro de la hora exactamente realizada la acción.

Estos registros de la tabla de auditoría AUDIT TRAIL está basado principalmente en las auditorías propiamente de objetos, por ejemplo: si algún usuario realizó mediante la actualización (update) de un determinado puesto de trabajo de la tabla HR.JOBS y de forma específica en el campo: MAX_SALARY el registro auditado solo registra que usuario realizó tal acción, pero no se podrá visualizar como se encontraba el registro antes de dicha actualización.

A continuación creamos la siguiente política de nombre DML_POL, la cual solo puede ser realizado por un usuario privilegiado:

```
CREATE AUDIT POLICY DML_POL
 Actions
  ALL on HR.DEPARTMENTS,
  ALL on HR.REGIONS,
  ALL on HR.COUNTRIES,
  ALL on HR.LOCATIONS,
  ALL on HR.DEPARTMENTS,
  ALL on HR.JOBS,
  ALL on HR.EMPLOYEES;
```

Por último, dicha política es asignada a los usuarios (usuario _01 y usuario _02) de las aplicaciones los cuales serán monitoreados con auditorías sobre los objetos de tablas de dicho esquema HR:

```
AUDIT POLICY DML_POL BY usuario _01, usuario _02;
```

A partir de la ejecución y activación de la política DML_POL el registro en el AUDIT_TRAIL comienza a capturar todas las acciones que puedan efectuar los usuarios monitoreados:

Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 40-51
https://revistas.ulasalle.edu.pe/innosoft

- USUARIO _01: realiza acciones de select y update en la tabla hr.countries
- USUARIO _02: realiza acciones de select sobre la tabla hr.locations

	OS_USERNAME	TERMINAL	DBUSERNAME	CLIENT_PROGRAM_NAME	EVENT_TIMESTAMP	ACTION_NAME	OBJECT_SCHEMA	OBJECT_NAME	UNIFIED_AUDIT_POLICIES
1	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	22/05/22 21:44:33,145000	SELECT	HR	COUNTRIES	DML_POL
2	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	22/05/22 21:44:39,830000	SELECT	HR	COUNTRIES	DML_POL
3	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	22/05/22 21:44:39,877000	UPDATE	HR	COUNTRIES	DML_POL
4	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	22/05/22 21:44:39,893000	SELECT	HR	COUNTRIES	DML_POL
5	DBSERVER\Administrador	DBSERVER	USUARIO_02	plsqldev.exe	22/05/22 21:56:56,179000	SELECT	HR	LOCATIONS	DML_POL

Figura 1. Captura del Registro de Auditoría de los objetos de tablas de HR

Como se puede observar en la Figura 1, nos muestra información de auditoría relevante y que responde preguntas:

¿Quién lo realizó? ¿De donde fue realizado? ¿En qué fecha y hora fue ejecutada dicha acción?, ¿Cuales fueron las tablas involucradas? ¿Desde que aplicación fue realizada? ¿Cuál fue la sentencia ejecutada?

c. Descripción del Registro de Auditoría de Operaciones

Este tipo de auditoría hará uso de disparadores (trigger) los cuales serán elaborados por el Administrador de base de datos y seguidamente serán cargados en la base de datos para el uso respectivo.

El objetivo de este tipo de auditoría es poder conocer las acciones que un determinado usuario realiza antes del cambio originado en la tabla principal o crítica, ya sea como una actualización, borrado o alguna inserción, sin embargo tengamos presente que los usuarios hacen uso de aplicaciones por lo las acciones señaladas son desde este origen.

También es importante dar a conocer que puede existir usuarios que tengan acceso en la base de datos por lo que constituye también un hecho importante monitorear sus actividades.

Supongamos que el USUARIO _01 mediante su aplicación esté realizando alguna actualización de un sueldo mínimo (MIN_SALARY) de la tabla HR.JOBS correspondiente al JOB_ID=AD_PRES, por lo que resulta importante resguarda el valor original antes del cambio, así por ejemplo tenemos lo siguiente:

Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 40-51
https://revistas.ulasalle.edu.pe/innosoft

Row 1	Fields	Info
JOB_ID	AD_PRES	varchar2(10), mandatory, Primary key of jobs table.
JOB_TITLE	President	varchar2(35), mandatory, A not null column that shows job title, e.g. AD_VP,
MIN_SALARY	20080	number(6), optional, Minimum salary for a job title.
MAX_SALARY	40000	number(6), optional, Maximum salary for a job title
ROWID	AAARyDAADAAACR1AAA	

Figura 2. Registro del JOB_ID=AD_PRES antes del cambio MIN_SALARY=20080

Row 1	Fields	Info
JOB_ID	AD_PRES	varchar2(10), mandatory, Primary key of jobs table.
JOB_TITLE	President	varchar2(35), mandatory, A not null column that shows job title, e.g. AD_VP,
MIN_SALARY	21080	number(6), optional, Minimum salary for a job title.
MAX_SALARY	40000	number(6), optional, Maximum salary for a job title
ROWID	AAARyDAADAAACR1AAA	

Figura 3. Registro del JOB_ID=AD_PRES después del cambio MIN_SALARY=21080

Si en este momento, se vuelve a consultar el registro de la tabla HR_JOBS, presentará únicamente el último cambio de 21080 pero no se conocerá el valor inicial antes de este cambio (update) y de solicitarse la trazabilidad de operaciones que pueda haber tenido este registro en la base de datos respecto no podría ser atenderse dicho requerimiento.

Con el despliegue de este tipo de auditoría y luego de la creación del disparador para la tabla HR.JOBS vamos a poder conocer la trazabilidad de operaciones que este registro ha tenido, originado por el USUARIO _01, así al final dicha registro se presenta de la siguiente manera:

Row 1	Fields	Info
SIDU	U	char(1), mandatory
FECHA_SIDU	23/05/22 15:02:52,011000	timestamp(6), mandatory
USUARIO	USUARIO_01	varchar2(20), mandatory
USUARIO_RED	DBSERVER\ADMINISTRADOR	varchar2(50), optional
COMPUTADORA	WORKGROUP\DBSERVER	varchar2(50), optional
IP_TRAZABILIDAD	127.0.0.1	varchar2(20), optional
PROGRAMA	PLSQLDEV.EXE	varchar2(100), optional
JOB_ID	AD_PRES	varchar2(10), mandatory
JOB_TITLE	President	varchar2(35), mandatory
MIN_SALARY	20080	number(6), optional
MAX_SALARY	40000	number(6), optional

Figura 4. Registro auditado de la tabla HR.AUDITANDO_JOBS respecto al JOB_ID=AD_PRES

En el caso desarrollado es importante señalar que se tiene una tabla de HR.AUDITANDO_JOBS la cual tiene la siguiente estructura:

CREATE TABLE HR.AUDITANDO_JOBS

(SIDU CHAR(1) NOT NULL,

FECHA_SIDU TIMESTAMP NOT NULL,

USUARIO VARCHAR2(20) NOT NULL,

USUARIO_RED VARCHAR2(50),

COMPUTADORA VARCHAR2(50),

IP TRAZABILIDAD VARCHAR2(20),

PROGRAMA VARCHAR2(100),

---Campos de la tabla HR.JOBS

------);

Asimismo el disparador (trigger), es el objeto que se encuentra cargado en la base de datos y que permitirá capturar la información de una auditoría, en este caso de la operaciones en la tabla HR.JOBS para efectos de trazabilidad, por lo que se muestra parte del siguiente código y en la cual se ha hecho uso de los verbos en Oracle [8]:

CREATE TRIGGER AUDITANDO.DISPARA_HR_JOBS

AFTER INSERT OR DELETE OR UPDATE ON HR.JOBS FOR EACH ROW

BEGIN

INSERT INTO HR.AUDITANDO_JOBS

……..

UPDATE INTO HR.AUDITANDO_JOBS

……..

DELETE INTO HR.AUDITANDO_JOBS

Como se puede observar en la Figura 4 y tan igual que la auditoría de objetos, este tipo también nos permitirá responder frente a incidencias o consulta sobre la trazabilidad de un determinado registro

¿Quién lo realizó? ¿De dónde fue realizado? ¿En qué fecha y hora fue ejecutada dicha acción?, ¿Cuáles fueron las tablas involucradas? ¿Desde qué aplicación fue realizada? ¿Cuál fue la sentencia ejecutada?

Revista Innovación y Software
Vol. 3, No. 2, Mes Septiembre-Febrero, 2022
ISSN: 2708-0935
Pág. 40-51
https://revistas.ulasalle.edu.pe/innosoft

De alguna forma se apoyará de la auditoría de objetos a fin de establecer y tener mayores elementos de revisión a fin de explicar un determinado suceso, para el caso señalado y que venimos desarrollando podemos visualizar las operaciones que el USUARIO _01 y USUARIO _02 han realizado

	OS_USERNAME	TERMINAL	DBUSERNAME	CLIENT_PROGRAM_NAME	EVENT_TIMESTAMP	ACTION_NAME	OBJECT_SCHEMA	OBJECT_NAME	UNIFIED_AUDIT_POLICIES
1	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:01:28,947000	SELECT	HR	JOBS	DML_POL
2	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:01:43,920000	SELECT	HR	JOBS	DML_POL
3	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:01:43,967000	UPDATE	HR	JOBS	DML_POL
4	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:01:43,967000	SELECT	HR	JOBS	DML_POL
5	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:02:51,633000	SELECT	HR	JOBS	DML_POL
6	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:02:52,118000	UPDATE	HR	JOBS	DML_POL
7	DBSERVER\Administrador	DBSERVER	USUARIO_01	plsqldev.exe	23/05/22 15:02:52,134000	SELECT	HR	JOBS	DML_POL
8	DBSERVER\Administrador	DBSERVER	USUARIO_02	plsqldev.exe	23/05/22 16:32:16,418000	SELECT	HR	JOBS	DML_POL
9	DBSERVER\Administrador	DBSERVER	USUARIO_02	plsqldev.exe	23/05/22 16:32:31,647000	SELECT	HR	JOBS	DML_POL
10	DBSERVER\Administrador	DBSERVER	USUARIO_02	plsqldev.exe	23/05/22 16:32:42,914000	SELECT	HR	JOBS	DML_POL
11	DBSERVER\Administrador	DBSERVER	USUARIO_02	plsqldev.exe	23/05/22 16:32:45,614000	DELETE	HR	JOBS	DML_POL
12	DBSERVER\Administrador	DBSERVER	USUARIO_02	plsqldev.exe	23/05/22 16:33:24,130000	SELECT	HR	EMPLOYEES	DML_POL

Figura 5. Registro auditada a nivel de objeto Tabla

Resultados y discusión

Mediante el modelo de auditoría desplegado en la base de datos en Oracle, se pudo capturar información de las tablas del esquema HR con el cual se desarrolló el laboratorio, consiguiendo el registro de trazabilidad de las operaciones que puede haber realizado un determinado usuario. Estos registros de trazabilidad vienen a conformar una colección de datos auditables, los cuales permitirán minimizar los riesgos relacionados a la alteración y/o eliminación no autorizada de la información.

La evidencia de las auditorías capturadas se logra a partir del modelo desarrollado y desplegado, lo cual demuestra fehacientemente y responde interrogantes como por ejemplo: ¿Quién lo realizó? ¿De dónde fue realizado? ¿En qué fecha y hora fue ejecutada dicha acción?.

Existen programas de auditoría del fabricante Oracle como por ejemplo Oracle Audit Vault and Database Firewall [9] que realizan tareas automatizadas de auditoría, sin embargo el modelo propuesto no solo ofrece información sustancial de auditoría, sino que es una alternativa de menor inversión.

La aplicación de nuestro modelo de auditoría, servirá de cimiento y una estructura sólida para construir un sistema de protección de bases de datos, el cual puede ser consolidado en un único contenedor de datos auditables ya sea en un ambiente de infraestructura local o en la nube [10].

Conclusiones

La propuesta del modelo para implementar una auditoría a nivel de base de datos en Oracle para la trazabilidad de operaciones, viene asociado al hecho de que debemos cautelar y proteger la información en las organizaciones, más aún como elemento importante de la protección de datos personales asociado a los elementos de confidencialidad, integridad y disponibilidad los cuales tiene que ir alineados a disposiciones legales. Por lo que los elementos de seguridad que se implemente tendrá un efecto directo en la calidad de la auditoría de seguridad [11].

En el desarrollo del presente artículo, se ha mostrado de forma intrínseca ciertas amenazas causadas por una configuración predeterminada y si no se adoptan medidas de seguridad para este activo de información, quedará expuesta a elementos internos y externos que pueden causar perjuicio a la organización. El impacto en los datos almacenados lleva consigo el detenimiento de los servicios que se ofrecen, causando daños cuantiosos principalmente en lo económico y de reputación [12].

Referencias

[1] Ladino, Martha Isabel; Villa, Paula Andrea; López, Ana María. Fundamentos de iso 27001 y su aplicación en las empresas. Scientia et technica, 2011, vol. 17, no 47, p. 334-339. [Online]. Disponible en: https://www.redalyc.org/articulo.oa?id=84921327061

[2] M. Doris. Metodologías de la seguridad informática. [On line]. Disponible en: http://seguridadinformatica.bligoo.ec/media/users/22/1142179/files/312461/Metodologia_de_la_Seguridad_Ing.pdf

[3] J. Eterovic y G. Pagliari, Metodología de Análisis de Riesgos Informáticos. [Online]. Disponible en: http:// www.cyta.com.ar/ta1001/v10n1a3.htm.

[4] Elmasri, R., Díaz Martín, J. M., Navathe, S. B. Fundamentos de sistemas de bases de datos. Madrid: Pearson Educación, 2011.

[5] Murillo, Johnny Villalobos. Auditando en las bases de datos. Uniciencia, 2008, vol. 22, no 1-2, p. 135-140. [Online]. Disponible en: https://www.redalyc.org/articulo.oa?id=475948929017

[6] Modelos y de muestra, “SQL Developer Data Modeler 2.0: scripts DDL de muestra” Oracle, 2022. [Online]. Available: https://www.oracle.com/cl/database/technologies/appdev/datamodeler-samples.html. [Accessed: May. 22, 2022].

[7] Yang, L. (2009). Teaching database security and auditing. SIGCSE Bulletin Inroads, 41(1), 241–245. https://doi.org/10.1145/1539024.1508954

[8] Database 2 day Developer’s, “6 Using Triggers” Oracle, 2022. [Online]. Available: https://docs.oracle.com/database/121/TDDDG/tdddg_triggers.htm#TDDDG50000 [Accessed: May. 23, 2022].

[9] Oracle. (2017). Oracle Audit Vault and Database Firewall. March. http://www.oracle.com/technetwork/database/database-technologies/audit-vault-and-database-firewall/overview/index.html

[10]O. Cinar, RH Guncer y A. Yazici, "Seguridad de bases de datos en nubes privadas de bases de datos", Conferencia internacional sobre ciencia y seguridad de la información (ICISS) de 2016, 2016, págs. 1 a 5, doi: 10.1109/ICISSEC.2016.7885847.

[11] -ul-Hasan, M., & Othman, S. H. (2019). A Conceptual Framework of Information Security Database Audit and Assessment. International Journal of Innovative Computing, 9(1), 7–13. https://doi.org/10.11113/ijic.v9n1.206

[12]García, M. J. (2013). Database Main Threats Analisys Using MS SQL Server. 1–5. http://www.unab.edu.co/sites/default/files/MemoriasGrabadas/papers/capitulo9_paper_10.pdf

Roles de Autoría

Cesar Augusto Mayta Avalos: Investigación, Metodología, Redacción - borrador original. **Fernando Rosales Castilla:** Conceptualización, Análisis formal, Investigación, Metodología, Redacción - borrador original. **Milca Gines Colana:** Análisis formal, Investigación, Metodología, Redacción - borrador original.