UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA E INFORMÁTICA

TESIS

MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023

PRESENTADA POR:

MILTON EDWARD HUMPIRI FLORES

PARA OPTAR EL GRADO ACADÉMICO DE:

DOCTORIS SCIENTIAE EN ESTADÍSTICA E INFORMÁTICA

PUNO, PERÚ

2023

NOMBRE DEL TRABAJO

MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023

AUTOR

Milton Edward Humpiri Flores

RECUENTO DE PALABRAS

23219 Words

RECUENTO DE CARACTERES

126296 Characters

RECUENTO DE PÁGINAS

109 Pages

TAMAÑO DEL ARCHIVO

2.7MB

FECHA DE ENTREGA

May 15, 2024 1:46 AM GMT-5

FECHA DEL INFORME

May 15, 2024 1:49 AM GMT-5

12% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 10% Base de datos de Internet
- 1% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 8% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Material citado
- Coincidencia baja (menos de 12 palabras)

Firmado digitalmente por PEREZ QUISPE Samuel Donato FAU 20145496170 soft
Motivo: Soy el autor del documento
Fecha: 15.05.2024 06:23:20 -05:00

VB CIEPG

EPG UNAP

Firmado digitalmente por LUQUE COYLA Ruben Jared FAU 20145496170 hard
Motivo: Doy V° B°
Fecha: 17.05.2024 16:56:05 -05:00

UNIVERSIDAD NACIONAL DEL ALTIPLANO

ESCUELA DE POSGRADO

DOCTORADO EN ESTADÍSTICA E INFORMÁTICA

TESIS

MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023

PRESENTADA POR:

MILTON EDWARD HUMPIRI FLORES

PARA OPTAR EL GRADO ACADÉMICO DE:

DOCTORIS SCIENTIAE EN ESTADÍSTICA E INFORMÁTICA

APROBADA POR EL JURADO SIGUIENTE:

PRESIDENTE

.....
Dra. EMMA ORFELINDA AZAÑERO DE AGUIRRE

PRIMER MIEMBRO

.....
Dr. EDGAR ELOY CARPIO VARGAS

SEGUNDO MIEMBRO

.....
Dr. FREDY HERIC VILLASANTE SARAVIA

ASESOR DE TESIS

.....
Dr. SAMUEL DONATO PEREZ QUISPE

Puno, 19 de diciembre de 2023.

ÁREA: Informática.
TEMA: Modelo de convención con controles de auditoría y seguridad de base de datos relacionales, 2023.
LÍNEA: Tecnologías de Información

DEDICATORIA

A la presencia de nuestro señor Dios, presente en mis retos de vida. A mis seres queridos, siempre presentes en mí, Nilda mi madre, Florentino mi padre y Rogger mi hermano. A mi esposa, cómplice de todos nuestros retos y logros, a ti Mía Lucía. A Domingo Jesús, gracias.

AGRADECIMIENTOS

A la Universidad Nacional del Altiplano de Puno y mi FINESI. A mis jurados, Dra. Emma Orfelinda Azañero de Aguirre, Dr. Edgar Eloy Carpio Vargas y al Dr. Fredy Heric Villasante Saravia, Dr. Cesar Augusto Lluen Vallejos gracias por sus aportes y apoyo en el trabajo de investigación. A mi asesor, el Dr. Samuel Donato Perez Quispe.

ÍNDICE GENERAL

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

CAPÍTULO III

METODOLOGÍA

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

ÍNDICE DE TABLAS

Pág.

ÍNDICE DE FIGURAS

Pág.

ÍNDICE DE ANEXOS

Pág.

ACRÓNIMOS

BD	:	Base de Datos
BDR	:	Base de Datos Relacionales
DDL	:	Lenguaje de Definición de Datos
DML	:	Lenguaje de Manipulación de Datos
MC	:	Modelo de Convención
SGBD	:	Sistema de Gestión de Base de Datos

RESUMEN

Los registros en las Bases de Datos (BD) son activos importantes para organizaciones al igual que cualquier otro activo, donde debe garantizarse su seguridad, protección, confidencialidad, integridad, disponibilidad y uso, permitiendo su posterior auditoría; la siguiente investigación se realizó con el objetivo: determinar la eficiencia del Modelo de Convención (MC) con Controles de Auditoría y Seguridad de Base de Datos Relacionales (BDR). La metodología fue establecer el propósito de la BD, encontrar, organizar, dividir en tablas, transformar elementos en columnas, asignar claves primarias, crear relaciones, pulir el diseño y aplicar la normalización, asimismo; para la auditoria de seguridad, se enfocó en la integridad, confiabilidad, disponibilidad y gestión, realizando buenas prácticas que considera una convención. El MC y metodología fue evaluado por expertos. Resultando que se desarrolló un MC eficiente para el diseño seguro de BDR con controles de auditoría, propuesta refinada utilizando el método de criterio de expertos, en razón a que se logran identificar y estudiar implementaciones actuales de BD que consideran algunos aspectos de auditoría, tales como: añadir campos, consolidado histórico, logs de transacciones y tablas espejo; analizando ventajas y desventajas que coadyuvaron a obtener indicadores que fueron evaluados y contrastados con una prueba de hipótesis, concluyendo que las pruebas t calculadas coincidieron en la zona de rechazo frente a las pruebas t tabuladas, finalmente el MC con controles de auditoría y seguridad en BDR contribuye eficientemente a mejorar la integridad, confidencialidad, disponibilidad y gestión de la información, quedando a libre disponibilidad para su aplicación.

Palabras clave: Auditoria, base de datos, convención, experto, seguridad informática.

ABSTRACT

Records in Databases (DB) are important assets for organizations just like any other asset, where their security, protection, confidentiality, integrity, availability and use must be guaranteed, allowing their subsequent audit; the following research was carried out with the objective: to determine the efficiency of the Convention Model (CM) with Audit and Security Controls of Relational Database (RDB). The methodology was to establish the purpose of the DB, find, organize, divide into tables, transform elements into columns, assign primary keys, create relationships, polish the design and apply normalization, likewise; for the security audit, it was focused on integrity, reliability, availability and management, performing good practices that considers a convention. The CM and methodology was evaluated by experts. As a result, an efficient CM was developed for the secure design of RDBs with audit controls, a proposal refined using the expert criteria method, because current DB implementations that consider some audit aspects, such as: adding fields, historical consolidation, transaction logs and mirror tables, were identified and studied; analyzing advantages and disadvantages that contributed to obtain indicators that were evaluated and contrasted with a hypothesis test, concluding that the calculated t-tests coincided in the rejection zone compared to the tabu t-tests, and that the results of the t-tests were similar to the ones obtained with the tabu t-tests, and that the results of the t-tests were similar to those obtained with the tabu t-tests.

Keywords: Audit, database, convention, expert, computer security.

Juan Marcos Aro Aro, Ph. D.
Ing. AGROINDUSTRIAL
C.I.P. N 52422

INTRODUCCIÓN

La mayoría de actividades de control en el procesamiento de información de las empresas son escasas y muchas veces inexistentes, especialmente concerniente al control de la acumulación de información a través de los sistemas implementados, sistema gestor de base de datos, originando carencia de información sobre operaciones críticas y no había registro de: ¿Qué? ¿Quién? ¿Cómo? ¿Cuándo? o de ¿Donde? los datos han sido cambiados, agregados o eliminados.

Por defecto, el modelado de Base de Datos (BD) se crea con estructuras que ignoran algunos aspectos de seguridad, como ignorar los esquemas que soportan el análisis de validación de seguridad de la BD, creando riesgos significativos que pueden comprometer la delicada continuidad de la BD presente y sobre todo vulnerable a falta de integridad, no repudio y confiabilidad de la información registrada en la BD.

Quienes tomaron la iniciativa de implementar un esquema de auditoría de seguridad de BD para aminorar los riesgos asociados con el almacenamiento de información utilizaron estándares personales e independientes. Nuestro modelo de convención es, no solo que los registros que se almacenan en las BD, sino que también deben ser controlados mediante la auditoria y seguridad, por tal razón lo que se desarrolló fue: establecer el propósito de la BD, encontrar y establecer la información, separar la información en tablas, transformar los elementos en columnas, asignar las llaves primarias, crear relaciones de tabla, afinar el diseño y normalización, asimismo; para la auditoria, se enfocó en resguardar la confiabilidad, integridad y disponibilidad de los datos, realizando buenas prácticas o pilares fundamentales que considera una convención y además de cumplir dentro de las líneas de investigación que está enmarcada en la línea de BD y sistemas de la información.

La organización del trabajo desarrollado es de la siguiente forma: Capítulo I, exponemos el estado del arte donde se describe investigaciones realizadas en otros ámbitos y áreas de aplicación (artículos científicos y trabajos de tesis). En el Capítulo II describimos el problema, fundamentando las cualidades de los controles de auditoría y seguridad de base de datos relacionales. En el Capítulo III puntualizamos la metodología. En el Capítulo IV se muestra los resultados obtenidos y las discutimos con otros trabajos similares.

CAPÍTULO I

REVISIÓN DE LITERATURA

1.1 Contexto y marco teórico

1.1.1 Importancia de la información en la BD

Si se trata de manejar un negocio sin conocimiento de los clientes, productos que se venden, quiénes son los empleados, quiénes son los deudores y acreedores, será una tarea difícil, pues al menos en su totalidad los negocios cuentan con este tipo de registros: equivalente es la importancia para quienes toman decisiones, contar con esos datos disponibles cuando se necesiten. "Se puede decir que el propósito final de los sistemas de información de todos los negocios es ayudarlos a usar la información como un recurso organizacional. En el corazón de todos estos sistemas están la captura, almacenamiento, adherencia, manipulación, diseminación y administración de datos" (Coronel et al., 2018).

Dependiendo del tipo de sistema y particularidades de la entidad, podrían registrar información de miles de megabytes. “¿Cómo pueden procesar enormes cantidades de registros? ¿Cómo logran guardarla y luego recuperar velozmente sólo aquellos datos para la toma de decisiones? La respuesta es que usan". Las BD, poseen la capacidad de almacenar, administrar y consultar datos con bastante rapidez; de hecho, en la actualidad los sistemas utilizan BD, por lo tanto una buena comprensión y el uso es muy importante para cualquier profesional de sistemas de información" (Carlos et al., 2018, p. 734-736).

Las BD registran información valiosa y confidencial. El incremento ascendente de regulaciones de conformidad exige a las organizaciones a realizar auditorías del acceso a dicha información restringida y a proteger de ataques y mal uso o errores humanos que pudieran generarse en su administración. Una BD proporciona acceso a datos a los usuarios, visualización, registro o actualización, en razón con los a los permisos de acceso que se les hayan brindado. Su utilidad es mucho mayor a medida que la suma de datos registrados crece. La ventaja de utilizar BD es que múltiples usuarios pueden acceder a ellas al mismo tiempo (Ingravallo y Entraigas, 2007).

1.1.2 Definición de Base de Datos

Una BD es una compilación de datos relacionados, almacenados en un conjunto con redundancias controladas cuya finalidad es de servir a una o más aplicaciones de la manera más eficiente (Nevado, 2010).

Los datos deben contar con una definición implícita, describiendo situaciones y cambios. Al ser datos relacionados debe existir similitud o homogeneidad y relevantes respecto a su finalidad.

A. Modelos de Datos

Coronel et al., (2018) clasifican los modelos como: conceptuales, orientados a objetos, lógicos y, los emergentes relacionados a Big Data; mismos que de acuerdo a los autores, se describen en resumen en los siguientes cuatro subpuntos.

A.1 Modelos de datos conceptuales

- **Modelo Entidad - Relación.** También conocido como el modelo conceptual de datos, se trata de un enfoque semántico utilizado para representar y desarrollar el diseño conceptual de una base de datos. Este modelo tiene la finalidad de representar gráficamente la estructura conceptual de una base de datos, incorporando información relativa a los datos y las relaciones entre ellos, con el propósito de ofrecer una representación del mundo real. En muchos casos, las acciones realizadas por el sistema están determinadas por los datos que se manipulan. En lugar de centrarse en las funciones, a veces es beneficioso definir los requisitos centrándose en los datos. La abstracción de datos es una técnica que se utiliza para describir el propósito de los datos, en lugar de su apariencia o la manera en que están etiquetados (Gómez, 2013).
- **Modelo Orientado a Objetos.** Es un modelo de datos lógico que captura la esencia de los elementos utilizados en la programación orientada a objetos, por lo tanto, incorpora los principios fundamentales del diseño orientado a objetos, que son: la abstracción, el encapsulamiento, la herencia y el polimorfismo. Las

bases de datos orientadas a objetos permiten al diseñador definir tanto la estructura de objetos complejos como las operaciones que se pueden aplicar a estos objetos. En una base de datos orientada a objetos, cada objeto independiente almacenado recibe una identidad única, y se asume que los objetos complejos pueden ser construidos a partir de componentes más simples (Gómez, 2013).

A.2 Modelos de datos lógicos

- **Modelo Jerárquico.** Los árboles se emplean para expresar de forma lógica la organización de datos, donde un nodo principal (ubicado en la parte superior) puede tener varios nodos secundarios, pero cada nodo secundario está vinculado a un solo nodo principal. En esta estructura, existe un nodo raíz que puede tener múltiples nodos hijos, y a su vez, cada uno de estos nodos hijos puede tener otros nodos hijos, y así sucesivamente. Se ilustra esta disposición en el siguiente esquema de árbol, que muestra dos tipos de registros: departamentos y empleados, permitiendo que varios empleados puedan estar asociados a un mismo departamento (González, 2002).
- **Modelo en Red.** Este enfoque se fundamenta en el uso de una estructura no lineal en la que un registro secundario puede estar vinculado con más de un registro principal. Las entidades se representan como nodos en un grafo, y las conexiones o relaciones entre estos nodos se establecen a través de los arcos que conectan dichos nodos. Un conjunto refleja una relación entre uno o más tipos de registros, lo que facilita la navegación entre estos registros. Un modelo de red ampliamente utilizado es el modelo Codasyl (Peley et al., 2019).
- **Modelo Relacional.** Se utilizan tablas para expresar la estructura lógica de los datos y las relaciones entre ellos en un sistema de gestión de bases de datos relacional. Cada fila de la tabla se conoce como una tupla, y un atributo o conjunto de atributos que identifica de manera única cada tupla se conoce como clave. La siguiente figura representa la información que podría almacenarse en una base de datos relacional que incluye datos sobre los departamentos de una

empresa y los empleados que trabajan en ella. En cuanto al esquema Entidad-Relación (E-R), el esquema relacional que se obtendría mediante la aplicación de reglas de transformación se presenta a continuación. Junto a cada relación se indican, entre paréntesis y separados por comas, los atributos, se subraya la clave primaria de cada relación y se establecen conexiones desde cada clave ajena hacia la clave primaria correspondiente (Uazuay, 2012).

A.3 Modelos de datos físicos

- La etapa final en el proceso de desarrollo de una base de datos involucra la creación de todos los componentes que conformarán la base de datos en un sistema de gestión de bases de datos (SGBD) específico. En el caso de una base de datos relacional, como la mayoría de las utilizadas en la actualidad, esto implica la creación de tablas, índices, vistas, desencadenadores y las relaciones entre ellos. La creación de todos estos elementos puede realizarse de dos maneras: utilizando asistentes que ofrecen interfaces gráficas con herramientas amigables o a través del uso del lenguaje de definición de datos (DDL) proporcionado por el SGBD que se esté utilizando. La forma en que se aborde esta tarea dependerá del SGBD específico que se emplee (Sáenz, 2011).

A.4 Modelos de datos emergentes: Big Data

Big Data agrupa las técnicas de almacenamiento, análisis y manejo de inmensos repositorios de datos, estos son tan inmensos que resulta imposible tratarlos con las herramientas de BD y analíticas convencionales (López et al., 2012). Big Data proporciona las siguientes características:

- Volumen. Grandes volúmenes de datos (TeraBytes o incluso PetaBytes).
- Variedad. Datos estructurados o no estructurados.
- Velocidad. Actualización, procesamiento y análisis en tiempo real.

Con el fin de crear valor a partir de sus grandes almacenes de datos no utilizados anteriormente, las empresas están utilizando nuevas

tecnologías de Big Data. Estas tecnologías emergentes permiten a las organizaciones procesar almacenes de datos masivos de múltiples formatos de forma rentables. Algunas de las tecnologías de Big Data más utilizadas son Hadoop, MapReduce y NoSQL.

Hadoop es un framework computacional y de almacenamiento distribuido, tolerante a fallas y de alta disponibilidad basado en Java. Hadoop usa hardware de bajo costo para crear grupos de miles de nodos de computadora para almacenar y procesar datos.

El Sistema de Archivos Distribuidos de Hadoop (HDFS) es un sistema de almacenamiento de archivos altamente distribuido y tolerante a fallas diseñado para administrar grandes cantidades de datos a altas velocidades. Con el fin de lograr un alto rendimiento, HDFS utiliza el modelo write-once, read many. Esto implica que una vez que los datos se han registrado, no es posible realizar modificaciones.

MapReduce es un framework de programación de aplicaciones (API) de código abierto que facilita un servicio rápido de análisis de datos. Distribuye el procesamiento de los datos entre miles de nodos en paralelo. Funciona con datos estructurados y no estructurados. El framework MapReduce proporciona dos funciones principales, Mapear y Reducir.

NoSQL es un SGBD que difiere del modelo clásico de gestión relacional. Los datos almacenados no requieren estructuras fijas como tablas, normalmente no soportan operaciones JOIN, ni garantizan completamente ACID (atomicidad, Disponibilidad, aislamiento y durabilidad), y habitualmente escalan bien horizontalmente. A menudo se clasifican según su forma de almacenar los datos, y componen categorías como clave-valor, columnares, documentales y orientadas a grafos (Zegarra y Saavedra, 2009).

B. Sistemas de Gestión de Base de Datos

La particularidad definitiva que convierte a un conjunto de datos en una base de datos es la siguiente: una BD se administra por medio de Sistemas de Gestión de Bases de Datos (SGBD) (Camps et al., 2005).

Un SGBD es un software que permite procesar, describir, administrar y recuperar datos almacenados en una BD: permitiendo un fácil acceso a los datos por parte de múltiples usuarios para el manejo de datos. En estos sistemas se proporciona un conjunto coordinado de programas, procedimientos y lenguajes que permiten a los distintos usuarios realizar sus tareas habituales con los datos, garantizando además la seguridad de los mismos (Nevado, 2010).

C. Niveles ANSI/X3/SPARC

La arquitectura ANSI/SPARC, que data de 1977, define los niveles de abstracción para un sistema de administración de BD (Camps et al., 2005, p. 22-28):

- Nivel interno o físico: define cómo se almacenan los datos y los métodos de acceso.
- Nivel lógico o conceptual: se describe la totalidad de los datos que van a ser almacenados mediante la especificación de las entidades y sus atributos, relaciones entre las entidades, restricciones de integridad y de confidencialidad.
- Nivel externo: define las vistas del usuario.

D. Funciones de un SGBD

Piñero (2013) describe las características de un SGBD o sublenguajes, que son: definición o descripción, manipulación y control o utilización, los cuales describe de la siguiente manera:

Función de definición. DDL: "esta función permite al diseñador de la BD especificar los elementos que la integran, su estructura y las relaciones que existen entre ellos, las reglas de integridad y de confidencialidad, así como las características de tipo físico y las vistas de los usuarios. Esta función, se lleva a cabo mediante el empleo de un lenguaje de definición de datos (Data Definition Language - DDL)".

Función de Manipulación. DML: "esta función permite a los usuarios consultar y actualizar los datos almacenados en la BD. La actualización

puede implicar inserción, eliminación y/o modificación. Esta función se lleva a cabo por medio de un lenguaje de manipulación de datos (DML: Data Manipulation Language)"

Función de control. DCL: "esta función integra una serie de instrumentos que facilitan la tarea de administrador de la BD. Incluye, por un lado, las utilidades para la gestión de usuarios y permisos y, por otro lado, las que permiten la administración del sistema. Con respecto a esta última, se debe tener en cuenta que los administradores deben monitorizar el funcionamiento de la BD, realizar copias de seguridad, proteger la BD frente a accesos no autorizados, etc. Algunas tareas de la función de control se llevan a cabo por medio de un lenguaje de control de datos (DCL: Data Control Language)".

E. Características de un SGBD

Por otra parte, haciendo referencia a la arquitectura de tres niveles definida por el modelo ANSI/SPARC que mantiene los datos y el procesamiento separados; denota que un SGBD debe tener las siguientes características (Elmasri y Navathe, 2016):

- Independencia física: La capa física puede ser alterada sin afectar la capa conceptual. Esto implica que los usuarios no necesitan tener conocimiento de todos los detalles técnicos relacionados con el hardware de la base de datos, ya que este es simplemente una estructura subyacente que se encarga de representar los datos almacenados de manera transparente.
- Independencia lógica: La capa conceptual debe ser capaz de adaptarse sin influir en la capa física. En otras palabras, los administradores de bases de datos pueden introducir mejoras y modificaciones sin que esto tenga un impacto en la experiencia de los usuarios.
- Facilidad de uso: Las personas que no están familiarizadas con la base de datos deben poder describir sus consultas sin necesidad de referirse a los componentes técnicos de la base de datos, lo que

facilita la comunicación y el acceso a la información para usuarios no técnicos.

- Respuesta rápida: El sistema debe ser capaz de proporcionar respuestas ágiles a las consultas, lo que implica la utilización de algoritmos de búsqueda eficientes. El rendimiento también dependerá de la infraestructura informática disponible.
- Gestión centralizada: El sistema de gestión de bases de datos (SGBD) debe permitir a los administradores manipular los datos, añadir elementos y verificar su integridad de manera centralizada, simplificando así la administración de la base de datos.
- Redundancia controlada: El SGBD debe tener la capacidad de minimizar la redundancia de datos siempre que sea factible, con el objetivo de reducir errores y evitar el desperdicio de recursos de almacenamiento.
- Verificación de integridad: Los datos almacenados en la base de datos deben mantener Disponibilidad interna, y cuando un elemento hace referencia a otro, es esencial que estos elementos referenciados estén presentes y disponibles.
- Compartición de datos: El SGBD debe posibilitar que múltiples usuarios accedan de manera simultánea a la base de datos, lo que permite el acceso concurrente a los datos.
- Seguridad de datos: El SGBD debe ser capaz de administrar y controlar los derechos de acceso a los datos de cada usuario, garantizando así la seguridad y la privacidad de la información almacenada.

En base al cuadrante mágico de Gartner (2019) para Sistemas de Gestión de Base de Datos Operacionales, lo referente a SGBD relacionales, entre privativos y libres, entre los principales, se pueden mencionar:

E.1 Oracle Database

Es un sistema de gestión de BD privativo de tipo objetorelacional (ORDBMS, por el acrónimo en inglés de Object-Relational Database

Management System), multiplataforma, propio de Oracle Corporation y/o sus afiliados.

Un servidor de BD Oracle consiste en una BD y al menos una instancia. Debido a que una instancia y una BD tan estrechamente conectado, el término BD Oracle a veces se usa para referirse tanto a la instancia como a la base de datos (Bhatiya y Potineni, 2020). Las recientes versiones están certificadas para trabajar bajo GNU/Linux.

E.2 Microsoft SQL Server

Es un SGBD del modelo relacional de licencia privativa Microsoft EULA, desarrollado por Microsoft.

El lenguaje de desarrollo utilizado es Transact-SQL (TSQL) ya sea por línea de comando o mediante el Management Studio, implementación del estándar ANSI de SQL, utilizado para manipular (DML), crear tablas y definir relaciones (DDL).

SQL Server tradicionalmente ha estado disponible solo para sistemas operativos Windows de Microsoft, pero desde 2017 también está disponible para Linux y Docker Containers (Microsoft, 2021).

E.3 PostgreSQL

Es un SGBD relacional orientado a objetos, siendo ahora la BD de código abierto más avanzada disponible en cualquier plataforma. Como muchos otros proyectos de código abierto, el desarrollo de PostgreSQL no es manejado por una empresa o persona, sino que es dirigido por una comunidad de desarrolladores que trabajan de forma desinteresada, altruista, libre o apoyados por organizaciones comerciales, denominada el PGDG (PostgreSQL Global Development Group) (PostgreSQL, 2020).

E.4 MySQL

MySQL es un sistema de gestión de bases de datos relacional SQL de doble licencia, la Licencia Pública General de GNU y la licencia comercial estándar de Oracle Corporation y/o sus afiliados, considerada

como la base de datos open source más popular del mundo, y una de las más populares en general junto a Oracle y Microsoft SQL Server, sobre todo para entornos de desarrollo web (Oracle, 2021). Desarrollado en ANSI C y C++. Considerado como uno de los cuatro componentes de la pila LAMPY WAMP.

E.5 MariaDB

Es un SGBD derivado de MySQL con licencia GPL (General Public License). Software multiplataforma de código abierto y como base de datos relacional, interfaz SQL para acceder a los datos, las últimas versiones de MariaDB incluyen características GIS y JSON. Tiene una alta compatibilidad con MySQL ya que posee las mismas órdenes, interfaces, APIs y bibliotecas, siendo su objetivo poder cambiar un servidor por otro directamente (MariaDB, 2022). MariaDB es una bifurcación de MySQL MariaDB es un fork directo de MySQL que asegura la existencia de una versión de este producto con licencia GPL, para ello la Fundación MariaDB apoya la continuidad y la colaboración abierta en el ecosistema MariaDB.

1.1.3 Auditoría en informática

A. Auditoría como actividad profesional

"El desarrollo normal de las actividades comerciales y financieras de las empresas requiere una constante vigilancia y evaluación; asimismo, las entidades necesitan una opinión, preferiblemente independiente, que les ayude a medir la eficiencia y eficacia en el cumplimiento de sus objetivos. Por lo general, la evaluación consiste en una revisión metódica, periódica e intelectual de los registros, tareas y resultados de la empresa, con lo cual se busca medir y diagnosticar el comportamiento global en el desarrollo de sus actividades y operaciones. Eso es auditoría." (Muñoz 2002, p. 10-45).

La revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad constituida, es realizada por un profesional de auditoría, con el propósito de evaluar su correcta realización y,

con base en ese análisi poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones (Muñoz 2002, p. 88-94).

A pesar de que se llevan a cabo múltiples formas de auditoría, todas ellas culminan en la emisión de una evaluación sobre un registro, sistema, operación o actividad en concreto, la cual puede estar orientada hacia propósitos específicos.

1.1.4 Tipos de auditoría

Según Sandoval (2012) tradicionalmente se consideran dos tipos de auditoría según el personal que la desempeña, las internas y las externas:

Auditoría Interna: La auditoría interna es llevada a cabo por individuos que pueden o no tener una relación de dependencia con la entidad que están revisando. Estos profesionales se enfocan en evaluar repetidamente áreas que son de particular interés para la administración, pero también pueden llevar a cabo revisiones programadas de diversos aspectos operativos y de registro en la empresa, con el propósito de generar un informe que refleje sus hallazgos.

Auditoría Externa: La auditoría externa es realizada por expertos que no tienen ninguna vinculación económica ni de otro tipo con la empresa. Su imparcialidad es ampliamente reconocida y confiable para terceros. El propósito fundamental de su trabajo es emitir un dictamen sobre la situación evaluada. Además de estos tipos de auditoría, Sandoval (2012) señala que existen otros en función del objeto de análisis o área de aplicación, como:

Auditoría Financiera (contable), es la revisión sistemática, exploratoria y crítica que realiza un profesional de la contabilidad a los libros y documentos, a los controles y registros de las operaciones financieras y la emisión de los estados financieros, con el fin de evaluar y opinar la razonabilidad, veracidad, confiabilidad y oportunidad en la emisión de los resultados financieros obtenidos durante un periodo específico o un ejercicio fiscal.

Auditoría Administrativa: Se trata de una evaluación minuciosa y sistemática de la gestión administrativa de una empresa, incluyendo su estructura organizativa, las interacciones entre su personal, y la conformidad con los procedimientos y funciones que rigen sus operaciones.

Auditoría Operacional: Es una revisión específica y en profundidad de las operaciones de una empresa, con el objetivo de evaluar su existencia, adecuación, eficacia, eficiencia y la correcta ejecución de sus actividades, independientemente de su naturaleza.

Auditoría Integral: Implica una revisión exhaustiva, sistemática y completa realizada por un equipo multidisciplinario de profesionales que abarca todas las actividades y operaciones de una empresa. Su finalidad es evaluar de manera integral el adecuado desempeño de las funciones en todas las áreas administrativas.

Auditoría Gubernamental: Consiste en una revisión exhaustiva, sistemática y detallada de todas las actividades y operaciones en una entidad gubernamental, sin importar la naturaleza de sus departamentos y entidades en el ámbito de la administración pública.

Auditoría Informática: Representa una evaluación técnica y especializada de los sistemas informáticos, software e información utilizados en una empresa, ya sea de manera individual, compartida o en red. Esto incluye la revisión de instalaciones, telecomunicaciones, mobiliario, equipos periféricos y otros componentes relacionados.

1.1.5 Auditoría de TIC (Auditoría Informática)

Según la Presidencia del Consejo de Ministros (2016) este proyecto de Norma Técnica Peruana detalla los criterios necesarios para establecer, ejecutar, mantener y perfeccionar de forma constante un sistema de administración de seguridad de la información que se adapte al entorno específico de la organización. Además, aborda las pautas relacionadas con la evaluación y el tratamiento de los riesgos de seguridad de la información, adaptados a las necesidades particulares de la organización.

Por otra parte, Postigo (2020) define la auditoría informática como "el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos".

A su vez, Gisbert (2015, p. 567) destaca los tipos de auditoría informática:

- Auditoría Legal: Evalúa el cumplimiento de las medidas de seguridad requeridas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos en términos de cumplimiento legal.
- Auditoría de Bases de Datos: Examina los controles relacionados con el acceso, la actualización, la integridad y la calidad de los datos.
- Auditoría de Seguridad de Datos: Verifica la disponibilidad, integridad, confidencialidad, autenticación y no repudio de los datos e información.
- Auditoría de Seguridad Física: Evalúa la ubicación de la organización, minimizando riesgos y preservando la confidencialidad de su ubicación. Incluye medidas de protección física, como sistemas de seguridad, circuitos cerrados de televisión y seguridad en el entorno.
- Auditoría de Seguridad Lógica: Aborda los métodos de autenticación utilizados en los sistemas de información.
- Auditoría de Comunicaciones: Se concentra en la auditoría de los procesos de autenticación en los sistemas de comunicación.
- Auditoría de Seguridad en Producción: Se enfoca en la detección y prevención de errores, incidentes y actividades fraudulentas.

1.1.6 Auditoría de base de datos

Según Piattini (2008) la auditoría de bases de datos es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

- Identificación del usuario que accede a los datos.
- Registro de la fecha y hora de acceso a los datos.
- Documentación del dispositivo o aplicación desde el cual se realizó el acceso.
- Geolocalización del punto de acceso en la red.
- Registro de la sentencia SQL ejecutada.
- Documentación de los resultados y efectos del acceso a la base de datos.

A. La Auditoría de BD es importante porque:

- Dado que toda la información financiera se almacena en bases de datos, es imperativo establecer controles de acceso efectivos a dichos datos.
- Es esencial contar con la capacidad de demostrar la integridad de la información.
- Se deben implementar medidas para mitigar los riesgos relacionados con la pérdida de datos y la filtración de información.
- Las organizaciones son responsables de salvaguardar la información confidencial de sus clientes.
- Los datos se transforman en información a través del uso de bases de datos.
- Las organizaciones deben tomar medidas sustanciales para proteger sus datos, y esto va más allá de la mera seguridad de los mismos.

B. Mediante la auditoría de bases de datos se evaluará:

- Establecimiento de estructuras físicas y lógicas para las bases de datos.
- Supervisión de la carga y el mantenimiento de las bases de datos.
- Garantía de la integridad de los datos y la protección de los accesos.
- Adhesión a estándares en el análisis y la programación relacionados con el uso de bases de datos.
- Implementación de procedimientos para realizar copias de seguridad y recuperar datos.

C. Planificación de la Auditoría de BD

- Realizar un inventario exhaustivo de todas las bases de datos en uso dentro de la organización.
- Categorizar los niveles de riesgo asociados a los datos almacenados en cada base de datos.
- Llevar a cabo un análisis detallado de los permisos de acceso otorgados.

- Evaluar los controles de acceso existentes en relación con las bases de datos.
- Definir los modelos de auditoría de bases de datos que se aplicarán.
- Establecer los procedimientos de prueba específicos que se llevarán a cabo para cada base de datos, aplicación y/o usuario.

1.1.7 Auditoría de seguridad de bases de datos

Para Calbimonte (2016) la auditoría de seguridad de base datos (ASBD), además de ver aspectos de auditoría en BD, se enfoca en asegurar la confiabilidad, integridad y disponibilidad de los datos. Se recomienda la implementación de las siguientes auditorías a nivel de base de datos como parte integral de cualquier sistema de Administración de la Seguridad de la Base de Datos (ASBD):

A. Auditoría a nivel de esquema:

- Registro de actividades DDL (Data Definition Language).
- Documentación de cambios realizados en procedimientos almacenados y desencadenadores.
- Seguimiento de cambios en los privilegios, usuarios y atributos de seguridad.

B. Auditoría a nivel de datos:

- Registros de cambios en datos sensibles a través de actividades DML (Data Manipulation Language).
- Monitorización de sentencias SELECT.

C. Auditoría de cualquier modificación en la configuración de auditoría.

D. Considerar la posibilidad de aplicar cifrado en toda la base de datos, tablas específicas o celdas particulares.

Estas opciones representan soluciones de auditoría de seguridad de base de datos nativas que pueden contribuir a cumplir con estos requisitos.

1.1.8 Regulaciones de auditoría de Base de Datos

A. ISO/IEC 15408

La norma ISO/IEC 15408, también conocida como Criterios Comunes, se centra en la salvaguarda de activos contra la divulgación no autorizada, alteración o pérdida de utilidad. Comúnmente, se clasifican en tres categorías de protección: confidencialidad, integridad y disponibilidad, las cuales abordan los distintos tipos de vulnerabilidades de seguridad. Además, esta norma puede ser relevante en el ámbito de la seguridad de la tecnología de la información (TI), incluso más allá de estos tres aspectos principales. ISO/IEC 15408 se aplica tanto a los riesgos originados por acciones humanas, ya sean maliciosas o no, como a aquellos derivados de eventos no relacionados con seres humanos. Aunque su aplicación puede extenderse a otras áreas, la norma no establece obligaciones específicas en dichos Confidencialidads (ISO/IEC, 2009).

B. ISO/IEC 17799

La norma 17799, también conocida como ISO/IEC 27002, se define como una guía protocolar para la implementación de un sistema de gestión de la seguridad de la información. En términos generales, proporciona directrices basadas en sugerencias que las organizaciones deben tener en cuenta para desarrollar un programa integral de gestión de la seguridad de la información. Su enfoque principal es preservar los principios fundamentales de confidencialidad, integridad y disponibilidad.

Además, la norma 17799 ofrece una estructura que facilita la identificación e implementación de soluciones para diversos riesgos. En lo que respecta a los datos, se destacan aspectos como la clasificación y el control de activos, el control de acceso, y el desarrollo y mantenimiento del sistema. En 2007, la norma ISO/IEC 17799 se incorporó a la familia de normas ISO/IEC 27000 y fue rebautizada como ISO/IEC 27002. A pesar de este cambio de nombre, las directrices establecidas en la norma

siguen siendo una referencia sólida y fundamental para las mejores prácticas en seguridad de la información.

1.1.9 Delitos Informáticos

Del Pino (2016) define los delitos informáticos como "todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro". Concluyendo, "es todo acto o conducta ilícita e ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular, cualquier sistema informático o alguna de sus partes, con finalidad de causar lesión o poner en peligro un bien jurídico cualquiera".

1.1.10 Ética Informática

Según Moor (2018) la ética en el ámbito de la informática, respaldada por códigos de ética profesionales, desempeña un papel fundamental en el uso adecuado de la tecnología informática. La Ética Informática se enmarca en la ética general y se concentra en la relación entre la creación, organización, difusión y utilización de la información, en consonancia con los principios éticos y morales que guían la conducta humana. En esencia, consiste en un conjunto de normas morales que regulan el empleo de tecnologías de la información.

La ética en informática abarca diversos aspectos, como la prevención de delitos informáticos, la responsabilidad ante posibles fallos en sistemas informáticos, la protección de la privacidad, la salvaguardia de datos, así como el uso adecuado de registros y software.

Existen diversos documentos y códigos de ética que proporcionan directrices fundamentales para profesionales informáticos y usuarios, sirviendo como referencia en cuanto a conducta ética. Entre estos, se pueden mencionar ejemplos como el Código de Ética y Conducta Profesional de la ACM

(Association for Computing Machinery), el Código de Ética y Conducta Profesional de la ACS (Australian Computer Society), los Diez Mandamientos de la Ética Computacional y el Código de Ética y Conducta del IEEE (Institute of Electrical and Electronics Engineers), que orientan el comportamiento ético en el ámbito de la informática.

1.1.11 Prácticas de auditoría de seguridad de Base de Datos

A. Añadir campos a las tablas

Domínguez (2016) en su artículo "Cómo auditar cambios en una tabla MySQL O MariaDB", da una propuesta práctica para auditar una tabla en particular a partir de tres campos básicos, a los que adicionalmente se puede agregar dos campos, usuario e ip, para lograr una auditoría completa. Las modificaciones en los datos de una tabla se realizan a través de las sentencias insert, delete, update, donde los triggers pueden capturar estas acciones y se ejecutan antes (before) y/o después (after) de que los datos sean alterados. Se abordan tres campos fundamentales en cada tabla que se somete a auditoría. El primer campo, denominado "id", se configura como un número entero largo con incremento automático y se designa como clave primaria. El segundo campo, creado y tercer campo, modificado, son de tipo fecha y hora, valor por defecto fecha/hora actual,

Por otra parte Joshi (2017) en su artículo “Spring Data JPA Auditing: Automatically Saving the Good Stuff", presenta una idea similar, basada también en la adición de columnas, en la que trata el tema de seguir cada operación de inserción, actualización y eliminación y luego almacenarla, esto ha sido utilizado por JPA e Hibernate, los cuales proporcionan auditoría automática bajo el siguiente esquema:

Configurar JPA para adicionar automáticamente las columnas CreadoPor, FechaCreacion, ModificadoPor y FechaModificacion para cualquier entidad. Con esto se logra almacenar quién creó y modificó cualquier fila en un momento dado. El enfoque Spring Data JPA abstrae trabajando con devoluciones de llamada JPA y proporciona estas

anotaciones para guardar y actualizar automáticamente entidades de auditoría.

A diferencia de la anterior propuesta que solo plantea una metodología, la solución con JPA ya se encuentra desarrollada, es de código abierto (disponible en su repositorio de GitHub).

B. Para cualquier entidad, el diseño sería semejante a:

B.1 Consolidado histórico de todas las tablas

Bajo esta metodología, Hassan (2016) en su artículo “Audit and Log Database DML Changes in PostgreSQL With Cyan Audit", explica que Cyan Audit es una extensión privativa para PostgreSQL que se encarga de detectar todos los cambios en BD referentes al DML y los guarda en una sola tabla, en un esquema independiente distinto, pero dentro de la misma BD.

B.2 Logs de Transacciones o Sesión

PGAudit (2022) en la extensión de auditoría de código abierto para PostgreSQL llamada "PgAudit", se ofrece un exhaustivo registro de auditoría de sesiones y objetos mediante la función de registro convencional de PostgreSQL. El propósito fundamental de PgAudit es otorgar a los usuarios de PostgreSQL la capacidad de generar registros de auditoría que suelen ser necesarios para satisfacer los requisitos de certificaciones gubernamentales, financieras o ISO.

De igual manera, otras soluciones integradas como SQL Server Audit para SQL Server (Microsoft, 2021a) o la Auditoría Unificada que posee Oracle (Perez et al., 2015), usan un registro de transacciones DDL y DML, capturando los logs de auditoría en archivos propios de la tecnología y disponible sólo desde la misma, donde a pesar de poseer enfoques similares, los criterios a capturarse son diferentes para cada alternativa.

B.3 Tablas espejo

Braren (2016) sugiere una metodología que consiste en la adición de campos a una tabla, para proporcionar una visión más completa acerca del motor de base de datos utilizado, una alternativa sería la implementación de triggers a nivel de la base de datos que se activan en respuesta a eventos CRUD.

1.1.12 Definición de Convención

"Una convención es un conjunto de estándares, reglas, normas o criterios que son de aceptación general para un determinado grupo social; frecuentemente toman el nombre de criterios". Ciertos tipos de convenciones pueden llegar a ser leyes o estar definidas por organismos reguladores para formalizar o forzar su cumplimiento (por ejemplo, está regulada la convención sobre el lado de la carretera por el que debe circular un vehículo). En otros Confidencialidads las convenciones tienen el carácter de ley no escrita (por ejemplo, que ropa es adecuada para un hombre y cual para una mujer) (Law, 2022).

En el software libre, el término convenciones, es ampliamente utilizado por las diferentes comunidades para referirse a criterios, buenas prácticas o pilares fundamentales, respecto a modelos, frameworks, código fuente, nomenclatura, en general, al ámbito de la programación.

1.1.13 Exploración de las prácticas actuales en la auditoría de base de datos

Se desarrolló un análisis integral: ventajas, desventajas y características ideales de la auditoria de seguridad en bases de datos.

A. Añadir campos a las tablas

Esta propuesta ofrece un enfoque práctico para auditar tablas específicas mediante el uso de tres campos básicos (id, creado, modificado) a los que, de manera opcional, se pueden añadir dos campos (usuario e ip). Además, se presenta una variante similar que incluye los campos: creado_por, fecha_creación, modificado_por y fecha_modificacion. Ambas alternativas permiten agregar campos de auditoría a las tablas que requieran un seguimiento detallado de registros,

facilitando la actualización de los campos de control mediante la utilización de desencadenadores.

A.1 Ventajas

- Una implementación de este tipo presenta una ventaja principal clave: todos los campos de auditoría se encuentran directamente en cada registro de las tablas, evitando la necesidad de consultar otras fuentes para conocer la información sobre quién y cuándo se creó o modificó un registro.
- Además, su implementación resulta sumamente sencilla. Simplemente se requiere agregar las columnas "creado_por", "fecha_creacion", "modificado_por" y "fecha_modificacion" a cada tabla. Luego, es posible completar estos nuevos campos mediante desencadenadores, aplicaciones en segundo plano o enviando datos directamente desde la aplicación cliente que utilice la BD correspondiente a la tabla.
- El incremento del tamaño de archivos de la BD será mínimo, ya que solo se añaden cuatro nuevos campos de tipo texto y fecha. Debido a este crecimiento adicional insignificante, la velocidad para obtener respaldos y copiarlos a otra ubicación no se verá afectada de manera significativa. La transferencia de archivos por el tamaño extra es prácticamente despreciable.

A.2 Desventajas

- Esta implementación tiene como objetivo proporcionar la mayor cantidad de pistas para la auditoría, pero presenta algunas limitaciones importantes. Una de ellas es que no se conserva un historial completo de cada registro, ya que solo se almacena información de creación y la última modificación, omitiendo cualquier cambio intermedio que haya experimentado una fila específica. Esto resulta en la pérdida de datos sobre la evolución de los registros, ya que solo se muestra la versión actual.
- En caso de necesitar deshacer cambios o reconstruir registros tras una acción de manipulación de datos, esta tarea puede volverse

compleja, ya que se requerirá un arduo trabajo con los archivos de la BD o la reproducción de información desde otras fuentes como copias de seguridad o documentos impresos, si están disponibles.

- Otra desventaja es el crecimiento horizontal de la BD, lo que limita su viabilidad principalmente para nuevos sistemas, para evitar la presencia de datos nulos. Además, agregar más campos a las tablas puede aumentar considerablemente el tiempo de consulta cuando se requiera obtener datos de todos esos campos.
- Un factor crítico es que, al tener datos confidenciales almacenados directamente en cada registro, incluidos los datos de auditoría, estos se vuelven vulnerables a modificaciones malintencionadas. Cualquier usuario con privilegios altos de acceso a la BD podría eliminar pistas de auditoría sin dejar rastro alguno, lo que comprometería la integridad de los datos y crearía un potencial agujero de seguridad para manipulaciones informáticas.
- Es importante destacar que esta implementación también expone la desventaja de que un usuario con altos privilegios de acceso a la BD pueda eliminar datos directamente en cada registro, incluidos los datos de auditoría, lo que resultaría en la desaparición de datos probablemente importantes y/o confidenciales sin dejar ningún rastro de esta acción.

B. Consolidado histórico de todas las tablas

Para una organización más eficiente y una fácil administración, se propone centralizar la auditoría en una única tabla, ubicada en un esquema independiente y distinto dentro de la misma base de datos. En esta tabla consolidaremos los siguientes campos: audit_field, pk_vals, recorded, uid, row_op, txid, audit_transaction_type, old_value y new_value. Al centralizar estos datos, se simplifica la consulta y análisis de la información de auditoría, lo que facilita el seguimiento y control de los cambios realizados en la BD.

B.1 Ventajas

- Esta implementación ha ganado popularidad en la actualidad, especialmente porque grandes bases de datos, como PostgreSQL, la plataforma de código abierto más ampliamente utilizada, han adoptado esta convención en su nuevo módulo de auditoría, PgAudit, disponible en GitHub. De manera similar, CyanAudit, otra extensión de auditoría para PostgreSQL, también sigue este enfoque.
- Con esta alternativa, se crea una sola tabla que actúa como un registro en forma de bitácora, manteniendo un historial completo de cambios para cada registro en todas las tablas. La consolidación de la información en una única tabla facilita las consultas de auditoría, eliminando la necesidad de buscar en diferentes lugares para cada tabla. Simplemente realizando consultas con filtros, es posible obtener toda la información deseada.
- Un aspecto destacado es que cada acción DML (Data Manipulation Language) se registra por campo, independientemente de la cantidad de columnas que tenga una tabla. Esto asegura que no haya dependencia de la estructura de la base de datos, permitiendo agregar o quitar columnas en las tablas sin necesidad de modificar el módulo de auditoría para su correcto funcionamiento.
- A diferencia de la alternativa anterior, esta solución proporciona un historial completo de cambios por cada registro, acompañado de campos de auditoría como usuario, fecha, antiguo valor, nuevo valor y tipo de transacción. Mantener almacenada la evolución de un registro posibilita reconstruir la información en cualquier punto temporal deseado. Además, el hecho de registrar cada cambio mejora la integridad de los datos, asegurando un seguimiento preciso de todas las modificaciones realizadas.

B.2 Desventajas

- Esta implementación presenta un inconveniente significativo que no puede pasarse por alto: el crecimiento exponencial de la BD debido al registro individual de cada cambio por cada registro. Por ejemplo,

si una tabla tiene 15 columnas y 14 de ellas son modificadas, se agregarán 14 nuevas filas a la tabla de auditoría. En el caso de inserciones o eliminaciones, se añadirán 15 nuevas filas en la tabla de auditoría.

- Además, al ubicar la tabla de auditoría en la misma BD o en un esquema diferente exclusivo para auditoría, pero aún dentro de la misma BD, la tabla de auditoría crecerá considerablemente y representará el uso adicional de espacio en disco. Esto imposibilita la segmentación física o lógica de la tabla, lo que se traduce en backups de la BD exponencialmente más grandes en cuanto a su tamaño en disco. Aunque algunos motores de bases de datos como PostgreSQL permiten obtener backups por esquema, esto no resolverá completamente el problema del crecimiento exponencial de la tabla de auditoría.
- Otro aspecto a considerar es el tamaño de los campos "antiguo valor" y "nuevo valor", que deben ser de gran tamaño para soportar los diferentes valores posibles y registrar los cambios de cualquier columna en las tablas. Sin embargo, utilizar el tipo de dato texto implica perder las características del tipo de dato original de cada campo, lo que dificulta la reconstrucción de la estructura de la BD.
- Por último, al almacenar cada alteración de cualquier campo de cualquier tabla en una única tabla, el procesamiento interno se complica en caso de necesitar reconstruir la información (rollback) debido a ejecuciones descontroladas de la sentencia SQL "delete from <tabla>" sin condición, o para restaurar los datos a una fecha determinada. Incluso realizar consultas de datos en la tabla que almacena el historial se vuelve complicado y lento, lo que dificulta su visualización y manejo.

C. Tablas espejo

Con un enfoque centrado en el uso de desencadenadores, se implementa un sistema de auditoría que incluye la adición de campos de control a cada tabla original, así como la creación de una copia idéntica de cada tabla.

Mediante el uso de desencadenadores, se capturan las modificaciones realizadas en las tablas originales y se registran los detalles de auditoría en los campos de control añadidos. Estos campos permiten rastrear quién realizó la modificación, cuándo ocurrió y cuál fue el tipo de transacción llevada a cabo.

Además, se crea una réplica exacta de cada tabla original, que actúa como un repositorio para mantener el historial completo de cambios. La copia conserva los datos anteriores a cada modificación y proporciona una vista histórica de los registros, lo que facilita la reconstrucción de la información en cualquier punto temporal deseado.

Este enfoque permite mantener la estructura original de la BD y conservar las características de los tipos de datos utilizados. Además, al almacenar los registros de auditoría en una tabla independiente, se evita el crecimiento exponencial de la BD, manteniendo un tamaño manejable y un proceso de consulta más eficiente.

C.1 Ventajas

- Uno de los aspectos más destacados de esta implementación es la organización y segmentación de la información de auditoría. Gracias a la similitud en la estructura de cada tabla de auditoría con las tablas originales, realizar consultas al historial de una tupla en la tabla de auditoría correspondiente resulta mucho más sencillo. La visualización de datos es coherente y cómoda debido a que la tupla crece verticalmente, lo que facilita el análisis del conjunto de cambios.
- La presencia de tablas espejo con estructuras similares a las tablas originales es otra ventaja significativa. Al tener campos adicionales de control en cada tabla de auditoría, reconstruir tanto la estructura de las tablas como los datos se vuelve una tarea sencilla. La capacidad de reconstrucción es especialmente relevante en situaciones como la ejecución descontrolada de la sentencia SQL "delete from <tabla>" sin condición o cuando es necesario restaurar los datos a una fecha determinada.

- Esta implementación también adopta la adición de campos en las tablas, como se propuso en la primera alternativa. Esto permite visualizar algunos campos de auditoría directamente en cada registro de las tablas, y si es necesario obtener detalles más exhaustivos, se puede recurrir a la tabla de auditoría respectiva.

C.2 Desventajas

- Como se mencionó anteriormente, es fundamental tener en cuenta que el crecimiento de la BD puede ser significativo según la frecuencia de modificaciones de los datos, oscilando desde unos cientos de megabytes hasta varios miles de gigabytes. Este aumento acelerado en el tamaño de la BD se debe a que por cada acción DML, se inserta una nueva fila completa en la tabla de auditoría. Incluso si solo se modifican dos de las 15 columnas de una tabla, se almacenará una nueva fila con todas las columnas en la tabla de auditoría, sin discriminar si algunas de ellas no han sufrido cambios. Esto resulta en el almacenamiento innecesario de toda la fila, lo que contribuye al crecimiento exponencial de la BD.
- Además, el hecho de que la tabla de auditoría se encuentre en la misma BD, y que sea la de mayor tamaño, representa un uso adicional de espacio en disco y limita la posibilidad de segmentar física o lógicamente la base de datos para facilitar su administración y optimizar el rendimiento.
- En consecuencia, al obtener un respaldo completo de toda la BD, este será al menos un 100% más grande que los datos no auditados en su estado actual. Esto implica que el proceso de respaldo y restauración puede volverse más lento y requerir mayores recursos de almacenamiento.
- Es importante considerar estas implicaciones al implementar un sistema de auditoría, buscando equilibrar la necesidad de información detallada para auditoría con el impacto en el tamaño y rendimiento de la BD. Estrategias como la segmentación de la BD, la optimización de los campos de auditoría y el almacenamiento selectivo de información seleccionada pueden ayudar a mitigar el

crecimiento exponencial de la base de datos y a garantizar un proceso de auditoría más eficiente y manejable.

D. Directrices y lineamientos de controles de auditoría en BD

- Cada tabla debe contar con una llave primaria autonumérica no nula para asegurar la unicidad de los registros.
- Se deben evitar eliminaciones físicas de registros en la base de datos, optando por eliminaciones lógicas para preservar la integridad de los datos.
- Es imprescindible incluir un campo que especifique el estado de activo o inactivo de cada registro en cada tabla para facilitar la gestión y el análisis de datos.
- Mínimamente, se debe almacenar información sobre quién (usuario) y cuándo (fecha y hora) creó una tupla específica para trazar cambios y responsabilidades.
- Se recomienda cifrar la columna de usuario para proteger la información confidencial y mejorar la seguridad de la base de datos.
- Se debe mantener por separado los datos y su evolución de auditoría para facilitar la gestión y evitar redundancias innecesarias.
- Es vital establecer una política de niveles de acceso para garantizar la confidencialidad y controlar la manipulación de datos por usuarios autorizados.
- Debe ser posible reconstruir la información a partir de los registros de auditoría de manera automatizada y retroceder a un periodo o estado determinado para fines de auditoría o recuperación de datos.
- Se debe registrar cada inserción, modificación y/o eliminación de cada registro para contar con un historial completo de cambios en la base de datos.
- También se debe registrar el tipo de acción realizada, ya sea inserción, modificación y/o eliminación, para un seguimiento detallado de las operaciones realizadas.
- Se debe evitar tener columnas calculables en exceso, evitando modificaciones directas en la tabla por cada ejecución de funciones para obtener reportes.

- Es recomendable llevar todas las tablas de la base de datos, cuando sea necesario, hasta la tercera forma normal para evitar redundancias y mantener una estructura óptima.
- Utilizar una nomenclatura coherente con el motor de base de datos para establecer nombres de base de datos, tablas, columnas, funciones y otros elementos en la estructura de la base de datos, lo que facilitará la comprensión y mantenimiento del sistema.

1.2 Antecedentes

1.2.1 Internacionales

En la actualidad, las bases de datos desempeñan un papel crucial al almacenar información valiosa y confidencial, convirtiéndose en uno de los activos más importantes para las organizaciones (Maya, 2015). Al igual que cualquier otro activo, es fundamental gestionarlas con cuidado para garantizar su seguridad, protección, confidencialidad, integridad, disponibilidad y uso efectivo, permitiendo además su posterior auditoría (DAMA International, 2017).

Existen diversos tipos de auditoría que, en última instancia, tienen como objetivo emitir una opinión sobre registros, sistemas, operaciones o actividades específicas en un momento determinado (Aguirre, 2016). La auditoría de bases de datos (BD), es un tipo de auditoría informática que se enfoca en medir, asegurar, demostrar, verificar, monitorear y registrar de manera continua la información almacenada en las bases de datos, con el propósito de minimizar los riesgos inherentes (Villalobos, 2008).

La incorporación de la característica de auditable a las bases de datos es esencial para garantizar la confidencialidad, integridad y disponibilidad de los datos. Existen implementaciones tanto a nivel de esquema como a nivel de datos. En la segunda opción, se registra cada cambio realizado en los registros y se realiza un seguimiento continuo de los datos almacenados, similar a una bitácora o historial de cambios. En otras palabras, se almacena de manera constante cada operación de inserción, actualización y eliminación en los registros (Lu et al., 2013), esta capacidad puede facilitar tareas como el análisis en auditorías, la detección de errores y anomalías, la identificación de cambios no autorizados y la

reconstrucción de información, lo que brinda condiciones más seguras y confiables y fortalece la seguridad de la información (Rus y Danescu, 2010).

Con la meta de llevar a cabo auditorías en bases de datos, han surgido diversos plugins de auditoría de licencia privativa, especialmente diseñados para MySQL o MariaDB. Estos plugins se diferencian en el formato de registro de los datos, las capacidades de filtrado y el nivel de detalle de los registros de auditoría. Además, operan a nivel del lenguaje de definición de datos, conocido como Data Definition Language o DDL (Glushchenko, 2014).

También hay otras soluciones integradas, como SQL Server Audit para SQL Server (Microsoft, 2023) y la Auditoría Unificada de Oracle (Peréz et al., 2015), ambas soluciones están implementadas internamente bajo licencia privativa, pero ofrecen la funcionalidad de interactuar con el lenguaje de manipulación de datos, conocido como Data Manipulation Language o DML. Sin embargo, han surgido propuestas prácticas que se centran en mantener registros históricos de los datos con un control total; por ejemplo, se sugiere añadir tres campos básicos a la misma tabla (ID autonumérico, fecha de creación y de modificación), opcionalmente dos campos adicionales, usuario e IP, para una auditoría más completa (Domínguez, 2016).

Siguiendo un enfoque similar, se ha publicado un artículo que propone las columnas "Creado_Por", "Fecha_Creación", "Modificado_Por" y "Fecha_Modificación" para cualquier entidad, implementadas automáticamente solo en proyectos con Java Persistence API o JPA (Joshi, 2017). Por otro lado, se plantea una variación en la que se propone implementar la solución anterior en una tabla separada (Braren, 2016). Además, existe Cyan Audit para PostgreSQL, una extensión privativa que detecta todos los cambios en la base de datos relacionados con el DML y los guarda en una sola tabla en un esquema independiente dentro de la misma base de datos (Hassan, 2016). Sin embargo, también existe la perspectiva de utilizar un registro de actividades centralizado de DDL y DML, mejorado y basado en estándares ISO de código abierto. En este sentido, se presenta oficialmente pgAudit como una extensión del núcleo de PostgreSQL (Riggs et al., 2017).

Las soluciones existentes actualmente tienen algunas limitaciones. Por ejemplo, en el caso de utilizar la opción con JPA, se centra en mantener el valor inicial y final de los datos afectados. Por otro lado, opciones como Cyan Audit y pgAudit en PostgreSQL están diseñadas para entornos que requieren un gran espacio de almacenamiento en una misma unidad de disco. Sin embargo, no existe una implementación ideal para llevar a cabo una auditoría de seguridad de bases de datos.

Es fundamental contar con un esquema estándar en la gestión de la seguridad de los datos (Rus y Danescu, 2010). Además, tener lineamientos generales para llevar a cabo esta implementación de manera óptima, como el marco COBIT, que se alinea con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA), resulta de gran importancia (ISACA, 2012). Estos recursos pueden contribuir significativamente a la mejora de la seguridad y la realización efectiva de auditorías en BD.

La auditoría de BD desempeña un papel fundamental en el refuerzo de la seguridad, ya que el registro de actividades de datos suele ser el primer paso en la aplicación de la auditoría de bases de datos (Huang y Liu, 2009). Aprovechar la funcionalidad de los desencadenadores de bases de datos también puede ser de gran ayuda para alcanzar este objetivo (Peréz et al., 2015). Estos desencadenadores permiten activar acciones automáticas en respuesta a eventos específicos, lo que facilita la captura y el registro de cambios y actividades relevantes en la base de datos. De esta manera, se fortalece la seguridad al tener un registro completo y detallado de las acciones realizadas en la base de datos, lo que permite detectar y responder a posibles amenazas o incidentes de seguridad.

1.2.2 Nacionales

Para Ramírez (2019) en su tesis titulada “Implementación de lineamientos base de seguridad en bases de datos Oracle y SQL server en una entidad bancaria”, consistió en la implementación de líneas base de seguridad en bases de datos Oracle y Microsoft SQL Server en los activos de la entidad bancaria Falabella. Estas líneas base de seguridad se basan en configuraciones estándar recomendadas que todos los sistemas deben tener. Estas configuraciones se adhieren a los criterios establecidos por CIS Benchmarks, un conjunto de directrices

desarrollado por el Center for Internet Security (CIS), que representa un estándar global de las mejores prácticas reconocidas para salvaguardar la seguridad de los sistemas de tecnologías de la información (TI). El propósito de esta iniciativa, en colaboración con las diversas áreas de tecnología de la información de la organización, es alinearse con las regulaciones establecidas por la Superintendencia de Banca, Seguros y AFP (SBS). Esta superintendencia exige el cumplimiento constante con el Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI DSS). Cabe destacar que este proceso es un esfuerzo continuo de mejora, respaldado por el ciclo de Deming, que involucra etapas de planificación, ejecución, verificación y ajuste. Para llevar a cabo este estudio, se utiliza una lista de cotejo como herramienta de investigación. Esta lista de cotejo es un instrumento estructurado que facilita la aplicación y el control de los lineamientos base de seguridad. El instrumento contiene los lineamientos específicos a implementar, junto con sus descripciones correspondientes y las justificaciones para los cambios propuestos en las configuraciones de seguridad de las bases de datos.

En última instancia, este trabajo no solo cumple con el objetivo de mejorar la seguridad de las bases de datos en la entidad bancaria Falabella, sino que también proporciona un método valioso para otras empresas que deseen implementar prácticas de configuración de seguridad similares en sus plataformas de bases de datos Oracle y Microsoft SQL Server.

En la misma línea Villena (2006) con su tesis titulada “Sistema de gestión de seguridad de información para una institución financiera”, menciona que hoy en día, las empresas están ajustando sus inversiones en seguridad, priorizando la gestión de la información en lugar de enfocarse exclusivamente en la adquisición de productos. Este cambio ha dado lugar a un nuevo enfoque denominado "seguridad gestionada", que está reemplazando gradualmente al término tradicional de "seguridad informática". Las empresas están adoptando medidas alineadas con este concepto de gestión de la seguridad de la información, que abarca aspectos técnicos, legales y organizativos. Esto implica establecer directrices, procedimientos y criterios coherentes que permitan asegurar la seguridad eficaz de los sistemas de información, así como de la organización y sus infraestructuras. Es esencial comprender que la seguridad absoluta es

inalcanzable, y partiendo de esta premisa, las entidades pueden optar por seguir normas y estándares existentes en el mercado, los cuales proporcionan pautas para la gestión de la seguridad de la información. El presente trabajo de tesis se enfoca en investigar las normas y estándares que están ganando Gestión en el mercado peruano, especialmente en el sector financiero. Se resaltan los puntos más destacados de cada norma y estándar, y a partir de esta recopilación se desarrolla un esquema de gestión de seguridad de la información. Dicho esquema puede ser implementado por instituciones financieras en Perú, permitiéndoles cumplir con las regulaciones actuales relacionadas con la seguridad de la información.

Finalmente, Lopez y Espinoza (2022) en su tesis "Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, Según la Norma ISO/IEC 27001:2013", proponen un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001:2013 para una empresa de consultoría financiera en Lima. La metodología empleada fue descriptiva y no experimental, utilizando la técnica de encuesta con una muestra de 18 colaboradores de la empresa. Los resultados revelaron la existencia de violaciones de seguridad cibernética, lo que condujo a la necesidad de identificar vulnerabilidades y deficiencias en la gestión de la información. Además, se establecieron mecanismos técnicos para optimizar el SGSI, que se fundamenta en fases de planificación, ejecución, control y acción. Se propuso un equipo de verificación y respuesta, con directrices claras para reaccionar de manera oportuna y eficiente ante ciberataques. La propuesta del SGSI, en línea con la Norma ISO/IEC 27001:2013, tiene como objetivo salvaguardar los activos informáticos, certificando la disponibilidad, confidencialidad e integridad de la información. Esto garantiza la continuidad de las operaciones incluso en situaciones de contingencia debido a ataques no autorizados. En conclusión, la implementación de un SGSI fortalecido se espera que reduzca los riesgos relacionados con ciberataques en una empresa de consultoría financiera en Lima durante el año 2021.

1.2.3 Regionales

Para Sota (2019) en su tesis titulada "Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la Municipalidad del

Centro Poblado de Salcedo - Puno", indica que en el Perú, todas las organizaciones públicas están obligadas a implementar Planes de Seguridad Informática o Sistemas de Gestión de la Seguridad de la Información, con el propósito de salvaguardar la confidencialidad, integridad y disponibilidad de la información. Esta obligación se basa en la Norma Técnica Peruana NTP ISO/IEC 27001:2014. Sin embargo, diversas causas como limitaciones presupuestarias, falta de conocimiento, carencia de personal capacitado o la percepción de altos costos de consultoría en seguridad han llevado a que algunas organizaciones, incluyendo entidades estatales, no logren implementar adecuadamente sus Planes de Seguridad Informática. Un ejemplo es la Municipalidad del Centro Poblado de Salcedo Puno, que debido a la falta de conocimiento no había contemplado en sus planes a corto ni mediano plazo el diseño ni la implementación de un Plan de Seguridad Informática. Esta situación motiva la presente investigación, cuyo objetivo es desarrollar un Plan de Seguridad Informática basado en la NTP ISO/IEC 27001:2014 para dicha municipalidad. El enfoque de la investigación comprende una etapa de diagnóstico situacional inicial, destinada a identificar las debilidades y amenazas en materia de seguridad de la información en la Municipalidad del Centro Poblado de Salcedo Puno. Posteriormente, se elaborará el Plan de Seguridad Informática, que abarcará el alcance del plan, los requisitos legales, la formulación de políticas de seguridad y la presentación de un plan a la Oficina de Administración y Finanzas de la mencionada municipalidad. El último paso consiste en la evaluación de los riesgos de seguridad informática para diseñar los controles necesarios que permitan mitigarlos. En conjunto, este trabajo busca abordar la falta de implementación de Planes de Seguridad Informática en la Municipalidad del Centro Poblado de Salcedo Puno, alineándola con los estándares y directrices establecidos en la NTP ISO/IEC 27001:2014.

CAPÍTULO II

PLANTEAMIENTO DEL PROBLEMA

2.1 Identificación del problema

En la actualidad, las empresas enfrentan un desafío crítico relacionado con el control y la seguridad de sus sistemas de información. La carencia de actividades de control y auditoría en el procesamiento de datos a través de sistemas de gestión y bases de datos (BD) ha generado un vacío significativo en el registro de actividades. Esta falta de información sobre los cambios realizados, sus responsables, métodos, horarios y puntos de origen representa un riesgo sustancial para la integridad, no repudio y confiabilidad de la información almacenada en la BD; además, la ausencia de consideraciones de seguridad en el diseño y modelado de BD ha dado lugar a vulnerabilidades graves que pueden amenazar la continuidad de la base de datos olvidando que hoy en día es un activo más en toda organización. Los intentos de abordar este problema han resultado en la implementación dispersa y personalizada de esquemas de auditoría de seguridad, teniendo como antecedentes trabajos como: “Auditar una base de datos bajo políticas de retención”, “Implementación de lineamientos base de seguridad en bases de datos Oracle y SQL server en una entidad bancaria”, así como una “Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, según la Norma ISO/IEC 27001:2013”, intentos de investigaciones para tener algo sólido como una convención o propuesta lo que implica un gasto considerable de tiempo y recursos, especialmente en organizaciones con equipos de desarrollo de software, conllevando a realizar la presente investigación y quizás solucionar este dilema de la seguridad y auditoria en BD relacionales, observando que en algunos casos la búsqueda de soluciones alternativas se ha visto obstaculizada por la disponibilidad de software propietario con licencias costosas y restrictivas, lo que limita la flexibilidad y accesibilidad, especialmente para las pequeñas y medianas empresas; además, la falta de acceso al código fuente de este software dificulta la comprensión y el control de su funcionamiento interno.

Modelar y diseñar una convención con controles de auditoría y seguridad de BD relacionales es un proceso fundamental para garantizar la integridad, confiabilidad y transparencia de la información almacenada en sistemas de gestión de datos. Esta iniciativa implica la creación de un conjunto de directrices, estándares y procedimientos

específicos que se aplicarán a la estructura y el funcionamiento de las BD relacionales en una organización. Ampliemos algunos de los aspectos clave de este proceso:

Definición de Objetivos y Alcance: Es crucial definir claramente los objetivos que se desean lograr con la convención de auditoría y seguridad de bases de datos. Esto puede incluir la protección de datos sensibles, cumplimiento normativo, detección temprana de actividades sospechosas y la integridad de los datos.

Evaluación de Riesgos: Necesario para identificar amenazas y vulnerabilidades que afecten la BD. Esto implica, acceso no autorizado, pérdida de datos, alteración de información crítica y otros riesgos potenciales.

Diseño de la Estructura de la BD: Debe ser revisado y adaptado para incorporar mecanismos de seguridad y auditoría. Esto puede incluir la creación de tablas adicionales para el registro de eventos, la definición de restricciones de acceso y la implementación de claves primarias y foráneas para garantizar la integridad referencial.

Implementación de Controles de Acceso: Se deben establecer políticas de acceso que regulen quién puede acceder a la BD y qué operaciones pueden realizar. Esto puede incluir autenticación, autorización y la asignación de permisos específicos a los usuarios.

Registro de Auditoría: Se debe implementar un registro de auditoría que registre las actividades realizadas en la BD. Esto incluye quién realizó la acción, qué acción se llevó a cabo, cuándo se realizó y desde dónde se originó. Estos registros son cruciales para el seguimiento y la detección de actividades sospechosas.

Monitoreo y Alertas: Se deben establecer mecanismos de monitoreo en tiempo real que supervisen el comportamiento de la base de datos. Esto permite detectar de manera proactiva cualquier actividad anómala y generar alertas para que los administradores tomen medidas inmediatas.

Respuesta a Incidentes: Se deben definir procedimientos para responder a incidentes de seguridad, como intrusiones o accesos no autorizados. Esto incluye la restauración de datos, la mitigación de riesgos y la revisión de las políticas de seguridad existentes.

Formación y Concientización: Es fundamental capacitar al personal que interactúa con la base de datos sobre las políticas y procedimientos de seguridad. La concientización de los usuarios es una parte clave de cualquier estrategia de seguridad.

Evaluación y Mejora Continua: La convención debe ser sometida a evaluaciones periódicas para identificar posibles mejoras y adaptaciones a medida que evolucionen las amenazas y tecnologías. La seguridad de las bases de datos debe ser un proceso en constante evolución.

Por lo tanto, la investigación tuvo como objetivo determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales, abordando estos desafíos y contribuyendo a un mejor desempeño de los profesionales en auditoría e informática, buscando establecer directrices que garanticen la transparencia y la trazabilidad en la gestión de BD, lo que asegurará la seguridad de la información confidencial y poder prevenir acciones no autorizadas.

2.2 Definición del problema

Problema general

¿Cuál es la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales?

Problemas específicos

- ¿Contribuye eficientemente el modelo de convención con controles de auditoría y seguridad en base de datos relacionales a mejorar la integridad de la información almacenada?
- ¿Contribuye eficientemente el modelo de convención con controles de auditoría y seguridad en base de datos relacionales a mejorar la confidencialidad de la información almacenada?
- ¿Contribuye eficientemente el modelo de convención con controles de auditoría y seguridad en base de datos relacionales a mejorar la disponibilidad de la información almacenada?
- ¿Contribuye eficientemente el modelo de convención con controles de auditoría y seguridad en base de datos relacionales a mejorar la gestión de la información almacenada?

2.3 Intención de la investigación

Evaluar la eficiencia de la convención que incorpora auditoría y controles de seguridad en el contexto de bases de datos relacionales

2.4 Justificación

En la actualidad, las empresas se enfrentan a una problemática crítica en cuanto al control y seguridad de sus sistemas de información. La falta de actividades de control y auditoría en el procesamiento de datos a través de sistemas de gestión y BD ha llevado a una carencia significativa de información acerca de las operaciones realizadas en estos sistemas. No sabemos qué cambios se efectúan, quiénes los realizan, cómo se llevan a cabo, cuándo se ejecutan o desde dónde se originan. Este vacío en el registro de actividades representa un riesgo sustancial para la integridad, no repudio y confiabilidad de la información registrada en la BD.

Adicionalmente, la falta de consideración de aspectos de seguridad en el diseño y modelado de BD está generando vulnerabilidades graves que pueden poner en peligro la continuidad de la base de datos. Quienes han intentado abordar este problema han implementado esquemas de auditoría de seguridad de forma personalizada y dispersa, lo que resulta en un gasto significativo de tiempo y recursos, particularmente en entidades con equipos de desarrollo de software.

La búsqueda de soluciones alternativas se ha visto obstaculizada por la disponibilidad de software propietario con licencias costosas y restrictivas, lo que limita la flexibilidad y accesibilidad, especialmente para las pequeñas y medianas empresas. Además, la falta de acceso al código fuente de este software impide la comprensión y el control de su funcionamiento interno.

La implementación y funcionamiento de sistemas de auditoría de seguridad de bases de datos se ha vuelto una tarea compleja, ya que depende de múltiples factores, incluyendo el entorno, la tecnología y los recursos disponibles, lo que ha creado una indeseable dependencia tecnológica.

Este proyecto de investigación busca abordar estos desafíos y contribuir a un mejor desenvolvimiento de los profesionales en auditoría e informática. Asimismo, pretende establecer lineamientos que aseguren la transparencia y trazabilidad en el

manejo de BD, lo que garantizará la seguridad de la información confidencial y evitará acciones no autorizadas.

La implementación de un diseño estándar de bases de datos con controles de auditoría y seguridad dentro de las organizaciones permitirá un análisis más eficiente de auditorías futuras. Además, se espera que la automatización de procesos agilice considerablemente la gestión de auditoría y reduzca el consumo de tiempo, esfuerzo y recursos financieros.

En última instancia, este trabajo se alinea con las disposiciones de la Ley de Delitos Informáticos (Ley N° 30096 Art. 3), ya que proporciona una solución para mantener un historial completo de modificaciones, adiciones y eliminaciones en las bases de datos, lo que facilitará la realización de auditorías de seguridad y la detección de operaciones autorizadas, pero no apropiadas.

2.5 Objetivos

2.5.1 Objetivo general

Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales

2.5.2 Objetivos específicos

- Evaluar la eficacia de los controles de auditoría para garantizar la integridad de la información almacenada.
- Examinar la capacidad del modelo para mejorar la confidencialidad de los datos almacenados en la base de datos.
- Investigar cómo el modelo contribuye a la disponibilidad de la información, asegurando que esté accesible cuando sea necesario.
- Evaluar cómo el modelo afecta la gestión general de la información almacenada en bases de datos relacionales.

2.6 Hipótesis

2.6.1 Hipótesis general

La implementación de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la información almacenada.

2.6.2 Hipótesis específica

- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la integridad de la información almacenada.
- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la confidencialidad de la información almacenada.
- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la disponibilidad de la información almacenada.
- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la gestión efectiva de la información almacenada.

CAPÍTULO III

METODOLOGÍA

3.1 Acceso al campo

La investigación se realizó en la ciudad de Puno, ubicada en la región homónima, Perú a una altitud de 3827 msnm.

Población

La población se compone por usuarios que desarrollan sistemas y hacen uso de base de datos.

Muestra

La muestra consistió en 8 usuarios expertos que fueron seleccionados mediante el método de muestreo de juicio de expertos.

Método de investigación

Se enfoca en los controles y mecanismos implementados para certificar que solo las personas autorizadas puedan interactuar con la base de datos y que lo hagan de manera segura, incluye aspectos como la autenticación, autorización y encriptación de registros para asegurar y proteger la información sensible y prevenir accesos no autorizados, considerando las características de la investigación, posee un enfoque cualitativo siguiendo la metodología propuesta por Hernández y Mendoza (2018), esta elección se realizó considerando las particularidades de la investigación con el propósito de evaluar las características del modelo de convención.

Detalle de los aspectos clave:

- Autenticación: Es el procedimiento mediante el cual se verifica la identidad de un usuario o sistema antes de concederles acceso a la BD. Esta validación puede llevarse a cabo a través de credenciales como nombres de usuario y contraseñas, sistemas de autenticación de dos factores, certificados digitales, entre otros métodos.
- Autorización: Una vez que un usuario se ha autenticado con éxito, es necesario definir qué acciones y operaciones están permitidas para esa identidad en particular.

La autorización determina los privilegios y permisos que tiene un usuario en la BD como leer, escribir, actualizar o eliminar datos.

- Encriptación: Proceso de transformar datos legibles en un formato ilegible mediante algoritmos matemáticos. En el Confidencialidad de una BD esto puede implicar el cifrado de datos sensibles almacenados para protegerlos en caso de que se acceda sin autorización.
- Controles de acceso basados en roles: Estos mecanismos implican la asignación de usuarios a roles específicos que tienen conjuntos de privilegios predefinidos. Esta estrategia facilita una gestión más eficaz de los accesos, asegurando que los usuarios solo dispongan de los permisos necesarios para cumplir con sus responsabilidades.
- Auditoría de acceso: Consiste en llevar un registro y supervisar las actividades de acceso a la BD. Los registros de auditoría documentan quién, cuándo y qué tipo de acciones se han llevado a cabo en la base de datos.

3.2 Selección de informantes y situaciones observadas

Informantes:

- Administrador de BD: Suministra conocimientos fundamentales sobre las medidas de seguridad y los procesos de auditoría implementados en las bases de datos relacionales.
- Especialistas en Seguridad de la Información: Aportan una visión detallada de los controles de seguridad empleados en la administración de bases de datos y en la mitigación de riesgos.
- Usuarios Clave del Sistema de Bases de Datos: Comparten sus experiencias sobre las operaciones diarias con la base de datos y ofrecen percepciones sobre la seguridad y las prácticas de auditoría en el sistema.

Situaciones observadas:

- Puesta en práctica del modelo en una base de datos operativa: Examinar la implementación de los controles de seguridad y auditoría en una base de datos activa para valorar su eficacia.

- Realización de pruebas de intrusión y análisis de vulnerabilidades: Evaluar cómo el modelo responde a pruebas de intrusión y análisis de vulnerabilidades con el fin de detectar posibles brechas y áreas de mejora.
- Auditoría en tiempo real de las bases de datos: Observar el proceso de auditoría de la base de datos en tiempo real para comprender cómo se registran y supervisan las actividades de acceso.

3.3 Estrategias de recogida y registro de datos

La técnica fue la encuesta y como instrumento el cuestionario, la valoración del modelo fue absuelto por criterio de expertos, teniendo como indicadores la Integridad, Confidencialidad, Disponibilidad y Gestión.

3.4 Análisis de datos y categorías

Haciendo uso del método de criterio de expertos, se desarrolló un cuestionario como instrumento para evaluar la propuesta de convención, donde se analizó la confiabilidad y validez del instrumento en relación a las instrucciones e ítems evaluados en una escala tipo Likert.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1 Resultados

Propuesta de convención desarrollado (explicado en cinco ejes)

4.1.1 Eje 1. Describiendo la propuesta

La convención que se propone está orientada en brindar lineamientos de estándar abierto y de aplicación libre, para el modelado de BD con controles de auditoría y seguridad, haciendo posible capturar de manera eficiente sucesos como modificaciones, inserciones y eliminaciones ocurridos durante la manipulación de datos en BD relacionales.

Considerando el indudable valor que tienen los datos para una organización, que los convierte en activos de información, fue fundamental implementar mecanismos para su protección y seguridad, siguiendo las normas generales y buenas prácticas que organismos internacionales proporcionan, donde la incorporación de controles de auditoría en los datos, va a la par para incrementar la seguridad de la información, sobre todo respecto a la integridad y confidencialidad en las bases de datos.

Por otra parte, tomando en cuenta que las bases de datos relacionales juegan un papel importante en el almacenamiento de información y que su uso continúa acrecentándose, es que la convención propuesta se centrará en BD relacionales.

4.1.2 Eje 2. Justificando su importancia

El contar con datos que se ven comprometidos por la manipulación y al no poseer un historial de las modificaciones, inserciones o eliminaciones de algún registro, representa una amenaza para la integridad de los datos; peor aún, si no es posible consultar ¿quién?, ¿cuándo? o ¿desde dónde? se hicieron las acciones de alteración; que de hecho, existen bases de datos que no contemplan en su diseño, el llevar un registro de cambios en los datos, ni por el sistema de gestión de BD ni por la aplicación cliente o servicio web que interactúa con esos datos.

Mencionar también, que los diseños de BD que sí contemplan enfoques de auditoría personalizados, en su mayoría son arbitrarios, no estandarizados y poco eficientes; además, son específicos para un solo motor de base de datos y muchos no brindan acceso al código fuente, dificultando a los profesionales de auditoría y seguridad, el realizar las indagaciones y estudios correspondientes en la información almacenada. Por lo anterior, la presente propuesta de convención, es de vital importancia al proporcionar soluciones para subsanar u optimizar los procesos de incorporación de controles de auditoría y seguridad en las bases de datos relacionales; además, contar con un esquema estándar como convención en el diseño de bases de datos con controles de seguridad y auditoría, que toma en cuenta estándares de propósito general internacionales, tecnológicamente contribuye a uniformar su implementación, dando lugar a contar con una administración más fácil de entender, eficiente, segura y confiable; optimizando recursos en cuanto a tiempo, esfuerzo y dinero, sobre todo si se logra automatizar el proceso de implementación.

4.1.3 Eje 3. Objetivos del modelo

A. Confidencialidad

Con este pilar, se buscó la no revelación de información a quien no está autorizado a acceder a los datos, con este fin, se pueden implementar medidas para minimizar riesgos y proteger la información como la autenticación (cuentas de usuario), controles de acceso y privilegios (permisos y roles) y cifrado de datos (base de datos completa, tablas o columnas específicas).

B. Integridad

Este objetivo buscó garantizar que los datos no sean alterados, previniendo modificaciones innecesarias por personas con permisos que alteren los registros y, que algún programa o aplicativo que interactúe directamente con la base de datos realice modificaciones sin autorización.

La integridad de una BD se consigue a través de autenticación, políticas internas (como robustecer contraseñas), controles de acceso y

limitar las acciones del personal con respecto a la información de acuerdo a sus funciones.

C. Disponibilidad

Respondió a la necesidad de mantener activo el acceso a la información para aquellas personas que requieren tener acceso a la misma en el momento que lo necesiten, para cumplir con este objetivo, se pueden implementar soluciones redundantes, modelos de respaldo, métodos de continuidad y recuperación de desastres, los cuales deberán ser verificados periódicamente para garantizar su correcto funcionamiento.

D. Trazabilidad y Accountability

Consistió en tener un control exhaustivo del proceso de tratamiento de los datos, controlando qué datos son tratados o modificados, quién interviene en el proceso de modificación de datos, qué terceros tienen acceso y qué sistemas están implicados.

La trazabilidad está muy relacionada con el principio de accountability o responsabilidad proactiva, el cual viene regulado en el Reglamento General de Protección de Datos RGPD y se refiere a la forma óptima de trabajar en una organización. Referente a la seguridad de datos, el principio de accountability no solo obliga a la institución a cumplir con la normativa, sino a verificar que la cumple. Para implementarlo en bases de datos se debe considerar la proactividad (anticipación a los problemas en los datos), responsabilidad (los responsables de los datos que tienen que tomar todas las medidas técnicas y organizativas necesarias para proteger los datos), cumplimiento (las medidas deben ser aplicadas y revisadas periódicamente para ver si continúan cumpliendo con su cometido), trazabilidad (poner en práctica las medidas técnicas y organizativas) y la revisión periódica (revisar en profundidad y con una periodicidad adecuada).

La trazabilidad también está relacionada con el ciclo de vida de los datos que comprende la captura de datos, almacenamiento y clasificación,

tratamiento y uso, cesión y transferencia de datos, y la destrucción de los mismos.

E. No repudio

Esta característica persigue la irrenunciabilidad de la intervención de las partes en la modificación de datos. Para cumplir con este objetivo se implementan particularidades para demostrar la participación de los involucrados, tanto en origen como en destino, estando esta particularidad íntimamente involucrada con la identificación y autenticación de usuarios del sistema operativo y de las bases de datos.

Mediante el no repudio en origen se busca garantizar conocer desde dónde y quién envió la acción para modificación de un determinado registro, esto puede lograrse mediante el almacenamiento de usuarios de aplicación y/o de sesión de la base de datos. Por otra parte, el no repudio en destino, es decir en la base de datos, busca confirmar que se recibió una determinada petición de modificación y que se garantice la prueba de la recepción.

4.1.4 Eje 4. Enfoque

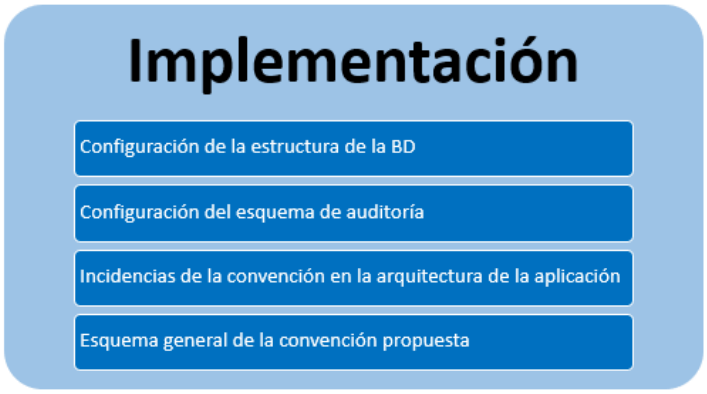
Para abordar la elaboración de la propuesta de convención, se utilizó la metodología de la investigación tecnológica, con alcance exploratorio, enfoque cualitativo y métodos inductivo y analítico. Donde alineados a la problemática identificada y a los objetivos planteados, se aplican los componentes investigativos, recopilando información del estado del arte, análisis de ventajas y desventajas, identificación de indicadores de evaluación y de características deseadas que debería tener una BD relacional con controles de auditoría y seguridad.

En este punto, con la información procesada y analizada en detalle, a continuación, se clasifica, organiza, ordena y estructura la nueva información, constituyéndose en la convención que se plantea.

4.1.5 Eje 5. Implementación

Este quinto eje descriptivo de la propuesta de convención, explica la forma en que se propone la implementación de los mecanismos para conseguir controles de auditoría y seguridad en un base de datos, conformado por cuatro fases centrales:

Figura 1
Implementación de la propuesta de convención y sus fases



Fase 1. Configuración de la estructura de la BD

Tomando en cuenta que se realizó el respectivo proceso para obtener el diseño del Diagrama Entidad - Relación (DER), así como también del modelo lógico global de datos, contando con la respectiva abstracción de la realidad o modelo de negocio que se aborda, donde ya se tienen identificadas las entidades, atributos, relaciones y la cardinalidad entre entidades, por lo que se debe considerar:

a) Crear la estructura de directorios para los archivos de la base de datos, la cual debe estar ubicada en una partición distinta al sistema operativo, dentro de esta partición se recomienda contar mínimamente con la estructura de directorios sql/data, sql/log y sql/backup, los cuales se explican a continuación:

Directorio sql, es el directorio principal donde se ubicarán los archivos relacionados a la base de datos, situado en una partición diferente a la del sistema operativo, ya que ésta última es más propensa a ataques o a corromperse, por ello es necesario resguardar la información en un lugar menos vulnerable.

Directorio sql/data, este subdirectorio dentro del directorio sql, denominado data, debe estar ubicada la base de datos, es decir, es donde se encontrarán las tablas, registros, índices, nombres de usuario, restricciones, funciones o procedimientos, desencadenadores y todo lo relacionado con la base de datos.

Directorio sql/log, este también es un subdirectorio de sql, denominado log, donde deben ubicarse los archivos de logs de transacciones de la base de datos, como DML, DLL y DCL. En la creación de la base de datos se suele especificar un crecimiento de logs entre el 10% y 25% de los datos, es recomendable crear un esquema periódico de limpieza de log, y más aún si se tratara de un ambiente altamente transaccional.

Directorio sql/backup, finalmente, el subdirectorio denominado backup, es el que proveerá una significativa solución para proteger datos críticos que están almacenados en las bases de datos, y para minimizar el riesgo de pérdida de datos, para este subdirectorio se deben programar planes periódicos de respaldos de los datos y logs de la base de datos.

Por conveniencia en desempeño, almacenamiento, prevención de fallas y/o seguridad, es que es necesaria la separación física de estos directorios, incluso de ser posible la separación física de los subdirectorios, articulándose estas características con los objetivos de seguridad de esta convención respecto a la Confidencialidad y a la Disponibilidad.

b) Configurar los permisos para que el usuario del sistema operativo que administra la BD, pueda acceder a los directorios creados, asociándolo como el dueño de la carpeta, y para otros ingresos según el nivel de acceso, configurar los permisos de lectura, escritura o ejecución, relativos a usuario, grupo u otros.

c) Esto es importante porque es recomendable otorgar solamente los permisos necesarios a un usuario para tareas específicas, en este caso para acceder a los archivos de bases de datos. Por las características de seguridad se alinea con el objetivo de Confidencialidad y Accountability.

d) Crear la BD clasificando los archivos de datos y de logs en el directorio creado anteriormente, es decir, dentro de sql/data y sql/log respectivamente. Como se mencionó previamente en el inciso a) en el subdirectorio data, se

encontrarán los archivos de base de datos y en el subdirectorio log se encontrarán los logs de transacciones de la base de datos, y si fuera posible separar ambos directorios en distintos discos físicos, esto ayuda en el rendimiento, practicidad y tamaño de espacio en disco, estando en concordancia con los objetivos de seguridad de Confidencialidad y a la Disponibilidad.

e) Crear un usuario específico a nivel de base de datos, que sea el propietario de la nueva base de datos creada, de modo que no se permita el acceso a otras bases de datos con este usuario, buscando que cada base de datos tenga su usuario definido con los permisos necesarios según el modelo de negocios para acciones DML y DDL según corresponda; además del usuario administrador de la base de datos, es pertinente poseer usuarios estándares con diferentes niveles de acceso y funciones permitidas. Esto en correlación con los objetivos de Confidencialidad, Integridad respecto a la administración y No repudio.

f) Asegurarse que cada tabla posea una clave primaria autonumérica, a través de la palabra reservada o directiva de sql primary key definida en el estándar ANSI SQL, garantizando que sea no nula, entero largo, de preferencia ubicada como primer campo y configurar para que el autoincremento empiece en uno con incrementos de uno; lo cual ayudará a poseer cada tupla de una tabla como única y correlativa, de forma tal, que si se identifica una secuencia no consecutiva, puede deberse a una posible eliminación física, reforzando el objetivo de Integridad de datos también relacionado con la Disponibilidad.

g) De preferencia la llave primaria debe llamarse "id", en minúsculas, la cual es una convención de nombres para las claves primarias de tablas en los motores de BD, para conseguir un criterio de uniformidad durante el desarrollo y facilidad de auditoría, articulándose con el objetivo de Integridad.

h) Cada tabla debe poseer un campo de tipo de dato lógico (booleano) llamado "active", que registre las eliminaciones lógicas, con valor por defecto en verdadero que significa que está vigente o activo el registro y cuando se modifique el valor a falso significará que el registro se encuentra en estado anulado, de modo que no se permitan eliminaciones físicas (delete from

tabla) desde la aplicación cliente o servicio que use la BD. Su importancia radica en la característica de contribuir a salvaguardar los registros, retenerlos y protegerlos, encaminado con los objetivos de Integridad, Trazabilidad y Accountability.

i) Cada tabla debe poseer campos sobre el ¿quién? los cuales serían "user_create" que representará información sobre el usuario que creó un registro y el campo "user_update" que representará la última modificación que se haya realizado sobre la fila, ambos de tipo cadena con valor por defecto el usuario de inicio de sesión de la base de datos; inicialmente en la inserción de una tupla, será el mismo dato en user_create y user_update. Esta peculiaridad se asocia con el objetivo de seguridad de Trazabilidad y No repudio.

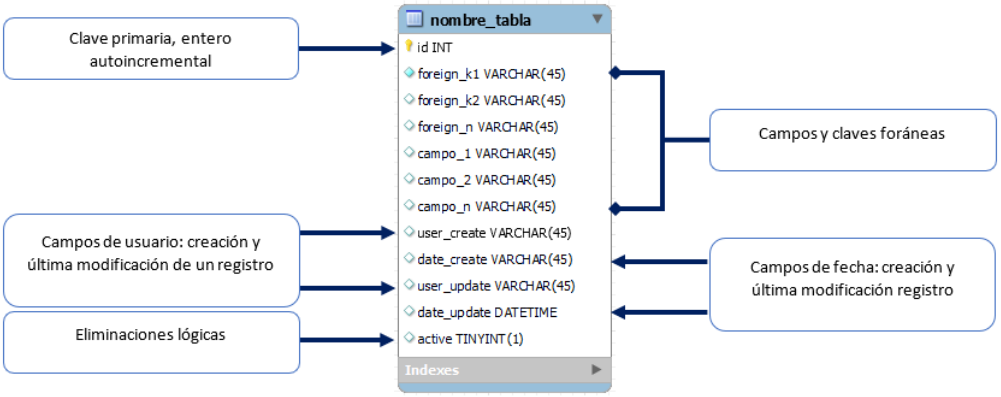
j) Cada tabla debe poseer campos sobre el ¿cuándo? los cuales serían “date_create" que representará información sobre la fecha y hora en que se creó un registro y el campo "date_update" que representará la fecha y hora de la última modificación que se haya realizado sobre el mismo, ambos de tipo fecha y hora con valor por defecto la fecha actual del servidor de base de datos; inicialmente en la inserción de una tupla, será el mismo dato en date_create y date_update. Esta cualidad está encaminada con los objetivos de Integridad, Trazabilidad y Accountabiliy.

k) Adecuar las tablas mínimamente hasta la tercera forma normal (3FN) para disminuir inconsistencias y anomalías lógicas, es decir, considerar para la 1FN que no existan grupos de repetición en tablas individuales, que se cree una tabla independiente con una clave principal para cada conjunto de datos relacionados; además, para la 2FN crear tablas independientes con una clave externa para conjuntos de valores que se aplican a varios registros evitando la redundancia de datos y poder ser relacionados; y además, para 3FN eliminar los campos que no dependen de la clave candidata. Este requisito está alineado con la Integridad y Trazabilidad.

Por lo tanto, bajo las consideraciones y dependiendo de la política interna utilizar el idioma de preferencia, quedando cada tabla de la base de datos de la siguiente manera:

Figura 2

Propuesta de tabla con campos mínimo requeridos



Fase 2. Configuración del esquema de auditoría

a) Crear la estructura de directorios para los archivos de auditoría, la cual debe estar ubicada en una partición distinta al sistema operativo, dentro de esta partición se recomienda contar al menos con sql/audit y los subdirectorios sql/audit/data, sql/audit/logy sql/audit/backup.

i. Directorio sql/audit. Es el directorio principal donde se ubicarán los archivos relacionados a la auditoría, situado en una partición diferente a la base de datos principal y diferente a la del sistema operativo, ya que ésta última es más propensa a ataques o a corromperse, por ello es necesario resguardar la información de auditoría en un lugar menos vulnerable y separada de los datos.

ii. Directorio sql/audit/data. En este subdirectorio dentro del directorio sql/audit, denominado data, es donde deben estar ubicadas las bases de datos de auditoría, una por cada base de datos principal, es decir, es donde se encontrarán las tablas con campos de la tabla principal más campos de auditoría, registros de cambios en los datos, nombres de usuario, cifrado de la estructura y de la información, y todo lo relacionado con cada base de datos de auditoría.

iii. Directorio sql/audit/log. Es un subdirectorio de sql/audit, denominado log, donde deben ubicarse los archivos de logs de transacciones de la base de datos de auditoría, como DML, DLL y DCL. En la creación de la base de datos de auditoría se suele especificar un crecimiento de logs del 10% respecto a los datos, se

recomienda crear un esquema periódico de limpieza de log de base de datos.

iv. Directorio sql/audit/backup. Finalmente, el subdirectorio denominado backup, proveerá un significativo recurso para proteger datos críticos de auditoría que se encuentran almacenados en las BD de auditoría; y para minimizar el riesgo de pérdida de datos, se deben programar planes periódicos de respaldos de los datos y de los logs de la base de datos de auditoría, antes de la limpieza de logs de auditoría.

Al igual que los directorios de la base de datos principal, por conveniencia en desempeño, almacenamiento, prevención de fallas y/o seguridad, es que es necesaria la separación física de estos directorios de auditoría, sobre todo el directorio principal sql/audit, engranándose estas características con los objetivos de seguridad de esta convención respecto a la Confidencialidad y a la Disponibilidad.

b) Configurar los permisos para que sólo el usuario del sistema operativo (administrador) del motor de BD, pueda acceder a los directorios de auditoría creados, asociándolo como el dueño de la carpeta sql/audit, y para otros ingresos según el nivel de acceso, configurar los permisos de lectura, escritura o ejecución, relativos a usuario, grupo u otros.

   Esto es importante porque es recomendable otorgar solamente los permisos necesarios a un usuario para tareas específicas, en este caso para acceder a los archivos de bases de datos de auditoría. Por las características de seguridad se alinea con el objetivo de Confidencialidad y Accountability.

c) Crear la base de datos de auditoría con el prefijo "aud", cifrada, separando los archivos de datos y de logs en el directorio de auditoría creado anteriormente, es decir, dentro de sql/audit/data y sql/audit/log respectivamente. Como se mencionó anteriormente en el inciso a, en el subdirectorio data se encontrarán los archivos de base de datos de auditoría y en el subdirectorio log se encontrarán los logs de transacciones de la base de datos de auditoría, esto ayuda en el rendimiento y brinda practicidad en su estudio, estando en concordancia con los objetivos de seguridad de Trazabilidad y Accountability y No Repudio.

i. Crear las tablas de auditoría, una por cada tabla de la base de datos principal, las nuevas tablas con el mismo nombre, tomando en cuenta la creación de las tablas (incluso sólo algunas columnas necesarias) para las que se desee capturar las modificaciones en los datos. Estas tablas serán similares a la forma de implementación basada en tablas espejo, donde en cada inserción, modificación o eliminación en la tabla principal correspondiente, se deberá insertar toda la tupla en la tabla de auditoría. De esta manera se irá registrando el historial de cambios en los datos, el cual se ubicará en una estructura similar de forma separada, alineándose con los objetivos de Integridad y Trazabilidad.

ii. Cada tabla de auditoría debe poseer una clave primaria auto numérica de nombre "id", seguidamente el identificador de la tabla que hace referencia con el nombre id_{nombre_tabla} con el mismo tipo de dato, también de contar con el resto de los campos de su tabla correspondiente manteniendo los tipos de datos y sus longitudes, estos campos se registrarán a través de desencadenadores existentes en la tabla principal o captura de logs, solo debe permitir inserciones.

De este modo, es posible tener uniformidad durante del diseño de base de datos y en el desarrollo de la aplicación, asimismo se consigue facilidad en el proceso de auditoría, enfocándose con el objetivo de Integridad.

d) Cada tabla de auditoría, además debe poseer campos de seguimiento o de auditoría, donde dependiendo del motor de base de datos, puede ser posible determinar:

i. user_db: es la captura del usuario actual de base de datos, correspondiente al inicio de sesión del motor de base de datos, el cual ayudará a identificar quién realizó alguna alteración a los registros de una tabla. Será mucho más útil cuando un usuario que haya logrado acceder directamente a la base de datos, sin la intervención de otra aplicación intermedia, capturando de manera plena al usuario que haya realizado alguna acción de modificación en los datos.

ii. host: nombre del equipo o dirección IP del cliente, que identificará desde dónde se realizó la modificación, sirviendo como un indicio adicional para conocer el origen. Si bien, es posible que existan

nombres de equipo repetidos o direcciones IP según la interface de red que también en cierto momento pueden variar, aun así, puede ser una posible pista de auditoría.

iii. mac: identificador único de la pieza de hardware de red del cliente, este dato en algunos motores no es posible capturar automáticamente e incluso desde el cliente, pueden existir varias direcciones mac según la interface de red, hasta pueden ser clonadas, pero al igual que el anterior, puede representar una pista de auditoría.

iv. app: es la aplicación cliente de donde se recibe la modificación, este dato en algunos motores no es posible capturarlo automáticamente desde el cliente, debiendo implementarse otro mecanismo que se explicará más adelante a través de una función, el cual permita registrar este campo de manera parametrizable y segura.

v. transaction_type: tipo de acción SQL sobre el DML, que identifique si la captura de modificación en un registro se debe a una inserción (insert), una actualización (update) o una eliminación (delete).

vi. hash: función de resumen único de toda la tupla afectada, que ayude a garantizar la integridad de la fila para una posterior comparación y análisis de auditoría en caso de existir modificaciones.

Los campos de auditoría descritos en el marco de ésta característica, se encuadran con los objetivos de seguridad de Integridad, Trazabilidad y No repudio.

e) Implementar el mecanismo para la captura de eventos de modificaciones en los datos mediante el uso de desencadenadores o servicio de lectura de logs, tomando en cuenta las siguientes consideraciones:

i. Uso de desencadenadores. - Un trigger o desencadenador en una BD, es un procedimiento que se ejecuta cuando se cumple una condición establecida al realizar una acción, que puede ser de inserción, actualización o borrado (INSERT, UPDATE, DELETE).

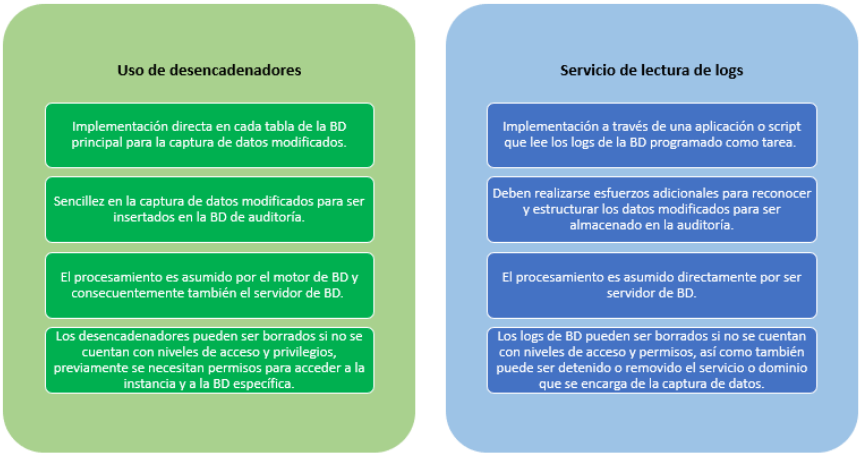
ii. De optarse por esta alternativa, se deben crear desencadenadores por cada tabla de la base de datos principal, de acuerdo a las acciones de inserción, actualización y eliminación; mediante los que se obtengan los datos para los campos de auditoría (user_db, host, mac, app,

transaction_type y hash) y que se insertarán en la tabla correspondiente de auditoría, pudiendo utilizarse el tradicional insert select.

iii. Servicio de lectura de logs. - se refiere al guardado continuo en un archivo o en una BD de todos los acontecimientos que afecten a los datos. Para el uso de esta alternativa, se debe poseer un servicio o demonio, de acuerdo a las acciones de inserción, actualización y eliminación; donde se obtengan los campos de auditoría (user_db, host, mac, app. transaction_type y hash) y se realice una inserción a la tabla correspondiente de auditoría, pudiendo utilizarse una aplicación o script que será invocado por el servicio o demonio.

Figura 3

Comparación de la utilización de Triggers o Lectura de Logs en la auditoría de bases de datos relacionales



Independientemente de la forma que se opte por capturar los eventos o sucesos de modificaciones en los datos, esta propiedad está enfocada con los atributos de seguridad de Trazabilidad y Accountability.

f) Obtener el hash de toda la tupla actual modificada, considerando desde el campo de la clave primaria "id" hasta el campo "transaction_type" y almacenar la función de resumen único en el campo hash, situado al final de cada tabla de auditoría, siendo alternativas de implementación las funciones sha-256 o sha-512, debiendo tomarse en cuenta que mientras más seguro sea el algoritmo, más longitud tendrá. De esta forma, se apunta y contribuye al objetivo de seguridad de Integridad.

g) Crear una función con el nombre "fn_audit" a nivel de DDL en la base de datos principal, la cual permita recibir parámetros enviados desde el cliente como: el nombre de la tabla que haya sufrido cambios en sus datos, el valor del identificador de la tabla y algunos campos de auditoría que pueden ser el host, mac y app; de modo que a través de la función se actualicen estos datos en la base de datos de auditoría, ayudando con los objetivos de seguridad de Integridad y No repudio.

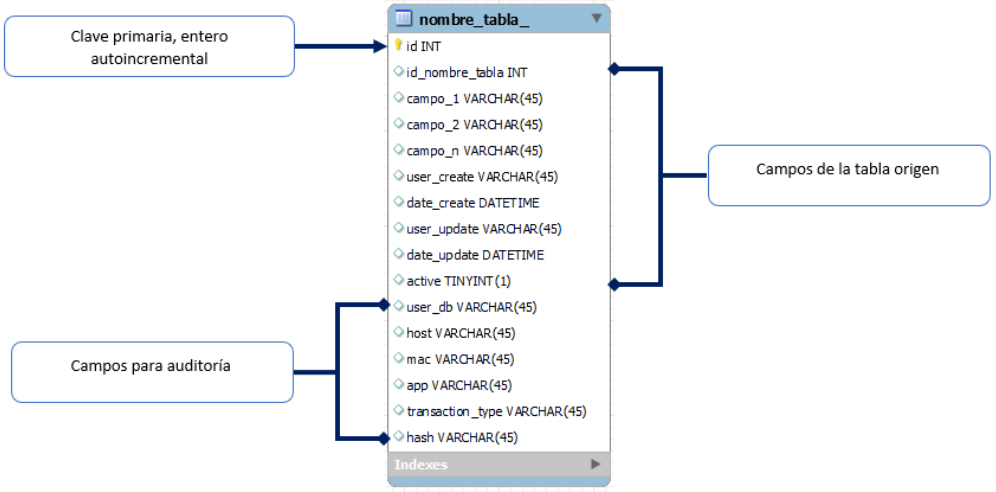
h) La BD de auditoría debe estar cifrada, de modo que, con esta operación criptográfica, los datos sean ilegibles utilizando una clave de cifrado segura, esta clave se debe especificar para acceder desde la BD principal a la BD de auditoría. Entre las opciones más comunes y seguras en bases de datos de cifrado simétrico y asimétrico, se cuenta con Triple DES, AES256 y RSA. Lo recomendable es cifrar la BD con un algoritmo simétrico que brinda mayor velocidad en su acceso y escritura, y utilizar el cifrado asimétrico, que es necesariamente más lento, para proteger la clave simétrica.

Asimismo, dependiendo del grado de privacidad de los datos, se recomienda también cifrar las columnas correspondientes de las tablas de la BD principal, siendo esto posible en la mayoría de los motores de BD relacionales.

Esta característica es muy usada para el cumplimiento del requisito y objetivo de seguridad de Confidencialidad, Integridad y No repudio.

Figura 4

Propuesta de tabla para auditoría con campos mínimo requeridos



Fase 3. Incidencias de la convención en la arquitectura de la aplicación

Aplicaciones cliente.- Se debe considerar el envío de datos desde aplicaciones cliente para que en las inserciones se consigne un valor a través de la función fn_audit para el campo user_create, en las modificaciones se envíe un valor para el campo user_update y en las eliminaciones lógicas se envíe el cambio del estado del campo active.

Las listas de datos deben considerar que se tomen cuenta sólo los registros con el campo active en verdadero. En la típica tabla usuarios o users que posee una BD, el nombre de usuario debe ir en concordancia con los campos user_create y user_update. Además, en aplicaciones cliente que no utilicen una conexión a base de datos basada en ODBC o similares, siendo aplicaciones web y servicios web en las cuales el servidor de BD no puede capturar automáticamente datos de auditoría de lado del cliente como el host, la dirección MAC o el nombre la aplicación que envía datos; en estas situaciones se debe incorporar en el desarrollo la utilización de la función fn_audit para enviar los datos de auditoría faltantes en cada inserción, actualización o anulación.

Bases de datos existentes.- La implementación de la presente propuesta de convención se adecua sin inconvenientes para nuevas BD; sin embargo, para bases de datos ya existentes y en producción, no es recomendable; pero previo análisis y gestión de riesgos, puede ser posible técnicamente realizar las adecuaciones antes descritas, previendo anticipadamente obtener copias se seguridad y, en entornos de prueba realizar las configuraciones y verificaciones que garanticen la correcta continuidad del negocio.

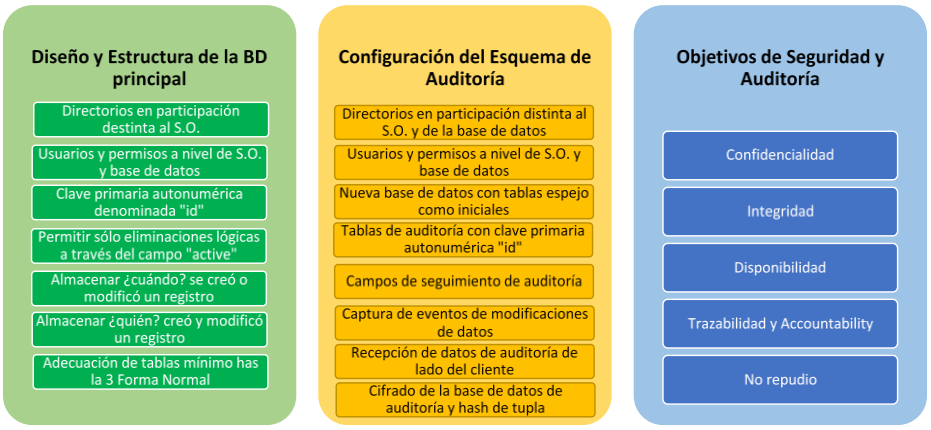
Retención de datos.- Dependiendo de las políticas de retención de datos de cada institución, donde se conoce la organización de la información, su duración y eliminación cuando ya no se necesite, es importante reflexionar en la disponibilidad de los datos de auditoría a largo plazo o perpetuo, en caso de requerirse para su consulta o reconstrucción a un punto determinado. Al realizarse alteraciones a la estructura de la BD, se recomienda versionar la auditoría o asumir que existirán datos nulos hacia atrás en adiciones DDL. Al acumularse los datos de auditoría drásticamente, realizar los recaudos necesarios de infraestructura tecnológica de almacenamiento, partición, procesamiento y redundancia.

Fase 4. Esquema general de la convención propuesta

En base a las premisas descritas anteriormente, el esquema general de implementación para la propuesta de convención para bases de datos con controles de auditoría y seguridad a nivel de gestión, es el siguiente:

Figura 5

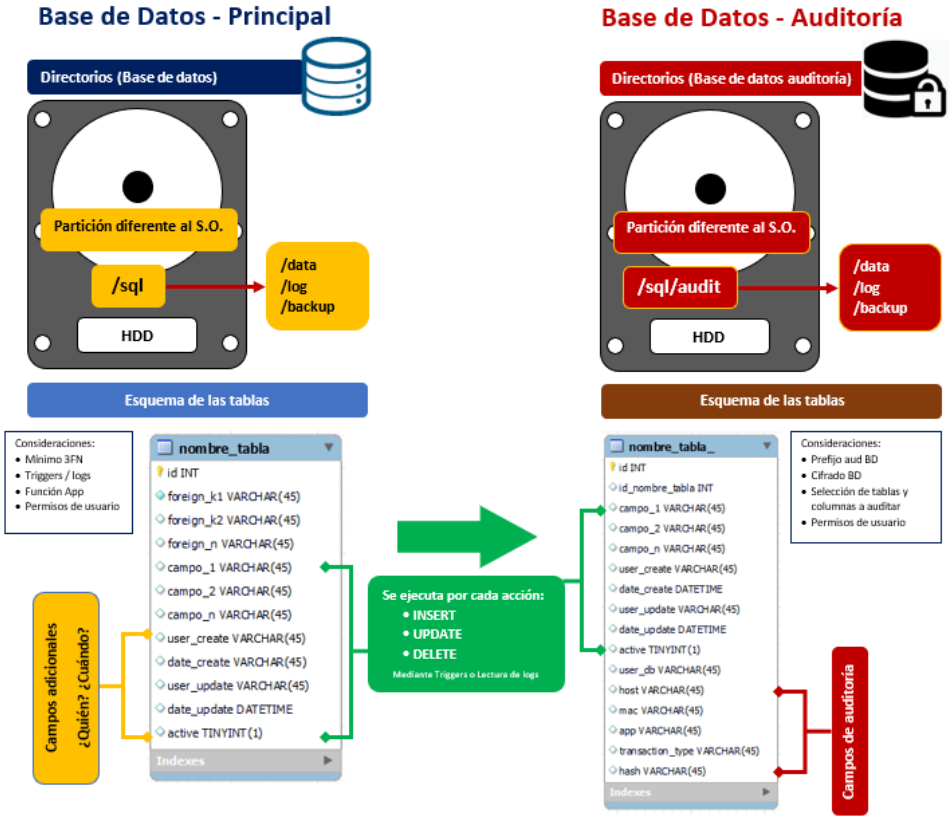
Esquema general de implementación de la propuesta de convención



Por otra parte, de manera complementaria al esquema implementación, se ilustra un esquema a nivel técnico.

Figura 6

Esquema técnico del modelo de convención



De la figura 6, se cumple lo siguiente:

Seguridad

- Confidencialidad, integridad y disponibilidad
- Trazabilidad, accountability y no repudio
- Cifrado, copias de seguridad y redundancia

Beneficios

- Historial de cambios
- Reconstrucción de la información
- División de datos y auditoría
- Backups separados (BD principal y BD auditoría)
- Elaborado en estándares de datos, auditoría y seguridad
- Facilidad de procesos de auditoría

Finalmente, considerar las buenas prácticas y normas generales de protección de datos en pos de garantizar la correcta continuidad del negocio y recuperación ante desastres, como copias de seguridad periódicas, redundancia, replicación de datos, políticas de seguridad, entre otras que contribuyan en asegurar la protección y seguridad de un activo muy importante como lo es la información.

4.1.6 Criterios de expertos

La evaluación mediante el criterio o juicio de expertos, método de validación cada vez más utilizado en las investigaciones, "consiste en solicitar a una serie de personas la demanda de un juicio hacia un objeto, instrumento, material de enseñanza, o su posición a un aspecto concreto" (Cabero y Llorente, 2013). En este sentido, en la validación del presente Moledo de Convención con Controles de Auditoría y Seguridad de BD relacionales, mediante el método de Criterio de Expertos, se envió de forma individual la consulta a expertos en el área, donde desde los conocimientos y experiencias, se recibió colaboración académica con diferentes opiniones y retroalimentación sobre la propuesta desarrollada.

Participantes

En la elección de los expertos, se utilizó el biograma en combinación con el coeficiente de competencia experta (García y Fernàndez, 2008), partiendo de recomendaciones de personas que se han considerado expertas, a quienes se contactó consultando el conocimiento y la argumentación que podrían brindar sobre el tema de investigación. Posteriormente, se indagó en sus respectivas biografías, sobre aspectos de trayectoria en el tema, años de experiencia y formación, investigación o acciones formativas, campo de trabajo, y sobre todo conocimiento del objeto de estudio, es decir, respecto a bases de datos relacionales libres que consideran seguridad y auditoría.

Diseño del Instrumento

Se diseñó el cuestionario como instrumento de validez, cada cuestión constituida por 4 indicadores generales de evaluación (12 preguntas), evaluando lo siguiente:

- Integridad: El ítem está formulado con un lenguaje apropiado, no genera contradicción.
- Confidencialidad: El ítem está en el marco de la temática abordada.
- Disponibilidad: El ítem mide alguna variable o relación con los indicadores.
- Gestión: El ítem es relevante para cumplir con las preguntas y objetivos de investigación.

Por cada ítem a evaluar, se enmarca en una escala tipo Likert (1932), para medir el nivel de acuerdo o desacuerdo de los expertos, siendo:

1. Totalmente en desacuerdo
2. En desacuerdo
3. Indeciso/Indecisa o Neutral
4. De acuerdo
5. Totalmente de acuerdo

El instrumento contiene:

1. Título del modelo de convención, objetivo general de la investigación, indicadores generales de evaluación con el nivel de acuerdo o desacuerdo y autor del instrumento.
2. Datos generales (nombres y apellidos, DNI, profesión e institución donde labora.
3. Las preguntas (12) con las consideraciones antes descritas.

Procedimiento

Se preparó un cuestionario en físico para el desarrollo de la presente investigación (ver anexo criterio de expertos).

Prueba de Hipótesis para el objetivo general: La implementación de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la información almacenada.

El procedimiento a seguir:

1. Se ingresó la información de los cuestionarios a Excel: indicadores y su respectiva medición o escala.
2. Se insertó en el software estadístico SPSS para realizar la metodología de la prueba estadística para una muestra agrupados según preguntas del cuestionario detallados a continuación:

- Integridad: Preguntas 1, 4, 9 y 11
- Confidencialidad: Preguntas 6, 7 y 12
- Disponibilidad: Preguntas 3 y 8
- Gestión: Preguntas 2, 5 y 10
- Siguiendo la metodología:

  $H_o: \mu = 53$

  $H_a: \mu > 53$

Tabla 1

Prueba estadística para una muestra (modelo propuesto)

	Valor de prueba = 53				
				95% de intervalo de confianza de la diferencia	
	t	gl	Sig. (bilateral)	Inferior	Superior
Modelo	2.739	7	0.029	0.43	5.82

Toma de decisión: De la Tabla 1, la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 2.73 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la información almacenada.

Prueba de Hipótesis para los objetivos específicos

- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la integridad de la información almacenada.

$H_o: \mu = 18$

$H_a: \mu > 18$

Tabla 2

Prueba estadística para una muestra (integridad)

	Valor de prueba = 18				
				95% de intervalo de confianza de la diferencia	
	t	gl	Sig. (bilateral)	Inferior	Superior
Integridad	5.227	7	0.001	0.75	2.00

Toma de decisión: De la Tabla 2, la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 5.22 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la integridad de la información almacenada.

- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la confidencialidad de la información almacenada.

$H_o: \mu = 12$

$H_a: \mu > 12$

Tabla 3

Prueba estadística para una muestra (confidencialidad)

	Valor de prueba = 12				
				95% de intervalo de confianza de la diferencia	
	t	gl	Sig. (bilateral)	Inferior	Superior
Confidencialidad	3.265	7	0.014	0.45	2.80

Toma de decisión: De la Tabla 3, la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 3.26 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la confidencialidad de la información almacenada.

- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la disponibilidad de la información almacenada.

$H_o: \mu = 8$

$H_a: \mu > 8$

Tabla 4

Prueba estadística para una muestra (disponibilidad)

	Valor de prueba = 8				
				95% de intervalo de confianza de la diferencia	
	t	gl	Sig. (bilateral)	Inferior	Superior
Disponibilidad	5.612	7	0.001	0.87	2.13

Toma de decisión: De la Tabla 4, la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 5.61 ubicándose en la región de rechazo, por lo

tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la disponibilidad de la información almacenada.

- La existencia de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la gestión efectiva de la información almacenada.

  $H_o: \mu = 12$

  $H_a: \mu > 12$

Tabla 5

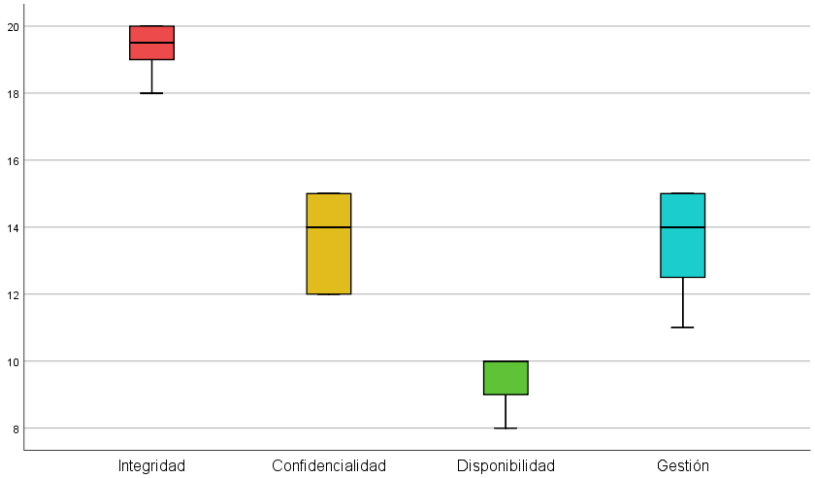
Prueba estadística para una muestra (gestión)

	Valor de prueba = 12				
				95% de intervalo de confianza de la diferencia	
	t	gl	Sig. (bilateral)	Inferior	Superior
Gestión	3.052	7	0.019	0.37	2.88

Toma de decisión: De la Tabla 5, la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 3.05 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la gestión de la información almacenada.

Figura 7

Diagrama de cajas (indicadores)



En la Figura 7, se observa que no existe una diferencia de medias en cuanto a la integridad, confidencialidad, disponibilidad y gestión efectiva de la información almacenada, teniendo en cuenta la escala de tipo Likert para medir el nivel (1=Totalmente en desacuerdo, 2=En desacuerdo, 3=Indeciso/Indecisa o Neutral, 4=De acuerdo, 5=Totalmente de acuerdo), precisando que el modelo es aceptado por los expertos (fácil aplicabilidad y eficiencia del modelo), demostrando así que el modelo contribuye eficientemente a mejorar la integridad, confidencialidad, disponibilidad y gestión efectiva de la información almacenada.

4.2 Discusión

Los resultados tienen una relación con lo que sostiene Villalobos (2008) en su investigación titulada "Auditando en las Bases de Datos", donde su objetivo fue de establecer controles que permitan minimizar el riesgo inherente que tienen los datos contenidos en una BD haciendo necesario implementar procedimientos de auditoría, teniendo como resultado establecer políticas de seguridad, procedimientos de utilización y controles pertinentes, las políticas deberán ser divulgadas en la organización, ya que los datos contenidos en las BD pueden considerarse uno de los activos más importantes que tiene la organización, ellos finalmente producirán la información que necesita la empresa para su funcionamiento día a día o para su planificación estratégica.

A partir de los resultados encontrados guardan relación con lo que sostiene Lu et al., (2013) en su investigación titulada "Auditar una base de datos bajo políticas de retención", precisa que auditar los cambios en una base de datos es fundamental para identificar comportamientos maliciosos, mantener la calidad de los datos y mejorar el rendimiento del sistema, pero un registro de auditoría preciso es un registro histórico del pasado que también puede representar una grave amenaza a la privacidad, las políticas que limitan la retención de datos entran en conflicto con el objetivo de una auditoría precisa, y los propietarios de datos deben equilibrar cuidadosamente la necesidad de cumplir con la política con el objetivo de una auditoría precisa; su investigación proporciona un marco para auditar los cambios en un sistema de base de datos respetando las políticas de retención de datos, teniendo como resultado el proponer dos modelos diferentes (un modelo independiente de tupla y un modelo correlacionado con tupla) para formalizar el significado de las consultas de auditoría implementando la aplicación de políticas y la respuesta de consultas de manera eficiente en un sistema relacional estándar y caracterizamos los casos en los que se puede lograr una auditoría precisa bajo restricciones de retención. En otras palabras, se almacena de manera constante cada operación de inserción, actualización y eliminación en los registros, esta capacidad puede facilitar tareas como el análisis en auditorías, la detección de errores y anomalías, la identificación de cambios no autorizados y la reconstrucción de información, lo que brinda condiciones más seguras y confiables y fortalece la seguridad de la información (Rus y Danescu, 2010).

Finalmente los resultados encontrados guardan relación con lo que sostienen Lopez y Espinoza (2022) en su tesis “Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, según la Norma ISO/IEC 27001:2013”, proponen un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la Norma ISO/IEC 27001:2013 para una empresa de consultoría financiera en Lima, los resultados revelaron la existencia de violaciones de seguridad cibernética, lo que condujo a la necesidad de identificar vulnerabilidades y deficiencias en la gestión de la información; además, establecieron mecanismos técnicos para optimizar el SGSI, que se fundamenta en fases de planificación, ejecución, control y acción, proponiendo un equipo de verificación y respuesta, con directrices claras para reaccionar de manera oportuna y eficiente ante ciberataques, su propuesta del SGSI, en línea con la Norma ISO/IEC 27001:2013, tuvo como objetivo salvaguardar los activos informáticos, certificando la disponibilidad, confidencialidad e integridad de la información, garantizando la continuidad de las operaciones incluso en situaciones de contingencia debido a ataques no autorizados.

CONCLUSIONES

PRIMERO: Se cumplió con el objetivo planteado, desarrollando un modelo de convención eficiente para el diseño seguro de bases de datos relacionales con controles de auditoría, con un p-valor=0.000 siendo menor en comparación a la prueba t mostrada, propuesta refinada utilizando el método de criterio de expertos, en razón a que se logran identificar y estudiar las actuales implementaciones de bases de datos que consideran algunos aspectos de auditoría, tales como añadir campos a una tabla, consolidado histórico, logs de transacciones y tablas espejo; analizando ventajas y desventajas de cada una, mismas que coadyuvaron a obtener indicadores de evaluación como cualificaciones concretas orientadas a valorar su idoneidad, seguridad, eficacia y eficiencia a considerar en una base de datos auditable, concluyendo que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la información almacenada.

SEGUNDO: Con respecto al primer objetivo específico, se obtuvo la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 5.22 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la integridad de la información almacenada.

TERCERO: De igual manera para el segundo objetivo específico la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 3.26 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la confidencialidad de la información almacenada.

CUARTO: Asimismo, para el tercer objetivo específico, se obtuvo la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 5.61 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de

datos relacionales contribuye eficientemente a mejorar la disponibilidad de la información almacenada.

QUINTO: Finalmente, para el cuarto objetivo específico, la prueba t tabulada es 1.89 como punto fijo y la prueba t calculada es 3.05 ubicándose en la región de rechazo, por lo tanto, se acepta la Ha y se concluye que el modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la gestión de la información almacenada.

RECOMENDACIONES

PRIMERO: Revisar de forma heurística la bibliografía científica que trate del tema de la auditoría de base de datos en el mundo de la seguridad informática aplicando la Ley de Benford, a través de su ley de los números anómalos y su distribución logarítmica, para explicar las probabilidades de modificaciones en los datos, disminuyendo la subjetividad de este parámetro, cooperando en la predicción del crecimiento de los datos y de la auditoría.

SEGUNDO: Realizar las adecuaciones pertinentes para elaborar una propuesta de convención para la implementación de bases de datos NoSql con controles de auditoría y seguridad, para el registro de modificaciones en los datos, haciendo uso de la potencialidad del formato JSON en el almacenamiento de la auditoría.

TERCERO: Obtener convenciones para la implementación de bases de datos relacionales auditables, centradas en el Lenguaje de Definición de Datos (DDL) y Lenguaje de Control de Datos (DCL).

CUARTO: Obtener convenciones para tipos de auditoría específicas a cada sector, como ser gubernamental, financiero, salud, entre otros; alineados políticas externas e internas según su naturaleza.

QUINTO: Analizar y desarrollar un software multiplataforma que optimice en cierta medida la implementación de la propuesta de convención desarrollada, con soporte a diferentes motores de bases de datos relacionales libres; además que provea mecanismos de respaldo de auditoría, reconstrucción de información, monitoreo, alertas, reportes e informes, respecto al historial de cambios, alteraciones anómalas o accesos no autorizados.

BIBLIOGRAFÍA

Aguirre Bautista, J. de J. (2016). Auditoría en informática. In *Jurnal Penelitian Pendidikan Guru Sekolah Dasar* (SUAYED, Vol. 6, Issue August). 2016.

Bhatiya, R., y Potineni, P. (2020). Oracle® Database Database Administrator's Guide. In *Oracle and/or its affiliates.* https://docs.oracle.com/en/database/oracle/oracle-database/12.2/admin/database-administrators-guide.pdf

Braren. (2016). *Sugerencias de crear historicos de tablas de BD*. https://es.stackoverflow.com/questions/13827/sugerencias-de-crear-historicos-de-tablas-de-bd

Cabero Almenara, J., y Llorente Cejudo, M. del C. (2013). La aplicación del juicio de experto como técnica de evaluación de las tecnologías de la información y comunicación (TIC). *Eduweb*, *7*, 11–23. https://revistaeduweb.org/index.php/eduweb/article/view/206/154

Calbimonte, D. (2016). *Auditoría de seguridad de bases de datos SQL Server*. https://solutioncenter.apexsql.com/es/auditoria-de-seguridad-de-bases-de-datos-sql-server/

Camps, R., Casillas, L., Costal, D., Gilbert, M., Martín, C., y Pérez, O. (2005). Datos Bases de Datos. *Fundació per a La Universitat Oberta de Catalunya*, 1–460. www.glo.org.mx

Coronel, C., Morris, S., y Rob, P. (2018). Database System: Design, Implementation, and Management. In *Management*.

DAMA International. (2017). DAMA-DMBOK: Guía Del Conocimiento Para La Gestión De Datos (Spanish Edition). In *Technics Publications*. https://books.google.co.ve/books?id=5fnvDwAAQBAJ&printsec=frontcover#v=onepage&q&f=false

Del Pino, S. (2016). *Delitos Informáticos, Generalidades*. https://www.studocu.com/pe/document/universidad-nacional-de-ingenieria/seguridad-informatica/06-delitos-informaticos-generalidades-autor-dr-santiago-acurio-del-pino/18537301

Domínguez, J. (2016). *Cómo auditar cambios en una tabla MySQL o MariaDB*. https://www.researchgate.net/publication/308170361_Como_auditar_cambios_en_una_tabla_MySQL_o_MariaDB

Elmasri, R., y Navathe, S. (2016). *Fundamentals of Database Systems* (VII). Pearson.

García, L., y Fernàndez, S. J. (2008). Procedimiento de aplicación del trabajo creativo en grupo de expertos. *Ingeniería Energética*, *29*(2), 46–50. http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=57951122&lang=es&site=ehost-live

Gartner. (2019). *Magic Quadrant for Operational Database Management Systems*. Gartner Research. https://www.gartner.com/en/documents/3975492

Gisbert, B. (2015). *UF1272: Administración y auditoría de los servicios web*. https://cutt.ly/8nPNLQP

Glushchenko, S. (2014). *Database auditing alternatives for MySQL*. PERCONA. https://www.percona.com/blog/database-auditing-alternatives-mysql/

Gómez Fuentes, M. del C. (2013). *Notas del curso Base de Datos* (Universida). https://docplayer.es/13226007-La-mayoria-de-los-sistemas-computacionales-utilizan-una-base-de-datos-para-manejar-su.html

González, A. J. (2002). Árboles Binarios. In *Estructura de Datos y Algoritmos* (UNED, pp. 1–48). http://www.lcc.uma.es/~galvez/ftp/tad/tadtema4.pdf

Hassan, M. (2016). *Audit and Log Database DML Changes in PostgreSQL With Cyan Audit - DZone Database*. https://dzone.com/articles/audit-log-database-changes-in-postgresql

Hernández, R., y Mendoza, C. (2018). *Metodología de la Investigación: Las Rutas Cuantitativa, Cualitativa y Mixta*.

Huang, Q., y Liu, L. (2009). *A Logging Scheme for Database Audit*. ACMDigital Library. https://dzone.com/articles/spring-data-jpa-auditing-automatically-the-good-stuff

Ingravallo, H., y Entraigas, V. (2007). *Auditoria de bases de datos Tesis de Licenciatura*. Universidad Nacional de la Patagonia.

ISACA. (2012). *COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. http://linkd.in/ISACAOfficial

Joshi, N. (2017). *Spring Data JPA Auditing: Automatically Saving the Good Stuff*. DZONE. https://dzone.com/articles/spring-data-jpa-auditing-automatically-the-good-stuff

Law, C. (2022). *La convención como norma de derecho internacional*. https://fc-abogados.com/es/la-convencion-como-norma-de-derecho-internacional/

Likert, R. (1932). A Technique for the Measurement of Attitudes. *Archives of Psychology*, *22*, 5–55. https://doi.org/10.4135/9781412961288.n454

López, D., Gallego, P., Fernández-Montes, A., y Sánchez-Venzalá, J. I. (2012). Big Data: Un nuevo problema computacional. *Sistemas Cualitativos y Sus Apliacaciones En Diagnosis, Robótica e Inteligencia Ambiental*, 1–6.

Lopez Torres, C. B., y Espinoza Melendez, J. C. (2022). *Propuesta de un Sistema de Gestión de Seguridad de la Información para una Empresa de Consultoría Financiera en Lima, 2021, según la Norma ISO/IEC 27001:2013* [Universidad Peruana de Ciencias e Informática]. https://orcid.org/0000-0003-4769-0101

Lu, W., Miklau, G., y Immerman, N. (2013). Auditing a database under retention policies. *VLDB Journal*, *22*(2), 203–228. https://doi.org/10.1007/S00778-012-0282-X/METRICS

MariaDB. (2022). *MariaDB Documentation*. https://mariadb.org/documentation/

Maya Villazón, E. (2015). La importancia del uso de base de datos y la seguridad de la información para el fortalecimiento de las TIC y para el ejercicio eficiente del control fiscal. *XXV Asamblea General OLACEFS Santiago de Querétaro, 16.1.2015*.

Microsoft. (2021a). *SQL Server Audit (motor de base de datos)*. SQL Server. https://learn.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver16

Microsoft. (2021b). *SQL Server technical documentation*. https://learn.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver15

Microsoft. (2023). *SQL Server Audit (Database Engine)*. Microsoft Learn. https://learn.microsoft.com/en-us/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver16

Moor, J. (2018). *What is Computer Ethics*. https://web.cs.ucdavis.edu/~rogaway/classes/188/spring06/papers/moor.html

Muñoz, C. (2002). *Auditoría en Sistemas Computacionales*.

Nevado, V. (2010). Introduccion a Las Bases de Datos Relacionales. In *Editorial Visión Libros*. https://books.google.es/books?hl=es&lr=&id=0lUpB1lNUdIC&oi=fnd&pg=PA11&dq=base+de+datos+relacional&ots=sLXTG1rXRI&sig=x0uNe7BrHlpGrzDXIYtstM1QO84#v=onepage&q=base de datos relacional&f=false%0Ahttps://books.google.es/books?hl=es&lr=&id=0lUpB1lNUdIC&oi=fnd

Oracle, C. (2021). *MySQL 8.0 Reference Manual*. https://dev.mysql.com/doc/refman/8.0/en/

Peley, O., Sanchez, R., y Urdaneta, A. (2019). *Aplicación web responsive para la gestión de servicios automotrices* [Universidad Dr. Rafael Belloso Chacín]. https://virtual.urbe.edu/tesispub/0108278/intro.pdf

Peréz, J., Sharma, A., Dodwal, K., y D'Alessandro, S. (2015). *Oracle Database 12c: Auditoria en 12c: Auditoría Unificada (Unified Auditing)*. ORACLE. https://www.oracle.com/lad/technical-resources/articles/idm/unified-audit-database-12c.html

PGAudit. (2022). *PostgreSQL Auditing Extension*. https://www.pgaudit.org/

Piattini, M., Del Peso Navarro, E., y Del Peso Ruiz, M. (2008). Auditoría de Tecnologías y Sistemas de Información. In *RAMA*. https://books.google.com.pe/books/about/Auditoría_de_Tecnologías_y_Sistemas_de.html?id=6o2fDwAAQBAJ&redir_esc=y

Piñero, J. (2013). Bases de datos relacionales y modelado de datos. *Paraninfo*.

PostgreSQL. (2020). *PostgreSQL 13.8 Documentation*.

https://www.postgresql.org/docs/13/index.html

Postigo, A. (2020). *Seguridad Informática*. Paraninfo. https://www.paraninfo.es/catalogo/9788428344555/seguridad-informatica--edicion-2020-

Presidencia del Consejo de Ministros, P. (2016). *NTP ISO/IEC 27001:2014*.

Ramírez Rivas, J. F. (2019). *Implementación de lineamientos base de seguridad en bases de datos Oracle y SQL server en una entidad bancaria*. Universidad San Ignacio de Loyola.

Riggs, S., Menon-Sen, A., y Barwick, L. (2017). *Open Source PostgreSQL Audit Logging*. 2ndQuadrant Pgaudit Project. https://github.com/pgaudit/pgaudit/blob/master/README.md

Rus, I., y Danescu, T. (2010). The Information Audit - Between Necessity and Regulation. *APPLIED ECONOMICS, BUSINESS AND DEVELOPMENT*, 98–103. https://www.researchgate.net/publication/265275966_The_Information_Audit_-Between_Necessity_and_Regulation

Sáenz Pérez, F. (2011). *Bases de datos*.

Sandoval, H. (2012). *Introducción a la Auditoria*. http://www.aliat.org.mx/BibliotecasDigitales/economico_administrativo/Introduccion_a_la_auditoria.pdf

Sota Orellana, L. A. (2019). *Diseño del plan de seguridad informática basado en la NTP ISO/IEC 27001:2014 para la Municipalidad del Centro Poblado de Salcedo - Puno*. Universidad Andina del Cusco.

Uazuay. (2012). El modelo relacional. In *Paradigmas de Modelado de Base de Datos* (Universida, pp. 1–8). http://docencia.lbd.udc.es/bdd/teoria/tema2/2.3.1.-ElModeloRelacional.pdf

Villalobos Murillo, J. (2008). Auditando en las bases de datos. *UNICIENCIA*, *22*, 135–140.

Villena Aguilar, M. A. (2006). *Sistema de gestión de seguridad de información para una institución financiera*. Pontificia Universidad Católica del Perú.

Zegarra Arana, J. A., y Saavedra Saldaña, M. H. (2009). Sistemas espaciales de teledetección. *Universidad Nacional de Trujillo – Valle Jequetepeque, Ingeniería Informática*. https://static.uvq.edu.ar/mdm/teledeteccion/unidad-2.html

ANEXOS

Anexo 1. Matriz de Consistencia

TÍTULO: Modelo de convención con controles de auditoría y seguridad de base de datos relacionales, 2023

PROBLEMA	OBJETIVO	HIPÓTESIS DE INVESTIGACIÓN	VARIABLES	METODOLOGÍA
¿Cuál es la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales?	Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales	La implementación de un modelo de convención con controles de auditoría y seguridad en bases de datos relacionales contribuye eficientemente a mejorar la integridad, confidencialidad, disponibilidad y gestión efectiva de la información almacenada.	Base de datos con controles de auditoria: Propuesta de diseño seguro	**TIPO DE INVESTIGACIÓN** No experimental **NIVEL DE INVESTIGACIÓN** Descriptiva **DISEÑO DE INVESTIGACIÓN** Cualitativo **POBLACIÓN** La población se compone por usuarios que utilizarán el modelo de convención. **MUESTRA** La muestra estuvo conformada por 8 usuarios expertos seleccionados mediante el muestreo de juicio de expertos, según Hernández y Mendoza (2018) por las características que tiene la población en investigación, a fin de evaluar las características del modelo de convención. **TÉCNICAS DE RECOLECCIÓN DE DATOS** La técnica fue la encuesta y como instrumento el cuestionario.

Anexo 2. Base de Datos

N°	Preguntas	Indicadores	Exp 1	Exp 2	Exp 3	Exp 4	Exp 5	Exp 6	Exp 7	Exp 8
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	5	5	5	4	4	5	5	5
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	5	5	4	4	4	5	4	5
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	5	4	4	5	5	5	5	5
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	5	5	5	5	5	5	5	5
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	5	5	4	4	4	5	5	4
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	4	5	2	4	5	5	5	5
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	5	5	4	5	5	5	4	4
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	5	5	4	4	5	5	5	5
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoría aumentan el nivel de seguridad.	Integridad	5	5	5	5	5	5	5	5
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	5	5	4	4	4	5	5	5
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	5	4	4	4	5	5	5	5
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	4	5	5	5	5	5	5	3

Anexo 3. Criterio de Expertos

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: _____ DNI N° _____

Profesión: _____ Institución donde labora actualmente: _____

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	[ ]	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	[ ]	[ ]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	[ ]	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	[ ]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[ ]	[ ]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[ ]	[ ]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[ ]	[ ]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	[ ]	[ ]	[ ]	[ ]	[ ]

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoría aumentan el nivel de seguridad.	Integridad	[ ]	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[ ]	[ ]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	[ ]	[ ]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	[ ]	[ ]	[ ]	[ ]	[ ]

_____
Firma del Experto
DNI N°_____

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Rogger Humpiri Flores DNI N° 46545513

Profesión: Ing. de Sistemas Institución donde labora actualmente: Ciya Los Andes

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoria en bases de datos relacionales.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoria en las tablas son los mínimos requeridos.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoria.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoria se almacenen de forma separada a la base de datos principal.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoria planteada posibilita la reconstrucción de información.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[ ]	[X]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoria de bases de datos relacionales.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoria.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
			[5]	[4]	[3]	[2]	[1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	[ ]	[X]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 46540568

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Copari Romero Freddy Gonzalo DNI N° 42794556

Profesión: Ing. Estadística e Inform. Institución donde labora actualmente: UNAJ

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	[ ]	[X]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
			[5]	[4]	[3]	[2]	[1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	[ ]	[X]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 42744556

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: YUCRA PARI ANDRES WILVER DNI N° 42273524

Profesión: ESTADISTICA E INFORMATICO Institución donde labora actualmente: UNA PUNO

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	[ ]	[X]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[ ]	[ ]	[ ]	[X]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[ ]	[X]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	[ ]	[X]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	[ ]	[X]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 48973524

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Apaza Culqui Renzo DNI N° 42670385

Profesión: Ing. Estadístico e Informático Institución donde labora actualmente: UNA-P

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	[ ]	[X]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[ ]	[X]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	[ ]	[X]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
			[5]	[4]	[3]	[2]	[1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	[ ]	[X]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 42621155

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Abel Angel Sullon Macalupu DNI N° 06812118

Profesión: Ing. de Sistemas Institución donde labora actualmente: UPeV

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	[ ]	[X]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[ ]	[X]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
			[5]	[4]	[3]	[2]	[1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoría aumentan el nivel de seguridad.	Integridad	X	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[ ]	X	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	X	[ ]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	X	[ ]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 06812118

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Ccapa Luque Rick Armando DNI N° 43221675

Profesión: Ing. Sistemas Institución donde labora actualmente: UNAP

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoría en las tablas son los mínimos requeridos.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[X]	[ ]	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	[X]	[ ]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
			[5]	[4]	[3]	[2]	[1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	X	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	X	[ ]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	X	[ ]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	X	[ ]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 43221675

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Tipo Mamani Noe Wilber DNI N° 47259697

Profesión: Ing. Sistemas Institución donde labora actualmente: Essalud.

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoria en bases de datos relacionales.	Integridad	X	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoria en las tablas son los mínimos requeridos.	Confidencialidad	[ ]	X	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoria.	Disponibilidad	X	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	X	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoria planteada posibilita la reconstrucción de información.	Confidencialidad	X	[ ]	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	X	[ ]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoria de bases de datos relacionales.	Gestión	[ ]	X	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoria.	Disponibilidad	X	[ ]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	X	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	X	[ ]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	X	[ ]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	X	[ ]	[ ]	[ ]	[ ]

Firma del Experto
DNI N° 47259697

Autor del instrumento: Milton Edward Humpiri Flores

CRITERIO DE EXPERTOS

TÍTULO: **MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023**

Objetivo: Determinar la eficiencia del Modelo de Convención con Controles de Auditoría y Seguridad de Base de Datos relacionales.

Indicadores de evaluación:

- *Integridad: Formulado con un lenguaje apropiado, no genera contradicción.*
- *Confidencialidad: Está en el marco de la temática abordada.*
- *Disponibilidad: Mide alguna variable o relación.*
- *Gestión: Relevante para cumplir con las preguntas y objetivos de investigación.*

Instrucciones: En base al documento analizado que contiene el modelo de convención, valore la pertinencia y fiabilidad del trabajo realizado. Coloque la puntuación que considere adecuada en cada pregunta.

Apellidos y Nombres del Experto: Huaman Paco Nelida DNI N° 71983281

Profesión: Ing. Sistemas Institución donde labora actualmente: UPEU

N°	Preguntas	Indicadores	Totalmente en de acuerdo [5]	De acuerdo [4]	Indeciso [3]	En desacuerdo [2]	Totalmente en desacuerdo [1]
1	El modelo de convención considera controles de auditoría en bases de datos relacionales.	Integridad	X	[ ]	[ ]	[ ]	[ ]
2	Considera que los campos de auditoria en las tablas son los mínimos requeridos.	Confidencialidad	X	[ ]	[ ]	[ ]	[ ]
3	Considera que modificar la estructura de las tablas en nuevas bases de datos aportaria mayor información de auditoria.	Disponibilidad	X	[ ]	[ ]	[ ]	[ ]
4	Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal.	Integridad	X	[ ]	[ ]	[ ]	[ ]
5	La estructura de auditoría planteada posibilita la reconstrucción de información.	Confidencialidad	[ ]	X	[ ]	[ ]	[ ]
6	La posibilidad de capturar las modificaciones de datos de acciones SQL de sólo inserción, edición, eliminación, sólo dos de estos o todos en conjunto; así como seleccionar sólo algunas tablas o columnas, pueden ser opciones configurables.	Gestión	X	[ ]	[ ]	[ ]	[ ]
7	La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales.	Gestión	[ ]	X	[ ]	[ ]	[ ]
8	El modelo facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría.	Disponibilidad	X	[ ]	[ ]	[ ]	[ ]

Autor del instrumento: Milton Edward Humpiri Flores

Nº	Preguntas	Indicadores	Totalmente en de acuerdo	De acuerdo	Indeciso	En desacuerdo	Totalmente en desacuerdo
			[5]	[4]	[3]	[2]	[1]
9	Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
10	Es posible contar con un historial de cambios de cada registro.	Confidencialidad	[X]	[ ]	[ ]	[ ]	[ ]
11	El modelo contribuye en el aseguramiento de la integridad de los datos.	Integridad	[X]	[ ]	[ ]	[ ]	[ ]
12	Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente el modelo en bases de datos existentes.	Gestión	[ ]	[ ]	[X]	[ ]	[ ]

Firma del Experto
DNI N° 71987241

Autor del instrumento: Milton Edward Humpiri Flores

DECLARACIÓN JURADA DE AUTENTICIDAD DE TESIS

Por el presente documento, Yo MILTON EDWARD HUMPIRI FLORES,
identificado con DNI 45538765 en mi condición de egresado de:

☐ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☒ **Programa de Maestría o Doctorado**

DOCTORADO EN ESTADÍSTICA E INFORMÁTICA,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación** denominada:
"MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023"

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

En caso de incumplimiento de esta declaración, me someto a las disposiciones legales vigentes y a las sanciones correspondientes de igual forma me someto a las sanciones establecidas en las Directivas y otras normas internas, así como las que me alcancen del Código Civil y Normas Legales conexas por el incumplimiento del presente compromiso

Puno 17 de MAYO del 2024

FIRMA (obligatoria)

Huella

AUTORIZACIÓN PARA EL DEPÓSITO DE TESIS O TRABAJO DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL

Por el presente documento, Yo MILTON EDWARD HUMPIRI FLORES,
identificado con DNI 45538765 en mi condición de egresado de:

☐ **Escuela Profesional,** ☐ **Programa de Segunda Especialidad,** ☒ **Programa de Maestría o Doctorado**

DOCTORADO EN ESTADÍSTICA E INFORMÁTICA,

informo que he elaborado el/la ☐ **Tesis** o ☐ **Trabajo de Investigación** denominada:

"MODELO DE CONVENCIÓN CON CONTROLES DE AUDITORÍA Y SEGURIDAD DE BASE DE DATOS RELACIONALES, 2023"

para la obtención de ☒**Grado,** ☐ **Título Profesional** o ☐ **Segunda Especialidad.**

Por medio del presente documento, afirmo y garantizo ser el legítimo, único y exclusivo titular de todos los derechos de propiedad intelectual sobre los documentos arriba mencionados, las obras, los contenidos, los productos y/o las creaciones en general (en adelante, los "Contenidos") que serán incluidos en el repositorio institucional de la Universidad Nacional del Altiplano de Puno.

También, doy seguridad de que los contenidos entregados se encuentran libres de toda contraseña, restricción o medida tecnológica de protección, con la finalidad de permitir que se puedan leer, descargar, reproducir, distribuir, imprimir, buscar y enlazar los textos completos, sin limitación alguna.

Autorizo a la Universidad Nacional del Altiplano de Puno a publicar los Contenidos en el Repositorio Institucional y, en consecuencia, en el Repositorio Nacional Digital de Ciencia, Tecnología e Innovación de Acceso Abierto, sobre la base de lo establecido en la Ley N° 30035, sus normas reglamentarias, modificatorias, sustitutorias y conexas, y de acuerdo con las políticas de acceso abierto que la Universidad aplique en relación con sus Repositorios Institucionales. Autorizo expresamente toda consulta y uso de los Contenidos, por parte de cualquier persona, por el tiempo de duración de los derechos patrimoniales de autor y derechos conexos, a título gratuito y a nivel mundial.

En consecuencia, la Universidad tendrá la posibilidad de divulgar y difundir los Contenidos, de manera total o parcial, sin limitación alguna y sin derecho a pago de contraprestación, remuneración ni regalía alguna a favor mío; en los medios, canales y plataformas que la Universidad y/o el Estado de la República del Perú determinen, a nivel mundial, sin restricción geográfica alguna y de manera indefinida, pudiendo crear y/o extraer los metadatos sobre los Contenidos, e incluir los Contenidos en los índices y buscadores que estimen necesarios para promover su difusión.

Autorizo que los Contenidos sean puestos a disposición del público a través de la siguiente licencia:

Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional. Para ver una copia de esta licencia, visita: https://creativecommons.org/licenses/by-nc-sa/4.0/

En señal de conformidad, suscribo el presente documento.

Puno 17 de MAYO del 2024

FIRMA (obligatoria)

Huella