UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

CARRERA DE SISTEMAS DE INFORMACIÓN

PROCESO DE TITULACION

NOVIEMBRE 2023 – ABRIL 2024

EXAMEN COMPLEXIVO DE GRADO DE CARRERA PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS DE INFORMACIÓN

TEMA:

Optimización y Fortalecimiento de la Seguridad en Bases de Datos Open Source de GADS Cantonales de Los Ríos

ESTUDIANTE:

TITO JOEL TUMBACO GUAMAN

TUTOR:

Ing. HARRY SALTOS VITERI. MGST

AÑO

2024

Resumen

El presente caso de estudio hace un análisis acerca de la optimización y fortalecimiento de la seguridad en bases de datos Open Source de GADS cantonales de Los Ríos, se muestra aquí una referencia importante acerca de la problemática existente que son las amenazas continuas a la seguridad de la información y los GAD están obligados a optar por sistemas de fuente abierta para la dinámica de sus sistemas, por tal razón se exploran dos bases de datos muy utilizadas en ambientes municipales y la forma de como optimizar y fortalecer su seguridad.

El objetivo de este caso de estudio es el de hacer un análisis en base de propuestas de estratégicas de optimización y fortalecimiento de la seguridad en bases de datos Open Source utilizadas por algunos GADS cantonales de Los Ríos, con el propósito de mitigar vulnerabilidades, salvaguardar la integridad de la información, por lo que se muestran unas tablas que se han investigado de cómo realizar técnicamente esa funcionalidad.

Como marco metodológico para tener resultados reales y claros, se ha realizado entrevistas a dos de los mas grandes GAD cantonales o municipios de la provincia de Los Ríos (Quevedo y Babahoyo), por lo que se han recogido así mismo, las mejores prácticas en relación a mejorar la seguridad de la información con bases de datos, las experiencias de los profesionales planteadas en la entrevista han enriquecido de manera favorable este documento, por lo que se la expone en los resultados a modo de síntesis y en el anexo 1 se encuentra de forma completa.

Además, se han consultado bases teóricas basadas en un marco conceptual que permite un punto de vista critico frente a la seguridad y diferentes motores de bases de datos; así mismo se concluye y se recomienda posibles alternativas que no tiene mucho que ver con configuración, sino mas bien se relacionan con buenas prácticas de prevención.

Palabras Claves

Open Source, GAD, fuente abierta, ciberseguridad, PostgreSQL, MySQL, MONGODB

Planteamiento del Problema

El manejo y resguardo de la información en instituciones públicas como es el caso de los GADs de la provincia de Los Ríos, aunque es un modelo general que se refleja en todo el país, este problema de estudio se enfoca en municipios que son las instituciones cantonales descentralizadas de la provincia fluminense, haciendo énfasis en especialmente en sus bases de datos Open Source , ya que estas presentan desafíos importantes en un contexto de amenazas cibernéticas que cada vez son más sofisticadas. La inexistencia de estrategias de seguridad efectivas puede desencadenar en la exposición de datos sensibles, comprometiendo de esta manera la integridad y confidencialidad de la información de estos niveles de gobierno.

En tal sentido, la falta de un enfoque integral y eficiente en la seguridad de las bases de datos Open Source utilizadas por instituciones públicas expone a dichas entidades a riesgos en cuanto a la violación de su seguridad, por accesos no autorizados y pérdidas de información sensible. Esta situación se agrava por la rápida evolución de las amenazas cibernéticas, la complejidad de las tecnologías de bases de datos Open Source y la necesidad imperante de mantener la confianza ciudadana en la gestión gubernamental de datos.

Las bases de datos Open Source a diario en las instituciones públicas se ven amenazadas por vulnerabilidades críticas, forjando escenarios donde se exponen a accesos no autorizados a los datos importantes de los GAD Cantonales, además de poder causar algunas posibles manipulaciones sin siquiera conocerlo. La ausencia la realización de un análisis exhaustivo de vulnerabilidades aumenta el riesgo de violaciones de seguridad, comprometiendo de esta manera la integridad de los datos Municipales. (Ross, 2019)

A pesar de que se puedan tener medidas de seguridad puestas en marcha, la no existencia o la ineficacia de las políticas, procedimientos y tecnologías actuales relacionadas con las bases de datos Open Source en las instituciones públicas deja una brecha preocupante. La falta de una evaluación frecuente entorno a estas medidas expone o vulnera a las entidades locales gubernamentales a posibles brechas en su seguridad, poniendo de esta manera en peligro los datos institucionales, así como la confidencialidad y disponibilidad de la información.

Cada incidente relacionado con vulnerar la seguridad que es descubierta influye en la confianza de la ciudadanía para con las instituciones gubernamentales. Podría verse o tenerse una percepción de que es una gestión descuidada de los datos, afectándose afecta la confianza pública, generando de esta manera ciertas dudas sobre si tienen o no la capacidad de una gobernabilidad sana no solamente en relación a salvaguardar la información de manera efectiva, sino en toda la gestión.

(Ross, 2019) considera que, en un panorama cibernético que evoluciona constantemente, las instituciones públicas de forma frecuente luchan por mantenerse al día para comprender las amenazas emergentes. La falta de estrategias que permitan la mitigación empleando nuevas tácticas para los ataques, dejan a las bases de datos Open Source expuestas a riesgos grandes, comprometiendo la seguridad informática de los GAD.

El incumplimiento de las normativas vigentes en cuanto a la seguridad de datos en las instituciones públicas plantea un riesgo que siempre puede existir. La desalineación con los requisitos legales muchas veces deja a los GAD vulnerables a sanciones y repercusiones legales, desestabilizando la integridad y credibilidad de la gestión gubernamental; esto puede además deberse a que los administradores o las autoridades de estos estamentos de gobierno desconocen de los desafíos informáticos s los que el área de tecnologías puede enfrentarse a diario.

Justificación

Se justifica este caso de estudio como una iniciativa importante que permitirá fortalecer la seguridad en torno a las bases de datos Open Source en los GAD,

garantizando la protección de la información, mejorando o recuperando la confianza ciudadana y apangándose al cumplimiento de normativas, en un contexto de amenazas digitales en constante renovación.

(Kleppmann, 2021) considera que, es necesario una optimización y fortalecimiento de las seguridades en bases de datos Open Source de instituciones públicas ya que estas son de vital importancia en el contexto creciente actual donde existen muchas amenazas cibernéticas y se demanda de transparencia en todos los sentidos.

Este estudio se justifica por que propicia una protección de información sensible, es decir, las instituciones públicas manejan grandes cantidades de información altamente sensible, como son: datos personales, financieros y operativos. La optimización continua y el aseguramiento de las bases de datos Open Source es esencial para la prevención de accesos no autorizados y lograr buenas prácticas que permitan la salvaguarda de la integridad de la información. (Winand, 2018)

Las ciber amenazas en evolución constante brindan un panorama de amenazas criticas cada vez más fortalecidas, es decir cada vez están cambiando las maneras o mejorando las maneras de atacar a instituciones para robo de información, hacer cambios importantes con esquemas técnicos y sofisticados. La investigación con este caso de estudio y las recomendaciones que puedan generarse, justifican claramente un panorama que lo hace imperativo para lograr anticipar y responder eficazmente ante nuevas tácticas utilizadas por actores maliciosos que buscan afectar datos institucionales. (Chauhan, 2020)

Además, es de vital importancia mantener la confianza ciudadana en los GAD´s, no se quiere escuchar que han sido cambiados los datos de deudas de predios urbanos, o talvez los datos donde se factura el agua potable y que a algún ciudadano le aparezca de la noche a la mañana que debe pagar grandes cantidades de dinero, las instituciones gubernamentales dependen en gran medida de la información que manejan, esa es la razón por la cual hay que protegerla. Al fortalecer la seguridad en bases de datos se esta contribuyendo a la construcción y confianza pública como una gestión integral, aun siendo solamente reflejada en los datos.

Las instituciones públicas, esto es los GAD tienen la responsabilidad de ejercer un cumplimiento basado en estándares estrictos, el aumento en la legislación en torno a la privacidad de datos y la utilización de software de fuente abierta impone medidas seguir que seguramente ahorraran costos a la institución. La optimización constante de la seguridad en las bases de datos Open Source no es algo que solamente se lo haga a lo de fuente abierta, todo debe tener estas exigencias normativas si es para lo público, reduciendo de esta manera los riesgos legales y sanciones posibles. (Schönig, 2018)

La implementación de medidas de seguridad efectivas en las instituciones públicas y la responsabilidad de cumplir con varios estándares muy estrictos no solo que protege contra varias amenazas, sino que también permite contribuir a la continuidad operativa. Prevenir incidentes o vulneraciones a la seguridad evita muchas interrupciones en los servicios de los GAD y asegura la eficiencia en la prestación de servicios hacia los ciudadanos. (Appigatla, 2022)

Objetivos del Estudio

Objetivo General

Analizar propuestas de estrategias de optimización y fortalecimiento de la seguridad en bases de datos Open Source utilizadas por algunos GADS cantonales de Los Ríos, con el propósito de mitigar vulnerabilidades, salvaguardar la integridad de la información.

Objetivos Específicos

- Identificar posibles puntos de riesgo y evaluando las amenazas potenciales que podrían comprometer la seguridad de la información.
- Evaluar la efectividad de las medidas de seguridad implementadas actualmente en las bases de datos Open Source de GADS Cantonales de Los Ríos.
- Diseñar e implementar estrategias que permitan ser base de propuestas de soluciones prácticas y adecuadas al contexto gubernamental.

Línea de Investigación y Articulación del Tema

Este trabajo de investigación se perfila con la línea de investigación: Sistemas de información y comunicación, emprendimiento e innovación, la misma que se articula estrechamente con la sub línea de investigación: Redes y tecnologías inteligentes de software y hardware.

El presente caso de estudio, además, se relaciona con la práctica pre profesional realizada y que tuvo despliegue con el desarrollo de bases de datos para personas con discapacidad en el departamento de bienestar estudiantil, esto permitió potenciar en gran magnitud la formación y experiencia estudiantil para una aplicabilidad directa durante la fase de titulación presentada como caso de estudio de poder asegurar con técnicas ingenieriles las bases de datos.

Marco Conceptual

Importancia de las Bases de datos

En el mundo actual las bases de datos son un elemento imprescindible porque permiten que se organicen grandes cantidades de información de forma estructurada y accesible. (Bazzell, 2020) afirmaron que no solo facilitan el acceso rápido a los datos, sino que también garantizan la integridad y seguridad de los datos mediante la aplicación de restricciones y control de acceso. Su importancia radica en su capacidad para proporcionar a la dirección información precisa y relevante para apoyar la toma de decisiones. Además, el almacén es escalable y flexible, lo que le permite adaptarse a las necesidades cambiantes de la organización. Facilitan la colaboración entre equipos y departamentos al proporcionar acceso simultáneo a la información.

Las Bases de Datos en el Sector Público

En el sector público, las bases de datos desempeñan un papel vital en la promoción de una gestión eficaz de la información y los recursos. Estas organizaciones procesan una amplia gama de datos, desde registros civiles y financieros hasta servicios públicos e información de políticas públicas. En este sentido, las bases de datos son importantes en varios aspectos clave. (Alex Singleton, 2019)

En primer lugar, la base de datos permite un manejo adecuado de los registros y la información de población. Medical Depot, por ejemplo, ayuda con la atención médica. profesionales para mantener historiales precisos de los pacientes, facilitar un mejor seguimiento del tratamiento y garantizar una atención médica más eficiente. En el sector financiero, los archivos tributarios e ingresos ayudan a gestionar eficazmente los impuestos y contribuciones de los ciudadanos. (Rabinovich-Einy, 2021)

Además, los repositorios son esenciales para mejorar la transparencia y la rendición de cuentas en el sector público. Al mantener registros detallados y accesibles del uso de recursos y la implementación de políticas, las bases de datos ayudan a garantizar que los funcionarios públicos sean responsables de sus acciones y decisiones. Otro aspecto importante es la eficiencia operativa. El almacenamiento permite automatizar procesos y agilizar las actividades administrativas, reduciendo el tiempo y los recursos necesarios para realizar tareas como la gestión de licencias, la concesión de licencias o el procesamiento de archivos. (Simon Marvin, 2021)

Además, los repositorios desempeñan un papel crucial en la planificación y la toma de decisiones del sector público. Al proporcionar datos confiables y actualizados, ayudan a los formuladores de políticas a comprender mejor las necesidades y prioridades de las personas y a desarrollar estrategias y programas que aborden eficazmente los desafíos sociales, económicos y ambientales. (Waer, 2021)

Los repositorios son una herramienta esencial para mejorar la eficiencia, la transparencia y la capacidad de respuestas del sector público. Facilitando de gran manera la gestión de la información, aumentan la rendición de cuentas, optimizan los procesos operativos y apoyan la toma de decisiones informadas, contribuyendo así al bienestar y desarrollo de toda la sociedad. (Appigatla, 2022)

Modelo General de uso de Bases de Datos en Municipios

1. Archivos financieros: se utilizan para gestionar los ingresos y gastos municipales y controlar los impuestos, gravámenes y otros aspectos financieros del gobierno local.
2. Repositorios de Servicios Públicos: Almacenan información sobre la prestación de servicios públicos como agua, electricidad, transporte público, gestión de

residuos, etc. Estos almacenes son esenciales para garantizar la eficiencia en la prestación de servicios a los ciudadanos.

3. Archivos Geoespaciales: Estos archivos contienen información geográfica y espacial sobre ciudades, como mapas, terrenos, infraestructura pública, áreas urbanas y rurales, etc. Son esenciales para la planificación urbana, el desarrollo territorial y la gestión ambiental.
4. Base de datos de empleados y personal: se utiliza para administrar la información del personal de la ciudad, incluidos datos de contratación, salario, capacitación y evaluación del desempeño. (Claudio Coletta, 2018)

Principales Aplicaciones o Motores de Bases de Datos Open Source

En Ecuador, como en otros lugares, la aplicación principal o el motor de base de datos de código abierto más utilizado puede variar dependiendo de las necesidades y preferencias de la organización. Sin embargo, algunos de los sistemas más populares incluyen:

1. MySQL: Es uno de los sistemas de gestión de bases de datos relacionales más populares y utilizados en el mundo. Conocido por su velocidad, confiabilidad y facilidad de uso, se utiliza en una amplia gama de aplicaciones, desde sitios web hasta sistemas empresariales. (Straub, 2022)
2. PostgreSQL: Otro sistema de gestión de bases de datos relacionales de código abierto muy popular. PostgreSQL es conocido por su solidez, funciones avanzadas y cumplimiento de los estándares ANSI SQL. Esta es una opción común para aplicaciones que requieren un alto nivel de seguridad y admiten datos complejos. (Turnbull, 2019)
3. MongoDB: esta es una base de datos NoSQL de código abierto que se utiliza para almacenar datos en forma de archivos JSON flexibles. MongoDB es especialmente popular para proyectos y aplicaciones web modernas que requieren escalabilidad y flexibilidad de esquemas de datos.

4. MariaDB: Es un sistema de gestión de bases de datos relacionales de código abierto compatible con MySQL. Gracias a las mejoras de rendimiento y funciones adicionales, MariaDB se está volviendo cada vez más popular como alternativa a MySQL. (Kerrisk, 2019)

Estas son sólo algunas de las excelentes opciones de almacenamiento de código abierto que se utilizan ampliamente en Ecuador.

Comparativa de Bases de datos Open Source

Tabla 1. *Comparativa de las bases de datos MySQL, PostgreSQL, MongoDB y MariaDB, reflejando algunas de sus principales ventajas y desventajas:*

Característica	MySQL	PostgreSQL	MongoDB	MariaDB
Tipo de Base de Datos	Relacional	Relacional	NoSQL	Relacional
Lenguaje de Consulta	SQL	SQL	NoSQL Query Language (JSON)	SQL
Escalabilidad	Buena escalabilidad vertical. Limitada escalabilidad horizontal.	Buena escalabilidad horizontal y vertical.	Excelente escalabilidad horizontal y vertical.	Similar a MySQL.
Replicación	Soportado, pero menos flexible que en algunas otras bases de datos.	Soportado y altamente configurable.	Soportado, pero la consistencia puede ser un desafío en configuraciones de replicación.	Soportado, con opciones de replicación avanzadas.
Transacciones ACID	Totalmente compatible.	Totalmente compatible.	No todas las operaciones son transaccionales.	Totalmente compatible.
Confiabilidad	Muy estable y probado en producción.	Muy estable y probado en producción.	Depende del diseño y configuración de la implementación.	Muy estable y probado en producción.
Compatibilidad	Compatible con muchos lenguajes de programación y plataformas.	Compatible con muchos lenguajes de programación y plataformas.	Ampliamente utilizado en entornos de desarrollo web y aplicaciones modernas.	Compatible con MySQL.
Soporte de Comunidad	Gran comunidad y abundante documentación.	Gran comunidad y abundante documentación.	Comunidad en crecimiento y documentación disponible.	Similar a MySQL.
Flexibilidad de Esquema	Menos flexible que las bases de datos NoSQL.	Flexible, pero menos que NoSQL.	Altamente flexible debido a su naturaleza de documentos.	Similar a MySQL.

Fuente : Análisis propio, usando referencias de sitios web de marcas de bases de datos

Aquí es importante tener en cuenta que estas son solo algunas referencias más usuales sobre ventajas y desventajas de cada motor de base de datos expuesto en la tabla pues la elección más adecuada dependerá de las necesidades puntuales del proyecto que se quiera emprender, así como las habilidades y experiencia con que cuenta el equipo de técnicos y otros factores importantes.

El Open Source y los Gobiernos Descentralizados Cantonales

Manteniendo la idea sobre el Open Source (código abierto) su importancia en estos últimos años no solo se ha enfocado en abarcar varios ámbitos tecnológicos, sino que también se ha visto vinculado en la esfera gubernamental de los gobiernos descentralizados cantonales, dando un enfoque transformado a través de algún tema de suma importancia debido a las dificultades de transparencia, participación ciudadana, eficiencia y ahorro de costos.

En el siguiente párrafo se tiene información de suma importancia de como el Open Source impacta a los gobiernos descentralizados cantonales.

1. Transparencia y Participación Ciudadana: Utilizar las soluciones del software Open Source en los gobiernos descentralizados impulsa la transparencia brindando el acceso público al código fuente de cualquiera aplicación que se haya usado. Teniendo en cuenta esta opción ayuda a los ciudadanos dando una posibilidad de comprender todas las funciones de las herramientas tecnológicas que maneja el gobierno, esto permite ayudar al desarrollo y mejorar las soluciones dado a que la participación ciudadana crea su propio entorno de colaboración entre el gobierno y sociedad.

2. Eficiencia y Flexibilidad: Los gobiernos descentralizados poseen una mayor flexibilidad a través del control Open Source debido a que se puede personalizar las soluciones de acuerdo con las necesidades específicas lo cual permite perfeccionar los procesos internos y brindar una mejora en la presentación de los servicios públicos. Por lo que al no depender de nadie posee una gran libertad de no sufrir restricciones de licencias.
3. Reducción de Costos: Reducir el costo asociado con la adquisición, implementación y mantenimientos de información de los sistemas en los gobiernos descentralizados utilizando Open Sources beneficia de gran manera al reducir los costos ya antes mencionado debido a que es de código abierto por lo que saben tener soluciones gratuitas o con un costos menor ya que al poseer acceso al código fuente los gobiernos evitan costos adicionales vinculados a las tarifas de soporte que dependen de proveedores externos.

4. Innovación y Desarrollo Local: optar por las soluciones de Open Source integra la innovación y el desarrollo local de los gobiernos descentralizados ya que, al abrir el acceso a las herramientas tecnológicas, desarrolla las habilidades en la comunidad local integrando programas con profesionales en TIC. Lo que nos da a entender que a través de esto permite a el ecosistema al innovar y adaptar todas las necesidades a cada cantón.

El Open Source en Ecuador y sus instituciones publicas

Open Source es unas de las opciones más utilizadas en la republica del Ecuador principalmente en las instituciones públicas debido a que su presencia en estos últimos años ha sido de gran ayuda ya que a demostrado la transparencia, la eficiencia y el ahorro de costos en la parte gubernamental. Reforzando con análisis de (Simon Marvin, 2021), a continuación, se relatan ciertos aspectos sobre la función del Open Source en el Ecuador y sus instituciones públicas.

1. Políticas y Normativas: El gobierno que administra a Ecuador ha permitido la utilización activa del Open Source llevado a cabo a través de las políticas y normativas las mismas que respaldan la implementación en todas las instituciones públicas. Todo esto se sustenta a través de ejemplos verídicos tales como el decreto ejecutivo 1014 emitido en el 2008 el mismo que habla sobre el uso prioritario de Open souce en las entidades públicas.

2. Iniciativas de Implementación: En vistas de la aceptación de Open Source en la republica del Ecuador varias instituciones públicas optaron por esta nueva modalidad en las distintas áreas de tecnología. Esta idea ha permitido reducir cotos a las instituciones dando una mejor eficiencia en la prestación de los servicios.

3. Colaboración y Desarrollo Comunitario: Open Source a llevado una gran colaboración impulsado a que la mayoría de instituciones opten por este software que ayudo a la creación de comunidades locales de usuarios y desarrolladores de software los mismo que permitió que compartan conocimientos y experiencias para que den soluciones de código abierto siempre y cuando se adapten a las necesidades locales

4. Capacitación y Desarrollo de Habilidades: El desarrollo de las habilidades de programación han integrado la implementación de soluciones de Open Source debido a que las instituciones públicas han promovido el desarrollo de habilidades en

programación por lo siempre el personal debe de estar capacitado para evitar confusiones en el código.

5. Alianzas con la Comunidad Internacional: La república del Ecuador definió sus alianzas con las comunidades asociadas sobre el uso del Open Source debido a que este método se comparten prácticas significativas intercambiando experiencias entre conocimientos que tiene al saber sobre eso software de los diferentes países que optaron por utilizar ese método siendo más el ámbito público quien lo utiliza.

En la actualidad el Open Source ha desempeñado un papel crucial en la republica del Ecuador siendo el primer contribuyente que trajo la modernización al sector público, la adopción de este software a medida de cómo va pasando el tiempo se hace una estimación de que en unos años mas exista avances importantes en este sentido debido a que se vincula con un ecosistema lleno de tecnología dentro del país llevando un gran desarrollo sostenible.

Normas de Control Interno de Contraloría para cumplimiento en GADS Cantonales

Llevando el uso de las bases de datos vinculando los sistemas de los municipios, es fundamental para garantizar una gestión contable con normativas fundamentales lo que implica hacer un análisis sobre el correcto uso de las bases de datos ya que el sistema en los municipios se relaciona con todas las normas vinculadas a la contraloría. (Claudio Coletta, 2018)

Pasando al termino de registro y control de la información, todas las finanzas, recursos humanos y contradicciones públicas se relacionan con las bases de datos y los sistemas de los municipios debido a que la información es de mucha importancia dado a que brinda una mejor trazabilidad completando todos los procesos y transacciones por la administración pública de la institución. (Kerrisk, 2019)

Implementando un control de seguimiento relacionado con los proyectos y procesos del sistema los municipios brindan la facilidad de dar un seguimiento y monitoreo a todas las supervisiones de plazos brindando el cumplimiento de la normativa del proceso. (Kerrisk, 2019)

Verificando que se tiene acceso a la base de datos la información se encuentra disponible en tiempo real para que la organización de control pueda llevar a cabo las auditorias del sistema de manera más efectiva. (Bazzell, 2020)

En general todos los municipios proceden a cumplir una serie de normativas con sus reglamentos establecidos a través de las entidades de control y vigilancia que estima la contraloría. Tener en cuenta el uso adecuado de las bases de datos facilita una garantía de cumplimiento de esas normativas ya que al brindar herramientas permitan llevar el proceso administrativo de gestión y control de esas instituciones facilita el trabajo colectivo con la información. (Kleppmann, 2021)

La normativa de contraloría busca garantizar la total transparencia y rendición de cuentas a través del acceso público de la información vinculando la base de datos para el cumplimiento de las obligaciones legales por pate de las autoridades municipales que administran la información de la institución. (Straub, 2022)

Es de suma importancia llevar una disponibilidad de información de manera clara un control y una accesibilidad para que facilite el seguimiento al ciudadano a través de un control. (Bazzell, 2020)

Los sistemas en los municipios establecen una parte fundamental con la base de datos ya que evita detectar fraudes en la información por lo que al contar con esta herramienta mantiene un control y monitoreo automatizado para poder identificar de forma rápida y eficiente posibles anomalías en la gestión pública, esto permite tomar medidas que eviten perjuicios para la administración que posee el municipio y la ciudadanía en general. (Straub, 2022)

Para concluir, se puede mencionar que, el uso de las bases de datos en los sistemas de los municipios mantiene un papel principal en esa institución ya que lleva el cumplimiento de la contraloría por lo que al brindar esta herramienta para el registro de información contribuye a dar mejor imagen de transparencia más verídica con aspectos fundamentales que garantiza a la administración pública dar un mejor servicio a la ciudadanía.

Tabla 2. Comparativa de algunas estrategias para optimizar bases de datos en PostgreSQL y MySQL:

Aspecto de Optimización	PostgreSQL	MySQL
Índices eficientes	PostgreSQL soporta índices B-tree, hash, GIN, GIST y otros tipos. Puedes crear índices únicos, parciales y de expresión.	MySQL soporta índices B-tree, hash y full-text. Puedes crear índices únicos, compuestos y de longitud prefijada.
Actualización de estadísticas	Utiliza el comando ANALYZE para actualizar las estadísticas de las tablas y ayudar al optimizador de consultas a generar planes de ejecución eficientes.	MySQL actualiza automáticamente las estadísticas cuando se realizan cambios en las tablas, pero también puedes usar ANALYZE TABLE para forzar la actualización.
Configuración del servidor	Ajusta parámetros como shared_buffers, work_mem, effective_cache_size, etc., según los recursos del sistema y las necesidades de la aplicación.	Ajusta parámetros como innodb_buffer_pool_size, key_buffer_size, query_cache_size, etc., para optimizar el rendimiento según los recursos del sistema y la carga de trabajo.
Particionamiento de tablas	PostgreSQL soporta particionamiento de tablas por clave, rango y lista. Puede mejorar el rendimiento y facilitar la administración de grandes conjuntos de datos.	MySQL soporta particionamiento de tablas por clave y rango. Puede mejorar el rendimiento y la administración de grandes conjuntos de datos.
Optimización de consultas	Utiliza herramientas como EXPLAIN y EXPLAIN ANALYZE para analizar y optimizar los planes de ejecución de las consultas. Ajusta índices, reformula consultas, etc., según sea necesario.	Utiliza EXPLAIN y EXPLAIN ANALYZE para analizar y optimizar los planes de ejecución de las consultas. Ajusta índices, reformula consultas, etc., según sea necesario.
Vacío y reindexado	Realiza regularmente vaciados (VACUUM) y reindexados (REINDEX) para eliminar espacio no utilizado y reorganizar índices. Puede mejorar el rendimiento de las consultas y operaciones de escritura.	Realiza regularmente optimizaciones de tablas (OPTIMIZE TABLE) para reorganizar datos y liberar espacio. Puede mejorar el rendimiento de las consultas y operaciones de escritura.
Uso de transacciones	Utiliza transacciones de manera eficiente para agrupar operaciones relacionadas y reducir el número de commits. Esto puede mejorar el rendimiento y la consistencia de los datos.	Utiliza transacciones de manera eficiente para agrupar operaciones relacionadas y reducir el número de commits. Esto puede mejorar el rendimiento y la consistencia de los datos.
Seguridad y mantenimiento	Mantén PostgreSQL actualizado con parches de seguridad y sigue las mejores prácticas de seguridad.	Mantén MySQL actualizado con parches de seguridad y sigue las mejores prácticas de seguridad.
Monitorización y ajuste	Utiliza herramientas de monitorización para supervisar el rendimiento de PostgreSQL y ajustar la configuración según sea necesario.	Utiliza herramientas de monitorización para supervisar el rendimiento de MySQL y ajustar la configuración según sea necesario.

Fuente: El Autor con Análisis de información de las webs de las marcas

Es imperativo tener presente que, tanto PostgreSQL como MySQL tienen características particulares y configuraciones especificas distintas que pueden influir significativamente en la forma de optimización de una base de datos. Siempre resultara favorable consultar la documentación oficial es decir del fabricante y realizar las pruebas exhaustivas recomendadas para determinar qué estrategias de optimización son las más efectivas para el proyecto o caso.

Tabla 3. Comparativa de cómo brindar seguridad utilizando Linux en una base de datos con PostgreSQL y MySQL:

Aspecto de Seguridad	PostgreSQL	MySQL
Autenticación y autorización	PostgreSQL proporciona autenticación basada en contraseña y autenticación basada en identificación de métodos (identificación de hosts, identificación de certificados, identificación de Kerberos, etc.). También ofrece un sistema de roles y privilegios granular para controlar el acceso a bases de datos y objetos.	MySQL proporciona autenticación basada en contraseña, autenticación basada en certificados y autenticación basada en plugins. Los privilegios de usuario pueden ser gestionados a nivel de base de datos, tabla, columna, etc.
Encriptación de datos	PostgreSQL soporta el cifrado de datos tanto en reposo como en tránsito. Puedes utilizar SSL/TLS para encriptar las conexiones entre clientes y servidor, así como encriptar datos sensibles en la base de datos utilizando funciones de encriptación integradas.	MySQL también soporta el cifrado de datos tanto en reposo como en tránsito. Puedes utilizar SSL/TLS para encriptar las conexiones entre clientes y servidor, así como encriptar datos sensibles en la base de datos utilizando funciones de encriptación integradas.
Control de acceso a archivos	PostgreSQL utiliza el sistema de archivos del sistema operativo para gestionar los archivos de datos y registro. Debes asegurar los permisos adecuados en los directorios y archivos de PostgreSQL para restringir el acceso no autorizado.	MySQL utiliza el sistema de archivos del sistema operativo para gestionar los archivos de datos y registro. Debes asegurar los permisos adecuados en los directorios y archivos de MySQL para restringir el acceso no autorizado.
Auditoría de eventos	PostgreSQL proporciona funcionalidades de auditoría integradas para registrar eventos de base de datos como conexiones, consultas, cambios de esquema, etc. Puedes configurar la auditoría para que registre eventos específicos y almacenar los registros en archivos o tablas.	MySQL ofrece funcionalidades de auditoría como registros binarios y registros de consulta. Puedes habilitar el registro binario para registrar cambios en la base de datos y usar el registro de consultas para registrar consultas ejecutadas en el servidor MySQL.
Actualizaciones de seguridad	PostgreSQL proporciona actualizaciones de seguridad regulares y parches para abordar vulnerabilidades conocidas. Debes mantener tu instalación de PostgreSQL actualizada instalando los últimos parches y actualizaciones de seguridad.	MySQL también proporciona actualizaciones de seguridad regulares y parches para abordar vulnerabilidades conocidas. Debes mantener tu instalación de MySQL actualizada instalando los últimos parches y actualizaciones de seguridad.
Separación de privilegios	PostgreSQL permite crear roles con privilegios específicos y asignarlos a usuarios y objetos de la base de datos. Debes seguir el principio de privilegios mínimos necesarios para reducir el riesgo de acceso no autorizado.	MySQL también permite crear roles con privilegios específicos y asignarlos a usuarios y objetos de la base de datos. Debes seguir el principio de privilegios mínimos necesarios para reducir el riesgo de acceso no autorizado.
Seguridad del sistema operativo	Debes seguir las mejores prácticas de seguridad del sistema operativo Linux para proteger el servidor donde se ejecutan PostgreSQL, como mantener el sistema actualizado, deshabilitar servicios no utilizados, usar cortafuegos, configurar la autenticación de usuario, etc.	Debes seguir las mejores prácticas de seguridad del sistema operativo Linux para proteger el servidor donde se ejecutan MySQL, como mantener el sistema actualizado, deshabilitar servicios no utilizados, usar cortafuegos, configurar la autenticación de usuario, etc.

Fuente: (Turnbull, 2019)

Es importante que se pueda destacar que el esquema de seguridad es un proceso continuo y tiene muchas formas. Se consideran muchas medidas de seguridad a nivel de base de datos, sobre todo de sistema operativo y la red para mantener una protección adecuada de los datos y sistemas contra amenazas maliciosas. Además, siempre es recomendable verificar la documentación oficial de los sitios web de PostgreSQL y MySQL, así como también las guías y reportes de seguridad de la comunidad Linux, esto

para tener instrucciones actualizadas y específicas acerca de cómo implementar medidas de seguridad en su organización.

Tabla 4. Comparativa con comandos específicos para asegurar una base de datos a nivel de sistema operativo y en cuanto a su encriptación en PostgreSQL y MySQL:

Aspecto de Seguridad	PostgreSQL	MySQL
Control de Acceso a Archivos	Asegura los permisos de los directorios y archivos de PostgreSQL. Esto puede hacerse con comandos como chmod y chown. Por ejemplo, para asegurar el directorio de datos de PostgreSQL en Linux: sudo chmod 700 /var/lib/postgresql/data sudo chown postgres:postgres /var/lib/postgresql/data	Asegura los permisos de los directorios y archivos de MySQL. Esto puede hacerse con comandos como chmod y chown. Por ejemplo, para asegurar el directorio de datos de MySQL en Linux: sudo chmod 700 /var/lib/mysql sudo chown mysql:mysql /var/lib/mysql
Autenticación de Usuarios	Configura la autenticación de usuarios en PostgreSQL. Esto puede hacerse editando el archivo pg_hba.conf y utilizando comandos como createuser y ALTER ROLE. Por ejemplo, para crear un nuevo usuario en PostgreSQL: sudo -u postgres createuser --interactive	Configura la autenticación de usuarios en MySQL. Esto puede hacerse editando el archivo my.cnf y utilizando comandos como CREATE USER y ALTER USER. Por ejemplo, para crear un nuevo usuario en MySQL: CREATE USER 'usuario'@'localhost' IDENTIFIED BY 'contraseña';
Encriptación de Datos	Configura SSL/TLS para encriptar conexiones entre clientes y servidor en PostgreSQL. Esto puede hacerse modificando el archivo postgresql.conf y el archivo pg_hba.conf. Por ejemplo, para habilitar SSL en PostgreSQL: ssl = on ssl_cert_file = 'ruta/al/certificado.crt' ssl_key_file = 'ruta/a/clave.key'	Configura SSL/TLS para encriptar conexiones entre clientes y servidor en MySQL. Esto puede hacerse modificando el archivo my.cnf. Por ejemplo, para habilitar SSL en MySQL: ssl = 1 ssl_cert = '/ruta/al/certificado.crt' ssl_key = '/ruta/a/clave.key'

Fuente : Comunidad de PostgreSQL y MySQL

Hay que tener en cuenta que estos solamente son referencias básicas de ejemplos de cómo asegurar PostgreSQL y MySQL a nivel de sistema operativo y su encriptación. Su implementación para producción puede diferenciarse dependiendo de la configuración de su sistema y servidores, así como las políticas de seguridad de la organización.

MARCO METODOLOGICO

En el marco de esta investigación sobre la Optimización y Fortalecimiento de la Seguridad en Bases de Datos Open Source de GADS Cantonales de Los Ríos, es esencial elegir una metodología de investigación apropiada que aborde el problema en cuestión y satisfaga los objetivos planteados.

Se utiliza una investigación cualitativa: que pretende comprender y describir fenómenos complejos y subjetivos, como percepciones, valores, creencias, experiencias y comportamientos humanos, desde la perspectiva de los participantes.

La técnica seleccionada para esta investigación es la entrevista en profundidad y no una encuesta, a una población objetivo que es 13 directores de Tecnologías por la cantidad de cantones de la provincia, de los cuales como muestra se han tomado 2 (por ser los cantones más grandes y de mayor presupuesto), esta entrevista se enfoca en explorar exhaustivamente las perspectivas y experiencias de los expertos. Se llevará a cabo una entrevista con un experto en bases de datos para obtener información detallada y recomendaciones completas.

En una investigación cualitativa, el instrumento se refiere a la herramienta o medio utilizado para recopilar datos cualitativos. Dado que se planea entrevistar a expertos, el instrumento principal será la "guía de entrevista". Esta consiste en un conjunto de preguntas y temas que orientan la conversación durante las entrevistas con los expertos.

Una vez recopilados los datos a través de las entrevistas en profundidad, se procederá con el análisis cualitativo de los mismos. Este análisis implicará la revisión detallada de las respuestas de los expertos, identificando patrones, tendencias y temas emergentes relacionados con la seguridad en bases de datos Open Source en entornos municipales.

Es importante destacar que la selección de expertos en bases de datos se ha realizado cuidadosamente, considerando su experiencia y conocimientos en el campo. Esto garantiza la calidad y relevancia de la información recopilada, así como la robustez de las recomendaciones que se derivarán de este estudio.

Además de las entrevistas, se llevará a cabo una revisión exhaustiva de la literatura existente sobre el tema, con el fin de complementar y enriquecer los hallazgos obtenidos

a través de las entrevistas. Esto proporcionará un contexto más amplio y una comprensión más profunda de los desafíos y estrategias relacionados con la seguridad en bases de datos Open Source en entornos municipales

RESULTADOS

Luego de haber realizado la entrevista a profesionales de las áreas de tecnologías de una muestra de los dos principales GAD's cantonales de la provincia de Los Ríos como son Babahoyo y Quevedo, estos profesionales accedieron a brindar una entrevista relacionada con la guía de entrevistas diseñada para tales efectos, por lo que como resultado se ha podido enriquecer este trabajo con la participación de estos profesionales con experiencia y que trabajan en el medio que es el objeto de estudio:

El análisis de las entrevistas proporcionadas por los expertos García e Ibarra ofrece una visión integral sobre los desafíos y las estrategias para mejorar la seguridad de las bases de datos Open Source en entornos gubernamentales como los GADS Cantonales de Los Ríos.

Ambos expertos coinciden en que uno de los mayores desafíos en términos de seguridad al trabajar con bases de datos Open Source radica en la gestión adecuada de parches y actualizaciones de seguridad. García destaca la importancia de identificar, aplicar y validar parches de seguridad de manera oportuna para mitigar el riesgo de exposición a nuevas vulnerabilidades. Por su parte, Ibarra menciona la necesidad de implementar actualizaciones regulares de seguridad como parte de una estrategia integral para mejorar la seguridad de las bases de datos Open Source.

En cuanto a la configuración de permisos y autenticación, ambos expertos resaltan su importancia en entornos gubernamentales donde la información es sensible y altamente regulada. García propone implementar políticas de seguridad sólidas y mecanismos de autenticación robustos, como la autenticación de dos factores, para mitigar el riesgo de accesos no autorizados. De manera similar, Ibarra aboga por la implementación de prácticas de principio de menor privilegio y la realización de auditorías periódicas para garantizar que solo el personal autorizado pueda acceder y modificar la información de manera segura.

En cuanto a la gestión de privilegios y accesos, ambos expertos coinciden en la importancia de implementar prácticas de principio de menor privilegio y llevar a cabo auditorías periódicas para detectar y mitigar posibles riesgos de seguridad. Ambos resaltan la importancia de establecer un proceso de revisión y auditoría periódica de los accesos para garantizar que solo el personal autorizado pueda acceder y modificar la información de manera segura.

En cuanto a la capacitación y concienciación del personal en temas de seguridad, ambos expertos coinciden en la importancia de diseñar un programa efectivo de educación que abarque aspectos técnicos y de comportamiento. García propone sesiones de capacitación práctica sobre el uso seguro de bases de datos Open Source , mientras que Ibarra destaca la importancia de fomentar una cultura de denuncia y colaboración entre los empleados para promover buenas prácticas en el manejo seguro de bases de datos Open Source .

Las entrevistas proporcionadas por los expertos García e Ibarra han ofrecido una visión integral y eficaz sobre los desafíos y las estrategias para mejorar la seguridad de las bases de datos Open Source en entornos gubernamentales. Ambos resaltan la importancia de implementar medidas técnicas y organizacionales, así como de promover una cultura de seguridad en toda la organización para proteger la información sensible de manera efectiva.

DISCUSION DE RESULTADOS

En relación a los autores (Straub, 2022) que indican que, MySQL Es uno de los sistemas de gestión de bases de datos relacionales más populares y ampliamente utilizados en todo el mundo. Es conocido por su velocidad, confiabilidad y facilidad de uso, y es ampliamente utilizado en una variedad de aplicaciones, desde sitios web hasta sistemas empresariales.

Y por otro lado el autor (Turnbull, 2019) que hace referencia a PostgreSQL como Otro sistema de gestión de bases de datos relacional de código abierto muy popular. PostgreSQL es conocido por su robustez, capacidades avanzadas y cumplimiento con los estándares ANSI SQL. Es una opción común para aplicaciones que requieren un alto nivel de seguridad y soporte para datos complejos.

> *El uso de bases de datos Open Source , como MySQL y PostgreSQL, ha aumentado significativamente en los últimos años debido a su popularidad, confiabilidad y flexibilidad. Sin embargo, la seguridad de estas bases de datos sigue siendo una preocupación importante para muchas organizaciones. En este análisis, exploraremos cómo MySQL y PostgreSQL abordan la seguridad y qué consideraciones deben tenerse en cuenta al utilizar estas plataformas.*
>
> *MySQL es ampliamente reconocido como uno de los sistemas de gestión de bases de datos relacionales más populares y utilizados en todo el mundo. Su reputación se debe en gran parte a su velocidad, confiabilidad y facilidad de uso. Sin embargo, en lo que respecta a la seguridad, MySQL ha enfrentado críticas en el pasado debido a ciertas vulnerabilidades y debilidades en su diseño. Aunque MySQL ofrece características básicas de seguridad, como la autenticación de usuarios y el cifrado de contraseñas, los administradores de bases de datos deben implementar medidas adicionales, como actualizaciones regulares y configuraciones adecuadas, para proteger sus datos de amenazas externas e internas.*

Por otro lado, PostgreSQL es otro sistema de gestión de bases de datos relacional de código abierto muy popular. A diferencia de MySQL, PostgreSQL se destaca por su robustez, sus capacidades avanzadas y su estricto cumplimiento con los estándares ANSI SQL. Estas características lo convierten en una opción común para aplicaciones que requieren un alto nivel de seguridad y soporte para datos complejos. PostgreSQL ofrece una amplia gama de características de seguridad, que incluyen control de acceso a nivel de fila, encriptación de datos, funciones de auditoría y autenticación avanzada. Además, la comunidad activa detrás de PostgreSQL garantiza que se aborden rápidamente las vulnerabilidades y se proporcionen actualizaciones regulares de seguridad.

A pesar de las diferencias entre MySQL y PostgreSQL, ambos sistemas de gestión de bases de datos Open Source comparten ciertas consideraciones de seguridad clave que deben tenerse en cuenta al utilizarlos en entornos de producción. En primer lugar, es fundamental mantenerse actualizado con las últimas versiones y parches de seguridad para mitigar el riesgo de vulnerabilidades conocidas. Además, se recomienda encarecidamente implementar prácticas de seguridad estándar, como el principio de menor privilegio, la auditoría de eventos y la gestión adecuada de contraseñas.

En conclusión, MySQL y PostgreSQL son dos opciones sólidas y confiables para la gestión de bases de datos Open Source . Sin embargo, la seguridad debe ser una preocupación primordial para cualquier organización que utilice estas plataformas. Al implementar medidas adecuadas de seguridad y seguir las mejores prácticas recomendadas, las organizaciones pueden aprovechar al máximo las ventajas de MySQL y PostgreSQL mientras protegen sus datos de posibles amenazas. Es importante recordar que la seguridad de la base de datos es un proceso continuo y que debe ser revisado y actualizado regularmente para mantenerse al día con las últimas amenazas y vulnerabilidades.

Además, para abaratar costos, es fundamental el ahorro en licencias y es necesario seguir los lineamientos de políticas gubernamentales que indican preferir lo Open Source.

CONCLUSIONES

Las entrevistas con expertos en tecnología, García e Ibarra, están estrechamente relacionadas con el objetivo de optimizar y fortalecer la seguridad en las bases de datos Open Source de los GADS Cantonales de Los Ríos. Estos hallazgos han proporcionado una guía que permitirá identificar los desafíos actuales que tienen las municipalidades y establecer buenas prácticas para mejorar la seguridad de las bases de datos en estos estamentos públicos.

Es importante la gestión eficiente de actualizaciones y parches de seguridad, esto además lo han resaltado los expertos que han sido entrevistados, alineándose directamente con el objetivo relacionado con la optimización de la seguridad en las bases de datos Open Source, ya que con la implementación oportuna de parches y actualizaciones puede lograrse una mitigación de riesgos y fortalecer la infraestructura de seguridad de los GADS Cantonales.

Se concluye también que es sumamente importe la configuración de permisos y autenticación mencionada por el Ing. García e Ibarra, pues confirma la necesidad de establecer políticas institucionales de seguridad sólidas apuntando específicamente en las bases de datos de los GADS Cantonales. Es necesaria la aplicación de mecanismos para una eficiente autenticación y la asignación de privilegios debe realizarse de manera planificada y con un análisis claro de los roles de cada usuario, son la clave para optimizar la seguridad y proteger la información de accesos no autorizados.

El buen manejo y gestión de privilegios de acceso, es destacada por expertos entrevistados, y es fundamental tomar esto en cuenta para garantizar que solo el personal autorizado tenga el acceso y pueda modificar la información de manera segura; esta consideración es fundamental para los GADS Cantonales, donde la integridad y confidencialidad de los datos son muy importantes para el funcionamiento eficiente de los servicios.

La capacitación no deja de ser importante en temas de seguridad y son relevantes para fortalecer una cultura participativa en todos los empleados de los GADS Cantonales, ya que al diseñar un programa de educación que abarque desde lo básico hasta aspectos

técnicos, se pueden promover buenas prácticas en el manejo seguro de las bases de datos Open Source.

RECOMENDACIONES

Se recomienda a los departamentos de Tecnologías de los GAD el desarrollo de políticas institucionales, con una socialización integral, así como también la gestión de actualizaciones y parches de seguridad para los sistemas, estableciendo protocolos claros que permita su identificar, aplicación y validación (parches y actualizaciones de seguridad) de forma oportuna. Esto les brindará una ayuda para mitigar algún riesgo de violaciones de seguridad a bases de datos y permitirá mantener una infraestructura sana y actualizada.

Así mismo, se recomienda reforzar configuraciones relacionados con roles y permisos de usuarios, esto es, incluir en las políticas de seguridad de bases de datos como se indicó anteriormente implementar una configuración y lógica o tabla de permisos y roles de forma adecuada que limite el acceso a la información sensible solo al personal necesario.

También se recomienda una mejora en la autenticación y controles de acceso, esto es, poner a funcionar mecanismos de autenticación robustos, desde el acceso al datacenter, conectividad en red a la base de datos (debería ser por una única IP y MAC para asuntos de mantenimiento). Además, se recomienda establecer controles de acceso granular que permita asignar privilegios según las responsabilidades y funciones específicas de cada usuario.

Evaluar periódicamente la eficiencia con la ayuda de auditorías externas o internas para desarrollar eficacia en cuanto a medidas de seguridad implementadas y que estas permitan detectar posibles vulnerabilidades o nuevas técnicas que puedan hacer débiles los sistemas de las instituciones.

Implementar programas de capacitación para todo el personal involucrado en la gestión de bases de datos Open Source de forma regular, estos deben abarcar aspectos

técnicos y de comportamiento, así como tener un enfoque en la identificación y respuesta adecuada frente a posibles amenazas y agujeros de seguridad.

Establecer de forma coordinada un equipo de respuestas inmediatas ante incidentes de seguridad, esto es designar a profesionales responsables de gestionar y responder a posibles incidentes de seguridad catalogados previamente para que de manera rápida se pueda intervenir. Este equipo debe contar con la capacitación suficiente y las credenciales de acceso a la infraestructura acorde con sus roles y funciones dentro de esta estrategia.

Al implementar estas recomendaciones, los GADS Cantonales de Los Ríos pueden fortalecer significativamente la seguridad de sus bases de datos Open Source y proteger la información sensible de manera efectiva. La seguridad de los datos es fundamental para el buen funcionamiento de los servicios gubernamentales y la confianza del público, por lo que invertir en medidas de seguridad sólidas es una prioridad para cualquier organización gubernamental.

Referencias Bibliográficas:

- Alex Singleton, S. S. (2019). *Urban Analytics.* University of Chicago Press.
- Appigatla, K. (2022). *MySQL 8 Cookbook: Over 150 recipes for high-performance database querying and administration.* nueva Dely: Packt Publishing.
- Bazzell, M. (2020). *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information.* Boston: Independently published.
- Chauhan, C. (2020). *PostgreSQL High Performance Cookbook.* Packt Publishing.
- Claudio Coletta, L. E. (2018). *Smart Cities: Introducing Digital Innovation to Cities.* Routledge.
- Kerrisk, M. (2019). *The Linux Programming Interface: A Linux and UNIX System Programming Handbook.* No Starch Press. doi:
- Kleppmann, M. (2021). *Designing Data-Intensive Applications: The Big Ideas Behind Reliable, Scalable, and Maintainable Systems.* Boston: O'Reilly Media.
- Rabinovich-Einy, E. K. (2021). *Digital Justice: Technology and the Internet of Disputes.* Oxford University Press.
- Ross, R. K. (2019). *The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling.* Wiley.
- Schönig, H.-J. (2018). *Mastering PostgreSQL 11: Expert techniques to build scalable, reliable, and fault-tolerant database applications, 2nd Edition.* Packt Publishing.
- Simon Marvin, A. L.-A. (2021). *Smart Urbanism: Utopian Vision or False Dawn?* Routledge.
- Straub, S. C. (2022). *Pro Git.* Barcelona: Apress.

- Turnbull, J. (2019). *The Art of Monitoring: A Field Guide for Novice to Professional.* Stambul: O'Reilly Media.
- Waer, M. D. (2021). *Smart Cities: Governing, Modelling and Analysing the Transition.* Routledge.
- Winand, M. (2018). *SQL Performance Explained (Everything Developers Need to Know about SQL Performance).* ilinois: Markus Winand.

ANEXOS

ANEXO 1

Guía de entrevista:

ENTREVISTA BASADA EN LA GUIA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Optimización y Fortalecimiento de la Seguridad en Bases de Datos Open Source de GADS Cantonales de Los Ríos

Nombre del Profesional:

Empresa: GAD del Cantón BABA

Cargo: Coordinador de TICS

Objetivo: Servir como referencia para el análisis de resultados relacionado con la seguridad de bases de datos Open Source

1. Desde su experiencia, ¿cuáles consideras que son los mayores desafíos en términos de seguridad al trabajar con bases de datos Open Source en entornos gubernamentales como los GADS Cantonales de Los Ríos

2. ¿Qué estrategias propondría para mejorar la seguridad de las bases de datos Open Source utilizadas por los GADS Cantonales, teniendo en cuenta tanto aspectos técnicos como organizacionales?

3. ¿Cómo abordaría la gestión de privilegios y accesos en las bases de datos Open Source para garantizar que solo personal autorizado pueda acceder y modificar la información de manera segura?

4. Considerando la importancia de la capacitación y concienciación del personal en temas de seguridad, ¿cómo diseñaría un programa efectivo de educación para el personal de los GADS Cantonales con el fin de promover buenas prácticas en el manejo seguro de bases de datos Open Source ?

ANEXO 2

RESPUESTA A ENTREVISTA BASADA EN LA GUIA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Optimización y Fortalecimiento de la Seguridad en Bases de Datos Open Source de GADS Cantonales de Los Ríos

Nombre del Profesional: ING. GALO GARCIA

Empresa: GAD del Cantón BABAHOYO

Cargo: Especialista de TICS

Objetivo: Servir como referencia para el análisis de resultados relacionado con la seguridad de bases de datos Open Source

1. **Desde su experiencia, ¿cuáles consideras que son los mayores desafíos en términos de seguridad al trabajar con bases de datos Open Source en entornos gubernamentales como los GADS Cantonales de Los Ríos?**

   Como experto en bases de datos, considero que uno de los mayores desafíos en términos de seguridad al trabajar con bases de datos Open Source en entornos gubernamentales radica en la gestión adecuada de los parches y actualizaciones de seguridad. Dado que las bases de datos Open Source están constantemente expuestas a nuevas vulnerabilidades, es esencial contar con un proceso sólido para identificar, aplicar y validar parches de seguridad de manera oportuna.

   Otro desafío importante es la configuración adecuada de los permisos y la autenticación. En entornos gubernamentales, donde la información es sensible y altamente regulada, es crucial garantizar que solo el personal autorizado tenga acceso a los datos pertinentes. Esto implica implementar políticas de seguridad sólidas, así como mecanismos de autenticación robustos, como la autenticación de dos factores, para mitigar el riesgo de accesos no autorizados.

2. **¿Qué estrategias propondría para mejorar la seguridad de las bases de datos Open Source utilizadas por los GADS Cantonales, teniendo en cuenta tanto aspectos técnicos como organizacionales?**

   Una estrategia integral para mejorar la seguridad de las bases de datos Open Source en los GADS Cantonales debería abordar tanto aspectos técnicos como organizacionales. En el ámbito técnico, se deben

implementar medidas como la encriptación de datos en reposo y en tránsito, el monitoreo continuo de la actividad de la base de datos para detectar posibles intrusiones, y la segmentación de la red para limitar la exposición de las bases de datos a posibles ataques.

A nivel organizacional, es fundamental establecer políticas y procedimientos claros en materia de seguridad de la información, así como fomentar una cultura de seguridad en toda la organización. Esto incluye la capacitación regular del personal en buenas prácticas de seguridad, la designación de responsables de seguridad de la información y la realización de auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad establecidas.

3. **¿Cómo abordaría la gestión de privilegios y accesos en las bases de datos Open Source para garantizar que solo personal autorizado pueda acceder y modificar la información de manera segura?**

Para abordar la gestión de privilegios y accesos en las bases de datos Open Source , propondría implementar un modelo de privilegios basado en el principio de "menos privilegios", donde cada usuario tenga únicamente los permisos necesarios para realizar sus funciones específicas. Esto implica definir roles de usuario con conjuntos de privilegios bien definidos y asignar estos roles de manera adecuada según las responsabilidades de cada usuario.

Además, se deben establecer mecanismos de autenticación sólidos, como la autenticación de dos factores o el uso de claves de acceso fuertes, para garantizar que solo el personal autorizado pueda acceder a la base de datos. También es importante llevar un registro detallado de las actividades de acceso y modificación de la información, para poder identificar y

responder rápidamente a posibles anomalías o intentos de acceso no autorizados.

4. **Considerando la importancia de la capacitación y concienciación del personal en temas de seguridad, ¿cómo diseñaría un programa efectivo de educación para el personal de los GADS Cantonales con el fin de promover buenas prácticas en el manejo seguro de bases de datos Open Source ?**

Diseñaría un programa de educación en seguridad de bases de datos Open Source que abarque tanto aspectos técnicos como comportamentales. Esto incluiría sesiones de formación práctica sobre cómo configurar y mantener de manera segura las bases de datos Open Source utilizadas por los GADS Cantonales, así como talleres interactivos sobre buenas prácticas en el manejo de contraseñas, el reconocimiento de posibles amenazas y la respuesta adecuada ante incidentes de seguridad.

Además, organizaría charlas y seminarios con expertos en seguridad de la información para sensibilizar al personal sobre la importancia de la seguridad y las implicaciones de un manejo inadecuado de la información sensible. También promovería la participación en cursos de certificación en seguridad de bases de datos Open Source para aquellos empleados que deseen profundizar sus conocimientos en este campo.

RESPUESTA A ENTREVISTA BASADA EN LA GUIA

Universidad Técnica de Babahoyo

Facultad de Administración, Finanzas e Informática

Optimización y Fortalecimiento de la Seguridad en Bases de Datos Open Source de GADS Cantonales de Los Ríos

Nombre del Profesional: ING. IBARRA MACIAS CRISTHIAN

Empresa: GAD del Cantón QUEVEDO

Cargo: COORDINADOR DE TECNOLOGIAS DE LA INFORMACION

Objetivo: Servir como referencia para el análisis de resultados relacionado con la seguridad de bases de datos Open Source

1. **Desde su experiencia, ¿cuáles consideras que son los mayores desafíos en términos de seguridad al trabajar con bases de datos Open Source en entornos gubernamentales como los GADS Cantonales de Los Ríos?**

   Los principales desafíos en seguridad al trabajar con bases de datos Open Source en entornos gubernamentales como los GADS Cantonales de Los Ríos incluyen la gestión adecuada de vulnerabilidades, la configuración segura de los sistemas, y la protección de los datos sensibles. Dado que las bases de datos Open Source son accesibles para cualquier persona, existe un mayor riesgo de exposición a amenazas externas e internas, lo que requiere una atención especial a la seguridad.

2. ¿**Qué estrategias propondría para mejorar la seguridad de las bases de datos Open Source utilizadas por los GADS Cantonales, teniendo en cuenta tanto aspectos técnicos como organizacionales?**

   Una estrategia integral debería incluir medidas técnicas y organizacionales. En el aspecto técnico, se deben implementar

actualizaciones regulares de seguridad, configuraciones robustas, cifrado de datos sensibles, y la utilización de herramientas de monitoreo y detección de intrusiones. A nivel organizacional, se debe establecer una política de seguridad clara y promover una cultura de seguridad, involucrando a todos los niveles de la organización en la protección de los datos.

3. **¿Cómo abordaría la gestión de privilegios y accesos en las bases de datos Open Source para garantizar que solo personal autorizado pueda acceder y modificar la información de manera segura?**

   La gestión de privilegios y accesos es fundamental para la seguridad de las bases de datos. Se deben implementar prácticas de principio de menor privilegio, asignando permisos de manera restrictiva según las funciones y responsabilidades de cada usuario. Además, es importante establecer un proceso de revisión y auditoría periódica de los accesos para detectar y mitigar posibles riesgos de seguridad.

4. **Considerando la importancia de la capacitación y concienciación del personal en temas de seguridad, ¿cómo diseñaría un programa efectivo de educación para el personal de los GADS Cantonales con el fin de promover buenas prácticas en el manejo seguro de bases de datos Open Source ?**

   Un programa efectivo de educación en seguridad debería abarcar aspectos técnicos y de comportamiento. Se pueden ofrecer sesiones de capacitación sobre el uso seguro de bases de datos Open Source , destacando las mejores prácticas en gestión de contraseñas, manejo de datos sensibles y detección de posibles amenazas. Además, es importante fomentar una cultura de denuncia y colaboración, donde los empleados se sientan cómodos reportando incidentes de seguridad y participando en la mejora continua del sistema de seguridad de la organización.