UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA

CARRERA DE SISTEMAS DE INFORMACIÓN

PROCESO DE TITULACIÓN

OCTUBRE 2023 - MARZO 2024

EXAMEN COMPLEXIVO DE GRADO DE CARRERA PRUEBA PRÁCTICA

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

TEMA:

ANÁLISIS DE SEGURIDAD EN EL DESPLIEGUE DE POSTGRES CON CONTENEDORES DOCKER PARA GARANTIZAR LA INTEGRIDAD DE LA INFORMACIÓN EN EL SUPERMERCADO ESCOBAR DEL CANTÓN VINCES

ESTUDIANTE:

SANTIAGO ALEJANDRO VERGARA BENAVIDES

TUTOR:

ING. FABIAN ALCOSER CANTUÑA.

AÑO

2024

Contenido

Resumen

En el presente caso de estudio se inicia con un planteamiento del problema y un desafío significativo en términos de seguridad de la información relacionado con la integridad de datos en el Super Mercado Escobar ya que es necesario su estudio para verificar continuamente su seguridad. También se presenta una justificación, pues radica una necesidad de evaluar, así como también de garantizar la seguridad en este despliegue de sus bases de datos, ya que de esta forma evita posibles vulnerabilidades que podrían comprometer la integridad y disponibilidad, así como la confidencialidad de la información crítica del mencionado supermercado.

El objetivo de este caso de estudio es analizar la seguridad en el despliegue de bases de datos PostgreSQL utilizando contenedores Docker con el propósito de garantizar la integridad de la información en el supermercado Escobar del cantón, para de esta forma lograr una temprana detección de vulnerabilidades de contenedores y mitigar alguna amenaza.

Cuenta con un marco metodológico orientado a un método de investigación cualitativo por lo que se ha realizado una entrevista al personal de tecnologías de la empresa y con lo cual se discuten y analizan los resultados para lograr concluir y recomendar las mejores practicas productos de este caso de estudio. El caso de estudio no solo ofrecerá a las recomendaciones prácticas favoreciendo la seguridad, sino también brinda un análisis en el contexto de las buenas prácticas que pueden existir en una organización, donde contribuyen personas capacitadas en seguridad informática y bases de datos para abordar desafíos reales.

Palabras Claves

Docker, Postgres, Contenedores, Linux, Seguridad

Abstract

This case study begins with a statement of the problem and a significant challenge in terms of information security related to data integrity in the Escobar Super Market since its study is necessary to continuously verify its security. A justification is also presented, since there is a need to evaluate, as well as guarantee security in this deployment of its databases, since in this way it avoids possible vulnerabilities that could compromise the integrity and availability, as well as the confidentiality of the critical information of the aforementioned supermarket.

The objective of this case study is to analyze the security in the deployment of PostgreSQL databases using Docker containers with the purpose of guaranteeing the integrity of the information in the Escobar supermarket of the canton, in order to achieve early detection of security vulnerabilities. containers and mitigate any threats.

It has a methodological framework oriented towards a qualitative research method, for which an interview has been carried out with the company's technology personnel and with which the results are discussed and analyzed to conclude and recommend the best practices products of this case of study. The case study will not only offer practical recommendations promoting security, but also provides an analysis in the context of good practices that may exist in an organization, where people trained in computer security and databases contribute to address real challenges.

Key Words

Docker, Postgres, Container, Linux, Security

Planteamiento del Problema

El supermercado Escobar que está ubicado en Vinces, ha decidido cambiar su sistema actual por un sistema de base de datos como PostgreSQL, Adicional a esto con contenedores Docker para de esta manera mejorar su flexibilidad y escalabilidad en relación a su infraestructura de sistemas tecnológicos. Sin embargo, se plantea una problemática y un desafío significativo en términos de seguridad de la información ya que la integridad de datos es fundamental para que funcione de manera adecuada el supermercado pues cualquier compromiso que atente con la seguridad puede resultar una pérdida o tratarse de una manipulación informática crítica afectando así a transacciones financieras registros de inventarios y hasta a datos de clientes.

El despliegue de PostgreSQL dentro de contenedores Docker introduce también posibles vulnerabilidades de seguridad, las cuales podrían ser generadas por amenazas externas o internas. Estas posibles vulnerabilidades podrían incluir técnicas de ataques donde se inyecta el código de SQL así como accesos no autorizados a la base de datos al no tener bien definida sus reglas y sus permisos además de la exposición de datos por la utilización de puertos que no han sido bloqueados desde un firewall o mal configurados así como brechas o espacios en la autenticación de los usuarios para la autorización de accesibilidad.

Por lo tanto, se considera que el problema principal que enfrenta el supermercado Escobar es el de garantizar la seguridad en la integridad de la información almacenada en sus bases de datos postres implementando contenedores Docker como medida de protección ante posibles amenazas futuras y actuales asegurando de esta manera la de sus operaciones sin comprometer integridad confidencialidad disponibilidad de datos críticos para el negocio.

Este caso de estudio se centrará en analizar investigar y por poner estrategias eficaces que permitan abordar estas preocupantes formas de inseguridad considerando evaluar las mejores prácticas y configuraciones, así como el monitoreo y gestión de todo riesgo existente en torno a su base de datos en el contexto del despliegue de postres con contenedores Docker en el entorno del supermercado Escobar de Vinces

En el ámbito actual de desarrollo de software se está utilizando mucho contenedores Docker los cuales se han convertido en una práctica común que facilita su implementación permitiendo escalar aplicaciones. Sin embargo, su seguridad depende mucho del despliegue de aplicaciones mediante contenedores bien diseñados y configurados especialmente en lo que refiere a la garantía de la integridad de la información la opción generalizada de esta tecnología no debe ser un riesgo, y es necesario que puedan abordarse configuraciones eficientes de manera efectiva.

En relación con este planteamiento problémico, se puede destacar la necesidad de realizar un análisis exhaustivo en el contexto de la seguridad e integridad de la información almacenada y procesada en las aplicaciones que serán desplegadas contenedores Docker. Estos contenedores, al encapsular sus aplicaciones y dependencias, ofrecen grandes beneficios entorno a la portabilidad y eficiencia, sin embargo también introducen posibles agujeros vulnerabilidades que podrían comprometer fuertemente la confidencialidad e integridad de los datos.

Justificación

El despliegue de postgreSQL dentro de Docker para el supermercado Escobar en el cantón Vinces representa una solución informática moderna brindándole flexibilidad para la gestión eficiente de su infraestructura de bases de datos, Pero esta decisión implica desafío significativos en cuanto a la seguridad de la información ya que estos son vitales para la continuidad de las operaciones del negocio

Se justifica este caso de estudio, pues radica una necesidad de evaluar así como también de garantizar la seguridad en este despliegue de sus bases de datos, ya que de esta forma evita posibles vulnerabilidades que podrían comprometer la integridad y disponibilidad así como la confidencialidad de la información crítica del mencionado supermercado. Esta evaluación realizada en el presente caso de estudio permitirá poner a funcionar medidas preventivas y correctivas de manera eficiente y adecuadas, asegurando una continuidad operativa inquebrantable de ser el caso, para que el negocio se mantenga operativo y sostenga una protección de sus datos sensibles ante amenazas posibles que pueden ser internas o externas.

Es importante mencionar que la elección de este caso de estudio se ha fundamentado en la creciente moda de tecnología con contenedores Docker al tener buenas referencias de este como una tecnología clave para el despliegue de aplicaciones.

La utilización generalizada de Docker para el despliegue de aplicaciones ha generado un cambio significativo en la construcción de software, por lo que este caso de estudio de fin de carrera se justifica dado que existe la necesidad de comprender y mitigar los posibles riesgos de seguridad inherentes en esta tecnología, particularmente en lo que respecta a la integridad y seguridad de la información.

La utilización de contenedores coloca nuevas capas de dificultad en la configuración del SO y, por lo tanto, generar posibles vulnerabilidades o agujeros y no ajustar podrían comprometer completamente la integridad de datos e información. Este documento seguramente contribuirá con identificar y abordar específicamente estas vulnerabilidades que pueden ir apareciendo.

La integridad de los datos e información es crucial para poder garantizar la confidencialidad y fiabilidad de los datos que se encuentran almacenados y ya procesados por aplicaciones en los entornos de Docker. En tal sentido, esta investigación permitirá evaluar y mejorar todos los mecanismos de seguridad que le permitan mantener una integridad de la información en todo momento.

El análisis propuesto permitirá proporcionar hallazgos valiosos para la comunidad académica y empresarial que consulte este documento, ofreciéndoles recomendaciones prácticas y estratégicas aplicadas a la seguridad donde estas puedan ser aplicadas directamente para mejorar la integridad de datos e información en despliegues con Docker.

Esta investigación además se justifica por su relevancia actual y su potencial para abordar vulnerabilidades que van apareciendo, así como el impacto en la confidencialidad y fiabilidad de datos que estas pueden generar al implantarse, además de, su contribución con la comunidad académica y empresarial por la importancia en la formación de profesionales en ciberseguridad. La seguridad en el despliegue de aplicaciones con contenedores Docker no puede ser una preocupación crítica que este caso de estudio pues se propone abordar para que sea una solución integral.

Objetivos

Objetivo General

Analizar la seguridad en el despliegue de bases de datos postgres utilizando contenedores docker con el propósito de garantizar la integridad de la información en el supermercado Escobar del cantón

Objetivos específicos

- Detectar vulnerabilidades específicas en la configuración, gestión de imágenes, redes y otros aspectos críticos de los entornos de contenedores que permitan mitigar amenazas
- Recomendar consideraciones técnicas y prácticas efectivas para fortalecer la seguridad y preservar la integridad de los datos en el contexto tecnológico de Docker.
- Investigar las amenazas específicas asociadas con el uso de bases de datos y contenedores y cómo afectan la integridad de la información.

Línea de Investigación

Este trabajo está alineado con la línea de investigación de: Sistemas de información y comunicación, emprendimiento e innovación, este además está estrechamente vinculado con una sublínea de investigación de: Redes y tecnologías inteligentes de software y hardware.

Es importante mencionar además que este estudio se articula con la práctica pre profesional que ha sido realizada en la Biblioteca de la Facultad de Ciencias de La Salud de la Universidad Técnica de Babahoyo, ya que se realizaron actividades que tenían relación con la gestión de bases de datos por lo que se utilizaba postgres para ciertos temas de registro y como no se contaba con servidores, se administraba la información de las bases de datos con cautela por lo que se pensaba en la posibilidad de encapsularlos en contenedores.

También es necesario informar, que la sub línea de investigación se la vincula estrechamente con actividades cotidianas y secundaria que se realizaban en el mencionado espacio de pasantías que son mantenimientos de sistemas operativos, computadoras, impresoras.

Marco Conceptual

Importancia de las Bases de Datos

Las bases de datos están presentes en todos lados, y tienen un papel fundamental en el mundo empresarial, siendo estos elementos esenciales en todos los aspectos de la vida cotidiana moderna. Son utilizadas desde aplicaciones para móviles hasta sistemas empresariales complejos y grandes, estos sistemas de bases de datos proporcionan medios eficientes y organizados para gestionar información. Esta importancia o beneficios deriva de una serie de factores claves que pueden abarcar desde la eficiencia entorno al almacenamiento de datos hasta ser un soporte en la toma de decisiones informadas. (Fontaine, 2020)

En primer lugar, se puede indicar que, las bases de datos representan una estructura organizada y eficiente que permiten almacenar grandes volúmenes de datos para transformarlos luego en información útil. (Norman, 2022)

Además, posee un almacenamiento eficaz, que proporciona a empresas capacidades avanzadas de recuperación y gestión datos de forma rápida y precisa. Mediante consultas SQL y comandos específicos, los usuarios pueden manipular y construir información relevante desde los datos que se encuentran en la base de datos en cuestión de pocos milisegundos, lo que permite una toma fácil de decisiones oportunas y fundamentadas en información real y dinámica. Estas capacidades de consulta también permiten que puedan analizarse datos históricos, para de esta manera sea más fácil el identificar patrones y tendencias, así como proyectar y pronosticar resultados futuros, lo que resulta invaluable conservar una planificación estratégica. (PostgreSQL Magazine, 2021)

Las bases de datos desempeñan un papel importante en la mejora de la eficiencia organizativa en diversos aspectos de la sociedad además de que su utilidad en entornos empresariales es extrema, en sectores como el de la salud, por citar un ejemplo, las bases de datos médicas le permiten a profesionales el acceso rápido a la información sobre tratamiento de pacientes y resultados de forma eficaz, lo que conlleva salvar vidas en situaciones de emergencia con ser simplemente eficiente y agiles. Así mismo, en el ámbito de la educación, el manejo de bases de datos académicas le facilitan un seguimiento del estado de los estudiantes, su progreso y la gestión de registros, así como también la planificación de programas educativos. (Abomhara, 2021)

La seguridad de Bases de Datos

La seguridad en el contexto de las bases de datos es uno de los aspectos más críticos de la ciberseguridad, donde se mueven billones de dólares al año por estos temas de protección de datos, donde la información es considerada uno de los activos más valiosos para gerentes, empresas y organizaciones. La protección de datos almacenados en sus bases de datos es de vital importancia, es una de las tareas más recurrentes en el ámbito tecnológico hacia dentro del Data Center pues es crucial garantizar la confidencialidad, integridad y disponibilidad de la información en todo momento, así como también para evitar riesgos de robo y extracción de datos, manipulaciones maliciosas e interrupciones en los servicios. (Slawomir Chodnicki, 2020)

Como punto de partida, puede indicarse que la seguridad de las bases de datos es necesaria y esencial para lograr proteger la información empresarial confidencial y sensible, las bases de datos en la mayoría de los casos suelen contener datos como información personal de clientes, datos de empleados, registros financieros, y secretos

comerciales que deben estar bien resguardados porque de eso puede depender una empresa en su totalidad. (Mercuri, 2021)

Además de su confidencialidad, el tema de la seguridad en bases de datos también hace referencia a la integridad de la información. Esto supone asegurarse de que los datos almacenados sean consistentes, precisos y que no hayan sido manipulados o cambiados de manera no autorizada. (Mercuri, 2021)

(Cynthia Dwork, 2021) Opinan que, otro de los aspectos importantes en relación a la seguridad en bases de datos es el poder garantizar la disponibilidad de la información, es decir, que se debe lograr su acceso en el momento cuando sea necesario. La existencia de interrupciones relacionadas con el servicio por los ciberataques, fallos en el hardware de los servidores o errores generan un impacto grande dentro de sus operaciones comerciales, causando molestias y financieras así como daños en la reputación. Para mitigar estos riesgos, es muy necesario implementar medidas estratégicas como mantener copias de seguridad automáticas generando patrones de redundancia de datos, además de desarrollar planes de recuperación ante de tener algún desastre. (Mercuri, 2021)

Los contenedores Docker

Los contenedores Docker han revolucionado a medida que se desarrollan, implementan y administran aplicaciones en entornos informáticos modernos. Estos contenedores proporcionan una solución liviana y portátil la cuál permite empacar, distribuir y ejecutar aplicaciones, de manera consciente se puede realizar en cualquier entorno. La importancia de los contenedores Docker en la tecnología se explotan en esta síntesis. (Paul C. van Oorschot, 2020)

Este contenedor tiene como ventaja la capacidad para crear aplicaciones y le garantiza reproducibilidad en diferentes plataformas y sistemas operativos. Para ejecutar una aplicación encapsulan todas las configuraciones necesarias para ejecutar, esto ayuda a eliminar los problemas de incompatibilidad y diferencias en este entorno de desarrollo. Esto facilita el desarrollo y la implementación de aplicaciones en entornos heterogéneos, lo que acelera el ciclo de vida del desarrollo de software, así como también mejora la eficiencia operativa. (Kuenzli, 2021)

En comparación con las máquinas virtuales tradicionales, el contenedor de acoplamiento también ofrece un mayor rendimiento. Debido a sus sistemas operativos arquitectónicos y básicos de luz, el uso habitual de los recursos, la hora de inicio del contenedor es más rápida, la huella es baja y el consumo de recursos es bajo. Esto permite una mayor densidad de contenedores en el mismo hardware físico, mejorando así la utilización de los recursos y la eficiencia del uso de la infraestructura de TI.

Otro factor importante en el contexto de los contenedores Docker es la capacidad que tiene para facilitar la integración y entrega continua en procesos preparados para desarrollo de software. Estos contenedores proporcionan entornos confiables y

consistente y predecibles para crear, poner a prueba y hasta implementar aplicaciones de forma automática, esto permite que los equipos de desarrollo hagan cambios en producción de forma rápida y oportuna con toda confianza. Además, fomenta la cultura de desarrollo colaborativo y ágil para que los equipos pueden mejorar continuamente sus aplicaciones sin comprometer seguridad ni estabilidad. (Paul C. van Oorschot, 2020)

Los Docker permiten una escalabilidad y mejora de aplicaciones distribuidas, estos contenedores resultan modulares y son fácilmente replicables permitiendo que las aplicaciones puedan escalar según las necesidades de las organizaciones, garantizando rendimientos óptimos de carga. (Gupta, 2022)

La tecnología de los contenedores Docker están modificando la forma en que se desarrollan, implementan y ejecutan algunas aplicaciones en ambientes informáticos renovados, la eficacia y capacidad que tienen para automatizar procesos permite a las organizaciones agilizar la entrega de productos de software y mantenerlos asegurados en una capsula, esto permite una mejora en las operaciones y son esto se adopta eficazmente arquitecturas distribuidas y una mejora en tecnologías de computación en la nube, convirtiéndolo a las organizaciones a un a cambios eficientes. (Almagro, 2020)

Seguridad de la Base de Datos Postgres con Docker

Proteger Docker y PostgreSQL es fundamental para proteger los datos confidenciales, mitigar los riesgos de seguridad, garantizar la continuidad del negocio, cumplir con las regulaciones y mantener la confianza del cliente. (Miguel A. Alba, 2019) consideran que, implementar sólidas medidas de seguridad y seguir las mejores prácticas en ambas plataformas es una máxima prioridad para cualquier organización que desee proteger sus activos digitales y seguir siendo competitivo en un entorno empresarial cada vez más digital y comprometido.

Se detalla a continuación algunas razones por las que hay que proteger a Docker y PostgreSQL, pueden contener datos confidenciales, como información personal, financiera o comercial, es necesario proteger estas tecnologías privando el acceso no autorizado, la manipulación maliciosas.

Ambos tienen vulnerabilidades de seguridad potenciales, si no se configuran adecuadamente, estos pueden pueden vulnerables a inyección de código, ataques DoS y otra explotación de vulnerabilidades conocidas.

Es fundamental para diversas actividades comerciales, dejar un agujero de seguridad en cualquiera de estas plataformas tecnologicas puede provocar interrupciones en el servicio y afectar la productividad de la empresa.

.

Análisis teórico Postgres y Docker

Tabla 1. Comparativo del ambiente de seguridad en el despliegue de PostgreSQL con y sin contenedores Docker para garantizar la integridad de la información

Aspecto Importante de Seguridad	Despliegue del PostgreSQL con Docker	Despliegue del PostgreSQL sin tener Docker
Escalabilidad	Docker puede facilitar la escalabilidad, permitiendo agregar o eliminar contenedores según le sea necesario para así satisfacer una demanda determinada. Esto puede ayudar a distribuir una carga de trabajo y a mantener rendimientos óptimos.	La escalabilidad puede ser realmente más compleja y requerir de algunas implementaciones manuales de instancias adicionales de PostgreSQL, lo que podría conllevar a más tiempo y esfuerzo.
Aislamiento de Aplicaciones	Contenedores Docker proveen aislamiento a nivel de aplicación, ayudando en si a prevenir las interferencias entre diferentes aplicaciones y permite reducir el impacto de algunas vulnerabilidades.	Sus aplicaciones pueden compartir recursos con el SO anfitrión, esto aumenta un poco el riesgo de interferencias y la propagación de vulnerabilidades críticas.
Seguridad de Contenedores	Docker proporciona, además, características de seguridad ya integradas, pala el aislamiento de recursos, control de acceso y capacidad de cifrado, esto ayuda a proteger los contenedores y su información.	La seguridad depende mucho de la configuración y el mantenimiento que se le dé al SO y a las aplicaciones, lo que puede ser muy propenso a errores y vulnerabilidades.
Gestión de Dependencias	Docker permite que se incluyan todas las dependencias necesarias para poder desplegar PostgreSQL dentro del contenedor, lo que garantiza que todas las bibliotecas y configuraciones requeridas van a estar presentes, de esta forma se genera consistencia en todos los entornos.	Sin Docker, se puede tener una gestión de dependencias abrumadora y puede ser más complicada, sobre todo propensa a errores, especialmente cuando se desea migrar entre diferentes sistemas o versiones en el caso de Bases de Datos
Gestión de Vulnerabilidades	Con Docker, es posible que se puedan utilizar herramientas automatizadas para el escaneo de vulnerabilidades y así identificar y poder corregir a tiempo posibles problemas de seguridad en contenedores y todas sus dependencias.	Sin Docker, la el manejo de las vulnerabilidades puede resultar mucho más manual y requerir de un monitoreo proactivo de actualizaciones de seguridad y parches del SO y aplicaciones.

Portabilidad	Los contenedores Docker son altamente portátiles, algo parecido a una máquina virtual y pueden ejecutarse o trasladarse a cualquier entorno compatible con Docker, lo que facilita en gran medida la migración entre servidores y las implementaciones hacia la nube.	Sin Docker, la portabilidad puede ser más compleja y requerir configuraciones adicionales que en muchos casos dificulta la adaptabilidad y en ocasiones requiere una instalación del SO completa

Fuente: El Autor (2024)

Este cuadro comparativo destaca algunas de las diferencias clave entre el despliegue de PostgreSQL con y sin contenedores Docker en términos de seguridad y gestión de la integridad de la información. La utilización de contenedores Docker ofrece varias ventajas en cuanto a aislamiento, escalabilidad, gestión de dependencias, seguridad y portabilidad, lo que puede contribuir a un entorno más seguro y eficiente para el despliegue de PostgreSQL y la protección de los datos críticos del negocio.

Tabla 2. Cuadro comparativo de los costos asociados con el despliegue de PostgreSQL utilizando Docker y sin Docker:

Aspectos a Considerar en Relación a Costos	Despliegue de PostgreSQL con Contenedores Docker	Despliegue de PostgreSQL sin Contenedores Docker
Costos de Licencias	Es de código abierto y gratuito, por lo que no hay costos de licenciamientos asociados con la utilización de Docker.	PostgreSQL así mismo, es de código abierto, gratuito, por lo que no hay costos de licencia asociados.
Costos en Infraestructura	Se requiere por lo general menos recursos en lo relacionado a infraestructura, lo que puede conduce a reducción de costos de hardware y una necesidad de servidores físicos dedicados.	Sin Docker, se necesita administrar instalaciones de PostgreSQL, como servidores dedicados o VM, esto puede conllevar a costos adicionales en infraestructuras.
Costos de Mantenimiento	Docker simplifica mucho la gestión y mantenimiento de PostgreSQL que le permiten implementar, escalar y administrar contenedores de manera autónoma. Lo que conlleva a reducir costos operativos asociados con el mantenimiento de PostgreSQL.	Sin Docker, puede ser necesario en ocasiones mucha perdida de tiempo y recursos de mantenimientos y configuraciones manuales de Bases de Datos PostgreSQL, incluido instalación, actualizaciones de seguridad, aplicación de parches y dependencias, lo que aumenta los costos operativos a largo plazo.
Costos de Capacitación	Docker requerir una curva de aprendizaje para lograr comprender su funcionamiento y las mejores prácticas, esto implica costos adicionales asociados con entrenamiento o la contratación externa de consultores.	Sin Docker, son más normales las operaciones tradicionales con PostgreSQL, lo que puede reducir los costos asociados adicionales de nuevos entrenamientos del personal.
Costos de Soporte Técnico	Así mismo, cuenta con una amplia comunidad activa y biblioteca de recursos, lo que puede reducir la necesidad de soportes costosos.	Sin Docker, podría resultar necesario contratar algún servicio especializado de soporte técnico especializado que brinde soluciones a problemas con PostgreSQL, y conlleva a gastar más en técnicos

Fuente: El Autor (2024)

Este cuadro comparativo destaca algunas de las diferencias clave en los costos asociados con el despliegue de PostgreSQL utilizando Docker y sin Docker. Si bien Docker puede implicar costos adicionales relacionados con la infraestructura y la capacitación inicial, también puede ofrecer beneficios en términos de eficiencia operativa, gestión simplificada y escalabilidad, lo que puede contribuir a una reducción de costos a largo plazo. Sin embargo, la elección entre desplegar PostgreSQL con o sin Docker dependerá de las necesidades específicas de cada organización, así como de su presupuesto y recursos disponibles.

Tabla 3. Cuadro comparativo de los costos estimados para la asesoría en el montaje de una base de datos segura utilizando Docker y sin Docker:

Aspectos de Costos	Asesorías para Docker	Asesorías sin Docker
Costos relacionados a Consultorías	Pueda variar, dependiendo de la experiencia y tarifas que tenga el ingeniero consultor. Puede ir entre $100 a $300 /hora.	Puede variar, depende de la experiencia y tarifas que tenga el consultor. Esto puede oscilar entre $100 a $300 /hora.
Duración de Asesorías	Todo puede depender de la complejidad del proyecto y el nivel de asesoramiento del caso. Podría ser entre 20 a 40 horas para montar un proyecto sencillo.	Depende también de la complejidad relacionadas con el proyecto y nivel de asesoramiento que se requiera. Un estimado puede ser entre 20 a 40 horas de un proyecto sencillo.
Costos Totales Estimados	De $2,000 a $12,000, Depende de la duración y tarifas que tenga el consultor.	De $2,000 a $12,000, Depende de tarifas que tenga el consultor.

Fuente: El Autor (2024)

Es importante tener en cuenta que estos costos son estimados en Ecuador, la experiencia del consultor y la complejidad del proyecto. Además, estos costos no incluyen posibles gastos adicionales, como herramientas o servicios complementarios que puedan ser necesarios para implementar las recomendaciones de seguridad.

Marco Metodológico

Este caso de estudio se orienta a comprender y analizar las medidas de seguridad implementadas en el supermercado Escobar del cantón Vinces, como mejoran la protección y que visión tienen para el cuidado de los datos e información, apuntando especialmente al despliegue de PostgreSQL con contenedores Docker, por lo que se empleará un enfoque cuantitativo que permita explorar en detalle las percepciones.

Metodología cuantitativa que se utilizará:

Se llevará a cabo entrevistas abiertas a personal de TIC del Super Mercado Escobar de Vinces, que permitirá comprender con una visión más cercana las formas de seguridad informática y la buena gestión de la información.

Instrumento de recolección de datos

Guía de entrevista que se ha diseñado para una exploración de aspectos técnicos claves relacionados con la forma de cómo se constituye la seguridad de la información en la organización.

Los datos recopilados

Serán una serie de pruebas llevadas a cabo con la ayuda del personal del super mercado, debido a que este caso de estudio solo es un análisis y no se quiere vulnerar seguridades ni se desea paralizar operaciones por querer realizar pruebas más invasivas.

El análisis técnico

Se lo realizará con herramientas open source que permiten verificar seguridades tipo pentesting y sobre estos hallazgos se podrá encontrar más detalles en los anexos.

Resultados

Entrevista A Personal de TIC en el supermercado Escobar del cantón Vinces

Nombre del entrevistado: Ing. Vicente Baquerizo

Fecha: 26-02-2024

Cargo: Jefe De Computo

OBJETIVO: Levantar información que permita un análisis de seguridad en el despliegue de Postgres con contenedores Docker para garantizar la integridad de la información en el supermercado Escobar del cantón Vinces

1) **Que herramientas de Bases de datos utilizan en la empresa**

   Se utilizad Postgres versión 13 porque tiene ya estabilidad madura

2) **De qué forma les brindan seguridad a las bases de datos en la empresa**

   Le aseguramos con CRON o tarea programada para que saque respaldos automatizados usando archivos script bash. Y dentro de un contenedor Docker

3) **Bajo qué sistema Operativo tienen el motor de bases de datos y cuál es la razón**

   La tenemos todo bajo Linux, porque no necesita licencias y ya llevamos varios años y conocemos el manejo de este sistema y trabaja muy bien postgres con Ubuntu Server v22

4) **Cuáles han sido las frecuentes fallas que han tenido con sus datos entre los últimos 6 meses**

   Fallas como tal no hemos tenido, solamente soportes y pruebas de nuevos complementos con el sistema y lo que se hace es sacar el contenedor que incluye la base de datos, la aplicación y la llevamos a un entorno de prueba, si todo funciona correcto solo lo copiamos donde estaba y listo.

5) **Que estrategia han utilizado para lograr el mayor tiempo de actividad con sus sistemas**

   Para lograr mayor tiempo de actividad tenemos toda una infraestructura básica de 2 servidores y uno adicional en Azure, los 2 servidores tienen ya 3 años y funcionan como nuevos aun y cuando se necesita alguna modificación solamente se utiliza el otro servidor y se vuelve casi imperceptible algún cambio.

6) **Cuál es el presupuesto que se necesita para levantar su infraestructura en caso de algún daño**

   Si es un daño de comenzar de cero, solo el costo de los servidores, que mas o menos resulta unos 8500$

7) **Como es el ambiente relacionado con los directivos para con los de Tecnologías en cuanto a apoyo de recursos.**

   Nos brindan todo el contingente necesario

8) **Que criterio usaron para colocar Docker**

   Porque tiene facilidad de despliegue, es decir, se instala fácil y uno puede encapsular el motor de bases de datos completo, además de su portabilidad que uno lo puede mover donde sea.

9) **Donde funciona mejor Docker**

   En Linux, eso pienso

10) **Como configurar Docker en la nube**

    Pues en Azure ya trae listos contenedores para solamente consumirlos o se prepara un Linux en la nube y se lo pone a funcionar ahí.

Entrevista A Personal de TIC en el supermercado Escobar del cantón Vinces

Nombre del entrevistado: Ing. Justin Benavides

Fecha: 26-02-2024

Cargo: Programador Junior

OBJETIVO: Levantar información que permita un análisis de seguridad en el despliegue de Postgres con contenedores Docker para garantizar la integridad de la información en el supermercado Escobar del cantón Vinces

1) **Que herramientas de Bases de datos utilizan en la empresa**

   Usamos Postgres versión 13

2) **De qué forma les brindan seguridad a las bases de datos en la empresa**

   Sacan respaldos automatizados usando archivos script bash. Y un contenedor

3) **Bajo qué sistema Operativo tienen el motor de bases de datos y cuál es la razón**

   Linux Ubuntu Server, porque es el mejor sistema operativo para servidores y es gratis

4) **Cuáles han sido las frecuentes fallas que han tenido con sus datos entre los últimos 6 meses**

   No tenemos Fallas, solo los usuarios fallan

5) **Que estrategia han utilizado para lograr el mayor tiempo de actividad con sus sistemas**

   La estrategia, mucha dedicación previa en el establecimiento de configuraciones de seguridad y sistemas bien actualizados acordes a las necesidades.

6) **Cuál es el presupuesto que se necesita para levantar su infraestructura en caso de algún daño**

   Eso lo maneja el Jefe

7) **Como es el ambiente relacionado con los directivos para con los de Tecnologías en cuanto a apoyo de recursos.**

   Carta Blanca

8) **Que criterio usaron para colocar Docker**

   Lo probamos porque era una tendencia tecnológica muy parecido a tener una máquina virtual, pero sin consumir grandes recursos del sistema operativo y ha funcionado bien, brinda seguridad buena a nuestros sistemas. Al menos para lo que tenemos en la empresa funciona perfecto.

9) **Donde funciona mejor Docker**

   En Ubuntu y la nube

10) **Como configurar Docker en la nube**

    Con los mismos comandos que en un servidor físico Linux fuera de línea

Entrevista A Personal de TIC en el supermercado Escobar del cantón Vinces

Nombre del entrevistado: Ing. Linda Vera

Fecha: 26-02-2024

Cargo: Facturadora Tecnica De Sistemas

OBJETIVO: Levantar información que permita un análisis de seguridad en el despliegue de Postgres con contenedores Docker para garantizar la integridad de la información en el supermercado Escobar del cantón Vinces

1) **Que herramientas de Bases de datos utilizan en la empresa**

   Usamos Postgres versión 13 y DBeaver para conexión de pruebas cliente

2) **De qué forma les brindan seguridad a las bases de datos en la empresa**

   Con respaldos 2 veces al día

3) **Bajo qué sistema Operativo tienen el motor de bases de datos y cuál es la razón**

   Linux Ubuntu Server v22, porque es estable y no presenta inconvenientes

4) **Cuáles han sido las frecuentes fallas que han tenido con sus datos entre los últimos 6 meses**

   No he conocido de fallas que llamen la atención realmente, mas fallan los equipos PC de otras áreas no conectadas a bases de datos

5) **Que estrategia han utilizado para lograr el mayor tiempo de actividad con sus sistemas**

   Mucha planificación y orden, así como mantener bitácoras para que todos logremos resolver

6) **Cuál es el presupuesto que se necesita para levantar su infraestructura en caso de algún daño**

   Supongo unos 10000

7) **Como es el ambiente relacionado con los directivos para con los de Tecnologías en cuanto a apoyo de recursos.**

   Apertura total

8) **Que criterio usaron para colocar Docker**

   Conozco que lo han usado como medida de seguridad y eficiencia para postgres y colocar otras aplicaciones

9) **Donde funciona mejor Docker**

   En Ubuntu

10) **Como configurar Docker en la nube**

    Eso mas lo maneja el Jefe y el otro ingeniero

Análisis de los Resultados

Los resultados se han obtenido de analizar la entrevista realizada a 3 expertos en bases de datos postgres con contenedores docker y seguridad de la información, este levantamiento de información se lo realizó en el super mercado Escobar de la ciudad de Vinces, donde participaron los del área de tecnologías, el Jefe y dos técnicos relacionados con el sistema de información, los cuales han brindado información y además han permitido hacer pruebas con un contenedor de pruebas muy parecido al de producción, colocado en una maquina virtual para verificar pruebas de rendimiento y de seguridades como las que se reflejan en los anexos de este documento.

Analizando las entrevistas realizadas a estos profesionales, se ha podido determinar ciertos aspectos técnicos como:

Utilizan Postgres 13 por ser un sistema ya maduro, aparentemente la idea que se tenía era de las últimas versiones, sin embargo, tiene un fundamento en cuanto a tener sistemas consolidados, además se indicó que cuentan con DBeaver para conexión de pruebas cliente.

Además, las seguridades a las bases de datos en la empresa y las respuestas fueron con respaldos automatizados con script bash, CRON de Linux, la utilización de contenedores Docker y los respaldos se hacen dos veces al día de forma transparente.

Así mismo, se consultó, bajo qué sistema Operativo tienen el motor de bases de datos y cuál es la razón, lo que respondió el jefe de cómputo que tienen todo bajo Linux, porque no necesita licencias y llevamos varios años usándolo y conocen el manejo de este sistema y trabaja muy bien su base de datos Postgres con Ubuntu Server v22, además se mencionó que es gratis, no presenta inconvenientes y es un SO estable.

Se consultó además cuales han sido las fallas que se han manifestado, por lo que han respondido que no han tenido fallas, solamente soportes y pruebas de nuevos complementos con el sistema y los contenedores que incluye la base de datos los colocarían nuevamente de existir algún fallo; los fallos únicamente son de otras áreas de usuarios fuera de acceso a bases de datos o Docker.

En cuanto al presupuesto de alguna recuperación total de infraestructura, la respuesta fue de aproximadamente 8500 por parte del Jefe, indicando que lo mas costoso son los 2 servidores con los que cuentan.

El ambiente con los directivos fue muy importante conocer, por lo que se indicó que les brindan todo el contingente necesario y no escatiman recursos cuando se trata de avanzar en lo tecnológico, representan actitudes beneficiosas para el desarrollo tecnológico en una organización.

En relación a que criterio usaron para colocar Docker, se ha respondido de que la facilidad de despliegue, es decir, se instala fácil y uno puede encapsular el motor de bases de datos completo, además de su portabilidad, ya que se lo puede mover donde sea copiarlo íntegramente como un archivo y colocarlo en otro servidor.

Todos indicaron que Docker funciona mejor en Linux Ubuntu Server versión 22 y que en la nube mantienen un Docker de contingencia también configurado como un Linux v22, la nube que utilizan de soporte se llama Azure y tienen muchos recursos que utilizan en esa plataforma. Se evidencia entonces que los resultados de las entrevistas tienen concordancia con parte del marco conceptual, donde se hace referencia a que Docker permite encapsular soluciones ampliando la cobertura de seguridad, todo siempre y cuando se haya configurado de forma eficiente la base, el Docker y la capa superior del Sistema Operativo.

Discusión de Resultados

Resaltando al autor (Kuenzli, 2021), que hace referencia a :

> *El contenedor Docker tiene como ventaja la capacidad para crear aplicaciones y le garantiza reproducibilidad en diferentes plataformas y sistemas operativos. Para ejecutar una aplicación encapsulan todas las configuraciones necesarias para ejecutar, esto ayuda a eliminar los problemas de incompatibilidad y diferencias en este entorno de desarrollo. Esto facilita el desarrollo y la implementación de aplicaciones en entornos heterogéneos, lo que acelera el ciclo de vida del desarrollo de software, así como también mejora la eficiencia operativa.* (Kuenzli, 2021)

En consecuencia de lo antes mencionado, la postura crítica del autor es, que este tipo de tecnología permite una transformación beneficiosa para desplegar aplicaciones, en este caso de estudio se analiza el de la base de datos postgres, por lo que se han realizado pruebas y montajes con la ayuda del personal de TICS de la empresa que muy amablemente han colaborado en atender las pruebas solicitadas y observar de cerca todo lo relacionado con las peticiones de pruebas (testing) que se le han requerido:

Medición del Contenedor Docker

Docker Ejecutando en la Base de Datos postgres del supermercado escobar del cantón Vinces

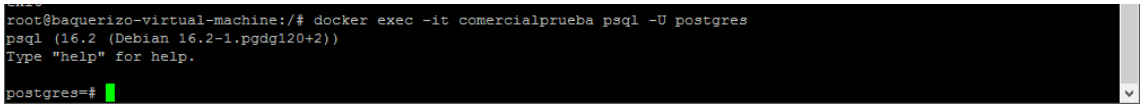
Para lo cual se utilizó:

- Servidor Proliant ML350
- con un procesador Xeon X5 3,5 Ghz,

- Memoria ram ECC 32 GB
- 4 discos solidos SSD con RAID de 4TB

Figura 1.

Dentro del Docker con nombre comercialprueba



Nota: A la Base de Datos se le realizó pruebas de penetración:

Pruebas de penetración

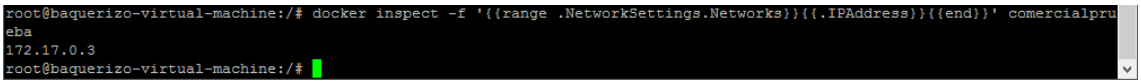
Pasos para realizar pruebas de penetración utilizando sqlmap:

Figura 2.

Instalamos nmap para probar vulnerabilidad

Figura 3.

Resultado de Verificar IP del Docker Comercialprueba



Nota: Se obtuvo la IP del contenedor comercialprueba: docker inspect -f '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}'comercialprueba

Figura 4.

Evidencia de falla de nmap

Nota: Las conexiones con SQLMap no se podían ejecutar, el servidor no permitía de ninguna forma su ingreso: por lo que fue una prueba fallida

Figura 5.

Archivo postgresql.conf

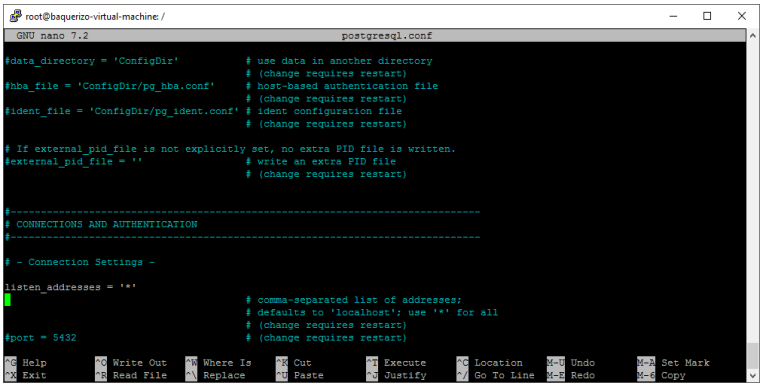
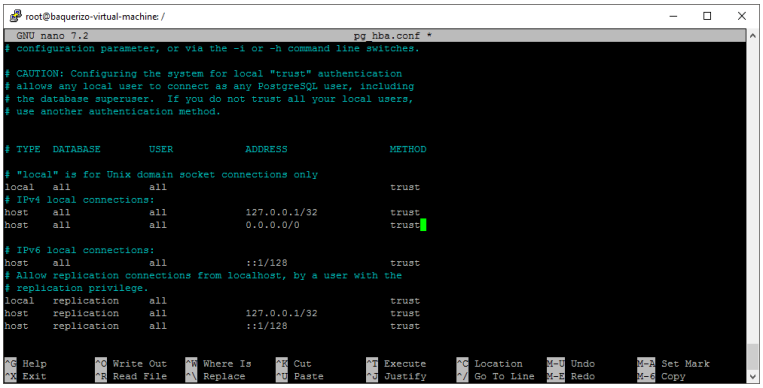


Figura 6.

Archivo : pg_hba.conf



Nota: Para brindar acceso recurrió a configuración de postgresql.conf y pg_hba.conf para verificar la configuración de autenticación y el acceso.

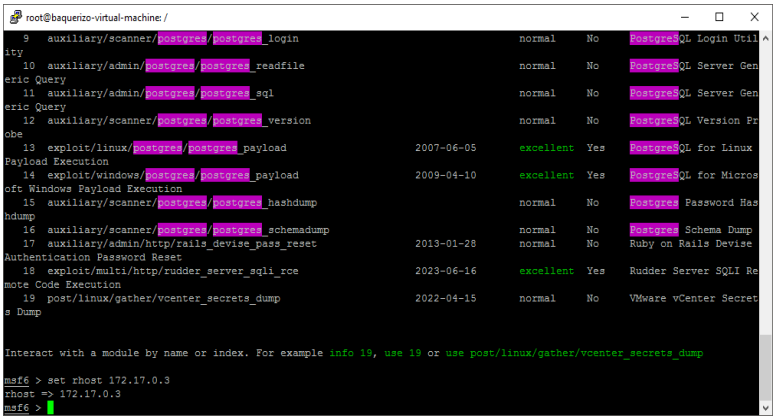
Figura 7.

Evidencia de Instalar metasploit

Nota: También se instaló metaexploit para realizar penetraciones, así mismo sin éxito estas penetraciones al Postgres con Docker

Figura 8.

Prueba de impactos metasploit con resultados



Nota: El cual se conectó brindándole las credenciales, pero sin impactos mínimos

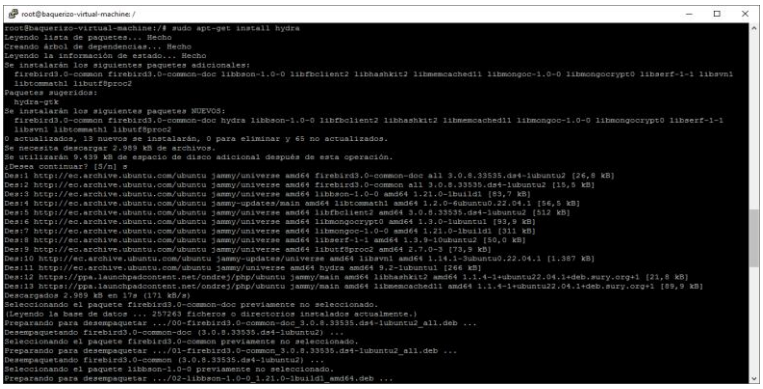
Figura 9.

Prueba de impactos metasploit con otra variante

Nota: Se probó otra versión para verificar si podría vulnerarse y tampoco fué eficaz.

Figura 10.

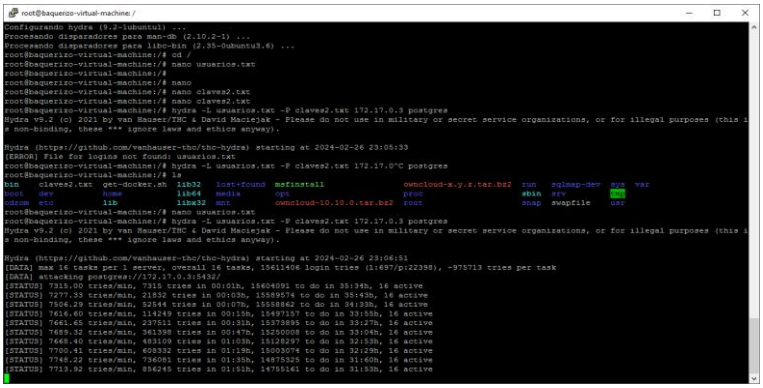
Instalación de Hydra para pruebas de penetraciòn con fuerza bruta



Nota: Luego se procedió a hacer el test con pruebas de ataque con Hydra:

Figura 11.

Hydra resultados hasta las 11:00 PM 26-02-2024



Nota: Para esto se usaron archivos de usuarios.txt y claves2.txt para atacar y mostrar alguna vulnerabilidad:

Figura 12.

Hydra resultados hasta las 7:35 *AM 27-02-2024*

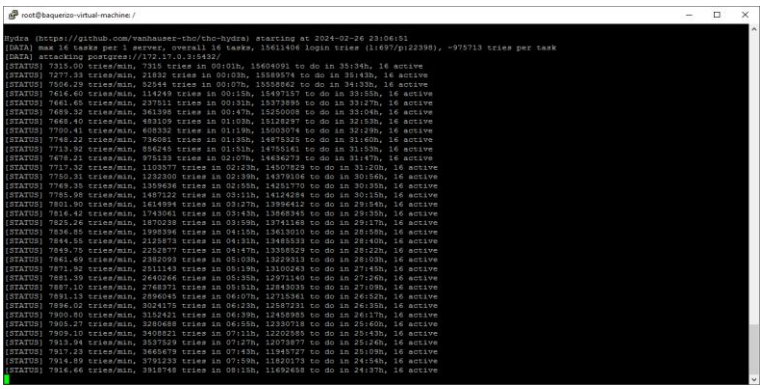
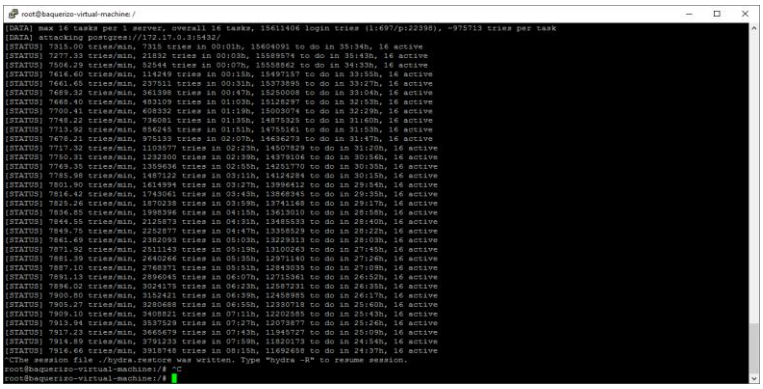


Figura 13.

Corte de pruebas con Hydra Sin resultados



Cortado ctrl+c puesto que ya ha transcurrido un tiempo prudente donde se pudo verificar que el ataque a fuerza bruta tampoco dio resultado, favoreciendo las configuraciones empleadas en la actualidad.

Toda esta muestra de despliegue para penetración y testeo de seguridad permite una aproximación a las buenas prácticas que se deben tener para mantener un ambiente seguro, tanto como con Docker o sin Docker se deben seguir parámetros de aseguramiento del Sistema Operativo, Firewall Perimetral, Docker y Postgres. Teniendo el escenario de que solo tengo el Linux y Postgres como servicio, se debe configurar de la misma como con Docker. La diferencia radica en que postgres pasa por un comando para transferir el puerto 5403 al sistema principal y este al exterior en la red.

consolalinux#docker run -d --name nom_contenedor -p 5432:5432 postgres

Conclusiones

Los expertos en tecnologías consultados indican que es una buena práctica la utilización de Docker para incorporar dentro de este contenedor aplicaciones de bases de datos como PostgreSQL pues de esa manera se garantiza integridad de la información en el supermercado Escobar del cantón

Luego de realizar varios análisis acompañados del personal de la empresa, se pudo verificar que, si preservan seguridad en cuanto a las redes, sistema operativo y configuraciones en general, sin embargo, cabe señalar que también es importante y fundamental mantener políticas internas de acceso de usuarios a la base de datos y a sus sistemas.

Las amenazas a la empresa por parte de cibercriminales son bastante bajas, teniendo en cuenta la naturaleza del negocio y el territorio donde se desenvuelve, sin embargo, no está demás mantener la disciplina de funcionamiento o integrarles adicionalmente a sus buenas prácticas algo de encriptación, esto asegura de que los datos van a estar bien protegidos durante su almacenamiento y transmisión en la red, reduciendo cualquier riesgo de comprometer la información sensible.

Se concluye, además que los administrativos del Supermercado Escobar brindan toda la apertura para el desarrollo tecnológico y esto les ha permitido crecer de forma potencial, ya que cuentan con servidores potentes que mantienen las operaciones sin interrupción, razón por la cual se ha podido poner a funcionar PostgreSQL con Docker, mejorando así el rendimiento de las aplicaciones y sobre todo garantizando mayor seguridad.

Recomendaciones

Se recomienda a los técnicos del Super Mercado Escobar mantener las buenas prácticas frente a la utilización de Docker con PostgreSQL y ajustar las demás aplicaciones a la misma lógica de funcionamiento para mantener el estándar de despliegue y de seguridad, ya que se ha evidenciado una disciplina operativa que se debe fortalecer cada vez mas porque aparecen nuevas amenazas, por eso proteger siempre los datos que serán el activo más valioso de la empresa manteniendo su disciplina que ha demostrado funcionar durante los tres últimos años sin dejar de innovar cada vez más.

Mantener actualizado el Linux que utilizan de forma periódica además del Docker y realizar pruebas para actualizar PostgreSQL a la versión actual estable, consolidando de esta manera una protección integral de todo el sistema en cuanto a infraestructura de software. Es necesario tener al día los últimos parches en lo que respecta a los contenedores Docker y PostgreSQL, aunque no sean las últimas versiones como en el caso de PostgreSQL, ya que se ha comentado en la entrevista que se utiliza una versión 13 sin embargo, se mantiene esta debido a la confianza y el desempeño presentado.

El monitoreo continuo y las auditorías a la seguridad son una buena práctica que permite detectar tempranamente amenazas y vulnerabilidades en todo sentido frente a un sistema informático y se mantiene en la lógica del despliegue de postgres dentro de contenedores Docker.

Capacitar al personal es una buena práctica por parte de la directiva por lo que se hace esta recomendación a los Propietarios del Super Mercado, ya que la tecnología evoluciona cada día y el equipo con el que se cuenta necesita seguir evolucionando en sus aprendizajes para favorecer a la organización.

Referencias

Abomhara, M. (2021). *A taxonomy of cyber attacks on SCADA systems. Computers & Security.* Panama.

Almagro, A. G. (2020). *Seguridad en bases de datos.* Madrid: RA-MA Editorial.

Applications, J. o. (2021). Docker: A Comprehensive Review.

Cynthia Dwork, A. R. (2021). *The Algorithmic Foundations of Differential Privacy.* Nueva York: Cambridge University Press.

Fontaine, D. (2020). *Mastering PostgreSQL in Application Development.* Packt Publishing.

Gupta, S. (2022). *Modern Database Management: Design and Implementation of Secure Databases.* Nueva Delhi: Pearson Education India.

Kuenzli, J. N. (2021). *Docker in Action.* Shelter Island, Estados Unidos: Manning Publications.

Luna, C. J. (2021). *Seguridad en Bases de Datos: Cómo proteger sus datos personales y corporativos.* Ciudad de México: Independently published.

Mercuri, R. (2021). *Database Security.* Nueva York: Springer.

Miguel A. Alba, M. J. (2019). *Seguridad en bases de datos Oracle.* Barcelona: Marcombo.

Norman, T. P. (2022). *PostgreSQL Security - Building Secure Database Ecosystems.* Apress.

Paul C. van Oorschot, A. S. (2020). *Computer Security and the Internet of Things.* San Francisco: Morgan Kaufmann.

PostgreSQL Magazine. (2021). *PostgreSQL Global Development Group*.

Ribeiro, M. (2020). *Journal of Computing Sciences in Colleges,.*

Slawomir Chodnicki, R. V. (2020). *Data Security for Modern Databases.* Cham: Springer.

ANEXOS

Anexo 1

Entrevista A Personal de TIC en el supermercado Escobar del cantón Vinces

1) Que herramientas de Bases de datos utilizan en la empresa

2) De qué forma les brindan seguridad a las bases de datos en la empresa

3) Bajo qué sistema Operativo tienen el motor de bases de datos y cuál es la razón

4) Cuáles han sido las frecuentes fallas que han tenido con sus datos entre los últimos 6 meses

5) Que estrategia han utilizado para lograr el mayor tiempo de actividad con sus sistemas

6) Cuál es el presupuesto que se necesita para levantar su infraestructura en caso de algún daño

7) Como es el ambiente relacionado con los directivos para con los de Tecnologías en cuanto a apoyo de recursos.

8) Que criterio usaron para colocar Docker

9) Donde funciona mejor Docker

10) Como configurar Docker en la nube

Anexo 2

Carta de autorización

Babahoyo, 28 de febrero del 2024

Magister
Eduardo Galeas Guijarro
DECANO DE LA FACULTAD DE ADMINISTRACIÓN FINANZAS E INFORMÁTICA
En su despacho.

De mis consideraciones:

Yo: EMMA CLORINDA APUNTE AGUIRRE, con cédula de identidad 0201084654, representante legal de la empresa SUPERMERCADO ESCOBAR, por medio de la presente me dirijo a usted para comunicarle que se ha AUTORIZADO a SANTIAGO ALEJANDRO VERGARA BENAVIDES estudiante de la carrera de Ingeniería en Sistemas de Información matriculado en el proceso de titulación periodo Octubre 2023 – Marzo 2024, con el Caso de estudio denominado ANÁLISIS DE SEGURIDAD EN EL DESPLIEGUE DE POSTGRES CON CONTENEDORES DOCKER PARA GARANTIZAR LA INTEGRIDAD DE LA INFORMACIÓN EN EL SUPERMERCADO ESCOBAR DEL CANTÓN VINCES.

Atentamente

Emma Clorinda Apunte Aguirre
C.I: 0201084654
Correo electrónico: supermercadoescobar@hotmail.com Telf. 0952790242

Anexo 3

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD ADMINISTRACION FINANZAS E INFÓRMATICA
DECANATO

Babahoyo, 19 de febrero de 2024
D-FAFI-UTB-0186-2024

Sra.
Emma Apunte Aguirre.
REPRESENTANTE LEGAL DE LA EMPRESA SUPERMERCADO ESCOBAR.
Ciudad. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El señor **SANTIAGO ALEJANDRO VERGARA BENAVIDES,** con cédula de identidad No. **125114019-8** estudiante de la Carrera de Ingeniería en Sistemas de Información, matriculado en el proceso de titulación en el periodo NOVIEMBRE 2023 – ABRIL 2024, trabajo de titulación modalidad examen de carácter complexivo, previo a la obtención del grado académico profesional universitario de tercer nivel como INGENIERO EN SISTEMAS DE INFORMACIÓN, solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar su Estudio de Caso con su tema: **"ANÁLISIS DE SEGURIDAD DE POSTGRES CON CONTENEDORES DOCKER PARA GARANTIZAR LA INTEGRIDAD DE LA INFORMACIÓN EN EL SUPERMERCADO ESCOBAR DEL CANTÓN VINCES".**

Atentamente,

UNIVERSIDAD TÉCNICA DE BABAHOYO FACULTAD ADMINISTRACION FINANZAS E INFORMATICA DECANATO

Lcdo. Eduardo Galeas Guijarro, MAE.
DECANO

MERCANTIL ESCOBAR C. E.

29/02/24
05:25 pm

c.c: Archivo

Av. Universitaria Km 2 ½ vía Montalvo. Teléfono (05) 2572024 e-mail: decanatofafi@utb.edu.ec	Elaborado por: Ing. Marilyn Coloma Aguilar	Revisado por: Lcdo. Eduardo Galeas Guijarro, MAE