# UNIVERSIDAD ANDINA SIMÓN BOLÍVAR
# SEDE CENTRAL
# Sucre – Bolivia

## MAESTRÍA EN SOFTWARE LIBRE

## PROPUESTA DE CONVENCIÓN PARA EL DISEÑO SEGURO DE BASES DE DATOS CON CONTROLES DE AUDITORÍA

**Tesis presentada para optar el Grado Académico de Magister en Software Libre**

**MAESTRANTE:** ESNOR NOEL ENRIQUE VACA MORENO

**Sucre - Bolivia**

**2021**

# UNIVERSIDAD ANDINA SIMÓN BOLÍVAR
# SEDE CENTRAL
# Sucre – Bolivia

## MAESTRÍA EN SOFTWARE LIBRE

## PROPUESTA DE CONVENCIÓN PARA EL DISEÑO SEGURO DE BASES DE DATOS CON CONTROLES DE AUDITORÍA

**Tesis presentada para optar el Grado Académico de Magister en Software Libre**

**MAESTRANTE:** ESNOR NOEL ENRIQUE VACA MORENO

**TUTOR:** MAURICIO CANSECO TORRES

**Sucre - Bolivia**

**2021**

**Dedicatoria**

**A Dios**.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

**A mi madre Jessica.**

Por sus consejos y sus valores, que me han permitido ser una persona de bien, pero más que nada, por su amor, por todo su esfuerzo y confianza en mí. Que en Paz Descanse.

**A mi esposa Roxana.**

Por su amor, paciencia, motivación y apoyo incondicional para alcanzar esta meta en la vida, sin ella todo hubiera sido más difícil.

**A mis familiares.**

A mi hermana Zorita, a mi hermano Fernando, por su cariño y, a todos aquellos que participaron directa o indirectamente en la elaboración de este trabajo.

**Agradecimientos**

A Dios por iluminar mis pensamientos y permitirme culminar con éxito esta meta, por haberme brindado sabiduría y fortaleza y, sobre todo la vida.

A mi familia y seres más queridos por su incondicional apoyo, comprensión y solidaridad, afecto y paciencia en el transcurso de esta maestría.

A mi tutor, al coordinador académico y a mis docentes de la maestría por la orientación, apoyo, tiempo y consejos que como verdaderos maestros estuvieron a mi alcance, durante la preparación, ejecución y conclusión de este trabajo, mis sinceros agradecimientos.

A los expertos en el área que desde su experiencia me brindaron sus valiosas opiniones y retroalimentación en la presente propuesta de convención.

A mis compañeros y amigos por las experiencias y, a todos aquellos que de alguna manera me apoyaron en todo momento, para no tropezar en el camino.

A la Universidad Andina Simón Bolívar por acogerme, brindarme los conocimientos y ayudarme a superarme como un profesional más competente.

**A TODOS MI SINCERA GRATITUD.**

## Resumen

La información almacenada en las bases de datos se ha convertido más que nunca en un activo valioso para las entidades, por lo que su resguardo y trazabilidad son aspectos importantes que deben asegurarse, de modo que contribuyan en la realización de procesos de auditoría, de forma unificada cuando sea requerido.

El objetivo del presente estudio es proponer una convención, de estándar abierto, para modelar bases de datos relacionales con controles de auditoría y seguridad, centrado en registrar las modificaciones, adiciones y eliminaciones de datos. Con esta finalidad, se utilizó la metodología de investigación tecnológica, con alcance exploratorio, enfoque cualitativo y con los métodos inductivo y analítico; donde se efectuó una distinción de las prácticas actuales de auditoría de base de datos en cuanto a sus ventajas y desventajas, así como la identificación de indicadores de evaluación y, directrices o características deseadas que debería poseer una base de datos con controles de auditoría y seguridad.

Finalmente, se elaboró una convención como propuesta para el diseño seguro de bases de datos relacionales con controles de auditoría, la cual fue refinada mediante el método de criterio de expertos en el área, estructurada en cinco ejes descriptivos: la descripción de la propuesta, justificación e importancia, objetivos de seguridad, el enfoque y la implementación a nivel de gestión y técnico; el instrumento utilizado de valoración consigue una confiabilidad del 91% y una validez del 88%, brindando dicha propuesta de convención a disposición de las comunidades para su aplicación libre.



*Palabras clave: auditoría de base de datos, convención de auditoría, seguridad de la información, control de auditoría de datos.*

## Abstract

*The information stored in the databases has become more than ever a valuable asset for the entities, so its protection and traceability are important aspects that must be ensured, so that contribute to the performance of audit processes, in a way unified when required.*

*The objective of this study is to propose an open standard convention for modeling relational databases with auditing and security controls, centered in record the updates, inserts and deletions data. For this purpose, the technological research methodology was used, with an exploratory scope, qualitative approach and with inductive and analytical methods; where a distinction was made of current database auditing practices in terms of their advantages and disadvantages, as well as the identification of evaluation indicators and, guidelines or desired characteristics that a database with audit and security controls should have.*

*Finally, a convention was elaborated as a proposal for the secure design of relational databases with audit controls, which was refined through experts judgment method in the area, structured in five descriptive axes: the description of the proposal, justification and importance, security objectives, the approach and the implementation at the managerial and technical level, the instrument used valuation achieved a reliability of 91% and a validity of 88%, bringing its proposed convention available to the communities for its free application..*



*Keywords: database auditing, auditing convention, information security, data auditing control.*

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# 1 Introducción

## 1.1 Antecedentes

Hoy en día las bases de datos almacenan información extremadamente valiosa y confidencial, misma que se ha convertido en un activo más en las organizaciones, en algunas en el más valioso (Maya Villazón & otros, 2015). Como cualquier otro activo, debe manejarse cuidadosamente, garantizando su seguridad, protección, confidencialidad, integridad, disponibilidad y el uso efectivo, permitiendo su posterior auditoría (DAMA Internacional, 2015).

Aunque se realizan diversos tipos de auditoría, todos ellos conducen a emitir una opinión sobre algún registro, sistema, operación o actividad en particular o con fines específicos en un momento determinado (FCASUA, 2008, págs. 1-8). La auditoría de Base de Datos (BD), es un tipo de auditoría informática que se basa en medir, asegurar, demostrar, verificar, monitorear y registrar continuamente la información almacenada en las bases de datos, buscando minimizar sus riesgos inherentes (Villalobos Murillo, 2008, págs. 135-140).

En consecuencia, añadir a las bases de datos la característica de auditable, debe permitir asegurar la confidencialidad, integridad y disponibilidad de los datos; existiendo implementaciones a nivel de esquema y a nivel de datos; la segunda significa seguir y registrar cada cambio que se hace en los registros, realizar un seguimiento de los datos almacenados, similar a una bitácora o historial de cambios; dicho de otra manera, almacenar continuamente cada operación de inserción, actualización y eliminación en los registros (Lu, y otros, 2013, págs. 203-228), esto puede facilitar tareas en el tratamiento de información como: análisis en auditorías, detección de errores y anomalías, identificación de cambios no autorizados, reconstrucción de información; otorgando mejores condiciones seguras y confiables, fortaleciendo la seguridad de la información (Ioan & Danescu, 2018).

En el afán de poder realizar auditorías a las bases de datos, han surgido una variedad de *plugins* de auditoría de licencia privativa, específicamente para MySQL o MariaDB, que se diferencian en el formato de registro de los datos, filtrado de capacidades y nivel de detalle de los registros de auditoría, a nivel del lenguaje de definición de datos, en inglés *Data Definition Language* o DDL (Glushchenko, 2014).

También existen otras soluciones integradas como SQL Server Audit para SQL Server (Macauley & Cai, 2020) o la Auditoría Unificada que posee Oracle (Perez, Sharma, Dodwal, & D'Alessandro, 2015), ambas implementadas internamente bajo licencia privativa, pero ya tienen la funcionalidad de interactuar con el lenguaje de manipulación de datos, en inglés *Data Manipulation Language* o DML. Sin embargo, aparecen propuestas prácticas enfocadas en poseer registros históricos de los datos con un control total; tal es el caso de tener adicionalmente tres campos básicos en la misma tabla (id autonumérico, fecha de creación y fecha de modificación) y opcionalmente otros dos campos, usuario e ip, para una auditoría más completa (Domínguez, 2016).

Con un pensamiento similar, se publicó un artículo con las columnas Creado_Por, Fecha_Creacion, Modificado_Por y Fecha_Modificacion para cualquier entidad, la cual es implementada de forma automática sólo para proyectos con *Java Persistence API* o simplemente JPA (Joshi, 2017). Por otra parte, con una variación, se propone implementar la solución anterior, pero en una tabla diferente (Braren, 2016); con otra perspectiva surge Cyan Audit para PostgreSQL que es una extensión privativa que se encarga de detectar todos los cambios de base de datos referentes al DML y los guarda en una sola tabla en un esquema independiente dentro de la misma base de datos (Hassan, 2016); sin embargo, con la perspectiva de utilizar un log de actividades centralizado de DDL y DML, con mejoras y basado en estándares ISO, de código abierto, oficialmente se presenta pgAudit como una extensión del núcleo de PostgreSQL (Riggs, Menon-Sen, & Barwick, 2017).

Los proyectos existentes son soluciones para mantener el valor inicial y final de los datos afectados en el caso de utilizar por ejemplo la opción con JPA, o para ambientes que requieren gran espacio de almacenamiento en una misma unidad de disco en el caso de utilizar la opción Cyan Audit y PGAudit en PostgreSQL, no existiendo una implementación idónea para un trabajo de auditoría de seguridad de BD.

Poseer un esquema estándar en la gestión de la seguridad de los datos es esencial (Rus, 2015, págs. 991-999), y contar con algunos lineamientos generales para llevar a cabo esta implementación de forma óptima como el marco COBIT, el cual está alineado con estándares de control y auditoría (COSO, IFAC, IIA, ISACA, AICPA), son de importante contribución (ISACA, 2012).

La auditoría de BD puede reforzar la seguridad de la base de datos, pues el registro de actividades de datos suele ser el primer paso de la aplicación de auditoría de base de datos (Liu & Huang, 2009, págs. 390-393) y aprovechar la funcionalidad de los desencadenadores de bases de datos puede ayudar a lograr este objetivo (Perez, Sharma, Dodwal, & D'Alessandro, 2015).

## 1.2 Situación Problemática

Las actividades de control en la manipulación de información en la mayoría de las entidades, son escasas y en muchos de los casos, inexistentes, sobre todo en el control de registro de datos mediante sus sistemas implantados, pues la mayoría no contemplan controles de eventos en los datos, ni por la aplicación cliente y mucho menos por el motor de BD. Ocasionando carencia de información de operaciones críticas, no contando con registros de: ¿qué?, ¿quién?, ¿cómo?, ¿cuándo?, o ¿desde dónde? se han modificado, adicionado o eliminado datos.

Por defecto, los diseños de BD nacen con una estructura que no consideran algunos aspectos de seguridad, tal es el caso de obviar un esquema que soporte análisis de auditoría de seguridad de BD, representando riesgos de gran impacto que pueden afectar la correcta continuidad del negocio, siendo vulnerable a pérdida de la integridad de datos, carencia del no repudio y de confiabilidad de la información almacenada en las BD.

Quienes han tenido la iniciativa de implementar un esquema de auditoría de seguridad de BD para mitigar riesgos asociados al almacenamiento de información, vienen utilizando criterios personales e independientes. En entidades que poseen equipos de desarrollo de software, cada integrante aplica un diseño independiente uno del otro, pensando bastante tiempo en cómo se debería configurar un esquema de BD para mantener un registro de los cambios; generando dificultad en la administración de las BD con procesos complejos de revisión de auditorías.

Buscando alternativas de solución a lo anterior, surgieron las implementaciones mencionadas que se instauraron respondiendo a estas necesidades; pero tienen inconvenientes como el ser de licencia privativa, lo que representa un costo económico por el derecho de uso, algunas a precios muy elevados que quedan fuera del alcance financiero para empresas pequeñas o representan un gasto significativo recurrente en las entidades medianas.

Por otra parte, la accesibilidad del software es limitada, ya que dependiendo del tipo de licencia de software privativa; su uso puede ser nulo, por ejemplo, al requerir una clave de activación o estar desarrollado para una plataforma en específico. O en su defecto un uso parcial, ofreciendo una funcionalidad limitada y generalmente por un corto periodo de tiempo.

Si se desea realizar modificaciones para adecuarlo a las necesidades como quitar funcionalidad innecesaria, agregar nuevos parámetros o requerir de algunos tipos de reportes, es imposible legalmente al no tener los permisos. Si simplemente se desea conocer la funcionalidad interna del software para tener mayor seguridad y control de lo que hace, tampoco es posible porque no se tiene permitido el acceso y/o estudio del código fuente. Desde el punto de vista de implementación, es difícil conseguir que se adecuen al esquema de las BD de una entidad, siendo la puesta en marcha condicionada a ciertos factores como ambientes, tecnología, personal, económico; ocasionando obligatoriamente una dependencia tecnológica.

Este trabajo reviste de mucha importancia en el sentido de lograr un aporte social debido a que no solo responde a las necesidades de facilitar un mejor desenvolvimiento profesional en auditores e informáticos, sino que también al mantener un historial de cambios de los registros, acrecienta la seguridad de información confidencial y altamente valiosa, concientizando a los usuarios y administradores de bases de datos a no realizar acciones no autorizadas. Por otra parte, el aporte a los procesos de auditoría y seguridad son de trascendencia, puesto que de manera fundamentada e ingenieril se definirán lineamientos que garanticen la transparencia, trazabilidad y seguridad en la administración de bases de datos, contribuyendo sobremanera a la cultura de seguridad de la información.

Asimismo, la implementación de un esquema estándar de auditoría de seguridad de base de datos, es tecnológicamente innovador y necesario, ya que se pretende proponer la estandarización de la forma de implementar un esquema de base de datos con controles de auditoría y seguridad dentro de las organizaciones, el cual se tome como referencia para diseñar bases de datos que consideren mantener un historial de los cambios en sus registros dando pie a que sean más seguros y confiables, que además faciliten posteriores análisis de auditorías de bases de datos.

Por otra parte, económicamente; considerando la forma habitual de llevar a cabo este tipo de procesos es bastante moroso, con la implementación de un sistema informático que automatice este proceso, representará la optimización de recursos en tiempo, esfuerzo y dinero, puesto que se realizará la misma tarea en cuestión de segundos y con una probabilidad de error mucho menor, por no decir casi nula; que permitirá a los profesionales encargados, disponer del tiempo ahorrado para dedicarse a otras labores y ser más productivos. Además, al basarse en software libre y estándares abiertos, no se incurrirán en costos por la adquisición de licencias de software.

Finalmente, de acuerdo a los art. 363 bis de manipulación informática y 363 ter de alteración, acceso y uso indebido de datos informáticos, del Código Penal, el presente trabajo brinda mecanismos para mantener un historial de las modificaciones, adiciones y eliminaciones de los datos en las BD (Ministerio de Justicia, 1997); permitiendo contar de forma más rápida y sencilla con información para una auditoría de seguridad de BD y detectar las acciones autorizadas, pero no adecuadas.

## 1.3 Planteamiento del Problema

¿Es posible establecer convenciones para implementar controles de auditoría y seguridad en bases de datos relacionales que ayuden en la ejecución de procesos de auditoría?

## 1.4 Objetivos

### 1.4.1 Objetivo General

Proponer una convención de estándar abierto para modelar una base de datos con controles de auditoría y seguridad que permita realizar el registro de modificaciones, adiciones y eliminaciones de datos en las bases de datos relacionales.

### 1.4.2 Objetivos Específicos

- Identificar las ventajas y desventajas de los actuales diseños de BD basados en auditoría, identificando indicadores de evaluación deseados.
- Elaborar la convención con las directrices y/o características deseadas que debe poseer una BD, con controles de auditoría y seguridad a nivel de gestión y técnico, que puedan considerarse como lineamientos base.
- Evaluar la aplicabilidad de la propuesta de convención establecida, así como el contexto óptimo de aplicación.

## 1.5 Alcances y Delimitaciones

- El presente trabajo engloba sólo las bases de datos relacionales.
- La implementación de la auditoría de seguridad de bases de datos se centra en la parte de modificación respecto al DML, es decir, en las acciones de inserción, edición y eliminación.
- No se podrá aplicar a tablas que no contengan llave primaria auto numérica.
- La convención tendrá control de los registros a través de desencadenadores en cada tabla.
- La convención debe pasar por un proceso de validación y socialización para poder constituirse del todo.

## 1.6 Revisión del Estado del Arte

Todos los autores abajo citados, en sus investigaciones, coinciden en la importancia de la auditoría en las bases de datos, que ayuda a fortalecer su seguridad y que hoy en día la información contenida en las bases de datos es altamente valiosa para la continuidad del negocio ya que lleva el registro de los movimientos de una organización.

Por ello proponen mecanismos para permitir el acceso autorizado y su protección contra el acceso no autorizado, partiendo de la idea de que el registro de las actividades es el inicio para implementar auditoria a una BD, logrando reducir el riesgo potencial de seguridad y permitiendo rastrear la fuente cuando ocurran anomalías. Se ordena esta revisión del estado del arte de forma cronológica según las publicaciones de las investigaciones.

Lianzhong, L. y Qiang, H. (2009), en su artículo: *A Logging Scheme for Database Audit. Computer Science and Engineering, International Workshop*. Vol. 2. pp. 390-393. doi>10.1109/WCSE.2009.837. El mismo tiene por objetivo presentar un esquema de registro para la auditoría de base de datos. A diferencia del mecanismo nativo de registro y auditoría de una base de datos, los autores proponen un esquema para monitorear y registrar las actividades de la base datos a través del análisis del tráfico de red. Las categorías principales en la investigación son la captura de paquetes, el análisis de paquetes y el almacenamiento de datos, sin algunos de estos componentes se perdería el sentido de su trabajo.

Liu y Huang, mediante el uso de herramientas de software para la captura del tráfico de paquetes a bases de datos, tienen como resultado la propuesta de un esquema final que consiste en tres pasos generales: el primero es la captura de paquetes hacia y desde la base de datos; luego estudiando los protocolos de comunicación de la base de datos, se deben analizar dichos paquetes capturados, para finalmente usar los resultados analizados para respaldar la auditoría de la base de datos.

En el mismo año (2009), Noreen, Z. & Hameed, I. & Usman, A. Publicaron su artículo: *Development of database auditing infrastructure*. Vol. 78. doi>10.1145/1838002.1838092. Donde el objetivo es describir el desarrollo de la infraestructura de Auditoría de Bases de Datos; eligieron MS SQL Server 2005 con todas sus herramientas internas como ambiente de prueba. Las categorías de la investigación giran en torno a seguridad, desencadenadores, trazas e información de las bases de datos; aplicables dentro de la estructura de la base de datos respectiva. Dando como resultado de la investigación una guía genérica en base a las categorías ya mencionadas que puede integrarse en una base de datos existente, logrando contar con registros a partir de su implementación.

Con modelos más detallados, Wentian, L., Gerome, M., Neil, I. (2013), en su artículo *Auditing a database under retention policies*. The VLDB Journal — The International Journal on Very Large Data Bases: Vol. 22 Issue 2. pp. 203-228. New York, Inc. Secaucus, USA. doi>10.1007/s00778-012-0282-x. Trabajan sobre el objetivo de proporcionar un *framework* para auditar los cambios de un sistema de base de datos y al mismo tiempo respetar las políticas de retención de datos; las categorías identificadas en la investigación son los datos históricos, consultas flexibles de auditoría y políticas de retención de datos; el ocultamiento de valores de atributos individuales y la eliminación de tuplas completas.

Dando como resultado, Wentian, L. y otros (2013), la propuesta de dos modelos diferentes; un modelo independiente de la tupla, es decir, registrar la auditoría en una tabla diferente dentro de la base de datos; y un modelo correlacionado con la tupla, es decir, que la estructura de la tabla es alterada para adicionar campos de auditoría; en ambos modelos, se caracterizan los casos en los que se puede lograr una auditoria precisa bajo restricciones de retención.

Por otra parte, Huijie, W. (2017). En su artículo: *A Security Framework for Database Auditing System*. pp. 350-353. doi>10.1109/ISCID.2017.64. Presenta un diseño e implementación de un Framework de auditoría eficaz con seguridad, el cual tiene como objetivo evitar causar retrasos en el rendimiento de la base de datos mediante el modo de omisión; exponiendo como resultado, a diferencia de un sistema de auditoría tradicional, un *framework* con ventajas como el uso de copia cero para adquirir y reorganizar tablas, limitar el universo de entidades a auditarse y almacenarlo en una bitácora centralizada con datos concisos de lo que se registrará.

Con otra perspectiva, Woo, J. y otros. (2020). *Database Auditing*. Estudian los requisitos de auditoría de los sistemas de tecnologías de la información, planteando tres regulaciones gubernamentales, de acuerdo a la clasificación de los sistemas de auditoría de base de datos propuesto por Bishop: el registro de logs, el análisis del tráfico y la notificación al usuario final.

Buscando un aumento en la calidad del proceso auditor utilizando tecnologías libres, Mendoza, A. y otros (2020), en el artículo, AUDAT 2.0: Sistema de Auditoría de Datos para la Contraloría General de la República, pp. 25-40, Vol. 13, No. 5, Cuba. Ayudan a optimizar el trabajo al minimizar la carga manual actual en el tratamiento de la información en el proceso de auditoría de datos, el software permite que los auditores puedan manipular las fuentes de datos de los sistemas auditados a partir de la importación de datos desde diferentes ficheros como: SQLite, Microsoft Access, dBase y CSV y de gestores de BD como PostgreSQL, MySQL, SQL Server y Oracle; muestra de forma gráfica los resultados de filtros o extracciones de registros.

En base a los aportes en el campo de la auditoria de base de datos de los anteriores autores, en cuanto a sus propuestas de modelos o frameworks, es que organizaciones como Oracle (Oracle Database) o Microsoft (MS SQL Server), y otras basadas en comunidades (PostgreSQL, MySQL, MariaDB), desde hace mucho tiempo implementaron herramientas o *plugins* para sus sistemas de administración de base de datos, siendo en su mayoría de licencias privativas y otras con acceso total al código fuente como en el caso PostgreSQL.

Hoy en día, se cuentan con funcionalidades nativas dependientes del motor de base de datos, como la Auditoría Unificada de Oracle Database, la solución integrada de SQL

Server Audit y ApexSQL Audit, Cyan Audit y PgAudit para PostgreSQL, y el plugin de auditoría incluida en la versión Enterprise de MySQL y MariaDB.

## 1.7 Metodología de la Investigación

El presente trabajo utiliza la metodología de la investigación tecnológica, con alcance exploratorio, con enfoque cualitativo y con los métodos inductivo y analítico.

Para la detección del problema se usa la observación propia del entorno en cuanto a los controles de auditoría y seguridad en las bases de datos; buscando la formulación del problema en base al análisis de causas y efectos, identificación del problema central y, análisis de objetivos para determinar las metas que se deben lograr para considerar el problema solucionado.

La búsqueda y recopilación de información en el área de estudio está enfocada en la exploración bibliográfica en revistas científicas de tecnología, tesis, libros, publicaciones, foros y listas de correos en las comunidades de software libre referente a auditorías en bases de datos; con el fin de conocer el estado del arte de las implementaciones o tendencias actuales sobre controles de auditoría y seguridad en bases de datos. Tocando, además, temáticas referidas a definiciones generales de bases de datos, modelos de bases de datos, gestores de bases de datos, tipos y normas de auditoría, descripción del procesamiento interno de las convenciones utilizadas actualmente y su grado de formalidad; para luego organizar la información de acuerdo a conceptos generales, estándares y técnicas.

Siguiendo el método analítico, se realiza la búsqueda de ideas, analizando cada una de las convenciones encontradas que actualmente están siendo utilizadas; identificando cualitativamente las ventajas y desventajas de cada una, para luego mediante la inducción identificar criterios de evaluación y elaborar una comparación entre cada alternativa existente respecto a los criterios planteados.

En consecuencia, estas ideas evaluadas servirán para el planteamiento de soluciones, en donde se pretende establecer las directrices que debería considerar un modelo de base de datos relacional auditable y proponer una primera aproximación de la convención; posteriormente es necesario realizar análisis y evaluación de la convención elaborada, a través de consultas con expertos para su afinación y obtener retroalimentación para la propuesta de convención refinada.

Mediante el método de criterio de expertos, se elabora un cuestionario como instrumento para la valoración de la propuesta de convención, donde es posible analizar la confiabilidad y validez del instrumento respecto a directrices e ítems valorados en una escala tipo Likert. Se determina el número y la selección de expertos mediante biogramas en combinación con el coeficiente de competencia experta, a quienes vía electrónica se envía la información necesaria de la propuesta de convención para su valoración experta. La consistencia interna y la confiabilidad se aborda con el Alfa de Cronbach y la validez con el Coeficiente de Validez de Contenido V de Aiken.

# 2 Marco Teórico

## 2.1 Base de Datos

### 2.1.1 Importancia de la información contenida en las Bases de Datos

Si se trata de operar un negocio sin saber quiénes son los clientes, qué productos se venden, quiénes son los empleados, quiénes son los deudores y acreedores, será una tarea difícil, pues al menos todos los negocios cuentan con este tipo de registros y muchos más; igual de importante es 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, el almacenamiento, agregado, la manipulación, la diseminación y la administración de datos” (Coronel & Morris, 2018, págs. 439-459).

Dependiendo del tipo de sistema de información y las particularidades de la entidad, podrían almacenar información de miles de *megabytes*. “¿Cómo pueden procesar enormes cantidades de datos? ¿Cómo pueden guardarla y después recuperar rápidamente sólo los datos que desean conocer quienes toman decisiones, justo cuando quieran verlos? La respuesta es que usan bases de datos”. Las bases de datos, poseen la capacidad de almacenar, administrar y consultar datos con bastante rapidez; de hecho, en la actualidad los sistemas utilizan bases de datos, “por lo cual una buena comprensión de cómo se crean estas estructuras y cómo se usan es vital para cualquier profesional de sistemas de información” (Coronel & Morris, 2018, págs. 734-736).

Las bases de datos almacenan información valiosa y confidencial. Una cantidad creciente de regulaciones de conformidad obligan a las organizaciones a hacer auditorías del acceso a dicha información restringida y a protegerla de los ataques y del mal uso o errores humanos que pudieran generarse en su administración. Una base de datos proporciona a los usuarios el acceso a datos, los pueden visualizar, ingresar o actualizar, en concordancia con los derechos de acceso que se les hayan otorgado. Su utilidad es mucho mayor a medida que la cantidad de datos almacenados crece. La principal ventaja de utilizar bases de datos es que múltiples usuarios pueden acceder a ellas al mismo tiempo (Ingravallo & Entraigas, 2007).

### 2.1.2 Definición de Base de Datos

Una base de datos es una colección 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 Cabello, 2010, págs. 22-40).

Los datos deben contar con un significado implícito, los cuales reflejan situaciones del mundo real y cambios en esas situaciones. Al ser datos relacionados debe existir homogeneidad en la colección, los datos se recopilan y registran con una finalidad, los datos deben ser relevantes con respecto a esa finalidad.

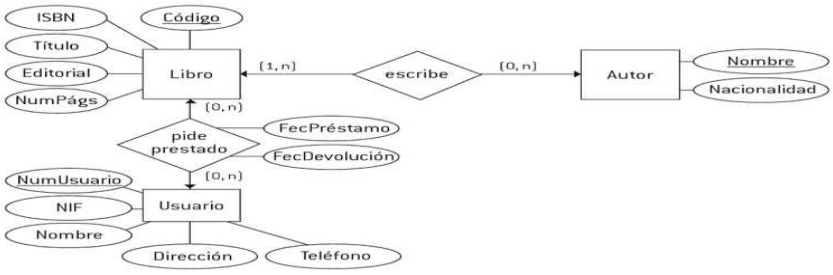
### 2.1.3 Modelos de Datos

Coronel y Morris (2018), clasifican los modelos de datos 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.

#### *2.1.3.1 Modelos de datos conceptuales*

**Modelo Entidad - Relación.** También llamado modelo conceptual de datos, es un modelo semántico que se utiliza para describir y construir el esquema conceptual de una base de datos, sirve para modelar un almacenamiento de datos, es una técnica especial de representación gráfica que incorpora información relativa a los datos y la relación existente entre ellos para dar una visión del mundo real. En muchos casos, los datos manipulados por el sistema determinan las acciones que se realizan. Puede ser útil definir los requerimientos concentrándose en los datos en lugar de las funciones. La abstracción de datos es una técnica para describir para qué son los datos, en lugar de cuál es su apariencia o cómo se denominan. En la siguiente figura se muestra un ejemplo de esquema E-R aplicable a una biblioteca:

Figura 2.1: Modelo Entidad – Relación



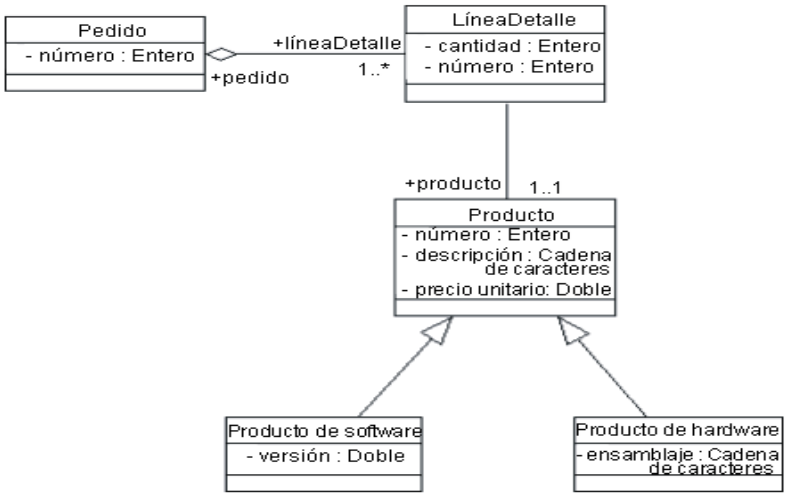

Fuente: Coronel y Morris (2018)

**Modelo Orientado a Objetos.** Es un modelo de datos lógico que captura la semántica de los objetos que se utiliza en la programación orientada a objetos. Por lo tanto, manejan conceptos básicos de 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 especificar tanto la estructura de objetos complejos como las operaciones que se pueden aplicar entre los mismos. Una base de datos orientada a objetos provee una identidad única a cada objeto independiente almacenado en la base de datos y se parte de la base de que los objetos complejos pueden construirse a partir de otros más simples.

La figura siguiente ilustra un diagrama de clase simple, sólo muestra los atributos (datos) de las clases.

Figura 2.2: Modelo Orientado a Objetos.



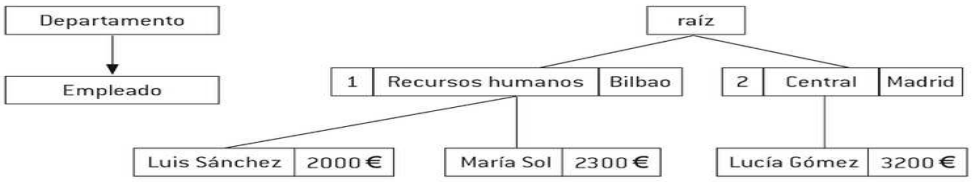

Fuente: Coronel y Morris (2018)

### *2.1.3.2 Modelos de datos lógicos*

**Modelo Jerárquico.** Se utilizan árboles para la representación lógica de los datos, en los que un padre (parte superior) puede tener cualquier número de hijos, pero cada hijo pertenece a un único padre. Existe en la estructura un nodo raíz que puede tener cualquier número de hijos, cada uno de los cuales a su vez puede tener cualquier número de hijos, y así sucesivamente. En la siguiente figura se muestra un diagrama de estructura de árbol con dos tipos de registros: departamento y empleado, donde en un departamento pueden trabajar varios empleados.

También se puede ver en la figura una posible instancia de base de datos:

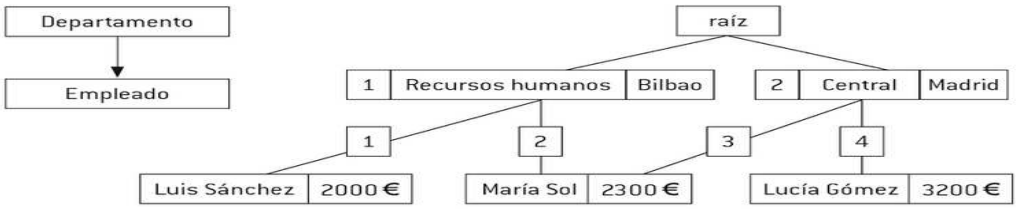
Figura 2.3: Modelo de datos lógico: Jerárquico




Fuente: Coronel y Morris (2018)

**Modelo en Red.** Se basa en la utilización de una estructura no lineal en la que cada registro hijo puede tener más de un nodo padre. Las entidades se representan como nodos de un grafo y las asociaciones o interrelaciones entre estas, mediante los arcos que unen dichos nodos. Un conjunto es una relación entre uno o más tipos de registros, que permite la navegación entre los registros. El modelo de red más extendido es el Codasyl. En la figura se muestra un ejemplo de representación de la información de este modelo:

Figura 2.4: Modelo de datos lógico: en Red.




Fuente: Coronel y Morris (2018)

**Modelo Relacional.** Se emplean tablas para la representación lógica de los datos y las relaciones entre ellos. Se llama tupla a cada fila de la tabla. Una clave es un atributo o conjunto de atributos que identifica de manera única a cada tupla. En la siguiente figura se representa la información que se podría almacenar en una base de datos relacional que contiene información sobre los departamentos que consta una empresa y los empleados que trabajan en ella:

Figura 2.5: Entidades modelo de datos lógico: Relacional

**Departamento**

| NumDep | NomDep | LocDep |
|---|---|---|
| 1 | Recursos humanos | Bilbao |
| 2 | Central | Madrid |

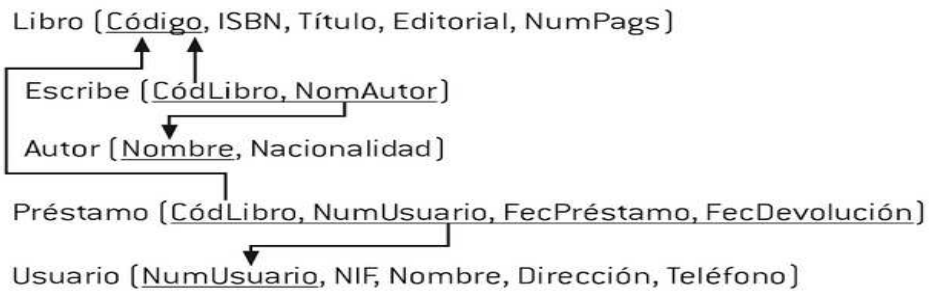
**Empleado**

| NomEmp | SalEmp | NumDep |
|---|---|---|
| Luis Sánchez | 2000 | 1 |
| María Sol | 2300 | 1 |
| Lucía Rodríguez | 3200 | 2 |

Fuente: Coronel y Morris (2018)

Para el esquema E-R, el esquema relacional que se obtendría aplicando reglas de transformación sería el siguiente, donde al lado de cada relación se indican entre paréntesis y separados por comas los atributos, se subraya la clave primaria de cada relación y se trazan flechas desde cada clave ajena a la correspondiente clave primaria:

Figura 2.6: Esquema E-R modelo de datos lógico: Relacional




Fuente: Coronel y Morris (2018)

#### *2.1.3.3 Modelos de datos físicos*

La última fase del diseño de una base de datos es el diseño físico, que consiste en crear en un sistema de gestión de base de datos (SGBD) concreto todos los elementos de que consta la base de datos. Si se trata de una base de datos relacional como la mayoría de las que se emplean hoy en día, implicaría crear tablas, índices, vistas, desencadenadores, y sus relaciones.

La creación de todos estos elementos se puede llevar a cabo de dos maneras: empleando asistentes con facilidades gráficas o mediante el empleo del lenguaje de definición de datos (DDL) que proporciona el SGBD que se esté utilizando. Por esto, en función al SGBD que se emplee, esta tarea se llevará a cabo de distinta forma.

#### *2.1.3.4 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. *Big Data* centra sus características en tres partes:

- Volumen. Grandes volúmenes de datos, a partir de *TeraBytes* o incluso *PetaBytes*.
- Variedad. El concepto de *Big Data* también suele venir acompañado de diversos tipos de fuentes de datos, ya sean estructurados o no estructurados.

- Velocidad. La frecuencia de las actualizaciones, su procesamiento y posterior análisis ha de realizarse prácticamente 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 significa que una vez que se escriben los datos, no se pueden modificar.

**MapReduce** es una interfaz de programación de aplicaciones (API) de código abierto que proporciona 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, coherencia, 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.

### 2.1.4 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 (Camps, y otros, 2005, pág. 39).

Un Sistema de Gestión de Base de Datos (SGBD) es el software que permite a los usuarios procesar, describir, administrar y recuperar los datos almacenados en una base de datos; 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 Cabello, 2010, págs. 22-40).

**Niveles ANSI/X3/SPARC**

La arquitectura ANSI/SPARC, que data de 1977, define los niveles de abstracción para un sistema de administración de bases de datos (Camps, y otros, 2005, págs. 22-28):

- **Nivel interno o físico**: define cómo se almacenan los datos y los métodos de acceso.
- **Nivel lógico o conceptual**: se describe a nivel lógico 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.

**Funciones de un SGBD.**

Piñeiro (2013), nombra las funciones esenciales de un SGBD o sublenguajes, que son la función de definición o descripción, la función de manipulación y la función de control o utilización, los cuales los describe de la siguiente manera (págs. 8-10):

- **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 (DDL: *Data Definition Language*)".
- **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*)”.

**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 & Navathe, 2016, págs. 33-52):

- **Independencia física**: El nivel físico puede ser modificado independientemente del nivel conceptual. Esto significa que el usuario no puede ver todos los componentes de hardware de la base de datos, que es simplemente una estructura transparente para representar la información almacenada.
- **Independencia lógica**: El nivel conceptual debe poder modificarse sin alterar el nivel físico. En otras palabras, el administrador de la base de datos debe poder introducir mejoras sin afectar la experiencia de los usuarios.
- **Facilidad de uso**: Las personas que no estén familiarizadas con la base de datos deben poder describir su consulta sin hacer referencia a los componentes técnicos de la base de datos.
- **Acceso rápido**: El sistema debe poder responder a las consultas lo más rápido posible. Esto requiere algoritmos de búsqueda rápidos. La infraestructura informática con que se cuente también será un factor importante en rendimiento.
- **Administración centralizada**: El SGBD debe permitirle al administrador manipular los datos, agregar elementos y verificar su integridad de manera centralizada.
- **Redundancia controlada**: El SGBD debe poder evitar la redundancia de datos siempre que sea posible, tanto para minimizar los errores como para prevenir el desperdicio de memoria.

- **Verificación de integridad**: Los datos deben ser internamente coherentes y, cuando algunos elementos hacen referencia a otros, estos deben estar presentes.
- **Uso compartido de datos**: El SGBD debe permitir que múltiples usuarios accedan simultáneamente a la base de datos.
- **Seguridad de los datos**: El SGBD debe poder administrar los derechos de acceso a los datos de cada usuario.

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:

#### *2.1.4.1 Oracle Database*

Oracle Database es un sistema de gestión de base de datos privativo de tipo objeto-relacional (ORDBMS, por el acrónimo en inglés de *Object-Relational Database Management System*), multiplataforma, propio de Oracle Corporation y/o sus afiliados.

Un servidor de base de datos Oracle consiste en una base de datos y al menos una instancia de base de datos, comúnmente conocida simplemente como instancia. Debido a que una instancia y una base de datos están tan estrechamente conectadas, el término base de datos Oracle a veces se usa para referirse tanto a la instancia como a la base de datos (Ashdown, Keessling, & Kyte, 2020). Las últimas versiones de Oracle han sido certificadas para poder trabajar bajo GNU/Linux.

#### *2.1.4.2 Microsoft SQL Server*

Microsoft SQL Server es un sistema de gestión de bases de datos del modelo relacional de licencia privativa Microsoft EULA, desarrollado por la empresa Microsoft.

El lenguaje de desarrollo utilizado es Transact-SQL (TSQL) ya sea por línea de comando o mediante el Management Studio, una implementación del estándar ANSI del lenguaje SQL, utilizado para manipular y recuperar datos (DML), crear tablas y definir relaciones entre ellas (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 , 2019).

#### *2.1.4.3 PostgreSQL*

PostgreSQL es un Sistema de gestión de bases de datos relacional orientado a objetos, siendo ahora la base de datos 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. Dicha comunidad es denominada el PGDG (*PostgreSQL Global Development Group*) (PostgreSQL, 2020).

#### *2.1.4.4 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 y/o sus afiliados, 2020). Está desarrollado en su mayor parte en ANSI C y C++. Tradicionalmente se considera uno de los cuatro componentes de la pila de desarrollo LAMP y WAMP.

#### *2.1.4.5 MariaDB*

MariaDB es un sistema de gestión de bases de datos derivado de MySQL con licencia GPL (*General Public License*). Se desarrolla como software multiplataforma de código abierto y como base de datos relacional, proporciona una interfaz SQL para acceder a los datos, de hecho, 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 Foundation, 2020). 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.

## 2.2 Auditoría en informática

### 2.2.1 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 Razo, 2002, págs. 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 análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones (Muñoz Razo, 2002, págs. 88-94).

Aunque se realizan diversos tipos de auditoría, todos llevan a emitir una opinión de algún registro, sistema, operación o actividad en particular o con fines específicos.

### 2.2.2 Tipos de auditoría

Según Sandoval, H. (2012), tradicionalmente se consideran dos tipos de auditoría según el personal que la desempeña, las internas y las externas (págs. 46-47):

**Auditoría Interna**. La auditoría interna la desarrollan personas que pueden o no depender de la entidad y actúan revisando, en más de una ocasión, aspectos que interesan particularmente a la administración, aunque pueden efectuar diferentes revisiones programadas sobre todos los aspectos operativos y de registro de la empresa, con el fin de emitir un informe sobre su revisión.

**Auditoría Externa**. La auditoría externa la efectúan profesionales que no dependen de la empresa, ni económicamente ni bajo cualquier otro concepto, y a los que se conoce un juicio imparcial merecedor de la confianza de terceros. El objeto de su trabajo es la emisión de un dictamen. De igual forma para Sandoval, H. (2012), también existen otros tipos de auditorías según el objeto de análisis o área de aplicación como (págs. 15-19):

**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,** es la revisión sistemática y exhaustiva que se realiza a la actividad administrativa de una empresa, sobre su organización, las relaciones entre sus integrantes y el cumplimiento de las funciones y actividades que regulan sus operaciones.

**Auditoría Operacional,** es la revisión exhaustiva, sistemática y específica que se realiza a las actividades de una empresa, con el fin de evaluar su existencia, suficiencia, eficacia, eficiencia y el correcto desarrollo de sus operaciones, cualesquiera que éstas sean.

**Auditoría Integral,** es la revisión exhaustiva, sistemática y global que realiza un equipo multidisciplinario de profesionales a todas las actividades y operaciones de una empresa, con el propósito de evaluar, de manera integral, el correcto desarrollo de las funciones en todas sus áreas administrativas.

**Auditoría Gubernamental,** es la revisión exhaustiva, sistemática y concreta que se realiza a todas las actividades y operaciones en una entidad gubernamental, cualquiera que sea la naturaleza de las dependencias y entidades de la administración pública.

**Auditoría Informática,** es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes.

### 2.2.3 Auditoría de tecnologías de la información y comunicación (Auditoría Informática)

Según la Contraloría General del Estado (2012), define que es el examen objetivo, crítico, metodológico y selectivo de evidencia relacionada con políticas, prácticas, procesos y procedimientos en materia de tecnologías de la información y la comunicación, para expresar una opinión independiente respecto:

a) A la confidencialidad, integridad, disponibilidad y confiabilidad de la información.
b) El uso eficaz de los recursos tecnológicos.
c) A la eficacia del control interno asociado a los procesos de las Tecnologías de la Información y la Comunicación.

Abarcando este tipo de auditoría a diferentes enfoques como a las seguridades, a la información, a la infraestructura tecnológica, al software de aplicación, y a las comunicaciones y redes.

Por otra parte, Postigo, A. (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” (pág. 10).

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

- Auditoría Legal: Cumplimiento legal de las medidas de seguridad exigidas por el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.
- Auditoría de bases de datos: Controles de acceso, de actualización, de integridad y calidad de los datos.
- Auditoría de la seguridad: Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- Auditoría de la seguridad física: Referido a la ubicación de la organización, evitando ubicaciones de riesgo, y en algunos casos no revelando la situación física de esta. También está referida a las protecciones externas (arcos de seguridad, CCTV, vigilantes, etc) y protecciones del entorno.
- Auditoría de la seguridad lógica: Comprende los métodos de autenticación de los sistemas de información.
- Auditoría de las comunicaciones: Se refiere a la auditoría de los procesos de autenticación en los sistemas de comunicación.
- Auditoría de la seguridad en producción: Frente a errores, accidentes y fraudes.

### 2.2.4 Auditoría de base de datos

Según Piattini & Del Peso (págs. 387-402) 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:

- Quién accede a los datos
- Cuándo se accedió a los datos
- Desde qué tipo de dispositivo/aplicación
- Desde que ubicación en la Red
- Cuál fue la sentencia SQL ejecutada
- Cuál fue el efecto del acceso a la base de datos

La Auditoría de BD es importante porque:

- Toda la información financiera reside en bases de datos y deben existir controles relacionados con el acceso a las mismas.
- Se debe poder demostrar la integridad de la información.
- Se deben mitigar los riesgos asociados a la pérdida de datos y fuga de información.
- La información confidencial de clientes, es responsabilidad de las organizaciones.
- Los datos convertidos en información a través de bases de datos.
- Las organizaciones deben tomar medidas mucho más allá de asegurar sus datos.

Mediante la auditoría de bases de datos se evaluará:

- Definición de estructuras físicas y lógicas de las bases de datos.
- Control de carga y mantenimiento de las bases de datos.
- Integridad de los datos y protección de accesos.
- Estándares para análisis y programación en el uso de bases de datos.
- Procedimientos de respaldo y de recuperación de datos.

Planificación de la Auditoría de BD

- Identificar todas las bases de datos de la organización.
- Clasificar los niveles de riesgo de los datos en las bases de datos.
- Analizar los permisos de acceso.
- Analizar los controles existentes de acceso a las bases de datos.
- Establecer los modelos de auditoría de BD a utilizar.
- Establecer las pruebas a realizar para cada BD, aplicación y/o usuario.

**Auditoría de seguridad de bases de datos**

Para Calbimonte, D. (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. Las siguientes implementaciones de auditoría son recomendadas al nivel de BD como parte de cualquier sistema de ASBD:

1. Auditoría a nivel de esquema:
    - Actividad DDL
    - Cambios hechos a los procedimientos almacenados y desencadenadores

   - Cambios en los privilegios, usuarios y atributos de seguridad
2. Auditoría a nivel de datos:
   - Cambios en datos sensibles (actividad DML)
   - Sentencias *SELECT*
3. Cualquier cambio en los ajustes de auditoría
4. Adicionalmente cifrar de toda la BD, tablas o celdas específicas

Estas son algunas soluciones de auditoría de seguridad de base de datos nativas que pueden ayudar a cumplir estos requerimientos.

## 2.3 Regulaciones de auditoría de Base de Datos

### 2.3.1 ISO/IEC 15408 Criterios Comunes

ISO/IEC 15408 aborda la protección de los activos de la divulgación no autorizada, modificación o pérdida de uso. Las categorías de protección en relación con estos tres tipos de fallas de seguridad son llamadas comúnmente la confidencialidad, integridad y disponibilidad, respectivamente. También puede ser aplicable a los aspectos de la seguridad de IT, externo a estos tres. ISO/IEC 15408 es aplicable a los riesgos derivados de las actividades humanas (malintencionado o no) y de los riesgos derivados de actividades no-humanas. Aparte de la seguridad IT, ISO/IEC 15408 se puede aplicar en otras áreas, pero no hace ninguna demanda de aplicación en estas áreas (ISO/IEC, 2009).

### 2.3.2 ISO/IEC 17799

Se define como una guía protocolar en la implementación del sistema de administración de la seguridad de la información. En general proporciona pautas para la implementación basada en las sugerencias que deben ser consideradas por una organización para poder construir un programa comprensivo de gestión de seguridad de la información. Se orienta a preservar los principios de confidencialidad, integridad y disponibilidad.

La norma 17799 también ofrece una estructura para identificar e implementar soluciones para diferentes riesgos, donde respecto a los datos, se destaca: la clasificación y control de activos, control de acceso, desarrollo y mantenimiento del sistema. En el año 2007 la norma ISO/IEC 17799 pasa a formar parte de la familia de normas ISO/IEC 27000, y es renombrada como la norma ISO/IEC 27002, pero las guías establecidas son un referente base a considerarse como buenas prácticas.

### 2.3.3 Conjunto ISO/IEC 27000

ISO/IEC 27000 es un conjunto de estándares desarrollados o en fase de desarrollo por ISO (*International Organization for Standardization*, en español Organización Internacional para la Estandarización) e IEC (*International Electrotechnical Commission*, en español Comisión Electrotécnica Internacional), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Las ISO relacionadas a la auditoria de BD son:

**ISO/IEC 27001**: 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. El requisito de control de registros de implementar los controles necesarios para la identificación, almacenaje, protección y disposición de registros; además de establecer los procedimientos para el manejo y almacenaje de la información para proteger la misma de una divulgación no autorizada o un mal uso; proporcionan los cimientos para considerarse en un esquema de auditoría de seguridad de bases de datos.

**ISO/IEC 27002**: 2013, es el nuevo nombre de la ISO/IEC 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización. Los lineamientos respecto al inventario e importancia de la información para garantizar su persistencia y análisis, aportan directrices importantes para orientar esfuerzos en la información contenida en las bases de datos con controles de auditoría y seguridad.

**ISO/IEC 27004**: 2016, proporciona pautas destinadas a ayudar a las organizaciones a evaluar el desempeño de la seguridad de la información y la eficacia de un sistema de gestión de seguridad de la información para cumplir con los requisitos de ISO/IEC 27001: 2013, es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Se destaca la importancia del seguimiento, coadyuvando a que los controles respecto a los datos, sean los más eficientes, ya que la información es un activo valioso en las organizaciones.

**ISO/IEC 27005**: 2018, respalda los conceptos generales especificados en ISO/IEC 27001 y está diseñado para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos, siendo aplicable a todo tipo de organizaciones que pretenden gestionar riesgos; donde mecanismos de auditoría en BD, pueden proporcionar un valor añadido para mitigar riesgos de modificaciones no controladas en los datos.

### 2.3.4 ISACA

La Asociación de Auditoría y Control de los Sistemas de Información ISACA (*Information Systems Audit and Control Association*), con 145.000 miembros en 188 países, que abarcan varios roles en aseguramiento, gobernanza, riesgo y seguridad de la información, es un líder global proveedor de conocimiento, certificaciones, comunidad, promoción y educación sobre aseguramiento y seguridad de sistemas de información (SSII), gobierno empresarial y gestión de TI y riesgo relacionado con TI y cumplimiento. Desde 1969, ISACA, celebra conferencias internacionales, publica el ISACA *Journal* y desarrolla estándares internacionales de control y auditoría de SSII.

También avanza y avala habilidades y conocimientos en TI mediante los globalmente reconocidos certificados (CISA) *Certified Information Systems Auditor*, (CISM) *Certified Information Security Manager*, (CGEIT) *Certified in the Governance of Enterprise IT* y (CRISCTM) *Certified in Risk and Information Systems Control TM*. ISACA actualiza continuamente el COBIT, el cual ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en aseguramiento, seguridad, riesgo y control y proporcionar valor al negocio (ISACA, 2012, pág. 2).

### 2.3.5 COBIT

COBIT (*Control Objetives for Information Systems and related Tecnology*) es un marco de negocio para el gobierno y la gestión de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. COBIT permite el desarrollo de políticas y buenas prácticas para el control de las tecnologías en toda la organización, enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los

objetivos del negocio. COBIT 5 es producto de la mejora estratégica de ISACA impulsando la próxima generación de guías sobre el gobierno y la administración de la información y los activos tecnológicos de las Organizaciones (ISACA, 2012, págs. 9-16).

### 2.3.6 MAGERIT

MAGERIT, la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. Actualmente está en su versión 3. Magerit ofrece una aplicación para el análisis y gestión de riesgos de un Sistema de la Información. Específicamente, en el libro II de Catálogo de Elementos, en el punto 6.2, proporciona lineamientos para la protección de datos/información como: protección de la información, copias de seguridad de los datos (*backup*), aseguramiento de la integridad, cifrado de la información, uso de firmas electrónicas, y, uso de servicios de fechado electrónico (*time stamping*); siendo aportes de lineamientos generales sobre los datos e información (Ministerio de Hacienda y Administraciones Públicas, 2012, pág. 54).

### 2.3.7 NIA

Las Normas Internacionales de Auditoría (NIA) emitidas por la Federación Internacional de Contadores (IFAC), son un conjunto único de estándares que se aplican a las auditorías para todas las organizaciones, indispensables para cualquier auditor. Donde respecto a las BD, en el volumen 1 de Conceptos Principales, dentro de los controles internos, realza la importancia de los controles automatizados, buscando mejorar la capacidad de lograr la segregación eficaz de funciones al implementar restricciones de acceso al sistema, adecuadas en aplicaciones, BD y sistemas operativos; buscando en los controles generales de TI, la seguridad sobre datos, infraestructura de TI y operaciones diarias con SGBD y programas de utilidades. Además, de aspectos de seguridad de contraseñas, cuentas y roles de usuarios, cifrado, historial de datos y control de calidad (IFAC, 2011).

### 2.3.8 Delitos Informáticos

Huerta y Líbano citados por Acurio Del Pino (2016), definen 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" (pág. 14). 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" (págs. 10-14).

### 2.3.9 Ética Informática

Según Moor (2007), la ética aplicada a la informática, así como de códigos de ética profesionales permiten un adecuado uso de la Informática, donde la Ética Informática es una rama de la ética que se refiere a la relación entre la creación, organización, difusión y uso de la información y los códigos ético morales que rigen la conducta humana, siendo un conjunto de normas morales que rigen el uso de las tecnologías. Generalmente, la ética en la informática se relaciona con delitos informáticos, responsabilidad por fallas informáticas, privacidad, protección de datos, los registros y el software (págs. 266-275).

Entre algunos documentos sobre códigos de ética que sirvan como guía de conducta básica a los profesionales informáticos y usuarios, se pueden mencionar: código ACM de ética y conducta profesional, código ACS de ética y conducta profesional, los diez mandamientos de la ética computacional, código IEEE de ética, código IEEE de conducta.

## 2.4 Prácticas de auditoría de seguridad de Base de Datos

### 2.4.1 Añadir campos a las tablas

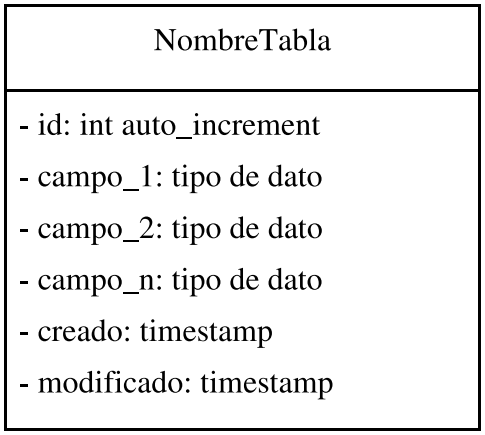
Domínguez (2016) en su artículo "Cómo auditar cambios en una tabla MySQL o MariaDB", da una propuesta práctica para auditar una tabla en particular a partir de tres campos básicos, a los que adicionalmente se puede agregar dos campos, usuario e ip, para lograr una auditoría completa. Las modificaciones 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 trabaja con tres campos básicos en cada tabla a auditar. El primer campo, id, de tipo entero largo, auto incremental y llave primaria. El segundo campo, creado y tercer campo, modificado, son de tipo fecha y hora, valor por defecto fecha/hora actual.

Con la información obtenida se podrán generar de forma sencilla reportes, tales como:

- Qué tablas han sufrido cambios recientemente.
- Qué tablas no sufrieron cambios el pasado año.
- Qué tablas no han sufrido cambios.
- Mostrar los cambios a las tablas por un periodo específico.
- Mostrar tablas más activas en un determinado periodo.

Para cualquier tabla, el diseño sería semejante a:

Figura 2.7: Diseño añadir campos a las tablas.




Fuente: Domínguez (2016)

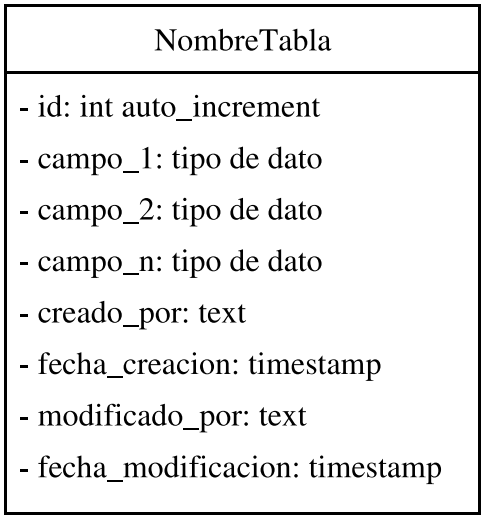
Por otra parte, Joshi (2017), en su artículo "*Spring Data JPA Auditing: Automatically Saving the Good Stuff*", presenta una idea similar, basada también en la adición de columnas, en la que trata el tema de seguir cada operación de inserción, actualización y eliminación y luego almacenarla, esto ha 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 y el código fuente está disponible en su repositorio de GitHub.

Para cualquier entidad, el diseño sería semejante a:

Figura 2.8: Diseño añadir campos a las tablas JPA.



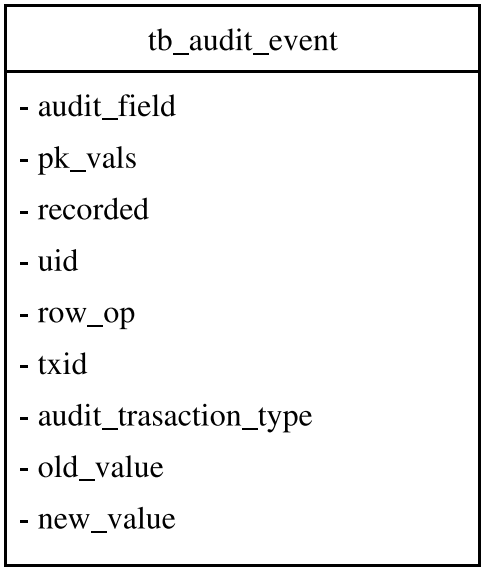

Fuente: Joshi (2017)

### 2.4.2 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 bases de datos referentes al DML y los guarda en una sola tabla, en un esquema independiente distinto, pero dentro de la misma base de datos.

La tabla consolidada de auditoría básicamente presenta el siguiente diseño:

Figura 2.9: Consolidado histórico de todas las tablas.




Fuente: Hassan (2016)

Como se puede ver claramente en la figura anterior, las columnas para almacenar los datos registrados: *audit_filed* tiene el ID de la columna en Cyan Audit, *pk_vals* tiene la clave primaria del registro, *recorded* representa la marca de tiempo en la que se realizó la operación, *uid* contiene el ID de usuario de Postgres, *row_op* mantiene el tipo de operación como actualizar, eliminar o insertar, *txid* mantener el ID de transacción registrado - útil para revertir la transacción, *audit_transaction_type* - *old_value* es el valor antiguo del registro y *new_value* es un nuevo valor del registro.

### 2.4.3 Logs de Transacciones o Sesión

Riggs & Menon-Sen (2017), en la extensión de auditoría de PostgreSQL "pgAudit" de código abierto, proporciona un registro detallado de auditoría de sesión y/u objeto a través de la función de registro estándar de PostgreSQL. El objetivo de pgAudit es dar a los usuarios de PostgreSQL la capacidad de producir registros de auditoría que a menudo se requieren para cumplir con las certificaciones gubernamentales, financieras o ISO.

Es posible capturar el registro de auditoría de sesión según: lectura (*SELECT* y *COPY*), escritura (*INSERT, UPDATE, DELETE* y *TRUNCATE*), funciones, roles (*GRANT*, *REVOKE, CREATE/ALTER/DROP ROLE*), acciones DDL, misc (*DISCARD, FETCH, CHECKPOINT, VACUUM, SET*). La información escuchada según configuración de entradas de auditoría, se escriben en la función de registro estándar con columnas separadas por comas como un único archivo centralizado, siendo accesible a través de la extensión de PostgreSQL pgAudit.

De igual manera, otras soluciones integradas como SQL Server Audit para SQL Server (Macauley & Cai, 2020) 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.

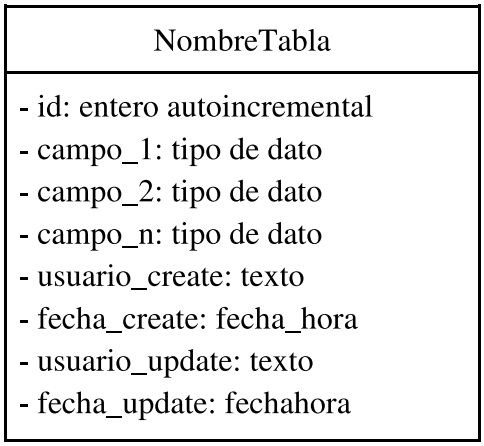
### 2.4.4 Tablas espejo

Barren (2016), propone una metodología basada en crear campos a una tabla, la cual ya fue descrita en el apartado 2.4.1 de este documento, por lo que, buscando proporcionar más información acerca del motor de BD que se usa, se podría tener como alternativa implementar a nivel de BD un *trigger* cuando se producen estos eventos del CRUD.

Los *triggers* se disparan según se los configure antes de un evento sobre una tabla; esto sería lo ideal para no preocuparse de ello desde el sistema. Lo ideal de la tabla que almacena el histórico como una auditoría sería que fuera idéntica a la tabla original, y ambas tablas deberían contar como mínimo con los campos: *user_create, date_create y user_update, date_update* para hacerle un seguimiento al registro.

Con esta propuesta, a cada tabla se añaden campos de control adicionales, estos campos pueden ser fecha de creación y modificación, y el dato de quién ha creado y modificado el registro. Paralelamente se hace una copia de la tabla original, como si fuera una tabla espejo, con un identificador único, en esta tabla se irán almacenando continuamente los cambios en el DML. Por ejemplo, la tabla original sería semejante a:

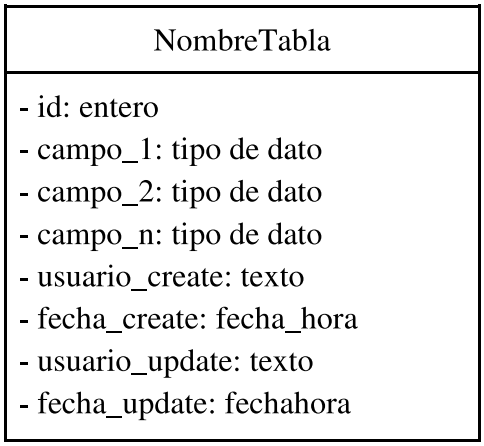
Figura 2.10: Tablas espejo: tabla original.




Fuente: Barren (2016)

Y la tabla espejo sería semejante a:

Figura 2.11: Tablas espejo: tabla espejo.




Fuente: Barren (2016)

## 2.5 Software Libre

### 2.5.1 Definición de Software Libre

La Fundación del Software Libre FSF (Free Software Foundation), define software libre, como el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, se debe pensar en "libre" como en "libre expresión", no como en "barra libre". En inglés, a veces en lugar de "*free software*" se dice "software libre", empleando ese adjetivo francés o español, derivado de "libertad", para mostrar que no se quiere decir que el software es gratuito.

Se promueven estas libertades porque todos merecen tenerlas. Con estas libertades, los usuarios (tanto individualmente como en forma colectiva) controlan el programa y lo que este hace. Cuando los usuarios no controlan el programa, se dice que dicho programa "no es libre", o que es "privativo". Un programa que no es libre controla a los usuarios, y el programador controla el programa, con lo cual el programa resulta ser un instrumento de poder injusto e intrusivo.

### 2.5.2 Las cuatro libertades del Software Libre

Para la FSF, un programa es software libre si los usuarios tienen las cuatro libertades esenciales:

- La libertad de ejecutar el programa como se desea, con cualquier propósito (libertad 0).
- La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.
- La libertad de redistribuir copias para ayudar a su prójimo (libertad 2).
- La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3). Esto le permite ofrecer a la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

Un programa es software libre si otorga a los usuarios todas estas libertades de manera adecuada. De lo contrario no es libre.

Existen diversos esquemas de distribución que no son libres, y si bien se puede distinguirlos en base a cuánto les falta para llegar a ser libres, se los considera contrarios a la ética a todos por igual. En cualquier circunstancia, estas libertades deben aplicarse a todo código que se piense hacer que otros utilicen.

"Software libre" no significa que "no es comercial". Un programa libre debe estar disponible para el uso comercial, la programación comercial y la distribución comercial. La programación comercial de software libre ya no es inusual; el software libre comercial es muy importante. Puede haber pagado dinero para obtener copias de software libre, o puede haber obtenido copias sin costo. Pero sin tener en cuenta cómo obtuvo sus copias, siempre tiene la libertad de copiar y modificar el software, incluso de vender copias.

### 2.5.3 El manifiesto de GNU

El manifiesto GNU escrito por Richard Stallman (1985), declara públicamente los principios e intenciones respecto al proyecto GNU como parte del Movimiento del Software Libre, que promueve la libertad de los usuarios de software. GNU quiere decir que "GNU No es Unix". En el manifiesto se solicita apoyo a cualquier persona para colaborar en el sistema operativo GNU, mismo que podrá entregarse libremente a cualquier persona; dando la posibilidad, sin restricción de modificar y redistribuir. Por sobre todo, no autorizando las modificaciones privativas, buscando asegurarse que todas las versiones de GNU permanezcan libres.

### 2.5.4 Código Abierto

La esencia de código abierto se especifica en las cuatro libertades descritas en la *General Public License* (GPL) de la Fundación de Software Libre, es decir, que cualquier usuario pueda usar, estudiar, redistribuir y mejorar el código fuente de un software. La gente debe poder mejorarlo, adaptarlo y rectificarlo (Open Source Initiative, 2007).

### 2.5.5 Estándar Abierto

Según la Open Source Initiative (2007), un estándar abierto se refiere a que se cumpla mínimamente con los siguientes requisitos:

- Sin secretos intencionales: el estándar NO DEBE retener ningún detalle necesario para una implementación interoperable. Como los defectos son inevitables, la norma DEBE definir un proceso para corregir fallas identificadas durante las

pruebas de implementación e interoperabilidad e incorporar dichos cambios en una versión revisada o una versión sustituta de la norma que se publicará en términos que no violen los Requerimientos de Estándar Abierto (OSR).

- Disponibilidad: el estándar DEBE estar disponible libre y públicamente (por ejemplo, desde un sitio web estable) bajo condiciones libres de regalías a un costo razonable y no discriminatorio.
- Patentes: todas las patentes esenciales para implementación de la norma DEBEN:
  - obtener licencia bajo términos libres de regalías para uso no restringido, o
  - estar cubierto por una promesa de no afirmación cuando es practicado por software de código abierto.
- Sin acuerdos: NO DEBE haber ningún requisito para la ejecución de un acuerdo de licencia, de confidencialidad, de concesión, *click-through* o cualquier otra forma de papeleo para desplegar conforme implementaciones del estándar.
- Sin dependencias incompatibles con los OSR: la implementación de la norma NO DEBE requerir ninguna otra tecnología que no cumpla con estos criterios.

### 2.5.6 Licencias de Software Libre

Megías, y otros (2004), definen "una licencia de uso de software es un instrumento legal que autoriza a los usuarios del software a realizar ciertos actos que la ley normalmente reserva de manera exclusiva al titular de los derechos de autor o de patente. Asimismo, permite al autor reservarse los derechos que no se ceden e imponer y otorgar al usuario otras obligaciones y derechos no necesariamente vinculados con el derecho de autor (confidencialidad, etc.). Establece, por lo tanto, lo que el usuario puede y no puede hacer con el software" (pág. 33).

Una clasificación general sobre este tipo de licencias son las licencias de software propietario o privativo que son bastantes restrictivas, y las licencias de software libre que permiten asegurar a los usuarios las libertades de uso, modificación y redistribución.

Mediante las licencias de software libre, el titular del software no pretende proteger sus derechos exclusivos de explotación. Al contrario, mediante la licencia de software libre el titular permite expresamente a los usuarios usar, modificar, así como redistribuir el software, con o sin modificaciones. En este sentido, para que una licencia de software sea "libre", debe garantizar, al menos, las cuatro libertades básicas (págs. 34-36).

### 2.5.7 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 contextos las convenciones tienen el carácter de ley no escrita (por ejemplo, que ropa es adecuada para un hombre y cual para una mujer) (Por Igual Más, 2014).

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.

# 3 Análisis de Prácticas Actuales en Auditoría de Base de Datos

De acuerdo a lo descrito en una sección anterior, en el punto 2.4 referente a las prácticas de auditoría de seguridad de base de datos, se realiza un análisis de las ventajas y desventajas de las mismas, además en base a ese análisis, se presentan características deseadas que debería contemplar una base de datos con controles de seguridad y auditoría.

## 3.1 Ventajas y desventajas de las prácticas de auditoría de base de datos

### 3.1.1 Añadir campos a las tablas

Es una propuesta práctica para auditar una tabla en particular a partir de tres campos básicos (id, creado, modificado), a los que opcionalmente se puede agregar dos campos (usuario e ip). También, existe una variación similar, que se compone por los campos: creado_por, fecha_creación, modificado_por y fecha_modificacion. En ambas alternativas, se añaden los campos a cada tabla en que se desea llevar el control de registros, realizando la actualización de los campos de auditoría mediante la utilización de desencadenadores.

**Ventajas.**

- La ventaja principal de este tipo de implementación es que se tienen todos los campos de auditoría directamente en cada registro de las tablas, evitando consultar otros lugares para conocer quién y/o cuándo se creó y/o modificó un registro.
- Además de que su implementación resulta bastante sencilla, basta con añadir las columnas de creado_por, fecha_creacion, modificado_por y fecha_modificacion, a cada tabla. Posteriormente, trabajar en el llenado de estos nuevos campos a través de desencadenadores, aplicaciones en segundo plano o enviando los datos directamente desde la aplicación cliente que use la base de datos correspondiente a la tabla.
- El aumento del tamaño de los archivos de la base de datos será muy pequeño, ya que sólo se añaden cuatro nuevos campos de tipo de dato texto y fecha. Al ser muy reducido el crecimiento adicional del tamaño de la base de datos, la velocidad de obtención de respaldos y copia de estos a otra ubicación no será muy diferente a la habitual, pues la transferencia de archivos por el tamaño extra es despreciable.

**Desventajas.**

- Como la auditoría busca tener la mayor cantidad de pistas, con este tipo de implementación, no se cuenta con el historial de cada registro, ya que sólo se tiene disponible información de creación y de la última modificación, y no así de todas las veces que una determinada fila hubiera sufrido cambios. Incluso los cambios en cualquier registro se pierden, mostrando solamente el dato actual y no la evolución del mismo.
- Luego de ejecutar una acción de manipulación de datos, no es sencillo deshacer los cambios o reconstruir los registros, esto se lograría luego de un arduo trabajo con los archivos *Logs* de la base de datos o reproduciendo la información desde otras fuentes como *backups* o documentos impresos si existieran.
- El crecimiento en la estructura de la base de datos es horizontal, haciéndolo válido sólo para nuevos sistemas, para evitar tener datos nulos. Cabe resaltar que, al adicionar más campos a las tablas, el tiempo de consulta aumentará cuando se desee obtener los datos de todos los campos.
- Al tenerse datos confidenciales directamente en cada registro, los datos, incluyendo los de auditoría son vulnerables a modificación, pues quien tenga altos privilegios de acceso a la base de datos, podrá eliminar cualquier pista de auditoría sin dejar rastro alguno. No existiendo integridad en los datos, siendo un potencial hueco de seguridad para manipulación informática.
- También cuenta con la desventaja de que un usuario con altos privilegios de acceso a la base de datos, proceda a eliminar datos directamente en cada registro, incluyendo los datos de auditoría son vulnerables a modificación bajo esta situación, lo que provocaría que datos probablemente importantes y/o confidenciales desaparezcan sin dejar rastro alguno de esta acción.

### 3.1.2 Consolidado histórico de todas las tablas

Guarda en una sola tabla, en un esquema independiente y distinto dentro de la misma base de datos, consolidando los campos *audit_field, pk_vals, recorded, uid, row_op, txid, audit_trasaction_type, old_value, new_value*.

**Ventajas.**

- Este tipo de implementación está de moda actualmente, ya que por ejemplo PostgreSQL, la base de datos libre más grande del mundo, usa esta convención en su módulo de auditoría PgAudit recientemente disponible en GitHub. De igual modo, CyanAudit, otra extensión de auditoría para PostgreSQL, también usa este tipo de modelo.
- Utilizando esta alternativa, se tiene una sola tabla que almacena en forma de bitácora todo el historial de cambios de cada registro de todas las tablas, teniendo un consolidado como la única opción para consultar los registros de auditoría, no habiendo la necesidad de buscar en diferentes lugares por cada tabla, basta con realizar consultas con filtros a los registros para obtener la información deseada.
- Al registrar cada acción DML por cada campo sin importar la cantidad de columnas que tenga una tabla, no se tiene dependencia de la estructura de la base de datos, siendo transparente el adicionar o quitar columnas a las tablas, pues no es necesario realizar ninguna adecuación en el módulo de auditoría para su normal funcionamiento.
- A diferencia de la anterior alternativa, ahora sí se cuenta con un historial de los cambios por cada registro acompañado de campos de auditoría como usuario, fecha, antiguo valor, nuevo valor, tipo de transacción. Además, el hecho de mantener almacenada la evolución de un registro, hace posible reconstruir la información a una determinada fecha. Por último, por su peculiaridad de registrar cada cambio, la integridad se incrementa.

**Desventajas.**

- Un inconveniente notorio que no se puede obviar, es el crecimiento exponencial de la base de datos, debido a que se registra cada cambio por cada registro, es decir, si una tabla tiene por ejemplo 15 columnas y 14 de ellas son modificadas, se insertarán 14 nuevas filas en la tabla de auditoría, o en el caso de una inserción o eliminación se añadirán 15 nuevas filas en la tabla de auditoría.
- También debido a que la tabla de auditoría se encuentra en la misma BD o en el caso de las extensiones de PostgreSQL, se encuentran en un esquema diferente exclusivo de auditoría, pero sigue estando ubicado en la misma base de datos.

Además, la tabla de auditoría será la de mayor tamaño, esto representa el uso adicional de espacio en disco, no siendo posible segmentar física o lógicamente. En consecuencia, al obtener un *backup* de toda la BD, éste será exponencialmente más grande en cuanto a su tamaño en disco, a pesar de que es posible obtener *backups* por esquema en algunos motores de base de datos como PostgreSQL.

- Por otra parte, los campos, antiguo valor y nuevo valor de tipo de dato texto, deben ser de gran tamaño para soportar los diferentes valores posibles, pues registran el cambio de cualquier columna en las tablas. También se debe tomar en cuenta que al utilizar el tipo de dato texto, se pierden las características del tipo de dato original de cada campo, lo que dificulta reconstruir la estructura de la BD.
- Por último, al almacenar en una única tabla, una tupla por cada alteración en un campo de cualquier tabla, es más difícil el procesamiento interno en caso de reconstrucción de la información (*rollback*), por motivos de la ejecución descontrolada de la sentencia SQL *delete from <table>* sin condición, o en caso de volver los datos a una fecha determinada. Incluso, realizar consultas de datos a la tabla que almacena el historial resulta complicado y moroso, hasta la visualización de los datos es ampulosa y extensa para manejarla.

### 3.1.3 Tablas espejo

Centrado en el uso de desencadenadores, se añaden campos de control de auditoría a cada tabla original y además se realiza una copia idéntica de cada tabla.

**Ventajas.**

- Lo más trascendente de este tipo de implementación, es que la información de auditoría se encuentra más organizada y segmentada, siendo más sencillo realizar consultas al historial de una tupla en la tabla de auditoría correspondiente, pues la estructura de cada tabla en cuanto a nombres de campos y tipo de datos, son similares; siendo la visualización de datos semejante, ya que, al crecer verticalmente la tupla, resulta cómodo analizar el conjunto de cambios.
- Asimismo, al contar con tablas espejos con estructuras semejantes a las originales, pues cada tabla de auditoría posee campos adicionales de control, resulta sencilla la reconstrucción de la estructura de las tablas y también de los datos. La característica que posee de reconstrucción de información, es importante en el

caso de la ejecución descontrolada de la sentencia SQL *delete from <table>* sin condición, o en caso de volver los datos a una fecha determinada.

- Se usa la adición de campos en las tablas como en la primera alternativa presentada, permitiendo visualizar algunos campos de auditoría directamente en cada registro de las tablas y en caso de que se deseen conocer mayores detalles se recurre a su tabla de auditoría respectiva.

**Desventajas.**

- Al igual que la anterior, según la frecuencia de modificaciones de los datos el crecimiento de la base de datos puede ser bastante considerable, desde unos cientos de megabytes hasta unos miles de gigabytes. El crecimiento acelerado del tamaño de la base de datos, se debe a que se inserta toda una nueva fila en la tabla de auditoría por cada acción DML, es decir, si una tabla tiene por ejemplo 15 columnas y sólo 2 de ellas son modificadas, se insertará una nueva fila con todas las columnas en la tabla de auditoría, no importando si una o todas son modificadas, el resultado será almacenar toda la fila sin discriminación, aunque algunas columnas no hayan sufrido ningún cambio.
- También el crecimiento se debe a que la tabla de auditoría se encuentra en la misma base de datos, siendo esta tabla la de mayor tamaño; esto representa el uso adicional de espacio en disco, no siendo posible segmentar física o lógicamente. En consecuencia, al obtener un *backup* de toda la base de datos, éste será mínimamente un 100% más grande que los datos no auditados en su estado actual.

## 3.2 Identificación de Indicadores de Evaluación para Bases de Datos con Controles de Auditoría y Seguridad

Los siguientes indicadores de evaluación para BD relaciones, están orientados en priorizar al máximo posible una estructura que considere controles de auditoría, alineados a los principios de la seguridad informática y normas internacionales.

**Campos de Auditoría.-** Son datos o columnas adicionales que brindan mayor información sobre las modificaciones de un determinado registro o fila en una tabla, los cuales pueden ser utilizados con fines de auditoría; los campos de auditoría más usuales pueden referirse al usuario y a la fecha y hora, respecto a la creación del registro y/o última modificación del mismo.

Se pueden optar por muchos más campos de auditoría según se considere necesario o según lo permita el motor de base de datos, columnas como el rol, conexión, dirección IP, dirección MAC, tipo de acción SQL, pueden ser algunas opciones a adicionarse.

**Cambio en la estructura de las tablas originales.-** Se refiere a la característica que tome en cuenta un cambio en la estructura DDL de las tablas iniciales de la BD, es decir, aquellas columnas que sean recomendadas adicionar a cada tabla con fines de auditoría.

Generalmente, el tener campos adicionales de auditoría directamente en cada registro, facilita la consulta y procesamiento de los mismos, pero afecta al diseño original de las tablas, lo que probablemente obligará a que se realicen adecuaciones en el desarrollo de las aplicaciones clientes o servicios web.

El no modificar la estructura original de las tablas puede ayudar a implementar controles de auditoría en las BD de forma más rápida, pero a pesar de ello, puede ser favorable contar con datos de auditoría básicos directamente en cada registro.

**Estructura de Auditoría.-** Se enfoca al conjunto de reglas o de cambios necesarios para implementar controles de auditoría en los datos, según se explicó conceptualmente en el apartado 2.4 de prácticas de auditoría de seguridad de BD y en el punto anterior 3.1 donde se analizaron ventajas y desventajas de los mismos, de acuerdo a los 4 enfoques utilizados actualmente, que son: añadir campos a una tabla, consolidado histórico de todas las tablas, *logs* de transacciones o sesión, y tablas espejo.

Al respecto, hay implementaciones disponibles de software bajo licencia privativa y otros de código abierto; de algunos la forma de control de auditoría es una caja negra y otros utilizan alternativas dependientes de una tecnología no estandarizada.

**Posibilidad de reconstruir la información.-** Hace énfasis a la capacidad de restaurar registros iniciales que se hayan modificado o eliminado, representando una de las características más importantes para una auditoría de BD. Considera la posibilidad de apuntar a registros de un momento específico en la recuperación de información.

Este indicador resulta muy útil en caso de que un administrador de BD ejecute una actualización o eliminación de registros sin la condición correspondiente, con una equivocada, o incluso si ejecuta una acción no autorizada; provocando una modificación masiva en los datos, en estas situaciones será necesario reconstruir la información.

**Identificación del tipo de acción DML.-** Este indicador busca llevar un registro del tipo de acción SQL que se utilice para realizar una alteración en los datos, identificando si corresponde a nuevo registro (*INSERT*), una actualización (*UPDATE*) o eliminación física (*DELETE*), consiguiendo mayor especificidad de detalles según las acciones DML.

Esta cualidad, se complementa con otros indicadores para realizar estudios de auditoría que involucran reconstrucción de información, historial de cambios e integridad de datos.

***Backups* de datos de la BD y de la auditoría.** Está enfocado en las opciones disponibles para la obtención de copias de seguridad de la BD con fuentes primarias, así como en la captura de datos de auditoría por separado; encontrándose relacionado con otras características como la localización de almacenamiento y el tamaño del mismo, desde una perspectiva de separación del negocio, de los datos y de la auditoría, apuntando a optimizar el rendimiento y robustecer la seguridad.

**Restricción de acceso a la auditoría.** La seguridad de los datos es sin duda un factor importante a considerarse para mitigar riesgos en la información, por lo que este indicador está orientado a contar con niveles de acceso a los registros de auditoría; al ser datos sensibles, una modificación en los mismos puede afectar la integridad de datos si no cuenta con la garantía de seguimiento de modificaciones. Aún cuando la auditoría se encuentre en una ubicación segura y que la misma cuente con redundancia, es conveniente asegurar la confidencialidad de la información implementando restricciones de acceso a los datos primarios y de auditoría.

**Tipo de consulta a la auditoría.** Se refiere a cómo se podrá realizar consultas a los datos de auditoría almacenados, si los mismos están juntamente con los datos primarios, si existe alguna limitación de acceso por los usuarios autorizados o si están cifrados, si el formato en que se encuentren resguardados necesita de conversiones adicionales, la complejidad y el tiempo de elaboración y ejecución de las consultas; son aspectos valiosos a considerar.

**Velocidad de consultas en la BD.** Alude a las condiciones en que se encontrará la base de datos luego de implementar controles de auditoría y seguridad, considerando las repercusiones que tendrán estas adecuaciones en cuanto al tiempo de ejecución de consultas, sobre todo en las peticiones complejas, analizando si el nuevo rendimiento obtenido es aceptable dentro de los parámetros habituales.

**Forma de captura de datos de auditoría.** Es el método, forma, estrategia o política que se implementa para capturar y registrar el seguimiento de cambios, que vaya en dirección con otros indicadores con niveles de seguridad; siendo algunas de estas formas a través del uso desencadenadores en cada tabla configurable por campos, o a través de la lectura del monitoreo de *logs* de transacciones obtenidas con funciones nativas del motor de BD o el desarrollo de servicios personalizados para capturar las modificaciones realizadas.

**Historial de cambios.** Sin duda, contar con el seguimiento de cambios en los datos, es uno de los indicadores más valiosos, y será un punto a favor para brindar mejores condiciones cuando se realicen auditorías; sirviendo como pistas para investigar anomalías, rastrear irregularidades, reportar estadísticas de cambios frecuentes, o simplemente para demostrar un normal funcionamiento en las operaciones de la BD. Por supuesto, para tener la confiabilidad en el historial de cambios, deben estar implementados mecanismos de seguridad que contemplen la integridad de los datos.

**Ubicación de almacenamiento.** Se orienta en separar los datos del modelo de negocio con los datos de seguimiento de auditoría, con el objetivo de securizar la información, dividir el tamaño de almacenamiento y mejorar la velocidad de las consultas. Asimismo, abarca el análisis respecto a si la auditoría se encuentra en un sólo archivo o en un conjunto de archivos, el tipo de formato de archivo, si están ubicados los datos y la auditoría en el mismo directorio o en la misma unidad de disco.

**Tamaño de espacio total en disco.** Contempla el aumento en disco que representaría incorporar controles de auditoría y seguridad, dependiendo de la forma de captura de datos en cuanto a la cantidad de filas y columnas monitoreadas. Esta característica es importante para determinar la cantidad de datos auditables a registrarse, y con esto obtener una aproximación del crecimiento de la BD, permitiendo calcular las necesidades y gestionar la adquisición de almacenamiento a corto, mediano y largo plazo.

**Integridad de datos.** Se enfoca en mantener la consistencia, precisión y confiabilidad de los datos durante su ciclo de vida, tomando medidas que garanticen que accesos no autorizados no puedan alterar los datos o quienes tengan algún nivel de privilegios para modificaciones solo les sea permitido realizar cambios en el marco de sus competencias, además de registrar el seguimiento de cambios en medios seguros con una adecuada redundancia en la información.

Tabla 3.1: Modelo Indicador - Ventaja y Desventaja.

| **Modelo Indicador - Ventaja y Desventaja** | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | ***Logs* de Transacciones o Sesión** | **Tablas espejo** |
| 1 | Campos de auditoría | **Ventaja.** Disponibilidad de campos de auditoría en cada tabla. **Desventaja.** No se almacena el registro de todas las actualizaciones. | **Ventaja.** Disponibilidad de campos de auditoría en un lugar centralizado. **Desventaja.** Toda la auditoría de las tablas se encuentra centralizada y mezclada. | **Ventaja.** Los datos de auditoría están disponibles en un log centralizado. **Desventaja.** Datos de auditoría mezclados, la terminación de los campos es dependiente de la tecnología utilizada. | **Ventaja.** Los datos pueden estar disponibles directamente en cada registro y en cada tabla espejo. **Desventaja.** Datos sin cambios se registran de forma repetida. |
| 2 | Cambio en la estructura de las tablas originales | **Ventaja.** Disponibilidad de los datos directamente en cada tupla. **Desventaja.** Afecta a la estructura de la BD, puede ser necesario recompilar la aplicación cliente. | **Ventaja.** No se agregan columnas a las tablas originales, no modificando la estructura. **Desventaja.** No se tiene información de auditoría en cada registro, se debe recurrir a la tabla consolidada. | **Ventaja.** Las tablas existentes no sufren cambios en la estructura, siendo transparente su implementación. **Desventaja.** No ofrece información preliminar básica de auditoría en cada registro de la BD. | **Ventaja.** En cada registro de las tablas originales se cuenta con información inicial del usuario y fecha. **Desventaja.** Se afecta la estructura de la BD original, siendo necesario realizar adecuaciones en el desarrollo. |

| Modelo Indicador - Ventaja y Desventaja (Continuación) | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | **Logs de Transacciones o Sesión** | **Tablas espejo** |
| 3 | Estructura de auditoría | **Ventaja.** Ofrece una implementación sencilla directamente en cada tabla.<br><br>**Desventaja.** Afecta a la estructura original, no mantiene logs de cambios, permite acceso no autorizado. | **Ventaja.** Al utilizar una sola tabla separada, no afecta la estructura original.<br><br>**Desventaja.** Al existir una sola tabla centralizada de gran tamaño, es necesario especificar la condición en las consultas; repite datos de auditoría, permite acceso no autorizado. | **Ventaja.** No afecta la estructura original, separa la auditoría con cifrado incluido, manejo de sesiones ayudan a no afectar en gran medida a la BD.<br><br>**Desventaja.** Esquemas independientes no estandarizados específicos para cada motor de BD o tecnología. | **Ventaja.** Fácil identificación de cambios en datos al mantener una estructura similar en las tablas espejo.<br><br>**Desventaja.** Al replicar todas las columnas, el crecimiento de la BD es acelerado, repite datos no modificados, permite acceso no autorizado. |
| 4 | Posibilidad de reconstruir la información | **Ventaja.** No aplica.<br><br>**Desventaja.** Sólo se cuenta con el registro de la última modificación, no se pueden consultar datos modificados con anterioridad. | **Ventaja.** Existe la alternativa de recuperar datos modificados o eliminados en un momento específico.<br>**Desventaja.** Se requiere bastante esfuerzo en programar scripts de reconstrucción debido a la estructura. | **Ventaja.** Con los logs capturados, se cuenta con lo necesario para intentar alternativas de reconstruir información.<br>**Desventaja.** Alta curva de aprendizaje para encontrar alternativas de solución para restaurar información. | **Ventaja.** Resulta sencillo recuperar datos alterados con un simple *insert select*, ante acciones no autorizadas o sin la condición correspondiente.<br>**Desventaja.** Se requiere bastante espacio de almacenamiento debido a la forma de captura de datos utilizada. |
| | | | | | |

| Modelo Indicador - Ventaja y Desventaja (Continuación) | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | **Logs de Transacciones o Sesión** | **Tablas espejo** |
| 5 | Identificación del tipo de acción DML | **Ventaja.** No aplica.<br><br>**Desventaja.** Sólo se cuenta con el usuario y fecha, tanto de creación como de la última modificación. | **Ventaja.** Es posible identificar acciones de inserción, modificación y eliminación en la tabla consolidada.<br><br>**Desventaja.** Si se modifican N campos, existirán N inserciones en la tabla consolidada con el tipo de acción DML. | **Ventaja.** Monitoreo de acciones DML, además de acciones DDL, según configuración guardando la sentencia.<br><br>**Desventaja.** Registra las sentencias SQL como logs de auditoría donde además almacenas palabras reservadas de forma repetida. | **Ventaja.** Según la acción DML, en la tabla espejo correspondiente se especifica el tipo para cada tupla.<br>**Desventaja.** Aunque se modifique uno o n campos, se tendrá una nueva fila con todas las columnas en la tabla espejo. |
| 6 | *Backups* de datos de la BD y de la auditoría | **Ventaja.** Al encontrarse los campos de auditoría juntos, se obtiene un solo *backup* íntegro. **Desventaja.** Los *backups* tienen mayor tamaño, no siendo posible separar los datos de auditoría. | **Ventaja.** Al estar la tabla consolidada en la misma BD, se obtiene un solo *backup*. **Desventaja.** Los *backups* son de mayor tamaño dependiendo de la frecuencia de modificación, los datos de auditoria no se separan en los *backup* de BD. | **Ventaja.** Es posible obtener *backups* separados de los logs de auditoría, la velocidad de obtener copias es reducida, evita que se corrompan como una unidad total. **Desventaja.** Puede perder la correspondencia de logs si se manejan archivos de fechas diferentes. | **Ventaja.** Al contar con las tablas espejo en la misma BD, es posible obtener un sólo *backup* completo e íntegro. **Desventaja.** Los *backups* completos son de un tamaño exponencial considerable, siendo como mínimo el doble de los datos iniciales. |
| | | | | | |

| Modelo Indicador - Ventaja y Desventaja (Continuación) | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | **Logs de Transacciones o Sesión** | **Tablas espejo** |
| 7 | Restricción de acceso a la auditoría | **Ventaja.** No aplica.<br><br>**Desventaja.** Los datos de auditoría se pueden ver directamente en texto plano en cada registro en BD, vulnerando la confiabilidad de los datos. | **Ventaja.** No aplica.<br><br>**Desventaja.** Los datos de auditoría se pueden ver en texto plano consultando la tabla consolidada de auditoría, comprometiendo la confidencialidad de los datos. | **Ventaja.** Algunas soluciones actuales poseen controles de seguridad de acceso y registro.<br><br>**Desventaja.** Dependencia tecnológica con criterios no uniformes de seguridad. | **Ventaja.** No aplica.<br><br>**Desventaja.** Los datos de auditoría se pueden ver en texto plano visibles en las tablas espejo de auditoría, vulnerando la confiabilidad de los datos. |
| 8 | Tipo de consulta a la auditoría | **Ventaja.** Consultas directas en las tablas originales, observando la relación directa con el registro.<br><br>**Desventaja.** No es posible consultar el historial de todos los cambios en los campos, sólo se observa el último cambio realizado. | **Ventaja.** Consultas directas a la tabla consolidada, observando registros de únicamente los campos modificados.<br><br>**Desventaja.** Al ser similar a una BD columnar, se requiere mucho esfuerzo en elaborar las consultas. | **Ventaja.** Las consultas implementan seguridad de acceso a los datos con mecanismos específicos de consulta.<br><br>**Desventaja.** El formato de las consultas resulta complejo y específico de un SGBD. | **Ventaja.** Consultas simples directas a las tablas espejo, manteniendo la misma lógica de consultas.<br><br>**Desventaja.** Presenta huecos de seguridad, ya que permite consultar datos sin ningún tipo de restricción. |
| | | | | | |

| Modelo Indicador - Ventaja y Desventaja (Continuación) | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | **Logs de Transacciones o Sesión** | **Tablas espejo** |
| 9 | Velocidad de consultas en la BD | **Ventaja**. Con los campos adicionales, el rendimiento en las consultas se ve afectado mínimamente. **Desventaja.** Al consultar grandes volúmenes de datos, existe un tiempo adicional considerable debido a que también se analizan los campos de auditoría. | **Ventaja.** La velocidad de consulta a las tablas originales no se afecta. **Desventaja.** Al estar concentrada la auditoría en una sola tabla, las consultas sin los filtros adecuadas pueden demorar bastante. | **Ventaja.** La velocidad de consulta a los registros, se afecta mínimamente, pues existen procesos adicionales escuchando la captura de datos en las modificaciones. **Desventaja.** Sin el uso de los filtros adecuados y personalización, las consultas pueden ser morosas. | **Ventaja.** El rendimiento en las consultas se ve mínimamente afectado por los campos adicionales. **Desventaja.** Después de una amplia acumulación de registros, las consultas a la auditoría, pueden demorar mucho más de lo esperado. |
| 10 | Forma de captura de datos de auditoría | **Ventaja.** Flexible, admite la utilización de desencadenadores, aplicaciones en segundo plano o desde la aplicación cliente. También, al ser pocos campos de auditoría, el proceso es rápido. **Desventaja.** El uso de desencadenadores representa un procesamiento adicional para el motor de BD, lo mismo sucede con actualizaciones posteriores desde aplicaciones cliente o en segundo plano | **Ventaja.** Se basa en el uso de desencadenadores para cada acción DML, capturando únicamente los campos que sufran alteraciones. Es posible enviar datos de auditoría desde la aplicación cliente. **Desventaja.** En acciones de inserción, actualización y eliminación de forma masiva y constante, los desencadenadores pueden afectar el rendimiento de la BD. | **Ventaja.** Captura basada en el monitoreo de los logs de transacciones o de sesión, afectando mínimamente a las acciones DML y al tiempo de respuesta en la BD, le transfiere el procesamiento al servidor. **Desventaja.** Guarda las modificaciones de los datos y otras acciones DDL en un registro específico de la herramienta para su lectura en forma de sentencias SQL, esto dificulta la reconstrucción de datos. | **Ventaja.** Centrado en el uso de desencadenadores para monitorear acciones DML, logrando una captura completa de todo un registro como auditoría. **Desventaja.** El uso descontrolado de desencadenadores en las modificaciones masivas, puede afectar el rendimiento de la BD. La captura de datos toma en cuenta toda la fila, independientemente de si se modificó una o todas las columnas. |

| Modelo Indicador - Ventaja y Desventaja (Continuación) | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | **Logs de Transacciones o Sesión** | **Tablas espejo** |
| 11 | Historial de cambios | **Ventaja.** En tablas que no son sensibles, puede ser suficiente contar con información sobre el usuario y fecha de creación y última modificación. **Desventaja.** Cuando los campos de usuario y de fecha de la última modificación son diferentes al de creación, no es posible conocer el dato anterior. | **Ventaja.** Se toma en cuenta para su registro sólo las columnas que sufren modificación, además de los campos de seguimiento de auditoría. **Desventaja.** Por cada N campos modificados, se realizan N inserciones en la tabla de auditoría y en cada una se repiten los campos de control de auditoría. | **Ventaja.** Puede almacenar cada cambio en los datos, tanto DML como DDL, es configurable según las características de cada herramienta de auditoría del motor de base de datos. **Desventaja.** Resulta difícil comparar y analizar un registro modificado con datos anteriores, debido al formato en que se almacena la información de auditoría. | **Ventaja.** Con la configuración general, se capturan todas las modificaciones en los datos, pudiendo observarse en n filas el historial de cambios para un determinado identificador. **Desventaja.** Aunque sólo se modifique un campo de la fila, igualmente se inserta toda la fila en el historial de cambios de la auditoría. |
| 12 | Ubicación de almacenamiento | **Ventaja.** La auditoría está disponible en la mima BD, disgregada en la misma tabla y en la misma dirección física. **Desventaja.** Seguridad vulnerable en el acceso a la información, algún problema de almacenamiento o BD afectará también a la auditoría, no es posible dividir los datos y la auditoría. | **Ventaja.** El historial de auditoría está disponible juntamente con la BD, en una tabla centralizada transporte (datos primarios y de auditoría), siendo su de manera conjunta. **Desventaja.** Como los datos de auditoría están en la misma BD, cualquier problema en la BD afecta a ambos, siendo un problema de seguridad. | **Ventaja.** Los logs de auditoría se encuentran separados de la BD, dentro de la estructura de archivos del motor de BD, si se corrompe uno, no se pierden por completo los datos. **Desventaja.** Los datos de BD y la auditoría se encuentran ubicadas en el mismo directorio, estando en la misma unidad de disco, existiendo una vulnerabilidad de fallar el disco. | **Ventaja.** Los registros auditables de las tablas espejo, se encuentran en la misma BD, tabla y ubicación en disco. **Desventaja.** No es posible dividir los registros habituales con los de auditoría, donde cualquier problema ambos se comprometen, además que no hay restricciones de acceso ni se controlan las modificaciones en la auditoría. |

| Modelo Indicador - Ventaja y Desventaja (Continuación) | | | | | |
|---|---|---|---|---|---|
| **N°** | **Indicador de Evaluación** | **Modelo o Práctica Utilizada** | | | |
| | | **Añadir campos a una tabla** | **Consolidado histórico de todas las tablas** | **Logs de Transacciones o Sesión** | **Tablas espejo** |
| 13 | Tamaño de espacio en disco total | **Ventaja.** Independientemente de los datos, el especio adicional por la auditoría es pequeño. **Desventaja.** No es posible separar el almacenamiento en disco de los datos de auditoría. | **Ventaja.** El tamaño en disco aumenta dependiendo de la actualización de cada columna. **Desventaja.** Al ubicarse en la misma BD, el tamaño total en disco crece como una sola unidad, no separados. | **Ventaja.** No aplica. **Desventaja.** Al ubicarse los datos y la auditoría en el mismo directorio principal de archivos, el tamaño total en disco dedicado a datos crece en gran medida. | **Ventaja.** No aplica. **Desventaja.** El tamaño en disco total aumenta desde el doble hasta las N modificaciones o eliminaciones, siendo las copias de seguridad de gran tamaño. |
| 14 | Integridad de datos | **Ventaja.** No aplica. **Desventaja.** La integridad se pierde cuando la información se modifica o cuando parte de ella se elimina. | **Ventaja.** Se cuenta con todo el historial de modificaciones de los datos. **Desventaja.** No considera controles o restricciones de acceso en las modificaciones sobre la auditoría. | **Ventaja.** Se cuenta con todo el *log* de eventos en los datos según se haya configurado, permitiendo rastrear el seguimiento de cambios. **Desventaja.** Aún se deben fortalecer mecanismos de seguridad en los datos en la protección de archivos de auditoría. | **Ventaja.** Se cuenta con todo el historial de cambios en los datos de cada tabla. **Desventaja.** No considera seguimiento o restricciones de acceso en los cambios sobre la auditoría. |

Fuente: Elaboración propia.

## 3.3 Directrices y lineamientos de controles de auditoría para base de datos

- Cada tabla debe tener una llave primaria autonumérica no nula.
- No se deben eliminar registros de la base de datos de forma física, toda eliminación debe ser lógica.
- Cada tabla debe tener un campo que especifique el estado de activo o inactivo de un determinado registro.
- Mínimamente se debe almacenar quién (usuario) y cuándo (fecha y hora) se ha creado una determinada tupla.
- Es recomendable que la columna usuario, se almacene de forma cifrada.
- Los datos y su evolución de auditoría deben almacenarse por separado.
- Poseer una política de niveles de acceso.
- Debe ser posible reconstruir la información a partir de los registros de auditoría, de forma automatizada y a un periodo o estado determinado.
- Debe registrarse cada inserción, modificación y/o eliminación de cada registro, de forma que se cuente con un historial de cambios de cada registro.
- Debe registrarse el tipo de acción ya sea inserción, modificación y/o eliminación de cada registro.
- Se debe evitar tener columnas que sean calculables demasiado frecuente, por ejemplo, en cada ejecución de una función para obtener un reporte, ésta no debe realizar modificaciones directamente a la tabla por cada ejecución.
- Llevar todas las tablas de la base de datos mínimamente hasta la tercera forma normal si es necesario.
- Utilizar una nomenclatura de acuerdo al motor de base de datos para establecer los nombres de base de datos, tablas, columnas, funciones o cualquier elemento en la estructura de la base de datos.

Tabla 3.2: Indicador – directriz o característica deseada.

| N° | Indicador de Evaluación | Directriz o Característica Deseada |
|---|---|---|
| 1 | Campos de auditoría | Mínimamente se debe almacenar el quién (usuario) y cuándo (fecha y hora) se ha creado una determinada tupla. |
| 2 | Cambio en la estructura de las tablas originales | - Llevar todas las tablas de la base de datos mínimamente hasta la tercera forma normal.<br>- De acuerdo al motor de base de datos, utilizar una nomenclatura para establecer los nombres de base de datos, tablas, columnas, funciones o cualquier elemento en la estructura de la base de datos. |
| 3 | Estructura de auditoría | Es recomendable que la columna usuario se almacene de forma cifrada. |
| 4 | Posibilidad de reconstruir la información | Debe ser posible reconstruir la información a partir de los registros de auditoría, de forma automatizada a un periodo o estado determinado. |
| 5 | Identificación del tipo de acción DML | Debe registrarse el tipo de acción según sea inserción, modificación y/o eliminación de cada registro. |
| 6 | *Backups* de datos de la BD y de la auditoría | Debe ser posible obtener *backups* de forma separa de la base de datos y de la auditoria. |
| 7 | Restricción de acceso a la auditoría | Poseer una política de niveles de acceso. |
| 8 | Tipo de consulta a la auditoría | Las consultas a la auditoría deben direccionar a un esquema o base de datos distinta. |
| 9 | Velocidad de consultas en la BD | Crear índices para las consultas con condiciones frecuentes que no son llaves. |
| 10 | Forma de captura de datos de auditoría | El uso de desencadenadores debe controlar bloqueos en modificaciones masivas. |
| 11 | Historial de cambios | Debe registrarse cada inserción, modificación y/o eliminación de cada registro, de forma que se cuente con un historial de cambios de cada registro. |
| 12 | Ubicación de almacenamiento | Los datos y su evolución de auditoría deben almacenarse por separado. |
| 13 | Tamaño de espacio en | Debe evitarse tener columnas que sean calculables demasiado |

| | | |
|---|---|---|
| | disco total | frecuente, por ejemplo, en cada ejecución de una función para obtener un reporte, ésta no debe realizar modificaciones directamente a la tabla por cada ejecución. |
| 14 | Integridad de datos | - Cada tabla debe tener una llave primaria autonumérica no nula.<br>- No se deben eliminar registros de la base de datos de forma física, toda eliminación debe ser lógica. |

Fuente: Elaboración propia.

# 4 Propuesta de Convención

En la elaboración de la presente propuesta de convención para la implementación de bases de datos con controles de auditoría y seguridad, se aborda la estructura que representa la visión general sobre cómo se desarrolla la convención, conformada por cinco ejes descriptivos, los cuales se muestran en la siguiente figura:

Figura 4.1: Visión General de la Propuesta de Convención


Fuente: Elaboración propia.

## 4.1 Descripción de la propuesta de convención

La convención que se propone está orientada en brindar lineamientos, de estándar abierto y de aplicación libre, para el modelado de bases de datos 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 bases de datos relacionales.

Considerando el indudable valor que tienen los datos para una organización, que los convierte en activos de información, es 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 este tipo de bases de datos relacionales.

## 4.2 Justificación e 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 base de datos ni por la aplicación cliente o servicio web que interactúa con esos datos.

Mencionar también, que los diseños de base de datos 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, facilitando un mejor desempeño profesional en auditores e informáticos; y robustece la seguridad de la información al suministrar mecanismos seguros y confiables para mantener un historial de cambios en los datos.

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.

Al presentar bastantes bondades, resulta conveniente el hecho de compartir estos esfuerzos bajo una licencia de software libre GPL, mediante la cual se garantiza las cuatro libertades que conlleva, ente las más destacadas la libre distribución y estudio de la convención, buscando ofrecer a las comunidades de bases de datos una forma estandarizada libre para implementaciones con controles de seguridad y auditoría, además de la posibilidad de recibir contribuciones para mejoras a la convención.

## 4.3 Objetivos de Seguridad de la convención

### 4.3.1 Confidencialidad

Con este pilar, se busca 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).

### 4.3.2 Integridad

Este objetivo básicamente busca garantizar que los datos no sean alterados, previniendo: que alguien con permisos de modificación por error modifique los datos, que alguien sin permisos de modificación realice algún cambio y, que algún programa o aplicativo que interactúe directamente con la base de datos realice modificaciones sin autorización.

La integridad de una base de datos 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.

### 4.3.3 Disponibilidad

La disponibilidad en bases de datos, responde 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, esquemas de respaldo, planes de continuidad del negocio y recuperación de desastres, mismos que deberán ser probados periódicamente para garantizar su correcto funcionamiento.

### 4.3.4 Trazabilidad y *Accountability*

El objetivo de seguridad, trazabilidad, consiste 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. En lo relativo a la protección de datos, el principio de *accountability* no solo obliga a la empresa a cumplir con la normativa, sino a demostrar 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, clasificación y almacenamiento, uso y tratamiento, cesión y transferencia de datos, y la destrucción de datos.

### 4.3.5 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.

## 4.4 Enfoque

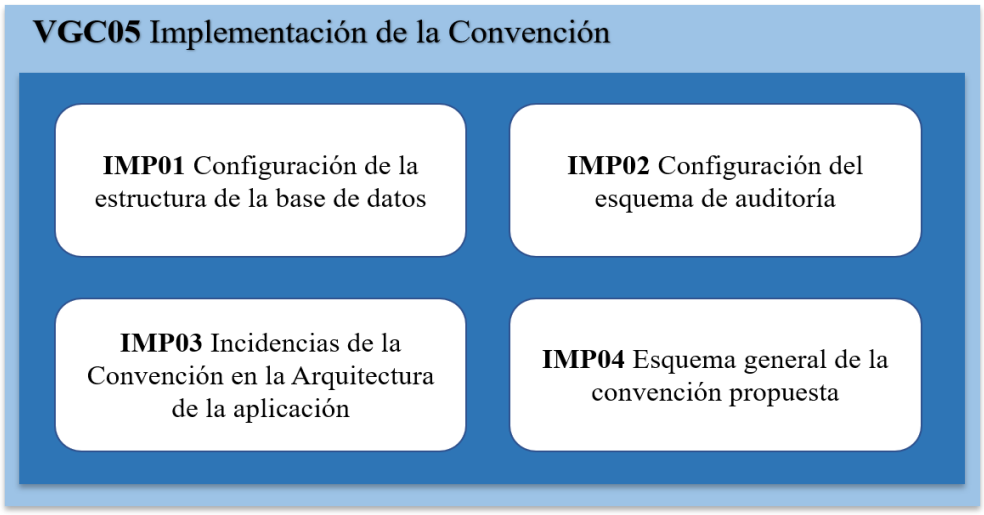
Para abordar la elaboración de la propuesta de convención, como se hace alusión en el apartado 1.7, se utiliza la metodología de la investigación tecnológica, con alcance exploratorio, con enfoque cualitativo y con los métodos inductivo y analítico. Donde alineados a la problemática identificada y a 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.

## 4.5 Implementación

En este quinto eje descriptivo de la propuesta de convención, se 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 como se muestra en la siguiente figura:

Figura 4.2: Visión General de la Implementación de la Propuesta de Convención




Fuente: Elaboración propia.

Por tanto, en la implementación del diseño de una nueva base de datos relacional con controles de auditoría y seguridad, se debe considerar los siguiente:

### 4.5.1 Configuración de la estructura de la base de datos

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:

i. 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.

ii. Directorio sql/data. En 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.

iii. 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 generar un esquema periódico de limpieza de *log*, y más aún si se tratara de un ambiente altamente transaccional.

iv. 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 (4.3.1) y a la Disponibilidad (4.3.3).

b) Configurar los permisos para que el usuario del sistema operativo que es administrador de la base de datos, 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.

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 (4.3.1) y *Accountability* (4.3.4).

c) Crear la base de datos separando 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 (4.3.1) y a la Disponibilidad (4.3.3).
d) 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 (4.3.1), Integridad respecto a la administración (4.3.2) y No repudio (4.3.5).
e) 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 (4.3.2) también relacionado con la Disponibilidad (4.3.3).
f) 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 (4.3.2).

g) 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 (4.3.2), Trazabilidad y *Accountability* (4.3.4).

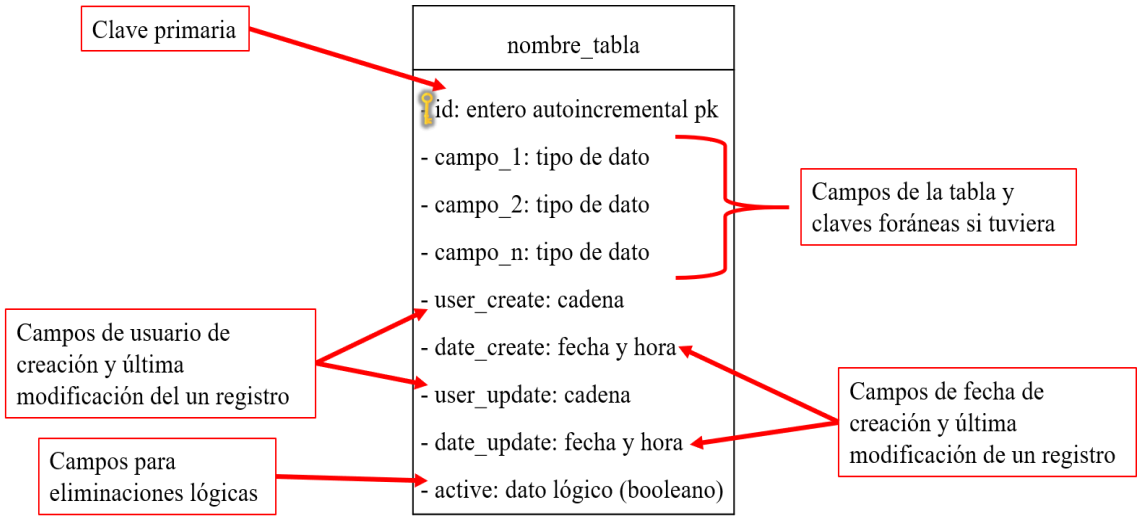
h) Cada tabla debe poseer campos sobre el ¿quién? los cuales serían "*user_create*" que representará información sobre el usuario que creó un registro y el campo "*user_update*" que representará la última modificación que se haya realizado sobre la fila, ambos de tipo cadena con valor por defecto el 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 (4.3.4) y No repudio (4.3.5).

i) 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 (4.3.2), Trazabilidad y *Accountabiliy* (4.3.4).

j) Adecuar las tablas mínimamente hasta la tercera forma normal (1FN, 2FN y 3FN) para disminuir inconsistencias y anomalías lógicas, es decir, considerar para 1FN que no existan grupos de repetición en tablas individuales, que exista una tabla independiente para cada conjunto de datos relacionados y que cada conjunto de datos relacionados cuente con una clave principal; además, para 2FN crear tablas independientes para conjuntos de valores que se aplican a varios registros evitando la redundancia de datos y relacionar estas tablas con una clave externa; y además, para 3FN eliminar los campos que no dependen de la clave candidata. Este requisito está alineado con la Integridad (4.3.2) y Trazabilidad (4.3.4).

Bajo estas 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 4.3: Propuesta Tabla Original




Fuente: Elaboración propia

### 4.5.2 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/log y 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. Este también 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, es recomendable generar un esquema periódico de limpieza de log de base de datos.

iv. Directorio sql/audit/backup. Finalmente, el subdirectorio denominado *backup*, proveerá una significativa solución para proteger datos críticos de auditoría que se encuentran almacenados en las bases de datos 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 (4.3.1) y a la Disponibilidad (4.3.3).

b) Configurar los permisos para que sólo el usuario del sistema operativo administrador del motor de base de datos, 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 (4.3.1) y *Accountability* (4.3.4).

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* (4.3.4) y No Repudio (4.3.5).

d) 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 (4.3.2) y Trazabilidad (4.3.4).

e) 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 (4.3.2).

f) 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 (4.3.2), Trazabilidad (4.3.4) y No repudio (4.3.5).

g) 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 base de datos, es un procedimiento que se ejecuta cuando se cumple una condición establecida al realizar una operación, que pueden ser de inserción (*INSERT*), actualización (*UPDATE*) o borrado (*DELETE*).

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*.

ii. Servicio de lectura de logs.- se refiere al guardado secuencial en un archivo o en una base de datos 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.

Tabla 4.1: Comparación de la utilización de Triggers o Lectura de Logs en la auditoría de bases de datos relacionales

| **Uso de desencadenadores** | **Servicio de lectura de *logs*** |
|---|---|
| Implementación directa en cada tabla de la BD principal para la captura de datos modificados. | Implementación a través de una aplicación o script que lee los *logs* de la BD programado como tarea. |
| Sencillez en la captura de datos modificados para ser insertados en la BD de auditoría. | Deben realizarse esfuerzos adicionales para reconocer y estructurar los datos modificados para ser almacenado en la auditoría. |
| El procesamiento es asumido por el motor de BD y consecuentemente también el servidor de BD. | El procesamiento es asumido directamente por ser servidor de BD. |
| Los desencadenadores pueden ser borrados si no se cuentan con niveles de acceso y privilegios, previamente se necesitan permisos | Los logs de BD pueden ser borrados si no se cuentan con niveles de acceso y permisos, así como también puede ser detenido o |

| | |
|---|---|
| para acceder a la instancia y a la BD específica. | removido el servicio o demonio que se encarga de la captura de datos. |

Fuente: Elaboración propia.

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* (4.3.4).

h) 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 (4.3.2).

i) 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 (4.3.2) y No repudio (4.3.5).

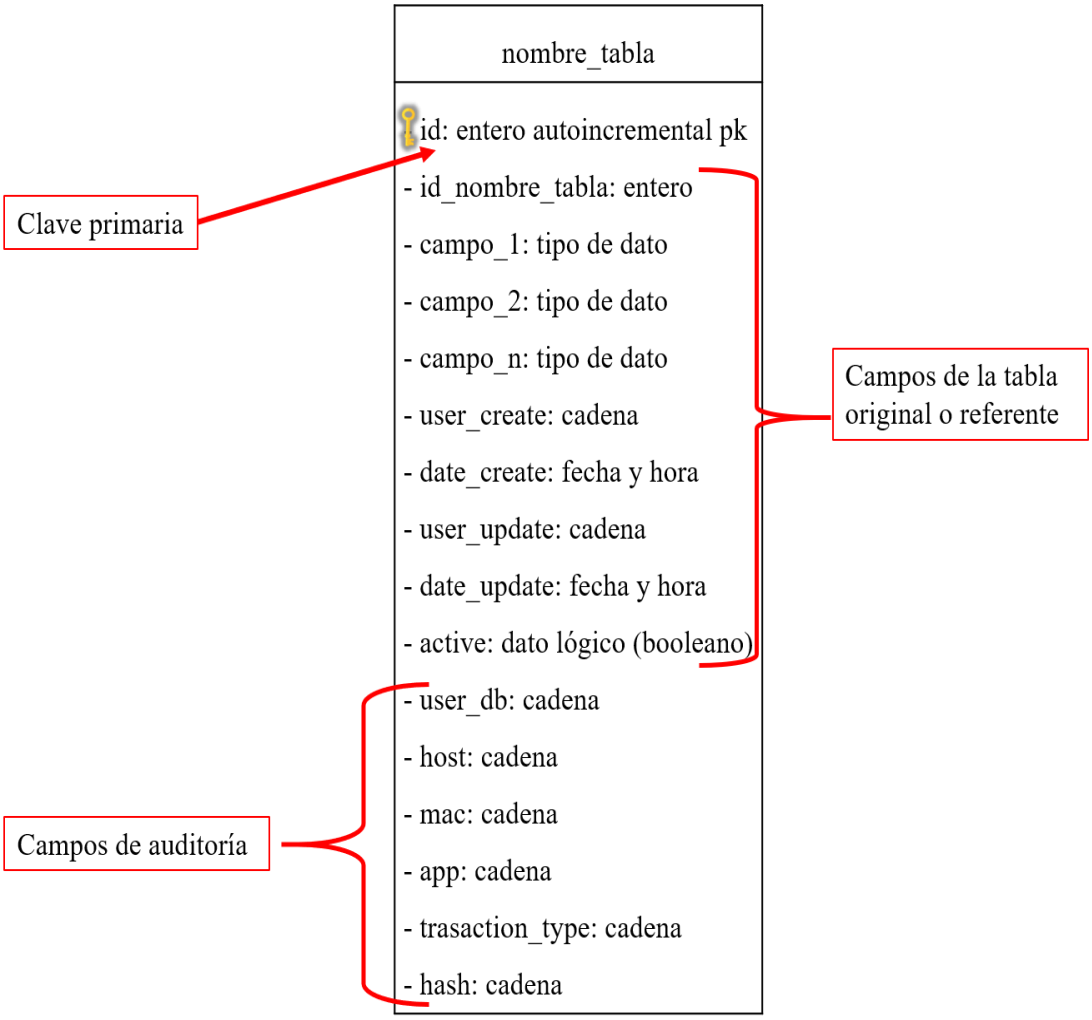
j) La base de datos de auditoría debe estar cifrada, de modo que, con esta operación criptográfica, los datos sean ilegibles utilizando una clave de cifrado segura, esta clave se debe especificar para acceder desde la BD principal a la BD de auditoría. Entre las opciones más comunes y seguras en bases 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 (4.3.1), Integridad (4.3.2) y No repudio (4.3.5).

Bajo estas consideraciones y dependiendo de la política interna, utilizar el idioma de preferencia, donde cada tabla de la base de datos de auditoría, en afinidad con los objetivos de seguridad de la convención, queda de la siguiente manera:

Figura 4.4: Propuesta Tabla de Auditoría




Fuente: Elaboración propia.

### 4.5.3 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 base de datos, 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 base de datos 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.

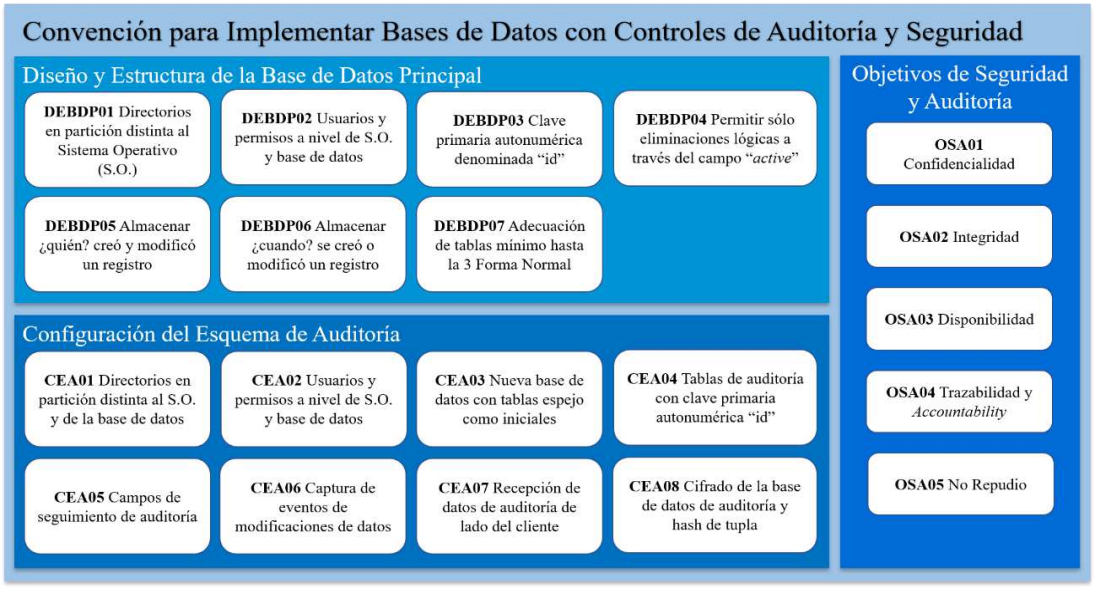
**Bases de datos existentes**.- La implementación de la presente propuesta de convención se adecua sin inconvenientes para nuevas bases de datos; sin embargo, para bases de datos ya existentes y en producción, no es recomendable; pero previo análisis y gestión de riesgos, puede ser posible técnicamente 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.

### 4.5.4 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:

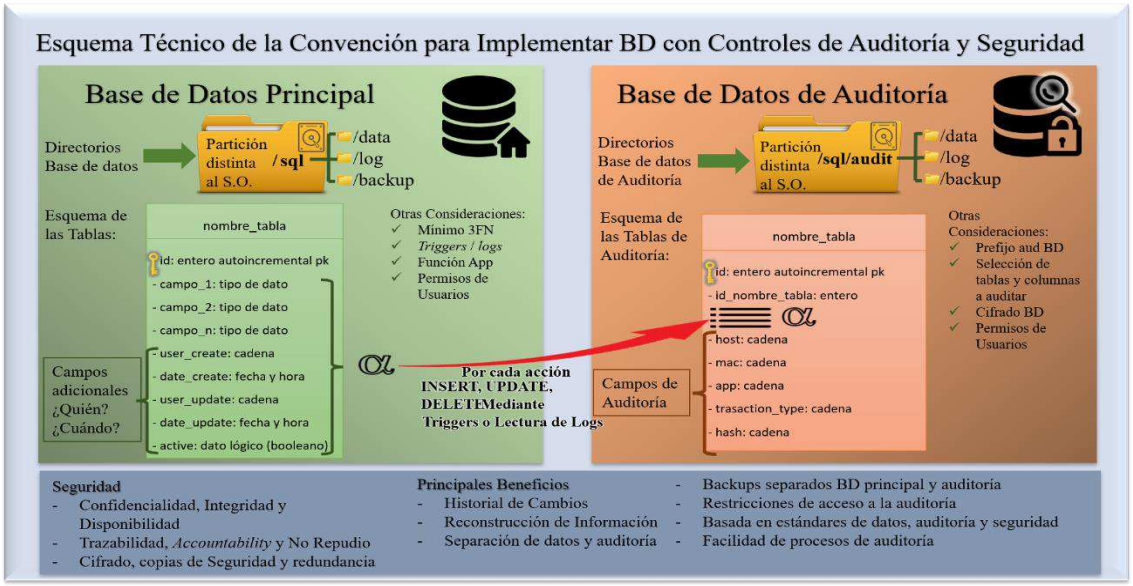
Figura 4.5: Esquema general de implementación de la propuesta de convención




Fuente: Elaboración propia.

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

Figura 4.6: Esquema técnico de la propuesta de convención




Fuente: Elaboración propia.

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.

# 5 Resultados y Discusión

## 5.1 Criterio de expertos

La evaluación mediante el criterio o juicio de expertos, método de validación cada vez más utilizado en la investigación, "consiste, básicamente, en solicitar a una serie de personas la demanda de un juicio hacia un objeto, un instrumento, un material de enseñanza, o su posición a un aspecto concreto" (Cabero & Llorente, 2013, págs. 25-38) .

En este sentido, en la validación de la presente Propuesta de Convención para el Diseño Seguro de Bases de Datos con Controles de Auditoría, mediante el método de Criterio de Expertos, se envió de forma individual la consulta a expertos en el área, tanto en el ámbito local y nacional, como internacional, donde desde los conocimientos y experiencias, se recibió colaboración académica con diferentes opiniones y retroalimentación sobre la propuesta desarrollada, brindando además validez y fiabilidad a la misma.

### Participantes

En la elección de los expertos, se utilizó el biograma en combinación con el coeficiente de competencia experta (Garcia & Fernandez, 2008, págs. 46-50), 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.

En una primera iteración para la validez de contenido, se tomaron a 4 expertos con un alto nivel de juicio para la obtención de retroalimentación (Delgado & otros, 2012). Luego de refinaciones a la propuesta, se seleccionó 20 profesionales que aceptaron participar en la revisión de la propuesta y responder el cuestionario, de los cuales 16 de ellos brindaron sus respuestas y opiniones en calidad de jueces, siendo una cantidad considerable de expertos (Garcia & Fernandez, 2008); el 56% del ámbito local, el 25% nacional y el 19% internacional (Chile y Costa Rica). La experiencia profesional o científica de los jueces es del 6% de 5 a 7 años, 0% de 8 a 10 años y el 94% tienen más de 10 años de experiencia.

**Diseño del Instrumento**

Una vez realizada la exploración del estado del arte, analizadas cualitativamente las ventajas y desventajas de las prácticas actuales, identificados y analizados los indicadores de evaluación y directrices en el marco del objetivo de este aporte, es que se elaboró la propuesta de convención, misma que se les facilitó a los expertos vía correo electrónico, recibiendo las apreciaciones cognitivas individuales para su refinamiento.

Se diseñó el cuestionario como instrumento de validez, con 3 dimensiones (BD principal, auditoría y seguridad), 12 cuestiones (preguntas) y la opinión del experto; cada cuestión constituida por 4 indicadores generales de evaluación, dando un total 48 ítems:

- Claridad: El ítem está formulado con un lenguaje apropiado, no genera contradicción.
- Contexto: El ítem está en el marco de la temática abordada.
- Coherencia: El ítem mide alguna variable o relación con los indicadores.
- Relevancia: 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 y 5: Totalmente de acuerdo.

En sí, el instrumento contiene: (1) el título de la propuesta de convención, objetivo general de la investigación, descripción del instrumento, instrucciones con la escala tipo Likert, indicadores generales de evaluación y autor del instrumento; (2) datos generales de los expertos como correo electrónico, nombres y apellidos, institución donde trabaja, ciudad – país, rango de años de experiencia profesional o científica; (3) las preguntas con las consideraciones antes descritas y (4) finalmente la opinión del experto. (Ver Anexo: Modelo del instrumento cuestionario).

**Procedimiento**

Como material de estudio, en abril de 2021, se preparó de forma separada lo concerniente al capítulo IV de esta investigación, el cual se centra en la propuesta de convención y se envió vía correo electrónico a cada uno de los primeros 4 expertos, quienes respondieron con sus apreciaciones en un tiempo aproximado de tres semanas. (Ver Anexo: Formato del primer correo electrónico enviado en la consulta a expertos).

Se analizaron y efectuaron las recomendaciones recibidas por los expertos, generando una nueva versión de la propuesta de convención, posteriormente se seleccionó a 20 profesionales incluidos los de la primera iteración y una vez concluido el diseño del instrumento, en julio de 2021, se facilitó de forma individual a los expertos lo siguiente:

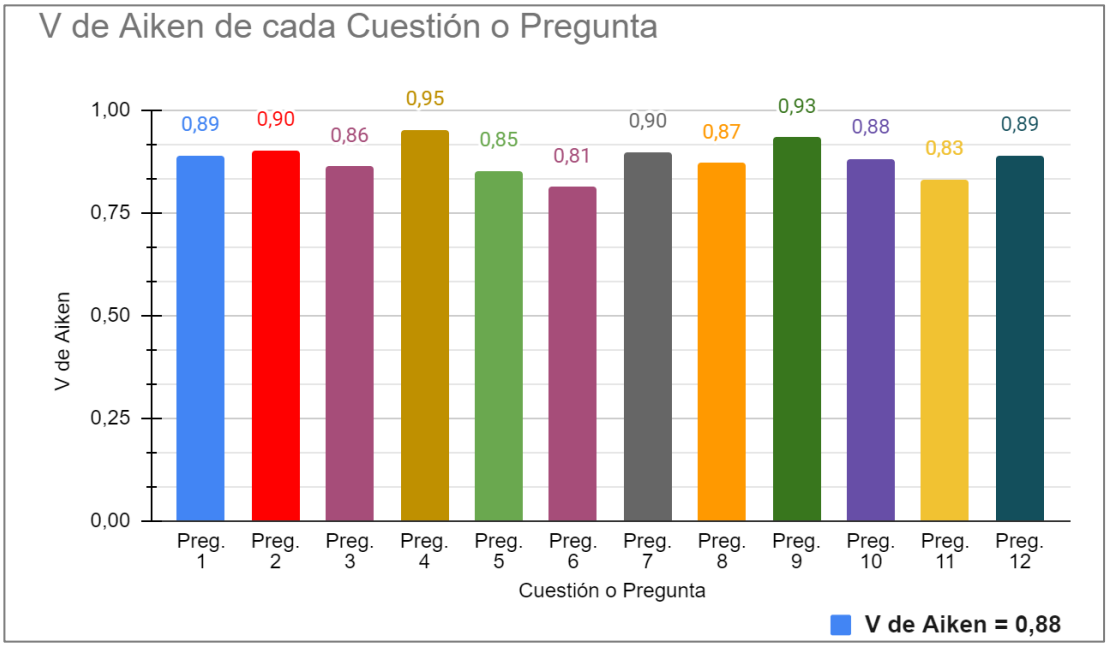
1. Correo electrónico de presentación y colaboración académica.
2. Documento de la propuesta de convención
3. Enlace al instrumento del cuestionario en línea para la valoración, cuyo enlace es: https://bit.ly/3xGnXQL

Mencionar que se mantuvo el anonimato entre los expertos, tanto de sus identidades como de los resultados durante el proceso, evitando posibles influencias entre opiniones.

**Validez y Confiabilidad**

Los detalles tabulados se muestran en los Anexos: Tabulación de resultados del instrumento de validez de contenido, en resumen, los resultados son los siguientes:

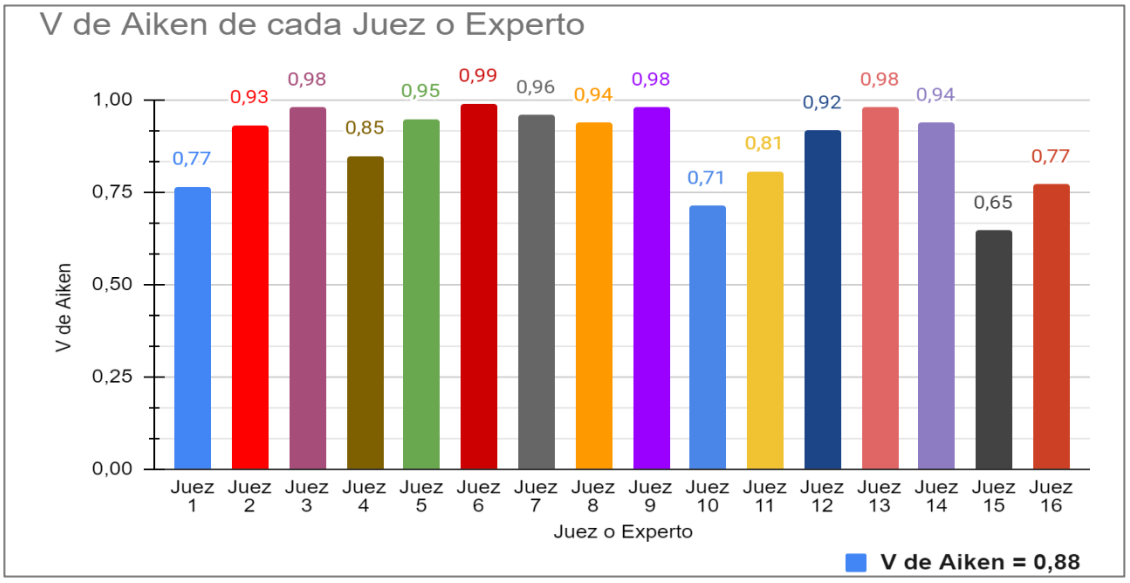
Figura 5.1: Resumen de resultado del instrumento de validez por preguntas.




Fuente: Elaboración propia

La figura muestra los valores entre 0 y 1 calculados a través del coeficiente de validez de contenido V de Aiken, el cual se explicará en breve, los datos procesados oscilan entre un mínimo 0,81 y un máximo de 0,95 correspondiente a la pregunta número 4, resultando en un nivel de acuerdo de los expertos de 0,88.

Figura 5.2: Resumen de resultado del instrumento de validez por expertos.




Fuente: Elaboración propia

En relación a los datos procesados de los jueces, los resultados oscilan entre 0,65 y 0,99, con una varianza total de los expertos de 25,44 y una validez de 0,88.

**Alfa de Cronbach**.- Utilizando el método de Criterio o Juicio de Expertos, para verificar la consistencia interna de la escala y confiabilidad del instrumento, se aplicó el Alfa de Cronbach. (Cronbach & Shavelson, 2004). Para el cálculo se utiliza la siguiente fórmula:

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum V_i}{V_t}\right]$$

Donde: K (número de ítems) = 12
Vi (varianza de cada ítem) = 4,30
Vt (varianza total) = 25,44
α (Alfa Cronbach) = 0,91

$$\alpha = \frac{12}{12-1}\left[1 - \frac{4{,}30}{25{,}44}\right] = 0{,}91$$

La interpretación de la confiabilidad del instrumento de 0.91 es Muy Alta mediante el Alfa de Cronbach, según indica (Ruíz Bolívar, 2015):

**0,81 a 1,00 = Muy Alta**
0,61 a 0,80 = Alta
0,41 a 0,60 = Moderada
0,21 a 0,40 = Baja
0,01 a 0,20 = Muy Baja

**Coeficiente de Validez de Contenido V de Aiken**.- Para obtener la validación, se utilizó el Coeficiente de Validez de Contenido V de Aiken, el cual cuantifica la relevancia de cada ítem respecto de un dominio de contenido formulado por N jueces, oscilando desde 0 hasta 1, siendo el valor de 1 indicativo de un perfecto acuerdo entre los jueces respecto a la mayor puntuación de validez de los contenidos evaluados. (Aiken, 1985).

Para el cálculo se utiliza la siguiente fórmula:

$$V = \frac{S}{n(c-1)}$$

| | | | |
|---|---|---|---|
| Donde: | S = la sumatoria de Si | = | 56,396 |
| | Si = Valor asignado por el juez i | | |
| | n = Número de jueces | = | 16 |
| | c = Número de valores de la escala de valoración | = | 5 |
| | V = S / (n*(c-1)) | = | 0,88 |

$$V = \frac{56{,}396}{16\,(5-1)} = 0{,}88$$

En este sentido, la validez del contenido V de Aiken del 0,88 supera el valor de aceptable en forma global y cada ítem fue aceptado al superar cada uno el 0,80 considerando la cantidad de ítems y expertos participantes; existiendo una relación entre la confiablidad (0,91) y la validez (0,88) de 0,89. (Juárez Hernandez & Tobón, 2018).

Además, respecto a la escala de valores utilizada, se consigue una media de 4,53 con una tendencia a variar de 0,67 (desviación estándar σ).

**Opiniones principales de los jueces o expertos**

Dentro del análisis de respuestas, se recibió la afirmación de que la propuesta suma capas de seguridad en el trabajo diario de los sistemas que hacen uso de bases de datos y brinda la integridad, disponibilidad y confiabilidad que deben acompañar a los procesos de auditoría, todo esto independientemente de la naturaleza del sistema en uso.

Considerando que, en el campo de la seguridad de la información y la seguridad informática, pueden ocurrir incidentes en cualquier momento, uno de los expertos opina que se debe sumar toda ayuda tecnológica y procedimental a todos los eventos vinculados a los procesos de datos, siendo estos el activo que proveen sustento a las decisiones de una empresa, para una constante gestión de seguridad de los procesos que intervienen.

Si bien los incidentes informáticos suelen ocurrir, es primordial que futuros incidentes no se repitan por las mismas razones, es decir, que, si existió un incidente con respecto a una mala gestión de permisos a nivel de sistemas, esto una vez identificado sea solucionado, archivado y asegurado. La presente propuesta de convención es un aporte importante que ofrece una solución a sectores que los sistemas privativos de auditoría han descuidado.

Por otro lado, denotar que el diseño de la propuesta tiene un enfoque analítico que coadyuva a la reducción del nivel de riesgos de pérdidas/fugas de información, cuyo impacto es significativo para las Organizaciones o Empresas; ya que la información es un bien valioso que debe protegerse. La estructura de Base de datos es acertada ya que hay la posibilidad de efectuar la trazabilidad de la información y además de recuperar la misma ante casos de incidencias, actuando los controles como preventivos y correctivos en casos particulares y momento dado.

Contar con una guía o convención, que permita tomar en cuenta aspectos relacionados al tratamiento de la información, sobre cualquier creación o modificación de datos, es un aporte importante y esta propuesta apunta hacia una formalización mediante la propuesta presentada.

Se recibe la recomendación de especificar el tema de clasificación de información relacionada con aspectos de seguridad, situación que la propuesta considera en los principios de seguridad de la convención para asegurar la disponibilidad y trazabilidad de la información, así como mencionar recaudos necesarios de infraestructura tecnológica.

Se aclara que el presente trabajo se circunscribe a las bases de datos relacionales, independiente del sistema operativo, pero con especial énfasis al sistema operativo Linux, y que la captura de información se centra en el DML, en las acciones de inserción, actualización y eliminación de datos, exceptuando la selección. Asimismo, la propuesta no es restrictiva a implementarse a nivel de aplicación, siendo más confiable monitorear los cambios al nivel más bajo posible.

Se hace énfasis que la implementación en nuevas bases de datos relaciones, no presenta inconvenientes; sin embargo, en bases de datos existentes, con los debidos recaudos y análisis de pertinencia, su implementación puede ser técnicamente factible considerando las incidencias descritas en la presente propuesta, pero no es del todo recomendable.

## 5.2 Conclusiones

Se cumple con los objetivos planteados al inicio de este trabajo, 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; de éstas se analizaron las 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.

Asimismo, se evaluaron los análisis generados, con los que se establecieron directrices y lineamientos deseados que debería poseer una base de datos relacional segura, aspectos alineados a los indicadores de evaluación procesados y normas de auditoría concernientes a bases de datos; con lo cual se logró elaborar una propuesta de convención para la implementación de bases de datos relacionales con controles de auditoría y seguridad, sentando las bases esenciales bajo un estándar abierto y acorde a normas internacionales de auditoría y seguridad de la información, estructurada en cinco ejes descriptivos, entre ellos la implementación, donde se describe la ejecución a nivel de gestión y técnico.

En consecuencia, se estudió la aplicabilidad de la propuesta de convención en el contexto de auditoría en bases de datos relacionales, sometiéndola a criterios de expertos en la temática, de quienes se obtuvieron opiniones y retroalimentaciones, contribuyendo en su refinamiento y dando lugar a la propuesta elaborada en este trabajo; verificando mediante el instrumento utilizado (cuestionario) una fiabilidad muy buena por el Alfa de Cronbach de 0,91 (91%) y una valoración mediante el Coeficiente de Validez de Contenido V de Aiken de 0,88 (88%), representando un alto nivel de acuerdos de validez.

Finalmente, atendiendo a la problemática descrita al inicio de esta investigación, se concluye que en el presente trabajo se proporciona una propuesta de convención de estándar abierto que se enfoca en modelar una base de datos con controles de auditoría y seguridad que permite realizar el registro de modificaciones, adiciones y eliminaciones de datos en las bases de datos relacionales libres como PostgreSQL, MySQL/MariaDB y que también es aplicable a bases de datos privativas; por sus características esta propuesta brinda grandes beneficios en la labor de auditoría y cuenta con los cimientos necesarios para constituirse en una convención dentro de la comunidad de bases de datos.

## 5.3 Líneas futuras

- Revisión heurística de 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.
- 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.
- Elaboración de 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).
- Elaboración de convenciones para tipos de auditoría específicas a cada sector, como ser gubernamental, financiero, salud, entre otros; alineados políticas externas e internas según su naturaleza.
- Análisis y desarrollo de 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

Acurio Del Pino, S. (Marzo de 2016). *Delitos informáticos: generalidades. Organización de Estados Americanos.* Obtenido de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aiken, L. (1985). Three Coefficients for Analyzing the Reliability and Validity of Ratings. *Educational and Psychological Measurement, Vol. 45*(1), pp. 131-142. doi:10.1177/0013164485451012

Ashdown, L., Keessling, D., & Kyte, T. (Diciembre de 2020). Introduction to Oracle Database. En *Oracle Database Database Concepts 21c.* Oracle and/or its affiliates. Obtenido de https://docs.oracle.com/en/database/oracle/oracle-database/21/cncpt/index.html

Braren. (2016). *Sugerencias de crear históricos de tablas de BD.* Obtenido de https://bit.ly/2RwZC0j

Cabero, J., & Llorente, M. d. (2013). La aplicación del juicio de experto como técnica de evaluación de las tecnologías de la información (TIC). *Eduweb, Vol. 7*(2), pp. 11-22. Obtenido de http://servicio.bc.uc.edu.ve/educacion/eduweb/v7n2/art01.pdf

Calbimonte, D. (2016). *Auditoría de Seguridad de Base de Datos SQL Server.* Solution Center, Apex SQL. Obtenido de https://bit.ly/3anY4ML

Camps, R., Casillas, L. A., Costal, D., Gibert, M., Escofet, C., & Pérez, O. (2005). *Software libre - Base de datos* (1ra. ed.). Barcelona: Eureca Media, Fundació a la Universitat Oberta de Catalunya. ISBN: 84-9788-269-5.

Contraloría General del Estado. (27 de Agosto de 2012). *Normas de Auditoría de Tecnologías de la Información y la Comunicación.* Bolivia: Resolución CGE/094/2012. Obtenido de https://www.contraloria.gob.bo/portal/Uploads/PDFportal/20130315_456.pdf

Coronel, C., & Morris, S. (2018). *Database Systems: Design, Implementation, & Management* (13th ed.). USA: Learning, Cengage. ISBN 978-1-337-68882-6.

Cronbach, L., & Shavelson, R. (2004). My Current Thoughts on Coefficient Alpha and Successor Procedures. *Educational and Psychological Measurement, Vol. 64*(3),

pp. 391-418. doi:10.1177/0013164404266386

DAMA Internacional. (2015). *Guía de Fundamentos para la Gestión de Datos.* (Publications Technics, LCC, Trad.) Nueva jersey: Technics Publications. (Obra original publicada en 2010). ISBN 978-0-9771400-8-4.

Delgado, E., & otros, y. (2012). Content validity evidences in test development: An applied perspective. *Intern J Clin Health Psych, Vol. 12*, pp. 449-459. Obtenido de https://www.redalyc.org/pdf/337/33723713006.pdf

Domínguez, J. (Septiembre de 2016). Cómo auditar cambios en una tabla MySQL o MariaDB. *Universidad Politécnica Territorial del estado Aragua*, pp. 1-3. Obtenido de https://www.researchgate.net/publication/308170361_Como_auditar_cambios_en_una_tabla_MySQL_o_MariaDB

Elmasri, R., & Navathe, S. (2016). *Fundamentals of Database Systems* (7th ed.). Pearson. ISBN: 978-0-13-397077-7.

FCASUA. (13 de agosto de 2008). *Auditoría en Informática.* Universidad Nacional Autonoma de Mexico, Mexico. Recuperado el 03 de abril de 2019

Federación Internacional de Contadores (IFAC). (2011). Conceptos Principales. En *Guía para el uso de las Normas Internacionales de Auditoría en auditorías de pequeñas y medianas entidades* (3ra. ed., Vol. I, págs. 81-162). New York, ISBN: 978-1-60815-396-1. Obtenido de https://www.ifac.org/system/files/publications/files/Guia-NIA-para-PYME-correcciones-V1.pdf

Free Software Foundation. (2019). *El manifiesto de GNU.* Obtenido de Proyecto GNU: https://www.gnu.org/philosophy/free-sw.es.html

Garcia, L., & Fernandez, S. (2008). Procedimiento de aplicación del trabajo creativo en grupo de expertos. *Energética, Vol. 29*(2), pp. 46-50. Obtenido de https://www.redalyc.org/articulo.oa?id=329127758006

Gartner. (25 de Noviembre de 2019). *Magic Quadrant for Operational Database Management Systems.* Obtenido de Gartner Research: https://www.gartner.com/en/documents/3975492

Gisbert, B. (2015). *UF1272 - Administración y auditoría de los servicios web* (1ra. ed.). Editorial Elearning, S.L. ISBN-13 : 978-8416424672.

Glushchenko, S. (Mayo de 2014). *Database auditing alternatives for MySQL*. Obtenido de Percona: https://www.percona.com/blog/2014/05/20/database-auditing-alternatives-mysql

Hassan, M. (18 de Septiembre de 2016). *Audit and Log Database DML Changes in PostgreSQL With Cyan Audit.* Obtenido de DZone: https://dzone.com/articles/audit-log-database-changes-in-postgresql

Hernández Nieto, R. (2002). *Contributions to Statistical Analysis.* Mérida, Venezuela: Universidad de Los Andes.

Huijie, W. (2017). A Security Framework for Database Auditing System. *International Symposium on Computational Intelligence and Design (ISCID), IEEE*(10th ed.), pp. 350-353. ISSN: 2473-3547. doi:10.1109/ISCID.2017.64

Ingravallo, H., & Entraigas, V. (2007). *Auditoría de Base de Datos. GAVA: Soporte para registración y análisis de cambios en los datos.* (Tesis de grado). Universidad Nacional de la Patagonia, Trelew.

Ioan, R., & Danescu, T. (2018). The Information Audit -Between Necessity and Regulation. *ResearchGate*. Recuperado el 2021, de https://www.researchgate.net/publication/265275966_The_Information_Audit_-Between_Necessity_and_Regulation

ISACA. (2012). *COBIT 5 Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* (I. M. Chapter, Trad.) Estados Unidos: ISACA. ISBN 978-1-60420-282-3. Obtenido de https://www.isaca.org/bookstore/cobit-5/wcb5

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

Juárez Hernandez, L. G., & Tobón, S. (2018). Análisis de los elementos implícitos en la validación de contenido de un instrumento de investigación. *Revista Espacios, Vol. 39*(53), 23. Obtenido de https://www.revistaespacios.com/cited2017/cited2017-23.pdf

Likert, R. (1932). *A technique for the measurement of attitude* (Vol. 140). Archives of Psychology,.

Liu, L., & Huang, Q. (2009). *A Logging Scheme for Database Audit* (Vol. 02). Computer Science and Engineering, International Workshop. doi:10.1109/WCSE.2009.837

Lu, Wentian, MIKLAU, Gerome, IMMERMAN,, & Neil. (2013). *Auditoría de una base de datos bajo las políticas de retención* (Vol. 22). Nueva Jersey: El VLDB Journal. doi:10.1007/s00778-012-0282-x

Macauley, E., & Cai, S. (2020). *Microsoft.* Obtenido de https://docs.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-database-engine

MariaDB Foundation. (04 de Noviembre de 2020). *About MariaDB.* Obtenido de https://mariadb.org/documentation/

Maya Villazón, E., & otros. (2015). *La Importancia del Uso de Bases de Datos y de la Seguridad de la Información para el Fortalecimiento de las TIC y para el Ejercicio Eficiente del Control.* Querétaro: OLACEFS - Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores. Obtenido de https://www.olacefs.com/conclusiones-tema-tecnico-n-2-la-importancia-del-uso-de-base-de-datos-y-de-la-seguridad-de-la-informacion-para-el-fortalecimiento-de-las-tic-y-para-el-ejercicio-eficiente-del-control-fiscal/

Megías , D., MAS, J., Bain, M., Gallego, M., Martínez, M., & Ruis, J. (2004). *Aspectos legales y de explotación del software libre.* (F. p. Catalunya, Ed.) Eureca Media, SL. XP08/M2114/00341. Obtenido de http://softlibre.unizar.es/manuales/legal/908.pdf

Mendoza, A., & Cardero, L. (Mayo de 2020). AUDAT 2.0: Sistema de auditoría de datos para la Contraloría General de la República. *Cuba: Serie Científica de la Universidad de las Ciencias Informáticas, Vol. 13 (No. 5)*, pp. 25-40. ISSN: 2306-2495, RNPS: 2343. Obtenido de https://publicaciones.uci.cu/index.php/serie/article/view/567/468

Microsoft . (2019). *SQL Server technical documentation.* Obtenido de https://docs.microsoft.com/en-us/sql/sql-server/?view=sql-server-ver15

Ministerio de Hacienda y Administraciones Públicas. (2012). MAGERIT – versión 3.0.

En *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Libro II - Catálogo de Elementos.* Madrid, España: Secretaría General Técnica, colección administración electrónica. NIPO: 630-12-171-8.

Ministerio de Justicia. (1997). *Código Penal.* La Paz: Gaceta Oficial de Bolivia.

Moor, J. (Agosto de 2007). hat Is Computer Ethics? *Metaphilosophy, Vol. 16*, pp. 226-275. doi:10.1111/j.1467-9973.1985.tb00173.x

Muñoz Razo, C. (2002). *Auditoría en sistemas computacionales* (1ra ed.). Mexico: Red Tercer Milenio. ISBN 978-607-733-137-7.

Nevado Cabello, V. (2010). *Introducción a las bases de datos relacionales.* Madrid: Vision Libros. ISBN: 978-84-9886-809-8.

Noreen, Z., Hameed, I., & Usman, A. (2009). *Development of database auditing infrastructure* (Vol. 78). USA: In Proceedings of the 7th International Conference on Frontiers of Information Technology (FIT '09). doi:10.1145/1838002.1838092

Open Source Initiative. (2007). *Definición de Código Abierto.* Obtenido de https://opensource.org/osd

Oracle y/o sus afiliados. (6 de Noviembre de 2020). *MySQL Server.* Obtenido de MySQL 8.0 Reference Manual: https://dev.mysql.com/doc/refman/8.0/en/

Organización Internacional de Normalización. (Diciembre de 2009). *ISO/IEC 15408-1 Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model* (3th ed.). ICS: 35.030 IT Security. Obtenido de https://www.iso.org/obp/ui/#iso:std:iso-iec:15408:-1:ed-3:v2:en

Organización Internacional de Normalización. (Febrero de 2018). *ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary* (5th ed.). ICS: 35.030 IT Security. Obtenido de https://www.iso.org/standard/73906.html

Organización Internacional de Normalización. (Junio de 2005). *ISO/IEC 17799 Information technology - Security techniques - Code of practice for information security management* (2th ed.). ICS : 35.030 IT Security. Obtenido de https://www.iso.org/standard/39612.html

Perez, J., Sharma, A., Dodwal, K., & D'Alessandro, S. (Mayo de 2015). *Oracle.* Oracle Database 12c: "Auditoría Unificada (Unified Auditing)". Obtenido de https://www.oracle.com/lad/technical-resources/articles/idm/unified-audit-database-12c.html

Piattini Velthuis, M., Del Peso Navarro, E., & Del Peso Ruiz, M. (2008). *Auditoría de Tecnologías y Sistemas de Información.* Madrid: RA-MA Editorial. ISBN: 978-84-7897-849-6.

Piñeiro, J. (2013). *Base datos relaciones y modelado de datos.* España: Ediciones Paraninfo S. A. ISBN 13: 978-84-283-3356-6.

Por Igual Más. (26 de Febrero de 2014). *Diferencia entre Convención, Ley, Tratado, Decreto, Ordenza y otros.* Obtenido de https://www.porigualmas.org/articles/270/diferencia-entre-convenci-n-ley-tratado-decreto-ordenanza-y-otros

PostgreSQL. (24 de Septiembre de 2020). *PostgreSQL 13.0 Documentation. The PostgreSQL Global Development Group.* Obtenido de https://www.postgresql.org/docs/13/index.html

Postigo, A. (2020). *Seguridad Informática* (1ra ed.). Madrid: Ediciones Paraninfo S. A. ISBN: 978-84-283-4455-5.

Riggs, S., Menon-Sen, A., & Barwick, I. (2017). *PGAudit - PostgreSQL Audit Extension. 2ndQuadrant y PGAudit Project.* Obtenido de https://www.pgaudit.org

Ruíz Bolívar, C. (2015). Instrumentos y Tecnicas de Investigación Educativa, Instrumentos y Tecnicas de Investigación Educativa. *DANAGA Training and Consulting*. Obtenido de https://www.academia.edu/37886948/Instrumentos_y_Tecnicas_de_Investigaci%C3%B3n_Educativa_Carlos_Ruiz_Bolivar_pdf

Rus, I. (2015). Technologies and Methods for Auditing Databases. Rumania: Procedia Economics and Finance, Vol. 26, pp. 991-999. doi:10.1016/S2212-5671(15)00921-1

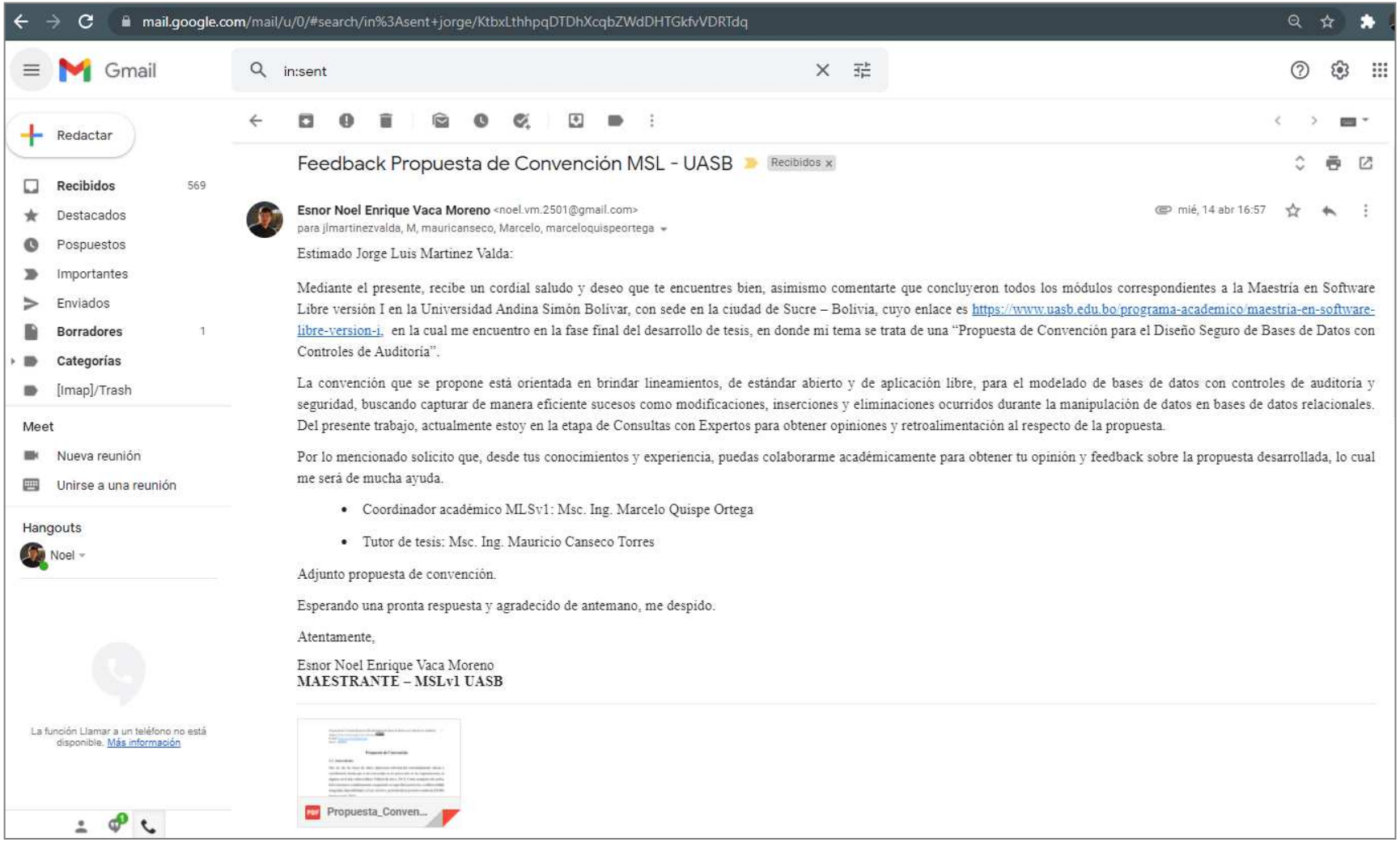
Sandoval, H. (2012). *Introducción a la Auditoría* (1ra ed.). México: Red Tercer Milenio S.C. ISBN 978-607-733-137-7.

Villalobos Murillo, J. (2008). *Auditando en las Bases de Datos* (Vols. 22, pp. 135-140). Heredia, Costa Rica: Uniciencia. ISSN-E 2215-3470. Obtenido de https://dialnet.unirioja.es/descarga/articulo/5381374.pdf

Woo, J., Lee, S., & Zoltowski, C. (2020). Database Auditing. Obtenido de https://www.semanticscholar.org/paper/1-Database-Auditing-Woo-Sael/8b17a1c311a6f06d159f9b4de18a5fc4edeba91a

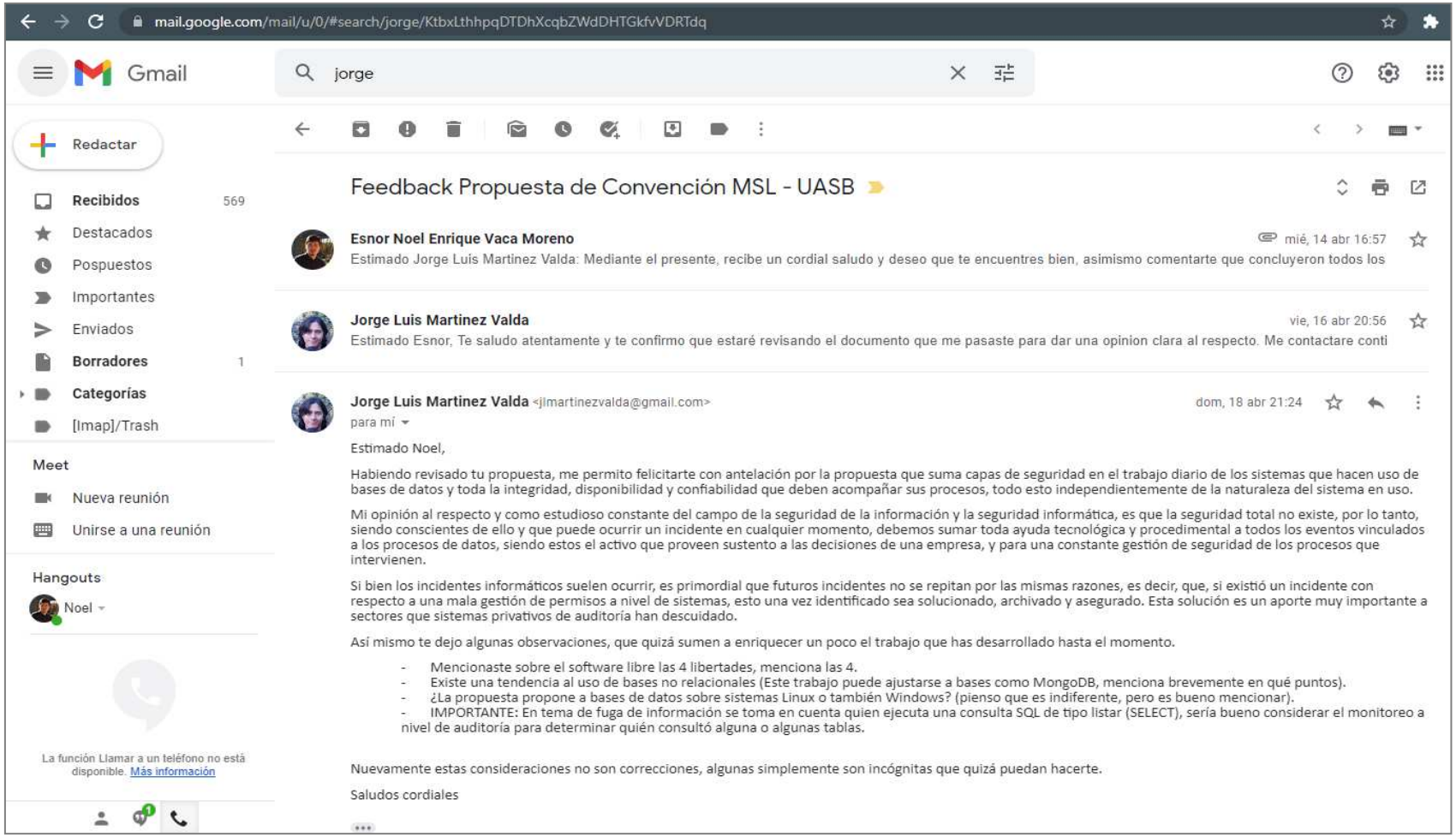
# ANEXOS

## Anexo 1. Formato del primer Correo Electrónico Enviado en la Consulta a Expertos



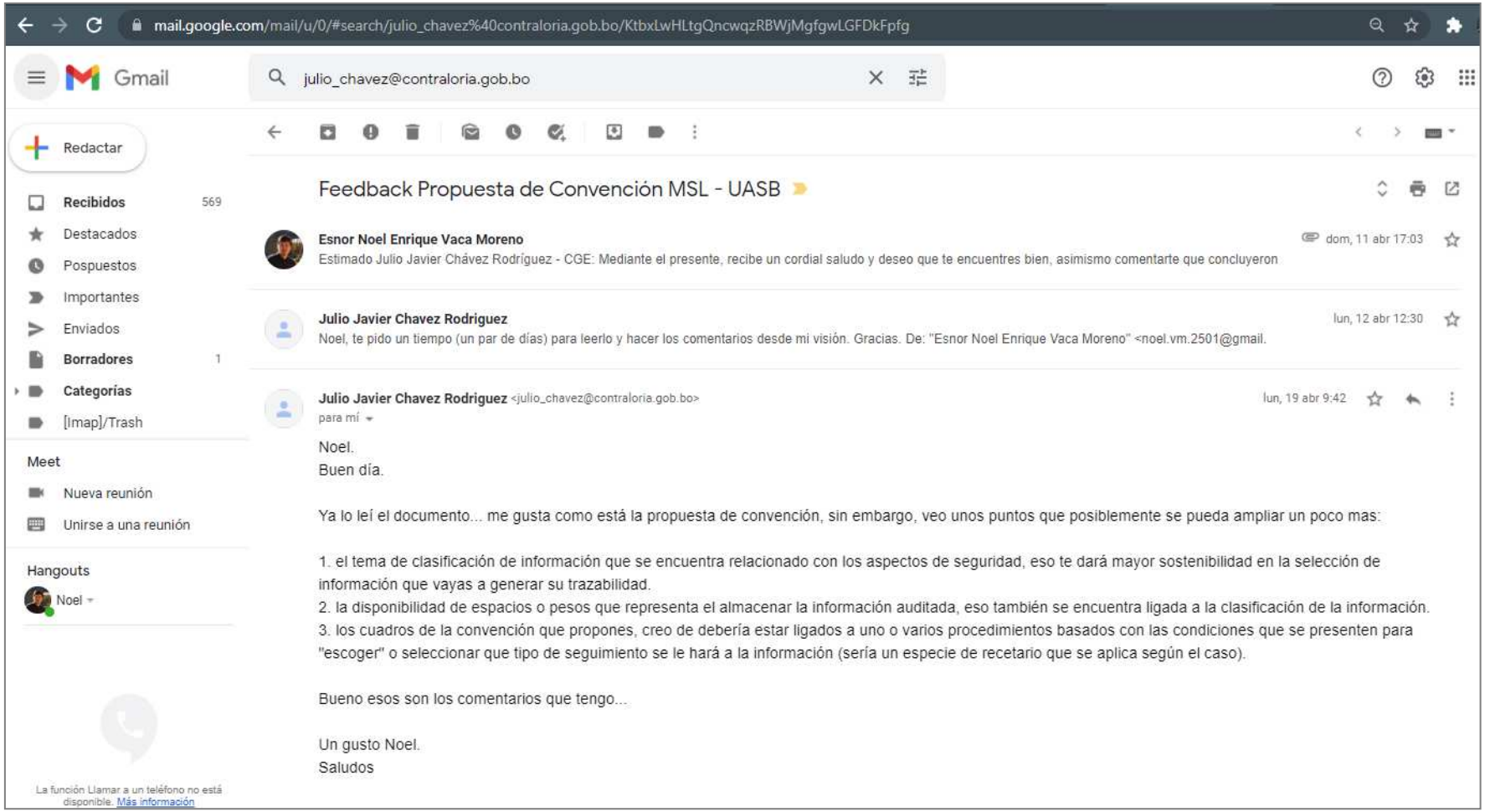
## Anexo 2. Respuesta Consulta Experto: Jorge Luis Martínez Valda

## Sucre – Bolivia



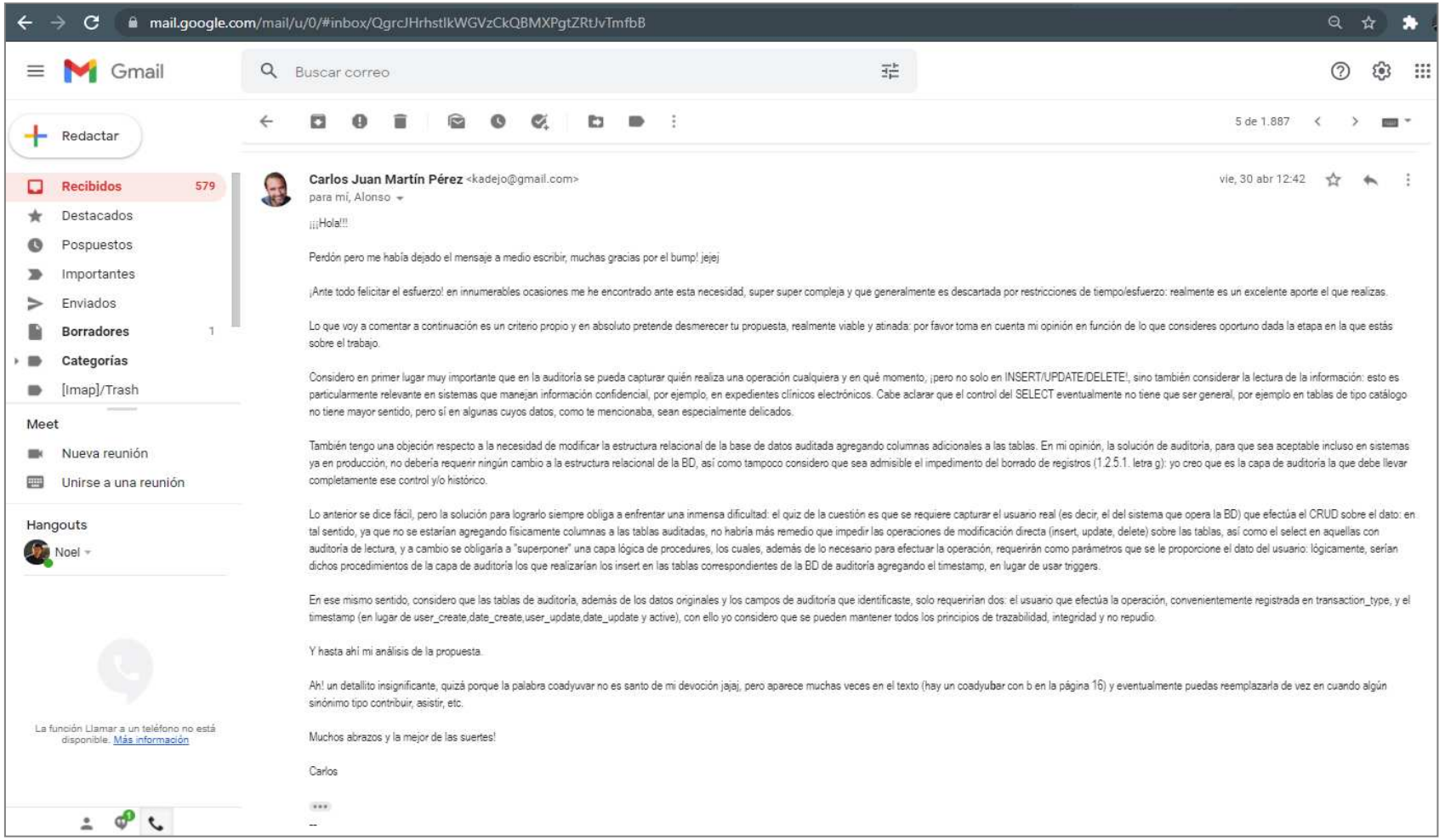
**Respuesta Consulta a Experto: Julio Javier Chávez Rodríguez**

**La Paz - Bolivia**



**Respuesta Consulta a Experto: Carlos Juan Martin Pérez**

**San Salvador – El Salvador**



**Respuesta Consulta a Experto: Rafael Hugo Poppe Aviles**

**Sucre – Bolivia**

## PROPUESTA DE CONVENCIÓN PARA EL DISEÑO SEGURO DE BASES DE DATOS CON CONTROLES DE AUDITORÍA

El objetivo principal para el desarrollo de una auditoria de Base de Datos es la de permitir registrar los accesos, así como monitorearlos además de tener la virtud de demostrar, asegurar y medir los mismos, para que con todo ellos se pueda determinar quién fue el que accedió a los datos, desde que dispositivo se llegó a acceder, cual fue la instrucción utilizada y cuál fue el efecto que ocasiono este acceso dentro la base de datos, entre otros.

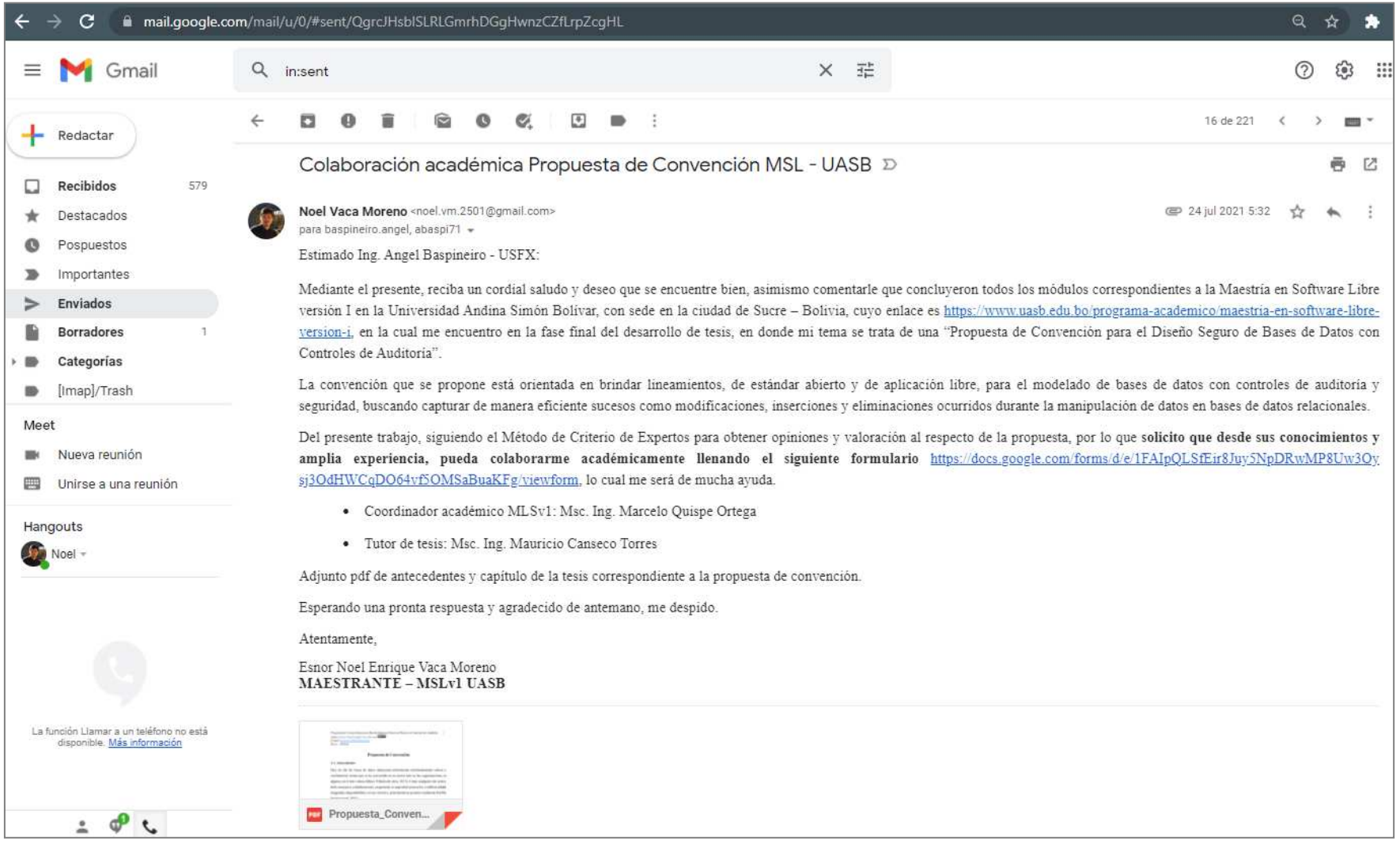
Revisando el documento puesto a consideración cumple con todos los aspectos necesarios que debería contener los controles de auditoria dentro de una base de datos, se vio de manera positiva la sugerencia de estandarización de dichos controles y la estructura que deberá contener las tablas de auditoria ya que proveen información rica y detallada sobre el manejo de la información, además de ofrecer todos los mecanismos de seguridad necesarios para resguardar la integridad de los mismos.

La disposición de la información y el relacionamiento ordenado con la tabla de auditoria proporcionaría una información detallada sobre los cambios realizados en la información y quien realizo dicho cambio y desde que dispositivo.

Dicho trabajo se encuentra realizado tomando en cuenta los estándares internacionales de control y auditoría.

En conclusión, todos los aspectos descritos en el presente trabajo de acuerdo a mi opinión personal, coadyuvaría a facilitar de forma segura y ordenada el proceso de auditoría, dicha propuesta contempla todos los aspectos necesarios que debería tener cualquier Base de Datos, Dispone de mecanismos que permiten tener trazas completas de auditorías de forma automática relacionadas con el acceso a las bases de datos, además de reducir los riesgos por el manejo inadecuado de los datos, es sin duda un análisis correcto y detallado a los requerimientos que debería contener cada Base de datos con respecto a un diseño seguro de las mismas.

## Anexo 3. Formato del segundo Correo Electrónico Enviado en la Consulta a Expertos



## Anexo 4. Tabulación de resultados del instrumento de validez de contenido

| Nº | Cuestiones | Indicadores | Juez 1 | Juez 2 | Juez 3 | Juez 4 | Juez 5 | Juez 6 | Juez 7 | Juez 8 | Juez 9 | Juez 10 | Juez 11 | Juez 12 | Juez 13 | Juez 14 | Juez 15 | Juez 16 | Media Indicador | Media | Varianza Indicador | Varianza | Desv. Est. Indicador | Desv. Est. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | La propuesta de convención considera controles de auditoría en bases de datos relacionales. | Claridad | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 4,63 | 4,56 | 0,234 | 0,340 | 0,484 | 0,583 |
| | | Contexto | 4 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 3 | 4 | 4,44 | | 0,371 | | 0,609 | |
| | | Coherencia | 4 | 4 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 3 | 4 | 4,50 | | 0,375 | | 0,612 | |
| | | Relevancia | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 4 | 5 | 5 | 5 | 4 | 4 | 4,69 | | 0,340 | | 0,583 | |
| 2 | Considera que los campos de auditoría en las tablas son los mínimos requeridos. | Claridad | 5 | 5 | 5 | 4 | 5 | 5 | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 3 | 4 | 4,63 | 4,61 | 0,359 | 0,332 | 0,599 | 0,576 |
| | | Contexto | 4 | 5 | 5 | 4 | 4 | 5 | 4 | 5 | 5 | 3 | 4 | 5 | 5 | 5 | 4 | 4 | 4,44 | | 0,371 | | 0,609 | |
| | | Coherencia | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 3 | 4 | 4,69 | | 0,340 | | 0,583 | |
| | | Relevancia | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4,69 | | 0,215 | | 0,464 | |
| 3 | Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría. | Claridad | 5 | 3 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4,50 | 4,45 | 0,375 | 0,373 | 0,612 | 0,611 |
| | | Contexto | 4 | 3 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4,44 | | 0,371 | | 0,609 | |
| | | Coherencia | 4 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 4 | 4 | 4,44 | | 0,371 | | 0,609 | |
| | | Relevancia | 4 | 3 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4,44 | | 0,371 | | 0,609 | |
| 4 | Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal. | Claridad | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4,94 | 4,81 | 0,059 | 0,184 | 0,242 | 0,428 |
| | | Contexto | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 4,75 | | 0,188 | | 0,433 | |
| | | Coherencia | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 4,81 | | 0,152 | | 0,390 | |
| | | Relevancia | 3 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4,75 | | 0,313 | | 0,559 | |
| 5 | La estructura de auditoría planteada posibilita la reconstrucción de información. | Claridad | 4 | 5 | 5 | 4 | 4 | 5 | 4 | 4 | 5 | 3 | 4 | 5 | 5 | 5 | 3 | 4 | 4,31 | 4,41 | 0,465 | 0,460 | 0,682 | 0,678 |
| | | Contexto | 4 | 5 | 5 | 4 | 4 | 5 | 4 | 4 | 5 | 3 | 5 | 5 | 5 | 5 | 4 | 4 | 4,44 | | 0,371 | | 0,609 | |
| | | Coherencia | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 3 | 4 | 5 | 5 | 5 | 3 | 4 | 4,44 | | 0,496 | | 0,704 | |
| | | Relevancia | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 3 | 4 | 5 | 5 | 5 | 3 | 4 | 4,44 | | 0,496 | | 0,704 | |
| 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. | Claridad | 2 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 5 | 5 | 5 | 4 | 2 | 4,25 | 4,25 | 1,188 | 1,094 | 1,090 | 1,046 |
| | | Contexto | 3 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 5 | 5 | 5 | 3 | 2 | 4,25 | | 1,063 | | 1,031 | |
| | | Coherencia | 3 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 5 | 5 | 5 | 3 | 2 | 4,25 | | 1,063 | | 1,031 | |
| | | Relevancia | 2 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 4 | 5 | 5 | 5 | 4 | 2 | 4,25 | | 1,063 | | 1,031 | |
| 7 | La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales. | Claridad | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 3 | 5 | 4,63 | 4,59 | 0,359 | 0,272 | 0,599 | 0,522 |
| | | Contexto | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | 4,63 | | 0,234 | | 0,484 | |
| | | Coherencia | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 4 | 5 | 4,56 | | 0,246 | | 0,496 | |
| | | Relevancia | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | 4,56 | | 0,246 | | 0,496 | |
| 8 | La propuesta facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría. | Claridad | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 3 | 5 | 4 | 5 | 4 | 4 | 3 | 4,50 | 4,48 | 0,500 | 0,406 | 0,707 | 0,637 |
| | | Contexto | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 5 | 4 | 4 | 3 | 4,50 | | 0,375 | | 0,612 | |
| | | Coherencia | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 4 | 4 | 3 | 4,44 | | 0,371 | | 0,609 | |
| | | Relevancia | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 4 | 4 | 3 | 4,50 | | 0,375 | | 0,612 | |
| 9 | Las recomendaciones de restricciones de acceso a la BD y a la auditoría aumentan el nivel de seguridad. | Claridad | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 3 | 5 | 4,75 | 4,73 | 0,313 | 0,226 | 0,559 | 0,476 |
| | | Contexto | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 4,75 | | 0,188 | | 0,433 | |
| | | Coherencia | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 4,75 | | 0,188 | | 0,433 | |
| | | Relevancia | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 4 | 5 | 4,69 | | 0,215 | | 0,464 | |
| 10 | Es posible contar con un historial de cambios de cada registro. | Claridad | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 3 | 4 | 4,63 | 4,53 | 0,359 | 0,374 | 0,599 | 0,612 |
| | | Contexto | 4 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 4 | 4 | 4,56 | | 0,246 | | 0,496 | |
| | | Coherencia | 4 | 5 | 5 | 4 | 5 | 5 | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 3 | 4 | 4,50 | | 0,375 | | 0,612 | |
| | | Relevancia | 3 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 3 | 4 | 4,44 | | 0,496 | | 0,704 | |
| 11 | La propuesta contribuye en el aseguramiento de la integridad de los datos. | Claridad | 3 | 4 | 5 | 4 | 5 | 4 | 5 | 5 | 5 | 3 | 4 | 5 | 5 | 4 | 2 | 5 | 4,25 | 4,33 | 0,813 | 0,720 | 0,901 | 0,849 |
| | | Contexto | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 4 | 5 | 5 | 4 | 3 | 5 | 4,44 | | 0,496 | | 0,704 | |
| | | Coherencia | 4 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 4 | 5 | 5 | 4 | 2 | 5 | 4,38 | | 0,734 | | 0,857 | |
| | | Relevancia | 3 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 3 | 4 | 5 | 5 | 4 | 2 | 5 | 4,25 | | 0,813 | | 0,901 | |
| 12 | Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente la propuesta en bases de datos existentes. | Claridad | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 4 | 4 | 4,69 | 4,56 | 0,215 | 0,340 | 0,464 | 0,583 |
| | | Contexto | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 | 4 | 5 | 5 | 3 | 4 | 4,50 | | 0,500 | | 0,707 | |
| | | Coherencia | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 4 | 4 | 5 | 4 | 4 | 4,50 | | 0,250 | | 0,500 | |
| | | Relevancia | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 3 | 5 | 5 | 5 | 4 | 4 | 5 | 4 | 4 | 4,56 | | 0,371 | | 0,609 | |
| | | **Promedio** | **4,06** | **4,73** | **4,92** | **4,40** | **4,79** | **4,96** | **4,83** | **4,75** | **4,92** | **3,85** | **4,23** | **4,67** | **4,92** | **4,75** | **3,58** | **4,08** | **4,53** | **4,53** | | **0,450** | | **0,671** |
| | | **Suma** | **195** | **227** | **236** | **211** | **230** | **238** | **232** | **228** | **236** | **185** | **203** | **224** | **236** | **228** | **172** | **196** | | | | | | |

Fuente: Elaboración propia Enlace de visualización de datos (hoja Tabulación): https://bit.ly/3g16rRg

# Anexo 5. Instrumento de validez de contenido: V de Aiken

| N° | Cuestiones | Indicadores | Juez 1 | Juez 2 | Juez 3 | Juez 4 | Juez 5 | Juez 6 | Juez 7 | Juez 8 | Juez 9 | Juez 10 | Juez 11 | Juez 12 | Juez 13 | Juez 14 | Juez 15 | Juez 16 | V de Aiken | Promedio V de Aiken |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | La propuesta de convención considera controles de auditoría en bases de datos relacionales. | Claridad | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,91 | 0,89 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,86 | |
| | | Coherencia | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,88 | |
| | | Relevancia | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,92 | |
| 2 | Considera que los campos de auditoría en las tablas son los mínimos requeridos. | Claridad | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,91 | 0,90 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,86 | |
| | | Coherencia | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,92 | |
| | | Relevancia | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,92 | |
| 3 | Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría. | Claridad | 1,00 | 0,50 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 0,88 | 0,86 |
| | | Contexto | 0,75 | 0,50 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 0,86 | |
| | | Coherencia | 0,75 | 0,50 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 0,86 | |
| | | Relevancia | 0,75 | 0,50 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 0,86 | |
| 4 | Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal. | Claridad | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,98 | 0,95 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,94 | |
| | | Coherencia | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,95 | |
| | | Relevancia | 0,50 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,94 | |
| 5 | La estructura de auditoría planteada posibilita la reconstrucción de información. | Claridad | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,83 | 0,85 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 1,00 | 0,50 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,86 | |
| | | Coherencia | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,86 | |
| | | Relevancia | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 0,86 | |
| 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. | Claridad | 0,25 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,50 | 1,00 | 1,00 | 1,00 | 0,75 | 0,25 | 0,81 | 0,81 |
| | | Contexto | 0,50 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,50 | 1,00 | 1,00 | 1,00 | 0,50 | 0,25 | 0,81 | |
| | | Coherencia | 0,50 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,50 | 1,00 | 1,00 | 1,00 | 0,50 | 0,25 | 0,81 | |
| | | Relevancia | 0,25 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,25 | 0,81 | |
| 7 | La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales. | Claridad | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 0,50 | 1,00 | 0,91 | 0,90 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 0,91 | |
| | | Coherencia | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 0,75 | 1,00 | 0,75 | 1,00 | 0,89 | |
| | | Relevancia | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 0,89 | |
| 8 | La propuesta facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría. | Claridad | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 1,00 | 0,75 | 1,00 | 0,75 | 0,75 | 0,50 | 0,88 | 0,87 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,75 | 1,00 | 0,75 | 0,75 | 0,50 | 0,88 | |
| | | Coherencia | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 0,50 | 0,86 | |
| | | Relevancia | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 0,50 | 0,88 | |
| 9 | Las recomendaciones de restricciones de acceso a la BD y a la auditoría aumentan el nivel de seguridad. | Claridad | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 1,00 | 0,94 | 0,93 |
| | | Contexto | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,94 | |
| | | Coherencia | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,94 | |
| | | Relevancia | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 0,92 | |
| 10 | Es posible contar con un historial de cambios de cada registro. | Claridad | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,50 | 0,75 | 0,91 | 0,88 |
| | | Contexto | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 0,75 | 0,89 | |
| | | Coherencia | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,50 | 0,75 | 0,88 | |
| | | Relevancia | 0,50 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 0,50 | 0,75 | 0,86 | |
| 11 | La propuesta contribuye en el aseguramiento de la integridad de los datos. | Claridad | 0,50 | 0,75 | 1,00 | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 0,75 | 0,25 | 1,00 | 0,81 | 0,83 |
| | | Contexto | 0,75 | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 0,75 | 0,50 | 1,00 | 0,86 | |
| | | Coherencia | 0,75 | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 0,75 | 1,00 | 1,00 | 0,75 | 0,25 | 1,00 | 0,84 | |
| | | Relevancia | 0,50 | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,50 | 0,75 | 1,00 | 1,00 | 0,75 | 0,25 | 1,00 | 0,81 | |
| 12 | Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente la propuesta en bases de datos existentes. | Claridad | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 0,92 | 0,89 |
| | | Contexto | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 1,00 | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 0,50 | 0,75 | 0,88 | |
| | | Coherencia | 0,75 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 0,88 | |
| | | Relevancia | 1,00 | 1,00 | 0,75 | 1,00 | 1,00 | 1,00 | 1,00 | 0,50 | 1,00 | 1,00 | 1,00 | 0,75 | 0,75 | 1,00 | 0,75 | 0,75 | 0,89 | |
| | | Promedio por Juez: | **0,77** | **0,93** | **0,98** | **0,85** | **0,95** | **0,99** | **0,96** | **0,94** | **0,98** | **0,71** | **0,81** | **0,92** | **0,98** | **0,94** | **0,65** | **0,77** | **0,88** | **0,88** |

Fuente: Elaboración propia, Enlace de visualización de datos (hoja V Aiken): https://bit.ly/3g16rRg

## Anexo 6. Confiabilidad del Instrumento en el Criterio de Expertos: Alfa de Cronbach

| Juez / Experto | Pregunta 1 | | | | Pregunta 2 | | | | Pregunta 3 | | | | Pregunta 4 | | | | Pregunta 5 | | | | Pregunta 6 | | | | Pregunta 7 | | | | Pregunta 8 | | | | Pregunta 9 | | | | Pregunta 10 | | | | Pregunta 11 | | | | Pregunta 12 | | | | Suma | Promedio |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | CL | CT | CH | RV | | |
| | Item 1 | Item 2 | Item 3 | Item 4 | Item 5 | Item 6 | Item 7 | Item 8 | Item 9 | Item 10 | Item 11 | Item 12 | Item 13 | Item 14 | Item 15 | Item 16 | Item 17 | Item 18 | Item 19 | Item 20 | Item 21 | Item 22 | Item 23 | Item 24 | Item 25 | Item 26 | Item 27 | Item 28 | Item 29 | Item 30 | Item 31 | Item 32 | Item 33 | Item 34 | Item 35 | Item 36 | Item 37 | Item 38 | Item 39 | Item 40 | Item 41 | Item 42 | Item 43 | Item 44 | Item 45 | Item 46 | Item 47 | Item 48 | | |
| Juez 1 | 5 | 4 | 4 | 5 | 5 | 4 | 5 | 4 | 5 | 4 | 4 | 4 | 5 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 2 | 3 | 3 | 2 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 3 | 3 | 4 | 4 | 3 | 5 | 4 | 4 | 5 | 195 | 4,063 |
| Juez 2 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 3 | 3 | 3 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 227 | 4,729 |
| Juez 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 236 | 4,917 |
| Juez 4 | 4 | 4 | 4 | 5 | 4 | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 211 | 4,396 |
| Juez 5 | 4 | 4 | 4 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 230 | 4,792 |
| Juez 6 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 238 | 4,958 |
| Juez 7 | 5 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 232 | 4,833 |
| Juez 8 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 3 | 4 | 3 | 228 | 4,750 |
| Juez 9 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 4 | 5 | 236 | 4,917 |
| Juez 10 | 4 | 4 | 4 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 3 | 3 | 3 | 5 | 5 | 5 | 5 | 185 | 3,854 |
| Juez 11 | 4 | 4 | 5 | 4 | 5 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 203 | 4,229 |
| Juez 12 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 224 | 4,667 |
| Juez 13 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 236 | 4,917 |
| Juez 14 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 228 | 4,750 |
| Juez 15 | 4 | 3 | 3 | 4 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 5 | 4 | 4 | 5 | 3 | 4 | 3 | 3 | 4 | 3 | 3 | 4 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 3 | 4 | 3 | 3 | 2 | 3 | 2 | 2 | 4 | 3 | 4 | 4 | 172 | 3,583 |
| Juez 16 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 2 | 2 | 2 | 2 | 5 | 5 | 5 | 5 | 3 | 3 | 3 | 3 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 4 | 4 | 4 | 4 | 196 | 4,083 |
| Varianza | 0,23 | 0,37 | 0,38 | 0,34 | 0,36 | 0,37 | 0,34 | 0,21 | 0,38 | 0,37 | 0,37 | 0,37 | 0,06 | 0,19 | 0,15 | 0,31 | 0,46 | 0,37 | 0,50 | 0,50 | 1,19 | 1,06 | 1,06 | 1,06 | 0,36 | 0,23 | 0,25 | 0,25 | 0,50 | 0,38 | 0,37 | 0,38 | 0,31 | 0,19 | 0,19 | 0,21 | 0,36 | 0,25 | 0,38 | 0,50 | 0,81 | 0,50 | 0,73 | 0,81 | 0,21 | 0,50 | 0,25 | 0,37 | 407,09 | 0,423 |

| Consistencia y confiabilidad: Alfa de Cronbach | |
|---|---|
| α (Alfa) = | 0,91 |
| K (número de ítems) = | 12 |
| Vi (varianza de cada ítem) = | 4,30 |
| Vt (varianza total) = | 25,44 |

Según Ruíz Bolívar (2015)
0 - 0.19 -> Muy baja
0.2 - 0.39 -> Baja
0.4 - 0.59 -> Moderada
0.6 - 0.79 - > Buena
0.8 - 1.00 -> Muy Buena

Según Herrera (1998)
0,53 a menos Confiabilidad nula
0,54 a 0,59 Confiabilidad baja
0,60 a 0,65 Confiable
0,66 a 0,71 Muy Confiable
0,72 a 0,99 Excelente confiabilidad
1.0 Confiabilidad perfecta

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\Sigma Vi}{Vt}\right]$$

| Juez / Experto | Item 1 | Item 2 | Item 3 | Item 4 | Item 5 | Item 6 | Item 7 | Item 8 | Item 9 | Item 10 | Item 11 | Item 12 | Suma |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Juez 1 | 4,5 | 4,5 | 4,25 | 4 | 4 | 2,5 | 4,25 | 4 | 5 | 3,75 | 3,5 | 4,5 | 48,75 |
| Juez 2 | 4,75 | 5 | 3 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 56,75 |
| Juez 3 | 5 | 5 | 5 | 5 | 5 | 4,75 | 5 | 5 | 5 | 5 | 5 | 4,25 | 59,00 |
| Juez 4 | 4,25 | 4,5 | 4,75 | 4,5 | 4,5 | 4 | 4,25 | 4,5 | 4,5 | 4,25 | 4 | 4,75 | 52,75 |
| Juez 5 | 4,25 | 4,75 | 4,75 | 5 | 4,5 | 5 | 5 | 5 | 4,75 | 4,5 | 5 | 5 | 57,50 |
| Juez 6 | 4,75 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4,75 | 5 | 59,50 |
| Juez 7 | 5 | 4,5 | 5 | 5 | 4 | 5 | 4,75 | 5 | 5 | 4,75 | 5 | 5 | 58,00 |
| Juez 8 | 5 | 5 | 4,75 | 5 | 4 | 5 | 4,75 | 5 | 5 | 5 | 5 | 3,5 | 57,00 |
| Juez 9 | 5 | 4,75 | 5 | 5 | 5 | 5 | 5 | 5 | 4,75 | 5 | 4,75 | 4,75 | 59,00 |
| Juez 10 | 3,75 | 3,75 | 4 | 5 | 3 | 3 | 4 | 3,75 | 4 | 4 | 3 | 5 | 46,25 |
| Juez 11 | 4,25 | 4,5 | 4 | 4 | 4,25 | 3,25 | 4 | 4,5 | 4 | 5 | 4 | 5 | 50,75 |
| Juez 12 | 5 | 5 | 4 | 5 | 5 | 5 | 4 | 4 | 5 | 5 | 5 | 4 | 56,00 |
| Juez 13 | 5 | 5 | 4,75 | 5 | 5 | 5 | 4,75 | 5 | 5 | 5 | 5 | 4,5 | 59,00 |
| Juez 14 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 4 | 4 | 5 | 57,00 |
| Juez 15 | 3,5 | 3,5 | 4 | 4,5 | 3,25 | 3,5 | 3,75 | 4 | 3,75 | 3,25 | 2,25 | 3,75 | 43,00 |
| Juez 16 | 4 | 4 | 4 | 5 | 4 | 2 | 5 | 3 | 5 | 4 | 5 | 4 | 49,00 |
| **Varianza** | **0,24** | **0,22** | **0,31** | **0,12** | **0,41** | **1,04** | **0,20** | **0,36** | **0,18** | **0,31** | **0,67** | **0,25** | **25,44** |

Fuente: Elaboración propia, Enlace de visualización de datos (hoja Alfa Cronbach): https://bit.ly/3g16rRg

**Anexo 7. Resumen de resultados del instrumento de validez por cuestiones.**

| N° | Cuestiones | Jueces (16) e Indicadores (4) ítems (48) | | | |
|---|---|---|---|---|---|
| | | Media | V de Aiken | Varianza | Desviación Estándar |
| 1 | La propuesta de convención considera controles de auditoría en bases de datos relacionales. | 4,56 | 0,89 | 0,340 | 0,583 |
| 2 | Considera que los campos de auditoría en las tablas son los mínimos requeridos. | 4,61 | 0,90 | 0,332 | 0,576 |
| 3 | Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoría. | 4,45 | 0,86 | 0,373 | 0,611 |
| 4 | Es recomendable que los datos de auditoría se almacenen de forma separada a la base de datos principal. | 4,81 | 0,95 | 0,184 | 0,428 |
| 5 | La estructura de auditoría planteada posibilita la reconstrucción de información. | 4,41 | 0,85 | 0,460 | 0,678 |
| 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. | 4,25 | 0,81 | 1,094 | 1,046 |
| 7 | La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoría de bases de datos relacionales. | 4,59 | 0,90 | 0,272 | 0,522 |
| 8 | La propuesta facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoría. | 4,48 | 0,87 | 0,406 | 0,637 |
| 9 | Las recomendaciones de restricciones de acceso a la BD y a la auditoría aumentan el nivel de seguridad. | 4,73 | 0,93 | 0,226 | 0,476 |
| 10 | Es posible contar con un historial de cambios de cada registro. | 4,53 | 0,88 | 0,374 | 0,612 |
| 11 | La propuesta contribuye en el aseguramiento de la integridad de los datos. | 4,33 | 0,83 | 0,720 | 0,849 |
| 12 | Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente la propuesta en bases de datos existentes. | 4,56 | 0,89 | 0,340 | 0,583 |
| | | **4,53** | **0,88** | **0,450** | **0,671** |

Fuente: Elaboración propia, Enlace de visualización de datos (hoja Resumen): https://bit.ly/3g16rRg

## Anexo 8. Resumen de resultado del instrumento de validez por jueces o expertos

| Expertos | Cuestiones (12) e Indicadores (4) Ítems (48) | | |
|---|---|---|---|
| | **Media** | **V de Aiken** | **Suma** |
| Juez 1 | 4,06 | 0,77 | 195 |
| Juez 2 | 4,73 | 0,93 | 227 |
| Juez 3 | 4,92 | 0,98 | 236 |
| Juez 4 | 4,40 | 0,85 | 211 |
| Juez 5 | 4,79 | 0,95 | 230 |
| Juez 6 | 4,96 | 0,99 | 238 |
| Juez 7 | 4,83 | 0,96 | 232 |
| Juez 8 | 4,75 | 0,94 | 228 |
| Juez 9 | 4,92 | 0,98 | 236 |
| Juez 10 | 3,85 | 0,71 | 185 |
| Juez 11 | 4,23 | 0,81 | 203 |
| Juez 12 | 4,67 | 0,92 | 224 |
| Juez 13 | 4,92 | 0,98 | 236 |
| Juez 14 | 4,75 | 0,94 | 228 |
| Juez 15 | 3,58 | 0,65 | 172 |
| Juez 16 | 4,08 | 0,77 | 196 |
| | **4,53** | **0,88** | **407,09** |
| | | | **Varianza** |

Fuente: Elaboración propia, Enlace de visualización de datos (hoja Resumen): https://bit.ly/3g16rRg

## Anexo 9. Modelo del instrumento cuestionario Criterio a Expertos

Enlace al cuestionario: https://bit.ly/3xGnXQL

# Criterio de Expertos

***** PROPUESTA DE CONVENCIÓN PARA EL DISEÑO SEGURO DE BASES DE DATOS CON CONTROLES DE AUDITORÍA *****

**Objetivo General de la investigación**: Proponer una convención de estándar abierto para modelar una base de datos con controles de auditoría y seguridad que permita realizar el registro de modificaciones, adiciones y eliminaciones de datos en las bases de datos relacionales.

**Instrumento**: Cuestionario de valoración de la propuesta de convención mediante Consulta con Expertos.

**Instrucciones**: En base al documento pdf enviado a su correo electrónico que contiene la propuesta de convención, mediante este instrumento como Experto Evaluador valore la pertinencia y fiabilidad del trabajo realizado. Deberá colocar la puntuación que considere adecuada a los diferentes enunciados de acuerdo a la siguiente escala:
**1**: Totalmente en desacuerdo, **2**: En desacuerdo, **3**: Indeciso/indecisa, **4**: De acuerdo, **5**: Totalmente de acuerdo

**Indicadores generales de evaluación**:
- Claridad: El ítem está formulado con un lenguaje apropiado, no genera contradicción.
- Contexto: El ítem esta en el marco de la temática abordada.
- Coherencia: El ítem mide alguna variable o relación con los indicadores.
- Relevancia: El ítem es relevante para cumplir con las preguntas y objetivos de investigación.

**Autor del instrumento**: Esnor Noel Enrique Vaca Moreno

*Obligatorio

Correo *

Tu dirección de correo electrónico

Nombres y Apellidos del experto *

Tu respuesta

Institución donde trabaja *

Tu respuesta

Ciudad - Pais *

Tu respuesta

Años de experiencia profesional o científica *

- ◯ 5 a 7 años
- ◯ 8 a 10 años
- ◯ Más de 10 años

1. La propuesta de convención considera controles de auditoria en bases de datos relacionales *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

2. Considera que los campos de auditoria en las tablas son los minimos requeridos *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

3. Considera que modificar la estructura de las tablas en nuevas bases de datos aportaría mayor información de auditoria *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

4. Es recomendable que los datos de auditoria se almacenen de forma separada a la base de datos principal *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

5. La estructura de auditoría planteada posibilita la reconstrucción de información *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

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 *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

7. La forma de captura datos mediante desencadenadores es un mecanismo válido para implementar auditoria de bases de datos relacionales *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

8. La propuesta facilita la obtención de backups de forma separada de la base de datos principal y de la base de datos de auditoria *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

9. Las recomendaciones de restricciones de acceso a la BD y a la auditoria aumentan el nivel de seguridad *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

10. Es posible contar con un historial de cambios de cada registro *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

11. La propuesta contribuye en el aseguramiento de la integridad de los datos. *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

12. Considera que es posible técnicamente que con las debidas precauciones y adecuaciones se implemente la propuesta en bases de datos existentes *

| | Totalmente en desacuerdo (1) | En desacuerdo (2) | Indeciso / indecisa (3) | De acuerdo (4) | Totalmente de acuerdo (5) |
|---|---|---|---|---|---|
| Claridad | ◯ | ◯ | ◯ | ◯ | ◯ |
| Contexto | ◯ | ◯ | ◯ | ◯ | ◯ |
| Coherencia | ◯ | ◯ | ◯ | ◯ | ◯ |
| Relevancia | ◯ | ◯ | ◯ | ◯ | ◯ |

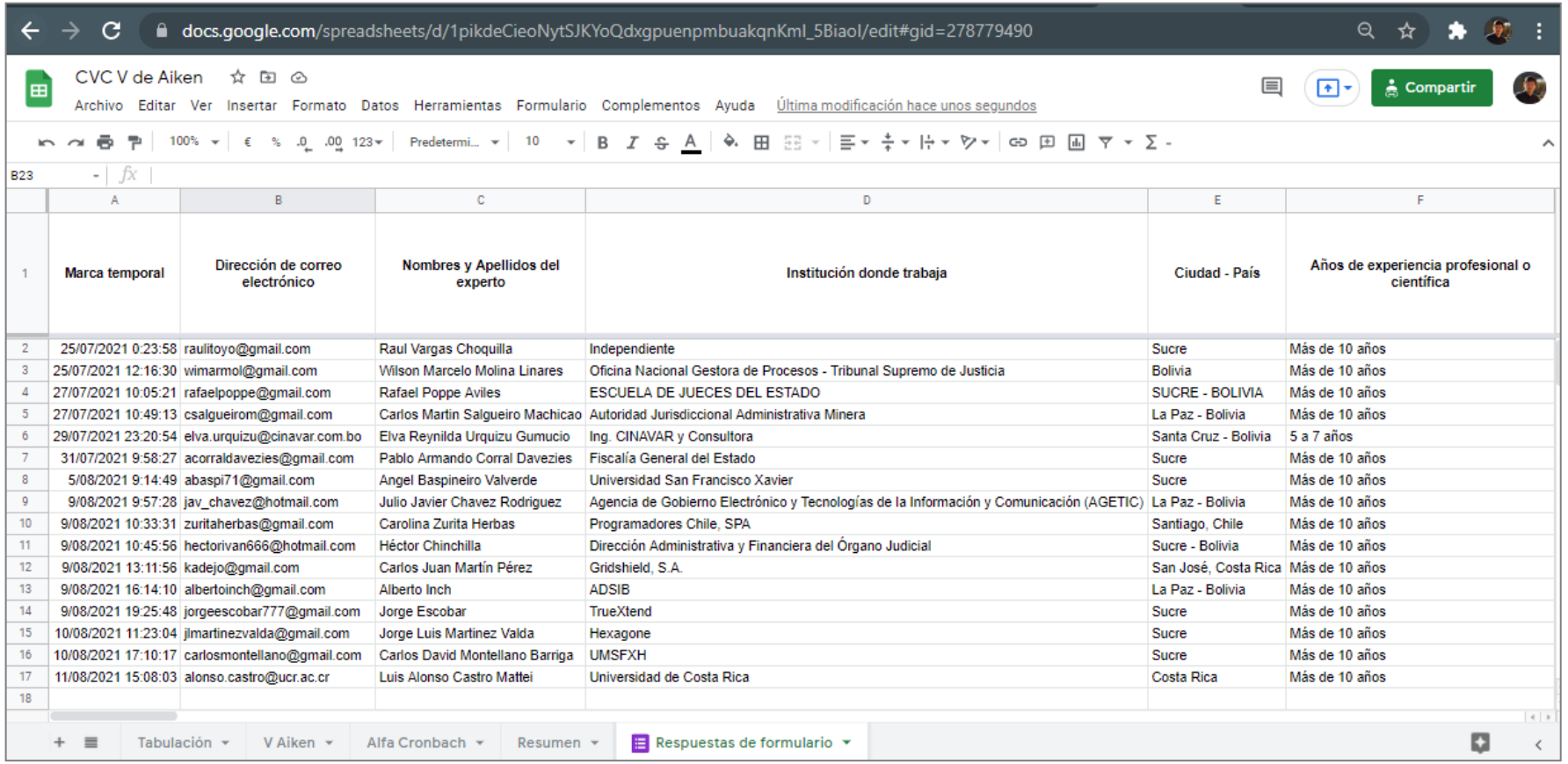
13. Opinión sobre la Propuesta de Convención para el Diseño Seguro de Bases de Datos con Controles de Auditoría *

Tu respuesta

Envíame una copia de mis respuestas.

Enviar

## Anexo 10. Lista de expertos que respondieron el instrumento cuestionario



docs.google.com/spreadsheets/d/1pikdeCieoNytSJKYoQdxgpuenpmbuakqnKml_5BiaoI/edit#gid=278779490

CVC V de Aiken

Archivo Editar Ver Insertar Formato Datos Herramientas Formulario Complementos Ayuda Última modificación hace unos segundos

Compartir

B23

| | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| 1 | Marca temporal | Dirección de correo electrónico | Nombres y Apellidos del experto | Institución donde trabaja | Ciudad - País | Años de experiencia profesional o científica |
| 2 | 25/07/2021 0:23:58 | raulitoyo@gmail.com | Raul Vargas Choquilla | Independiente | Sucre | Más de 10 años |
| 3 | 25/07/2021 12:16:30 | wimarmol@gmail.com | Wilson Marcelo Molina Linares | Oficina Nacional Gestora de Procesos - Tribunal Supremo de Justicia | Bolivia | Más de 10 años |
| 4 | 27/07/2021 10:05:21 | rafaelpoppe@gmail.com | Rafael Poppe Aviles | ESCUELA DE JUECES DEL ESTADO | SUCRE - BOLIVIA | Más de 10 años |
| 5 | 27/07/2021 10:49:13 | csalgueirom@gmail.com | Carlos Martin Salgueiro Machicao | Autoridad Jurisdiccional Administrativa Minera | La Paz - Bolivia | Más de 10 años |
| 6 | 29/07/2021 23:20:54 | elva.urquizu@cinavar.com.bo | Elva Reynilda Urquizu Gumucio | Ing. CINAVAR y Consultora | Santa Cruz - Bolivia | 5 a 7 años |
| 7 | 31/07/2021 9:58:27 | acorraldavezies@gmail.com | Pablo Armando Corral Davezies | Fiscalía General del Estado | Sucre | Más de 10 años |
| 8 | 5/08/2021 9:14:49 | abaspi71@gmail.com | Angel Baspineiro Valverde | Universidad San Francisco Xavier | Sucre | Más de 10 años |
| 9 | 9/08/2021 9:57:28 | jav_chavez@hotmail.com | Julio Javier Chavez Rodriguez | Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC) | La Paz - Bolivia | Más de 10 años |
| 10 | 9/08/2021 10:33:31 | zuritaherbas@gmail.com | Carolina Zurita Herbas | Programadores Chile, SPA | Santiago, Chile | Más de 10 años |
| 11 | 9/08/2021 10:45:56 | hectorivan666@hotmail.com | Héctor Chinchilla | Dirección Administrativa y Financiera del Órgano Judicial | Sucre - Bolivia | Más de 10 años |
| 12 | 9/08/2021 13:11:56 | kadejo@gmail.com | Carlos Juan Martín Pérez | Gridshield, S.A. | San José, Costa Rica | Más de 10 años |
| 13 | 9/08/2021 16:14:10 | albertoinch@gmail.com | Alberto Inch | ADSIB | La Paz - Bolivia | Más de 10 años |
| 14 | 9/08/2021 19:25:48 | jorgeescobar777@gmail.com | Jorge Escobar | TrueXtend | Sucre | Más de 10 años |
| 15 | 10/08/2021 11:23:04 | jlmartinezvalda@gmail.com | Jorge Luis Martinez Valda | Hexagone | Sucre | Más de 10 años |
| 16 | 10/08/2021 17:10:17 | carlosmontellano@gmail.com | Carlos David Montellano Barriga | UMSFXH | Sucre | Más de 10 años |
| 17 | 11/08/2021 15:08:03 | alonso.castro@ucr.ac.cr | Luis Alonso Castro Mattei | Universidad de Costa Rica | Costa Rica | Más de 10 años |
| 18 | | | | | | |

Tabulación | V Aiken | Alfa Cronbach | Resumen | Respuestas de formulario

Enlace de visualización de datos (hoja Respuestas de formulario): https://bit.ly/3g16rRg