REPÚBLICA DEL ECUADOR

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

PROPUESTAS METODOLÓGICAS Y TECNOLÓGICAS AVANZADAS PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN

TÍTULO DEL PROYECTO:

OPTIMIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA PARA PLATAFORMAS EDUCATIVAS EN LA EMPRESA PÚBLICA DE PRODUCCIÓN Y DESARROLLO ESTRATÉGICO DE LA UNIVERSIDAD ESTATAL DE MILAGRO (EPUNEMI): ALTA DISPONIBILIDAD, BALANCEO DE CARGA Y SEGURIDAD INFORMÁTICA

TUTOR

DR. BYRON WLADIMIR OVIEDO BAYAS

AUTOR

JOHANN ZAVALA VILLAMAR

MILAGRO, 2024

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO

Milagro, Abril, 2024

CERTIFICACIÓN DE ACEPTACIÓN DEL TUTOR

En calidad de Tutor del Proyecto de Investigación, nombrado por el Comité Académico del Programa de Maestría en Tecnologías de la Información de la Universidad Estatal de Milagro.

CERTIFICO

Que he analizado el Proyecto de Investigación con el tema **OPTIMIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA PARA PLATAFORMAS EDUCATIVAS EN LA EMPRESA PÚBLICA DE PRODUCCIÓN Y DESARROLLO ESTRATÉGICO DE LA UNIVERSIDAD ESTATAL DE MILAGRO (EPUNEMI): ALTA DISPONIBILIDAD, BALANCEO DE CARGA Y SEGURIDAD INFORMÁTICA**, elaborado por **JOHANN ANDRÉS ZAVALA VILLAMAR**, el mismo que reúne las condiciones y requisitos previos para ser defendido ante el tribunal examinador, para optar por el título de MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN.

Firmado electrónicamente por:
BYRON WLADIMIR
OVIEDO BAYAS

BYRON WLADIMIR OVIEDO
C.I: 0914200373

DECLARACIÓN DE AUTORÍA

La responsabilidad del contenido desarrollado en este Proyecto de Investigación, me corresponde exclusivamente; y la propiedad intelectual del mismo a la Universidad Estatal de Milagro.

Firmado electrónicamente por:
JOHANN ANDRES
ZAVALA VILLAMAR

ZAVALA VILLAMAR JOHANN ANDRES

C.I: 0920627882

UNEMI
UNIVERSIDAD ESTATAL DE MILAGRO

VICERRECTORADO DE INVESTIGACIÓN Y POSGRADO
DIRECCIÓN DE POSGRADO
CERTIFICACIÓN DE LA DEFENSA

El TRIBUNAL CALIFICADOR previo a la obtención del título de **MAGÍSTER EN TECNOLOGÍAS DE LA INFORMACIÓN**, presentado por **ING. ZAVALA VILLAMAR JOHANN ANDRES**, otorga al presente proyecto de investigación denominado "SERVIDORES VIRTUALES DE ALTA DISPONIBILIDAD PARA LA GESTIÓN DEL APRENDIZAJE EN LA EMPRESA PÚBLICA DE LA UNEMI", las siguientes calificaciones:

TRABAJO DE TITULACION	56.67
DEFENSA ORAL	36.00
PROMEDIO	**92.67**
EQUIVALENTE	**Muy Bueno**


Firmado electrónicamente por:
OSCAR XAVIER BERMEO ALMEIDA

Mgs BERMEO ALMEIDA OSCAR XAVIER
PRESIDENTE/A DEL TRIBUNAL


Firmado electrónicamente por:
FREDDY LENIN BRAVO DUARTE

Mgti. BRAVO DUARTE FREDDY LENIN
VOCAL


Firmado electrónicamente por:
LISSETT MARGARITA AREVALO GAMBOA

Mgti. AREVALO GAMBOA LISSETT MARGARITA
SECRETARIO/A DEL TRIBUNAL

AGRADECIMIENTO

Quiero agradecer en primer lugar a Dios por sus bendiciones, que me han permitido cumplir uno de mis objetivos profesionales, y que por su gracia podré seguir adelante en todo ámbito de mi vida, en unión de mi familia. A mis padres, por su apoyo incondicional en el cumplimiento de mis objetivos personales y profesionales. A mi esposa Mercedes que mediante su tenacidad ha sido mi motor para culminar esta fase de estudios.

Le agradezco a mi tutor, por su dedicación y paciencia, ya que con su guía pudimos culminar este trabajo y llegar a esta instancia tan anhelada. A todos los docentes de la Universidad Estatal de Milagro, por sus enseñanzas en este camino universitario y por transmitir sus conocimientos, que hoy me permiten culminar con éxito este título de cuarto nivel.

A todas y a cada una de las personas que me apoyaron para lograr llegar al final de este camino,

Gracias

Johann Zavala Villamar

DEDICATORIA

Este trabajo va dedicado a toda mi familia. A mis padres por estar siempre apoyándome en todo momento, por enseñarme e inculcarme los valores que hoy guían mi vida, por guiarme siempre por el camino de bien y ayudarme a ser la persona que soy el día de hoy.

A mi esposa que ha estado siempre ahí, impulsándome a ser una mejor persona, un mejor profesional, que me ayuda a siempre ser la mejor versión de mí y que me ha ayudado a afrontar siempre los problemas de una manera directa y se siempre mi apoyo incondicional.

Johann Zavala Villamar

RESÚMEN

En el contexto de la transformación digital de la educación, este proyecto aborda la optimización de la infraestructura tecnológica de la Empresa Pública de Producción y Desarrollo Estratégico de la Universidad Estatal de Milagro (EPUNEMI), enfocándose en mejorar la alta disponibilidad, el balanceo de carga y la seguridad informática para las plataformas educativas. Reconociendo la importancia crítica de la infraestructura tecnológica en el soporte de plataformas educativas como Moodle, se identifica un vacío significativo en la gestión eficiente de servidores que puede comprometer la calidad y la continuidad del servicio educativo.

La planificación del proyecto se centra en una evaluación detallada de la infraestructura tecnológica actual, seguida por el diseño de una solución basada en arquitectura en la nube con Google Cloud Platform (GCP), que promete una mejora significativa en términos de escalabilidad, seguridad y disponibilidad. La metodología adoptada combina enfoques descriptivos y proyectivos, incluyendo un análisis técnico profundo y el desarrollo de un modelo de implementación que se ajusta a las necesidades específicas de EPUNEMI.

Las etapas del proyecto abarcan desde la evaluación inicial de la infraestructura existente, el diseño de la arquitectura propuesta, hasta la elaboración de un plan de seguridad informática detallado. Se utilizan recursos como herramientas de diagnóstico de infraestructura, software de diseño arquitectónico y simulaciones de seguridad, complementados con un análisis coste-beneficio para justificar la transición hacia la solución propuesta.

El impacto esperado del proyecto incluye no solo una mejora tangible en la

estabilidad y seguridad de las plataformas educativas, sino también una contribución significativa al avance del conocimiento en la gestión de infraestructuras tecnológicas para la educación. Con este proyecto, EPUNEMI se posiciona a la vanguardia de la innovación educativa, asegurando un entorno de aprendizaje en línea más confiable y seguro.

Palabras clave: Optimización de Servidores, Alta Disponibilidad, Balanceo de Carga, Seguridad Informática, Infraestructura Tecnológica, Plataformas Educativas, Google Cloud Platform.

ABSTRACT

In the context of the digital transformation of education, this project addresses the optimization of the technological infrastructure of the Empresa Pública de Producción y Desarrollo Estratégico de la Universidad Estatal De Milagro (EPUNEMI), focusing on improving high availability, load balancing, and cybersecurity for educational platforms. Recognizing the critical importance of technological infrastructure in supporting educational platforms such as Moodle, a significant gap in the efficient management of servers is identified, which can compromise the quality and continuity of the educational service.

The project planning focuses on a detailed evaluation of the current technological infrastructure, followed by the design of a cloud-based solution with Google Cloud Platform (GCP), which promises a significant improvement in terms of scalability, security, and availability. The adopted methodology combines descriptive and projective approaches, including a deep technical analysis and the development of an implementation model that fits the specific needs of EPUNEMI.

The project stages range from the initial assessment of the existing infrastructure, the design of the proposed architecture, to the development of a detailed cybersecurity plan. Resources such as infrastructure diagnostic tools, architectural design software, and security simulations are used, complemented with a cost-benefit analysis to justify the transition to the proposed solution.

The expected impact of the project includes not only a tangible improvement in the stability and security of the educational platforms but also a significant contribution to advancing knowledge in the management of technological infrastructures for education. With this project, EPUNEMI positions itself at the forefront of educational

innovation, ensuring a more reliable and secure online learning environment.

Keywords: Server Optimization, High Availability, Load Balancing, Cybersecurity, Technological Infrastructure, Educational Platforms, Google Cloud Platform.

ÍNDICE

AGRADECIMIENTO V
DEDICATORIA VI
RESÚMEN VII
ABSTRACT IX
ÍNDICE DE FIGURAS XIII
INTRODUCCIÓN 1
CAPÍTULO 1 3
1.1. Planteamiento del problema 3
1.2. Objetivos 5
1.2.1. Objetivo General 5
1.2.2. Objetivos Específicos 5
1.2.3. Alcance 6
1.3. Estado del arte 7
1.3.1. Alta disponibilidad en Moodle 7
1.3.2. Balanceador de carga en Moodle 9
1.3.3. Redundancia de datos en Moodle 11
1.3.4. Seguridad informática en Moodle 12
1.3.5. Servidores virtuales en plataformas educativas 13
1.3.6. Plataformas educativas 16
1.3.7. Métricas clave en plataformas educativas 17
CAPÍTULO 2 20
2. Metodología 20
CAPÍTULO 3 22
3. Propuesta de solución 22
3.1.1. Evaluación la infraestructura tecnológica actual 22
3.1.2. Informe de Métricas y Servidor de Aula Virtual EPUNEMI 27
CONCLUSIONES Y TRABAJO FUTURO 44
Conclusiones 44
Trabajo futuro 45
RECOMENDACIONES 46
BIBLIOGRAFIA 47
ANEXOS 49

PLAN DE SEGURIDAD INFORMÁTICA 1

1. INTRODUCCIÓN 1

2. OBJETIVOS DEL PLAN *2*
2.1 Objetivo General 2
2.2 Objetivo General 2
3. JUSTIFICACIÓN *3*
4. ALCANCE Y DELIMITACIÓN DEL PLAN *4*
5. DISPOSICIONES DE SEGURIDAD *5*
5.1 SEGURIDAD FÍSICA 5
5.2 SEGURIDAD LÓGICA 5
6. Gestión de Accesos de Usuarios en la EPUNEMI *8*
7. Gestión de Credenciales de Usuario de la EPUNEMI *9*
8. CONTROL DE ACCESO A LA INFORMACIÓN *10*
8.1 Programas de Control 10
8.2 Contraseñas 10
8.3 Niveles de Acceso 10
9. ANTIVIRUS *12*
9.1 Funcionalidades Clave del Sistema Antivirus 12
9.2 Estrategias de Implementación y Mantenimiento 12
10. DISPOSICIÓN DE RESCATE Y CONTINGENCIA *13*
10.1 Identificación de Requisitos Operativos Mínimos 13
10.2 Elaboración de Planes de Contingencia 13
10.3 Herramientas de Continuidad del Negocio 13
10.4 Monitoreo y Revisión del Plan de Seguridad Informática 13
10.5 Procedimientos de Respaldos y Restauración 13
10.6 Creación de Imágenes de Servidores 13
10.7 Gestión de Hardware de Servidores 13
10.8 Sincronización de Sistema 14
10.9 Gestión de Activos Críticos 14
10.10 Socialización y Capacitación 14
11. POLÍTICAS DE SEGURIDAD *15*
11.1 Política de Acceso 15
11.2 Política de Contraseñas 15
11.3 Política de Gestión de Incidentes 15
11.4 Política de Copias de Seguridad 16
11.5 Política de Seguridad Física 16
11.6 Política de Seguridad en la Red 17
11.7 Política de Actualizaciones y Parches 17
11.8 Política de Capacitación y Concienciación 17
11.9 Política de Auditoría y Cumplimiento 18

11.10 Política de Eliminación de Datos 18

ÍNDICE DE FIGURAS

Figura 1..... 23
Figura 2..... 25
Figura 3..... 25
Figura 4..... 28
Figura 5..... 33
Figura 6..... 34
Figura 7..... 34
Figura 8..... 35
Figura 9..... 37
Figura 10..... 38
Figura 11..... 38
Figura 12..... 39
Figura 13..... 40
Figura 14..... 40
Figura 15..... 41
Figura 16..... 42

Tabla 1..... 30

INTRODUCCIÓN

En el contexto global, la tecnología ha revolucionado la educación, ofreciendo oportunidades de aprendizaje sin precedentes para educadores y estudiantes. "Un estudio reciente aborda los desafíos y oportunidades de utilizar tecnologías digitales en la enseñanza. Los investigadores concluyen que, aunque estas herramientas tienen un gran potencial para enriquecer el proceso educativo, su uso efectivo aún enfrenta obstáculos tanto para docentes como para estudiantes" (Morán-González & Gallegos-Macías, 2021). Este hallazgo resalta que, a pesar de los avances tecnológicos, aún existen desafíos que deben abordarse.

Descendiendo al ámbito regional y local, la incorporación de tecnología en el aula no sólo dinamiza la educación, sino que también mejora la gestión y administración educativa. "El documento resalta la importancia de plataformas tecnológicas como Moodle, Dokeos y Claroline en el ámbito educativo. Estas plataformas no sólo facilitan el proceso de enseñanza-aprendizaje, sino que también son cruciales para el desarrollo de habilidades específicas" (Morán-González & Gallegos-Macías, 2021). Instituciones como Empresa Pública de Producción y Desarrollo Estratégico de la Universidad Estatal de Milagro (EPUNEMI) están adoptando estas plataformas para hacer la educación más accesible y eficiente.

Según (Digital Guide IONOS, 2023) en la informática, el concepto de servidor puede ser examinado desde dos enfoques distintos: como un elemento de hardware y como una entidad de software. En su forma de hardware, un servidor se define como una computadora conectada a una red, destinada a proporcionar diversos recursos, y es comúnmente referida como "host". Esta capacidad no se limita a equipos

especializados, ya que cualquier ordenador puede asumir el rol de servidor mediante la implementación del software adecuado. Desde la perspectiva de software, un servidor se concibe como una aplicación diseñada para brindar servicios específicos a otros programas, denominados clientes. Estos servicios pueden ser accesibles local o remotamente a través de la red, y la naturaleza de dichos servicios varía según el tipo de software del servidor. La comunicación entre el servidor y los clientes se estructura bajo el modelo cliente-servidor, y se maneja mediante protocolos de transmisión específicos para el intercambio de datos.

En el nivel más detallado, los servidores son la columna vertebral que posibilita esta transformación tecnológica. "En un sistema diseñado para alta disponibilidad, los servidores se agrupan en clústeres y se estructuran en niveles para interactuar eficazmente con los balanceadores de carga. Si un servidor en un clúster específico se cae, un servidor duplicado en un clúster distinto está preparado para asumir su carga de trabajo" (Mishra et al., 2020). Específicamente, en entornos universitarios como EPUNEMI, la alta disponibilidad y el rendimiento eficiente de los servidores son fundamentales para el funcionamiento óptimo de plataformas educativas como Moodle.

El propósito de este proyecto fue abordar este vacío de conocimiento y ofrecer soluciones para optimizar la alta disponibilidad y el rendimiento de servidores en EPUNEMI. A lo largo del texto, se discutirán los desafíos y oportunidades que la tecnología presenta en el ámbito educativo, con un enfoque especial en la gestión de servidores para Moodle.

CAPÍTULO 1

1.1. Planteamiento del problema

La integración de las Tecnologías de la Información y la Comunicación (TIC) en el ámbito educativo ha revolucionado la manera en que se accede a los recursos didácticos y se implementan los métodos de enseñanza. Sin embargo, la adopción masiva de estas tecnologías ha traído consigo retos significativos en términos de infraestructura tecnológica, particularmente en lo que respecta a la gestión de servidores. La sobrecarga de estos sistemas puede comprometer seriamente la calidad de la educación, evidenciando la necesidad imperiosa de mejorar la infraestructura tecnológica para garantizar un servicio ininterrumpido.

En el contexto de la EPUNEMI, el sistema de gestión de aprendizaje MOODLE ha demostrado limitaciones claras al no poder soportar la carga de numerosos estudiantes accediendo simultáneamente, especialmente durante períodos críticos como exámenes en línea. Este fenómeno no es exclusivo de una sola institución, sino que refleja una problemática extendida a lo largo del sector educativo. La gestión ineficiente de los servidores que soportan plataformas como MOODLE, cruciales para el proceso educativo, afecta negativamente el acceso a materiales didácticos y la realización de evaluaciones, impactando directamente en la calidad de la educación.

La infraestructura tecnológica actual limita severamente la escalabilidad y la adaptabilidad a las nuevas tecnologías educativas. Este escenario plantea una barrera significativa a la innovación, restringiendo la capacidad de las instituciones para incorporar herramientas avanzadas que podrían enriquecer el proceso de aprendizaje. Por ejemplo, la incapacidad para soportar la integración de sistemas de inteligencia artificial para la personalización del aprendizaje evidencia la urgencia de

abordar estas limitaciones.

Además, la falta de disponibilidad de plataformas educativas tiene consecuencias directas en la continuidad y la eficacia del proceso educativo. Interrupciones en el acceso a materiales de estudio y en la realización de evaluaciones en línea no solo generan estrés y ansiedad entre los estudiantes, sino que también cuestionan la equidad y la validez de los procesos evaluativos implementados. Estos problemas no solo afectan el rendimiento académico de los estudiantes, sino que también pueden llevar a una disminución en la satisfacción estudiantil y afectar negativamente la percepción de la calidad educativa de la institución.

Desde una perspectiva económica, el mantenimiento de la infraestructura tecnológica actual supone un desafío significativo. Los costos asociados a la actualización y mantenimiento de servidores físicos, así como la necesidad de personal técnico calificado, son factores que inciden directamente en el presupuesto de las instituciones educativas. Sin embargo, es fundamental analizar estos costos en el contexto de los beneficios a largo plazo que se derivarían de una infraestructura más robusta y escalable. La migración a soluciones basadas en la nube emerge como una alternativa viable, prometiendo no solo una reducción en los costos operativos, sino también una mejora en la escalabilidad y disponibilidad de los servicios educativos.

La propuesta de mejorar la infraestructura tecnológica a través de la implementación de estrategias de balanceo de carga, redundancia de datos y migración a la nube, no solo busca resolver los problemas actuales, sino que también apunta a preparar el terreno para la adopción futura de innovaciones tecnológicas en

la educación. Este enfoque no solo tendría un impacto positivo en la calidad de la educación, sino que también contribuiría al desarrollo social y humano a largo plazo, alineándose con los objetivos de promover una sociedad más informada y capacitada.

En conclusión, la gestión eficiente de la infraestructura tecnológica en las instituciones educativas es fundamental para garantizar la calidad y la continuidad del proceso educativo. La adopción de soluciones tecnológicas avanzadas y la mejora de la infraestructura existente son pasos críticos hacia la optimización de los recursos educativos y la maximización del potencial de aprendizaje de los estudiantes. Este desafío, por tanto, no solo es técnico sino también estratégico, implicando una inversión en el futuro de la educación y, por ende, en el futuro de la sociedad.

1.2. Objetivos

1.2.1. Objetivo General

Determinar una infraestructura tecnológica mejorada para las plataformas educativas de la EPUNEMI, asegurando alta disponibilidad, balanceo de carga y redundancia de datos mediante el uso de soluciones en la nube y estrategias de seguridad informática avanzadas.

1.2.2. Objetivos Específicos

Evaluar la infraestructura tecnológica actual de la plataforma MOODLE de la EPUNEMI, identificando métricas clave y eventos críticos que puedan influir en la experiencia de los usuarios.

Diseñar, basándose en el análisis anterior, una metodología técnica detallada para implementar alta disponibilidad, balanceo de carga y redundancia de datos en la plataforma MOODLE de la EPUNEMI.

Establecer un plan de seguridad informática que proteja y garantice la

integridad de los datos almacenados en la plataforma, considerando posibles amenazas y vulnerabilidades.

1.2.3. Alcance

Este proyecto llevó a cabo una evaluación exhaustiva para identificar la infraestructura tecnológica más adecuada para la plataforma educativa MOODLE de EPUNEMI. Con un enfoque riguroso y adaptado a las particularidades de esta institución, se garantizó alta disponibilidad, balanceo de carga y redundancia de datos. El objetivo fue abordar los desafíos relacionados con la escalabilidad, el rendimiento y la seguridad de la plataforma.

En concreto, el proyecto analizó el marco tecnológico de la plataforma MOODLE en EPUNEMI, enfocándose en examinar métricas y eventos críticos que podrían afectar la experiencia del usuario.

Es importante destacar las limitaciones de este proyecto. Aunque se realizó un análisis exhaustivo, inicialmente no se implementaron las soluciones propuestas. Sin embargo, se sugirió un diseño de arquitectura para una futura implementación. El enfoque de seguridad se propuso mediante un Plan de Seguridad Informática, adaptado para salvaguardar integralmente los activos de información y la infraestructura tecnológica que soporta la plataforma educativa de EPUNEMI, incluyendo la protección contra amenazas internas y externas y la prevención de incidentes de seguridad que pudieran afectar la continuidad de las operaciones académicas y administrativas. Esta investigación se centró en la plataforma EPUNEMI MOODLE, por lo que los hallazgos podrían no ser generalizables a otros contextos. Además, se tomaron en cuenta factores de rentabilidad, optando por soluciones económicamente viables para la institución.

1.3. Estado del arte

1.3.1. Alta disponibilidad en Moodle

En el ámbito de la educación en línea, la alta disponibilidad de servidores virtuales es esencial para garantizar un acceso ininterrumpido a recursos educativos, según (Perafan et al., 2018). Acorde con esto, el estudio 'Diseño de un Clúster de Alta Disponibilidad para un Entorno Educativo Virtual Universitario' realizado por la Universidad de Carabobo aporta un enfoque práctico al describir cómo implementar un clúster de alta disponibilidad con Linux CentOS 7. Este enfoque tiene como finalidad optimizar la eficiencia y disponibilidad del Aula Virtual de Ingeniería de dicha institución.

Además de estos factores, la integración efectiva con otros Sistemas de Gestión Académica también juega un papel crucial en la alta disponibilidad. Según un estudio de la Tecnológica Universidad Israel, esta integración no solo mejora la sincronización de la información académica, sino que también podría aliviar la carga en los servidores de Moodle (Recalde et al., 2022).

La alta disponibilidad en plataformas educativas como Moodle es un tema multifacético que abarca desde la robustez del sistema hasta la integración con otros Sistemas de Gestión Académica. La eficaz sincronización de datos entre sistemas no solo mejora la eficiencia operativa, sino que también contribuye significativamente a la alta disponibilidad al reducir la carga en los servidores. Por lo tanto, una estrategia integral que aborde estos diversos aspectos es esencial para garantizar un entorno de aprendizaje en línea eficaz y fiable.

En el proceso de integración de Moodle con otros sistemas de gestión

académica, es crucial considerar tanto las ventajas como las desventajas. Según un estudio reciente, la compatibilidad, la implementación y la integración son tres criterios clave en este contexto. Por ejemplo, la compatibilidad con múltiples motores de bases de datos es una ventaja, pero la diversidad de estos motores puede ser una desventaja. En cuanto a la implementación, la adaptabilidad a los procesos de inscripción académica de cada institución es una fortaleza, aunque requiere un estudio previo para determinar la solución más adecuada. Finalmente, en términos de integración, aunque los procedimientos almacenados permiten una programación establecida, si el servidor vinculado falla, el proceso de integración no se completa (Recalde et al., 2022).

Un sistema con alta disponibilidad se diseña para minimizar las vulnerabilidades que podrían llevar a interrupciones del servicio. A medida que la demanda del servicio se incrementa, la robustez del sistema se vuelve crítica para asegurar un rendimiento sostenible y constante (Mesbahi et al., 2018). En comparación con la investigación realizada en la Universidad de Carabobo (Perafan et al., 2018), ambos estudios coinciden en la importancia de la alta disponibilidad, especialmente en entornos educativos. Mientras que el estudio de la Universidad de Carabobo se centra en la implementación de un clúster de alta disponibilidad para evitar pérdidas de tiempo y recursos, (Mesbahi et al., 2018) destaca la necesidad de minimizar vulnerabilidades para mantener un rendimiento constante.

Dentro del ámbito de plataformas educativas, donde el acceso a recursos didácticos y herramientas de aprendizaje es crucial, la alta disponibilidad adquiere una importancia adicional. Implementar servidores virtuales de alta disponibilidad en estas plataformas no solo mejora la confiabilidad del sistema, sino que también contribuye a mantener la confianza de los usuarios, que en este caso son estudiantes,

docentes y administradores. Ambos estudios subrayan la importancia de la alta disponibilidad en entornos educativos. (Mesbahi et al., 2018) se enfoca en la confiabilidad y la confianza de los usuarios, mientras que (Perafan et al., 2018) el estudio de la Universidad de Carabobo destaca que los sistemas de alta disponibilidad son esenciales para mantener servicios web y aplicaciones en funcionamiento, incluso en caso de fallos de hardware o software.

Uno de los aspectos cruciales para garantizar la alta disponibilidad en servidores virtuales para plataformas educativas es la implementación de un marco de referencia sólido. En este sentido, el artículo elaborado por (Mesbahi et al., 2018) propone un "Mapa de Referencia" estructurado en cuatro pasos clave. Este enfoque podría ser adaptado y aplicado en el diseño de un sistema de servidores virtuales de alta disponibilidad específico para plataformas educativas, asegurando así un rendimiento óptimo y una mayor confiabilidad.

Por lo tanto, la adaptación de principios de diseño como la eliminación de puntos únicos de fallo y la detección rápida de fallos, se vuelve esencial para garantizar un entorno de aprendizaje en línea eficaz y fiable. Aquí también hay un paralelismo entre los dos estudios. (Mesbahi et al., 2018) habla de la eliminación de puntos únicos de fallo y la detección rápida de fallos, mientras que el estudio de la Universidad de Carabobo (Perafan et al., 2018) propone una implementación específica utilizando CentOS 7 para garantizar que el servicio web esté siempre disponible.

1.3.2. Balanceador de carga en Moodle

El balanceo de carga es un mecanismo crítico para asegurar la alta disponibilidad en sistemas con tráfico intenso de usuarios. Funciona mediante la

distribución dinámica de las tareas entre los recursos disponibles del sistema, como direccionar diversas peticiones de datos a distintos servicios en un entorno de nube mixto. Mediante uno o más balanceadores, se asignan las cargas de trabajo a los recursos más aptos para manejarlas, previniendo así cualquier sobrecarga en un recurso específico (Mishra et al., 2020).

El autor (Mishra et al., 2020) aborda la importancia del equilibrio de carga en entornos de computación en la nube, destacando que es esencial para evitar fallos del sistema relacionados con el consumo de energía y el tiempo de ejecución. El estudio realiza una simulación en el simulador CloudSim para evaluar varios algoritmos de equilibrio de carga. De particular relevancia para este trabajo es la conclusión del artículo sobre el algoritmo MCT (Minimum Compilation Time), que mostró el menor tiempo de ejecución y consumo de energía en comparación con otros algoritmos evaluados.

En un sistema diseñado para alta disponibilidad, los servidores se agrupan en clústeres y se estructuran en niveles para interactuar eficazmente con los balanceadores de carga. Si un servidor en un clúster específico se cae, un servidor duplicado en un clúster distinto está preparado para asumir su carga de trabajo. Esta forma de redundancia facilita un mecanismo de 'failover', donde un elemento secundario se activa para realizar las tareas del elemento primario defectuoso, minimizando así el efecto en el rendimiento del sistema (Mishra et al., 2020).

En el contexto de este trabajo, que se enfoca en servidores virtuales de alta disponibilidad para plataformas educativas en la nube, el algoritmo MCT ofrece un enfoque prometedor para optimizar el rendimiento del servidor. Al minimizar tanto el tiempo de ejecución como el consumo de energía, el algoritmo contribuye a la alta

disponibilidad de los servidores, un aspecto crítico para garantizar un acceso ininterrumpido y eficiente a recursos educativos en línea. Por lo tanto, la implementación de estrategias de equilibrio de carga como MCT podría ser una vía efectiva para mejorar la robustez y la eficiencia de servidores virtuales dedicados a plataformas educativas.

1.3.3. Redundancia de datos en Moodle

En el contexto de sistemas de gestión de bases de datos, la redundancia de datos es un fenómeno que puede llevar a la inconsistencia y aumentar los costos de almacenamiento y acceso. Este problema se origina cuando los archivos son creados por diferentes programas y cambian con el tiempo, resultando en datos duplicados en múltiples ubicaciones. Para mitigar la redundancia, especialmente en el modelo relacional, es crucial eliminar las dependencias de valores múltiples mediante la construcción de tablas separadas para cada atributo de valores múltiples (Ramos Martín et al., 2006).

En este contexto, es evidente que la redundancia de datos es un problema significativo, especialmente en entornos educativos como plataformas en línea, donde la integridad y eficiencia de los datos son fundamentales para el aprendizaje y la administración. La redundancia no solo aumenta los costos de almacenamiento, sino que también puede llevar a inconsistencias que afectan la confiabilidad del sistema.

Para abordar este problema, la eliminación de dependencias de valores múltiples se presenta como una estrategia efectiva. Esta técnica es especialmente relevante en el diseño de servidores virtuales de alta disponibilidad para plataformas educativas, donde la eficiencia en el almacenamiento y la recuperación de datos es crucial para mantener un servicio ininterrumpido.

Finalmente, es importante subrayar que una gestión adecuada de la redundancia no solo mejora la eficiencia del sistema, sino que también es fundamental para garantizar su alta disponibilidad. Al minimizar los riesgos asociados con la inconsistencia de datos, se fortalece la confiabilidad del sistema, un aspecto crítico para el éxito de cualquier plataforma educativa en línea.

1.3.4. Seguridad informática en Moodle

En el ámbito de la computación en la nube, la seguridad es a menudo considerada como el principal requisito para alojar aplicaciones críticas. Los fallos de seguridad se dividen en tres modos generales: fallos del cliente, violaciones de la seguridad del software y fallos de la política de seguridad (Mesbahi et al., 2018).

Los mecanismos de seguridad en sistemas gestores de bases de datos son fundamentales para controlar el acceso y uso de la base de datos a diferentes niveles. Estos mecanismos garantizan la protección de los datos contra accesos no autorizados y ayudan a implantar restricciones de integridad en la base de datos (Ramos Martín et al., 2006).

En el ámbito de la seguridad informática aplicada a plataformas educativas como Moodle, las dos fuentes consultadas ofrecen perspectivas complementarias que enriquecen nuestra comprensión del tema. El artículo sobre Alta Disponibilidad se enfoca en la seguridad desde una perspectiva de infraestructura en la nube. Destaca cómo los fallos de seguridad, ya sean originados por el cliente o por vulnerabilidades en el software, pueden comprometer la alta disponibilidad del sistema. Este enfoque es particularmente relevante si consideramos que muchas instituciones educativas están migrando sus plataformas de aprendizaje a la nube para beneficiarse de su escalabilidad y flexibilidad.

Por su parte, el libro de Sistemas Gestores de Bases de Datos de (Ramos Martín et al., 2006) aborda la seguridad desde el ángulo de la gestión de datos. Se centra en los mecanismos que controlan el acceso y uso de la base de datos, subrayando la importancia de proteger los datos contra accesos no autorizados y de implantar restricciones de integridad. Este enfoque es crucial para cualquier sistema educativo en línea como Moodle, que maneja una gran cantidad de datos sensibles, desde información personal de los estudiantes hasta material didáctico y calificaciones.

Al comparar ambas fuentes, se hace evidente que la seguridad en un entorno educativo en línea es multifacética y requiere una estrategia integral que abarque tanto la infraestructura de la nube como la gestión de bases de datos. Mientras que el artículo sobre Alta Disponibilidad nos alerta sobre los riesgos de seguridad que pueden comprometer la disponibilidad del sistema, el libro nos ofrece herramientas para mitigar estos riesgos a nivel de base de datos. En conjunto, estas fuentes proporcionan un marco robusto para abordar la seguridad informática en Moodle, garantizando tanto la alta disponibilidad como la integridad de los datos.

1.3.5. Servidores virtuales en plataformas educativas

El objetivo de la investigación realizada en la Facultad de Informática de la Universidad Autónoma de Querétaro es proponer un modelo basado en u-learning y rotación. Este modelo busca dotar a los profesores de las competencias digitales y pedagógicas necesarias para desarrollar un aprendizaje significativo en sus estudiantes, independientemente del entorno en el que se encuentren. Este cambio en las modalidades de aprendizaje se ha vuelto especialmente relevante debido a las modificaciones en las prácticas educativas causadas por la pandemia de COVID-19

(Olivo García et al., 2022).

Una de las conclusiones más relevantes del artículo es la importancia de la preparación pedagógica y digital de los profesores para la transición exitosa de la educación presencial a la virtual. El estudio señala que los profesores a menudo utilizan herramientas como Google Classroom o Zoom, pero no de la manera más efectiva para facilitar un aprendizaje significativo. Este hallazgo es crucial para mi proyecto, ya que subraya la necesidad de formación docente específica en el uso de servidores virtuales y plataformas educativas para garantizar una educación de alta calidad y alta disponibilidad.

Finalmente, el artículo destaca la importancia de la infraestructura y el software en el proceso de enseñanza-aprendizaje virtual. Señala que estas herramientas deben facilitar la interacción clara entre profesores y estudiantes y centralizar la información para un aprendizaje ubicuo. Este punto refuerza la importancia de tener servidores virtuales de alta disponibilidad que sean seguros, eficientes y fáciles de usar tanto para profesores como para estudiantes.

En el artículo elaborado por (Aguilar Abanto et al., 2022) aborda la relevancia de los modelos híbridos de aprendizaje en el contexto educativo latinoamericano. Este estudio destaca cómo estos modelos, que integran elementos tanto presenciales como en línea, pueden ser una solución efectiva para superar los desafíos educativos en la región, especialmente en tiempos de pandemia.

En el contexto de servidores virtuales de alta disponibilidad para plataformas educativas, la adaptación de modelos híbridos de aprendizaje, como los discutidos en el artículo, se presenta como una estrategia viable para mejorar la eficiencia y la accesibilidad del sistema educativo. Estos modelos permiten una mayor flexibilidad

en la entrega de contenido y recursos, lo cual es crucial para mantener un servicio educativo de alta calidad y disponibilidad. La implementación de servidores virtuales robustos y altamente disponibles puede facilitar la adopción de estos modelos híbridos, al proporcionar la infraestructura necesaria para soportar tanto las actividades en línea como las presenciales.

La seguridad en entornos de virtualización de servidores es un pilar fundamental para garantizar la continuidad y la eficacia de las plataformas educativas como Moodle. Según (Arévalo Cordovilla et al., 2021), es imperativo aplicar políticas de aislamiento efectivo para las máquinas virtuales, asignando recursos fijos y estableciendo controles de seguridad en cada capa de la arquitectura virtual. Esto incluye desde el hipervisor hasta los sistemas operativos hospedados y la red virtual entre máquinas virtuales. Además, la implementación de herramientas de gestión como Trend Micro permite supervisar cambios críticos en los sistemas, una práctica que se alinea con la necesidad de mantener un entorno educativo virtual seguro y resiliente. La propuesta de (Arévalo Cordovilla et al., 2021) de un nuevo método para cuantificar el riesgo de seguridad en máquinas virtuales y su ubicación en servidores físicos maximiza la seguridad y la supervivencia de los servidores, lo cual es esencial para el funcionamiento óptimo de plataformas educativas en instituciones como EPUNEMI.

La pandemia de COVID-19 ha acelerado la necesidad de modelos educativos más flexibles y resilientes. En este sentido, los modelos híbridos de aprendizaje ofrecen una solución prometedora para enfrentar los desafíos actuales y futuros en la educación. Sin embargo, para que estos modelos sean efectivos, es fundamental contar con una infraestructura de servidores virtuales de alta disponibilidad que garantice un acceso ininterrumpido a los recursos educativos. Esto no solo mejora la

experiencia de aprendizaje, sino que también contribuye a reducir la brecha educativa en regiones donde el acceso a la educación de calidad es limitado.

Ambos estudios, aunque enfocados en diferentes niveles educativos y contextos, subrayan la importancia de adaptar los modelos educativos a las necesidades actuales. El estudio de la Universidad Autónoma de Querétaro, centrado en la educación superior, propone un modelo de "u-learning" que enfatiza la formación docente y la adaptabilidad tecnológica. Por su parte, el artículo sobre modelos híbridos en educación básica en América Latina destaca la flexibilidad y la resiliencia como elementos clave, especialmente en el contexto de la pandemia de COVID-19. En el marco de servidores virtuales de alta disponibilidad para plataformas educativas como Moodle, ambos enfoques ofrecen insights valiosos: la formación docente y la adaptabilidad tecnológica del estudio de Querétaro complementan la flexibilidad y resiliencia del modelo híbrido, proporcionando así un marco robusto para enfrentar los desafíos actuales y futuros en la educación en línea.

1.3.6. Plataformas educativas

El documento Plataformas tecnológicas y su aporte al aprendizaje en línea para la asignatura de matemática, resalta la importancia de plataformas tecnológicas como Moodle, Dokeos y Claroline en el ámbito educativo, especialmente en la enseñanza de la matemática. Estas plataformas no sólo facilitan el proceso de enseñanza-aprendizaje, sino que también son cruciales para el desarrollo de habilidades específicas como la resolución de problemas matemáticos (Morán-González & Gallegos-Macías, 2021).

La elección de una plataforma tecnológica adecuada, como Moodle, Dokeos o Claroline, es un factor determinante para el éxito del proceso educativo en

plataformas alojadas en la nube. Moodle no sólo facilita el proceso de enseñanza-aprendizaje, sino que también es esencial para el desarrollo de habilidades específicas, como la resolución de problemas matemáticos. Su adaptabilidad y su amplia adopción en múltiples países y en diversos idiomas lo convierten en una solución robusta y confiable. Este aspecto es especialmente relevante en entornos de nube, donde la confiabilidad y la escalabilidad son elementos clave para garantizar un acceso ininterrumpido y eficiente a los recursos educativos.

Además, el aprendizaje a distancia (DL) se ha convertido en un componente esencial de la educación moderna, ofreciendo nuevas oportunidades para el desarrollo de la educación universitaria. Los sistemas de DL, como Moodle, ofrecen funcionalidades clave que van más allá de la simple entrega de contenido, incluyendo herramientas de comunicación y la capacidad de crear currículos utilizando modelos de gestión de competencias. Estas funcionalidades hacen que los sistemas de DL sean especialmente útiles en la educación superior, donde la interacción y la personalización del aprendizaje son cruciales (Wagner et al., 2021).

1.3.7. Métricas clave en plataformas educativas

El estudio 'Análisis comparativo de las plataformas tecnológicas para el estudio de posgrados en línea en México' aborda la importancia de la innovación tecnológica en la educación superior, enfocándose en cómo diferentes plataformas educativas están siendo utilizadas en programas de posgrado en línea. Este análisis comparativo destaca la necesidad de adaptar nuevas tecnologías para mejorar la entrega y gestión de programas de posgrado en un entorno virtual (Penna et al., 2019).

La adaptación de nuevas tecnologías en la educación superior, particularmente en programas de posgrado en línea, es un pilar esencial para la gestión académica y

la enseñanza virtual. En este contexto, el análisis comparativo de plataformas educativas en México resalta la importancia de un enfoque multidimensional en la selección de tecnologías educativas. No se trata solo de elegir una plataforma con las mejores funcionalidades, sino también de considerar cómo se integra con la infraestructura existente, como servidores y sistemas de seguridad. En este sentido, la selección de una plataforma educativa adecuada se vuelve crucial y debe ser capaz de soportar un alto volumen de tráfico y garantizar un acceso ininterrumpido a los recursos educativos. Por lo tanto, la alta disponibilidad y la robustez del servidor se convierten en factores críticos para mantener la confiabilidad y eficiencia del sistema educativo en línea.

Un estudio reciente aborda los desafíos y oportunidades de utilizar tecnologías digitales en la enseñanza de matemáticas a nivel de bachillerato. Los investigadores concluyen que, aunque estas herramientas tienen un gran potencial para enriquecer el proceso educativo, su uso efectivo aún enfrenta obstáculos tanto para docentes como para estudiantes (Morán-González & Gallegos-Macías, 2021).

La adaptación de tecnologías digitales en la enseñanza de asignaturas específicas, como se observa en la investigación reciente sobre la enseñanza de matemáticas a nivel de bachillerato, resalta la necesidad de modernizar nuestras estrategias educativas y la infraestructura tecnológica que las soporta. Estas tecnologías no solo ofrecen un entorno más interactivo para el aprendizaje, sino que también requieren una infraestructura de servidor robusta y confiable para funcionar de manera óptima. Sin embargo, la misma investigación también destaca que la implementación de estas tecnologías enfrenta obstáculos, especialmente en la capacitación de docentes y estudiantes para su uso efectivo. Esto subraya la importancia de un enfoque integral que no solo incluya la implementación de

servidores virtuales de alta disponibilidad, sino también la formación adecuada para los usuarios finales. De esta manera, se logra un equilibrio entre la robustez tecnológica y la eficacia pedagógica en el ámbito educativo.

CAPÍTULO 2

2. Metodología

La metodología de investigación empleada se caracterizó por ser principalmente proyectiva y descriptiva, centrada en el análisis técnico del estado actual de la infraestructura de la plataforma educativa y en la formulación de una propuesta detallada de diseño de arquitectura en la nube con alta disponibilidad, junto con un plan de seguridad informática.

En la fase inicial, se llevó a cabo un exhaustivo análisis técnico de las vulnerabilidades presentes en la configuración del servidor dedicado en uso. Se recolectaron datos específicos sobre la arquitectura actual, incluyendo la disposición de los recursos, la política de seguridad existente y el coste total de operación. Este análisis técnico implicó una evaluación de la seguridad y rendimiento a través de herramientas de diagnóstico especializadas, lo que permitió identificar con precisión las debilidades y riesgos en la infraestructura actual sin la necesidad de realizar encuestas o entrevistas.

Posteriormente, en la fase proyectiva, se diseñó una solución conceptual para la migración hacia una infraestructura en la nube de Google Cloud Platform (GCP), con el fin de alcanzar un nivel óptimo de alta disponibilidad. Esta etapa implicó un análisis detallado de las opciones de servicios que ofrece GCP, seleccionando aquellos que mejor se alineaban con los requerimientos técnicos y de seguridad detectados previamente.

La propuesta del plan de seguridad informática se construyó tomando en cuenta las mejores prácticas del sector y los estándares internacionales,

personalizados a las necesidades específicas deducidas del análisis técnico. Se detallaron recomendaciones concretas para reforzar la seguridad, incluyendo estrategias de mitigación de riesgos adaptadas a las vulnerabilidades específicas encontradas.

Durante el proceso de diseño, se adoptó un enfoque iterativo, que consistió en el refinamiento progresivo de la propuesta. Se emplearon herramientas de diseño arquitectónico y simulaciones de seguridad para validar y ajustar la viabilidad y eficacia de la solución propuesta. A través de este método, se garantizó la integración de un diseño robusto y una estrategia de seguridad integral.

Un análisis coste-beneficio proporcionó una comparación financiera entre la solución de servidor dedicado actual y la infraestructura de GCP propuesta, enfocándose en la evaluación de la inversión inicial y los gastos operativos contra los beneficios de escalabilidad, seguridad y disponibilidad.

El trabajo culminó con la consolidación de la propuesta en un documento técnico, que incluyó las especificaciones técnicas del diseño de la arquitectura en GCP y del plan de seguridad informática. Se elaboraron diagramas de arquitectura y se definieron los pasos de una implementación teórica, detallando cómo cada elemento contribuiría a la solución integral.

Esta metodología, que une el análisis técnico detallado con un diseño proyectivo, permitió la creación de una propuesta sólidamente fundamentada, diseñada para mejorar la infraestructura de la plataforma educativa y elevar su perfil de seguridad informática sin la implementación práctica inmediata.

CAPÍTULO 3

3. Propuesta de solución

3.1.1. Evaluación la infraestructura tecnológica actual

Detalles del Servidor:

El servidor en el que está alojado el Aula Virtual EPUNEMI cuenta con las siguientes especificaciones y detalles:

Nombre del servidor: epunemi

Versión de cPanel: 110.0 (build 10)

Versión de Apache: 2.4.57

Versión de MySQL: 5.7.43

Arquitectura: x86_64

Sistema operativo: Linux

Dirección IP compartida: 88.99.149.112

Subdominio: virtual.epunemi.gob.ec

Versión de Perl: 5.16.3

Versión del Kernel: 3.10.0-514.2.2.el7.x86_64

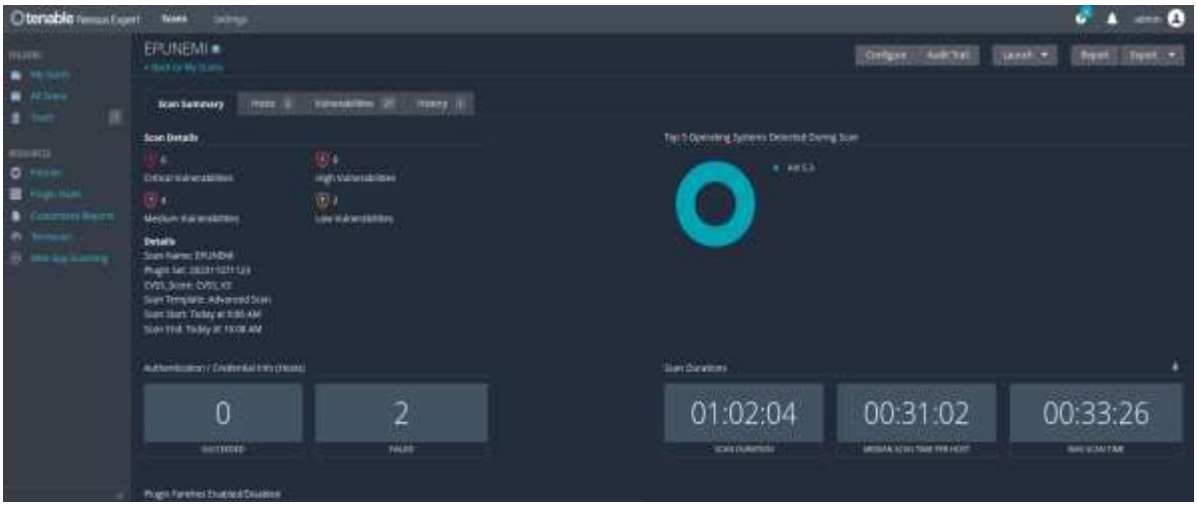
La evaluación de la seguridad de la infraestructura actual constituye un pilar fundamental en la propuesta de mejora de la arquitectura de la plataforma educativa. En este contexto, se prestó especial atención al análisis del servidor con dirección IP asignada y al nombre de subdominio correspondiente, componentes críticos dado su papel en la conectividad y accesibilidad de los servicios.

Para realizar un diagnóstico exhaustivo, se empleó la herramienta Nessus Expert, una de las soluciones de escaneo de vulnerabilidades más avanzadas y reconocidas en el campo de la ciberseguridad. A través de un 'Advanced Scan', se configuró Nessus para que ejecutara una batería comprensiva de pruebas destinadas a detectar una amplia gama de vulnerabilidades, desviaciones de las mejores prácticas de seguridad y posibles configuraciones erróneas que pudieran comprometer la integridad y disponibilidad del sistema.

La elección del 'Advanced Scan' se fundamentó en la necesidad de profundizar en la inspección más allá de las vulnerabilidades conocidas y catalogadas, buscando exponer fallos potenciales que requieren una atención inmediata y estrategias de mitigación específicas. Esta modalidad de análisis permite, además, un entendimiento más completo del estado de seguridad del servidor, al incluir pruebas de penetración no intrusivas y revisiones de configuraciones que abarcan tanto el software como el hardware.

Figura 1.

Momento del proceso de análisis realizado con Nessus Expert.



Fuente: Elaboración propia, (2023)

El resumen del escaneo de seguridad Figura 2, llevado a cabo con la herramienta Nessus Expert bajo el nombre de EPUNEMI, refleja un perfil de riesgo de la infraestructura evaluada en el cual se identificaron vulnerabilidades de severidad media y baja, sin registro de vulnerabilidades críticas o altas. La ausencia de vulnerabilidades críticas y altas indica que no se detectaron riesgos inminentes que pudieran causar interrupciones graves o comprometer de manera significativa la integridad de la plataforma educativa.

El conjunto de plugins utilizado para el análisis lleva el identificador 202311071123, garantizando que la evaluación se basó en las definiciones de vulnerabilidad y las prácticas de seguridad más actualizadas al momento del escaneo. La métrica CVSS_Score: CVSS_V3 mencionada en los detalles del escaneo, hace referencia al sistema de puntuación del Common Vulnerability Scoring System versión 3, que es un estándar abierto para evaluar la gravedad de las vulnerabilidades informáticas y proporciona una forma clara y unificada de comunicar las características y los impactos de las mismas.

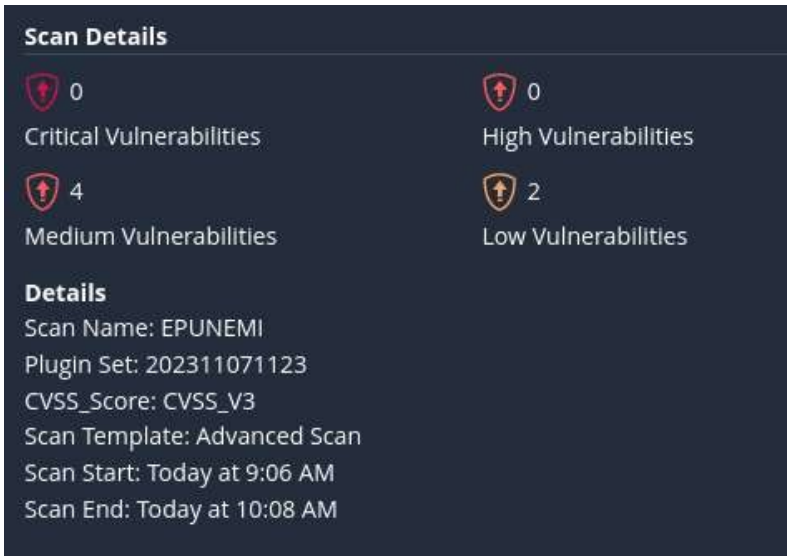
El escaneo tuvo una duración de una hora y dos minutos, comenzando a las 9:06 AM y concluyendo a las 10:08 AM, lo cual demuestra una capacidad de análisis eficiente. Durante este proceso, se detectaron un total de 4 vulnerabilidades de nivel medio y 2 de nivel bajo. La identificación de estas vulnerabilidades es crucial, ya que ofrece una oportunidad para reforzar la seguridad a través de medidas correctivas específicas antes de que puedan ser explotadas por actores maliciosos.

Este análisis proactivo forma la base sobre la cual se establecerán recomendaciones detalladas para la mitigación de riesgos y mejoras en la infraestructura de seguridad propuesta en el diseño de la nueva arquitectura en la

nube.

Figura 2.

Resumen del escaneo de seguridad.



Fuente: Elaboración propia, (2023)

El resumen proporcionado Figura 3, revela tres vulnerabilidades específicas detectadas en el sistema evaluado. A continuación, se presenta una descripción de cada una, el riesgo asociado y el impacto potencial en la disponibilidad del servicio o la integridad de los datos:

Figura 3.

Vulnerabilidades específicas detectadas en el sistema.

Fuente: Elaboración propia, (2023)

HSTS Missing From HTTPS Server (RFC 6797) - Severidad Media (CVSS v3.0: 6.5)

Descripción: La ausencia de la cabecera HTTP Strict Transport Security (HSTS) implica que el servidor no fuerza el uso de conexiones HTTPS, lo cual puede hacer que los usuarios sean susceptibles a ataques de intermediarios (man-in-the-middle) que pueden interceptar o alterar las comunicaciones.

Riesgo: Un atacante podría explotar esta vulnerabilidad para capturar o modificar datos en tránsito, como credenciales de sesión o información personal.

Impacto: La disponibilidad del servicio no se ve directamente afectada; sin embargo, la integridad y la confidencialidad de los datos podrían verse comprometidas, erosionando la confianza del usuario en el servicio.

SSL Anonymous Cipher Suites Supported - Severidad Media (CVSS v3.0: 5.9)

Descripción: La compatibilidad con suites de cifrado anónimas SSL indica que el servidor acepta conexiones cifradas que no autentican la identidad del servidor. Esto puede permitir que un atacante realice ataques de "man-in-the-middle".

Riesgo: La posibilidad de que un atacante intercepte y descifre las comunicaciones aumenta significativamente, debido a la falta de autenticación en el intercambio de claves.

Impacto: Similar al primer caso, esto no necesariamente afecta la disponibilidad, pero compromete gravemente la seguridad de las comunicaciones, permitiendo potencialmente el acceso a datos sensibles.

SMTP Service Cleartext Login Permitted - Severidad Baja (CVSS v3.0: 2.6)*

Descripción: Permitir el inicio de sesión en texto claro (sin cifrar) en el servicio SMTP facilita la posibilidad de que las credenciales de acceso sean interceptadas por un atacante que esté escuchando en la red.

Riesgo: El riesgo es que se puedan capturar las credenciales de usuario de correo electrónico, lo que podría llevar a accesos no autorizados y potencialmente al compromiso de la comunicación por correo electrónico.

Impacto: Este riesgo no afecta directamente la disponibilidad del servicio de correo electrónico, pero sí pone en peligro la confidencialidad de la información que se envía a través de este medio, pudiendo resultar en la filtración de datos sensibles y la posible manipulación del correo.

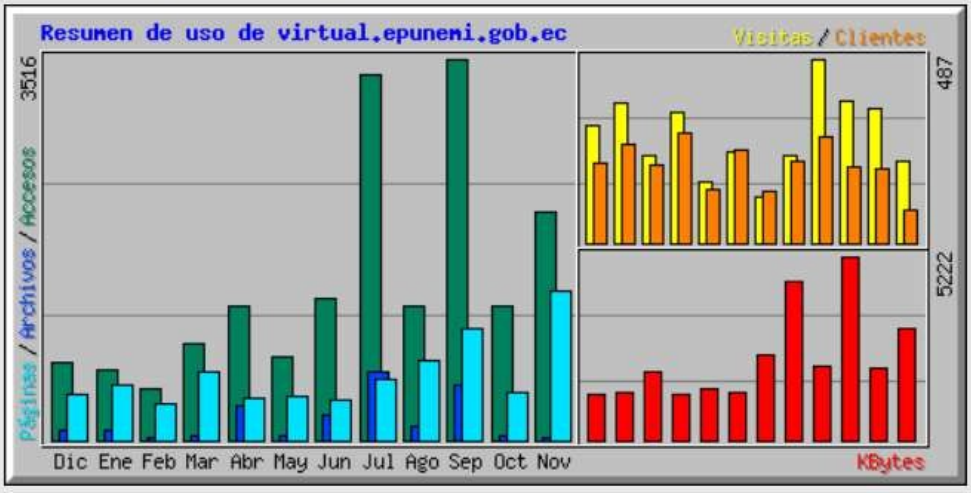
3.1.2. Informe de Métricas y Servidor de Aula Virtual EPUNEMI

Estadísticas de Uso:

El uso mensual del Aula Virtual de EPUNEMI ha presentado fluctuaciones notables Figura 4. Es preciso señalar que la capacidad para realizar un análisis detallado de dichas métricas es limitada, debido a la ausencia de herramientas analíticas adecuadas. Esta deficiencia representa una vulnerabilidad asociada a la infraestructura del servidor actual.

Figura 4.

Uso mensual del Aula Virtual de EPUNEMI.



Resumen por meses

Mes	Media diaria				Totales mensuales					
	Accesos	Archivos	Páginas	Visitas	Clientes	KBytes	Visitas	Páginas	Archivos	Accesos
Nov 2023	139	1	92	14	86	3193	215	1382	20	2096
Oct 2023	39	1	14	11	194	2031	355	446	40	1234
Sep 2023	117	16	34	12	201	5222	374	1031	507	3516
Ago 2023	40	4	23	15	279	2100	487	734	131	1240
Jul 2023	108	20	18	7	214	4523	229	561	625	3369
Jun 2023	43	8	12	4	137	2412	121	365	241	1300
May 2023	24	1	13	7	247	1348	241	404	38	767
Abr 2023	41	10	13	5	140	1439	160	398	323	1238
Mar 2023	28	1	20	11	289	1298	343	638	39	884
Feb 2023	17	1	11	8	204	1968	232	332	30	481
Ene 2023	20	3	16	12	263	1368	372	518	97	650
Dic 2022	23	2	13	10	211	1307	311	425	91	716
Totales						**28209**	**3440**	**7234**	**2182**	**17491**

Fuente: Elaboración propia, (2023)

3.1.3 Evaluación comparativa de las tecnologías para infraestructura de alta disponibilidad en la nube

La computación en la nube se ha consolidado como un elemento fundamental para empresas de todos los tamaños, transformando radicalmente la infraestructura

de TI. Esta tecnología no solo facilita el acceso a servicios de TI a través de Internet, sino que también destaca por su infraestructura de alto rendimiento, asegurando procesos eficientes y rápidos. La estabilidad es un aspecto clave, permitiendo a las operaciones empresariales continuar sin interrupciones y adaptarse a las variaciones en la carga de trabajo. La seguridad en la nube es otro punto crucial, ofreciendo protección robusta para datos y aplicaciones en un entorno digital avanzado. Desde una perspectiva económica, la nube es particularmente rentable, con modelos de pago por uso que permiten a las organizaciones maximizar su inversión en tecnología. La escalabilidad, permitiendo ajustar los recursos tecnológicos a las necesidades cambiantes, es esencial para mantener una ventaja competitiva en el mercado actual. En conjunto, estas características hacen de la computación en la nube una solución integral y flexible, capaz de satisfacer las demandas específicas de cada negocio en el contexto tecnológico contemporáneo.

Google Cloud se destaca en el ámbito de los servicios en la nube por su excepcional rendimiento de infraestructura, atribuido principalmente a su red global de alta velocidad y a sus centros de datos avanzados. Estos factores garantizan una latencia mínima y un procesamiento de datos rápido y eficiente, asegurando una alta disponibilidad y estabilidad, elementos críticos para cualquier aplicación empresarial. La estabilidad de Google Cloud no solo se refleja en la operatividad constante, sino también en su capacidad para manejar cargas de trabajo fluctuantes, lo que es crucial para mantener la continuidad del negocio (Google Cloud, 2023).

En términos de seguridad, Google Cloud implementa protocolos de seguridad de vanguardia y cumple con múltiples estándares de conformidad, convirtiéndose en una opción confiable para empresas que manejan datos sensibles. Su modelo de precios, basado en el pago por uso, ofrece una solución costo-eficiente, permitiendo

a las empresas optimizar sus gastos en tecnología de la información. Por último, la escalabilidad es una de las características más notables de Google Cloud, ofreciendo a las organizaciones la flexibilidad de escalar sus recursos de acuerdo a la demanda, sin incurrir en costos excesivos o enfrentar problemas de rendimiento (Google Cloud, 2023). Esta combinación de rendimiento, estabilidad, seguridad, eficiencia de costos y escalabilidad hace de Google Cloud una solución integral y atractiva en el campo de la computación en la nube.

(Amazon AWS, 2023) se presenta como una plataforma líder en el ámbito de los servicios de computación en la nube, destacando particularmente por su sobresaliente rendimiento de infraestructura. Dispone de una extensa red global de centros de datos, diseñados para garantizar un procesamiento de datos rápido y eficiente, lo cual es fundamental para aplicaciones empresariales que demandan alta velocidad y bajo tiempo de respuesta. Esta robusta infraestructura no solo proporciona un rendimiento excepcional, sino que también asegura una estabilidad significativa, manifestándose a través de su capacidad para mantener una operatividad constante y gestionar efectivamente las variaciones en la carga de trabajo, lo cual es esencial para la continuidad operativa de las empresas.

En cuanto a la seguridad, Amazon AWS implementa rigurosos protocolos de seguridad y cumple con un amplio abanico de estándares de conformidad internacionales, brindando un entorno confiable para la gestión de datos sensibles. Además, su estructura de precios flexible, basada en el modelo de pago por uso, ofrece a las organizaciones una solución altamente costo-eficiente. Esta eficiencia permite a las empresas optimizar sus gastos en tecnología sin sacrificar calidad ni rendimiento. Finalmente, la escalabilidad es uno de los aspectos más destacados de Amazon AWS. La plataforma proporciona a las organizaciones la capacidad de

ajustar sus recursos informáticos de manera rápida y sencilla, adaptándose a la demanda fluctuante sin incurrir en costos exorbitantes o comprometer el rendimiento. Esta combinación de rendimiento, estabilidad, seguridad, eficiencia de costos y escalabilidad convierte a Amazon AWS en una elección robusta y versátil para las necesidades de computación en la nube de las empresas modernas.

(Microsoft Azure, 2023) se posiciona como una plataforma de servicios en la nube altamente competitiva, enfocándose en varios aspectos clave. En cuanto al rendimiento de infraestructura, Azure se destaca por su red global de centros de datos, optimizados para proporcionar un procesamiento de datos veloz y eficiente, aspecto fundamental para aplicaciones críticas que requieren tiempos de respuesta rápidos y un procesamiento ágil de datos. La estabilidad es otro pilar fundamental de Azure, garantizando la disponibilidad continua y la capacidad para manejar de manera efectiva fluctuaciones en la carga de trabajo, vital para la operatividad ininterrumpida de los negocios.

En términos de seguridad, Azure adhiere a protocolos de seguridad rigurosos y cumple con numerosos estándares de conformidad global, ofreciendo un entorno seguro para la gestión de datos sensibles, un compromiso esencial para empresas que manejan información crítica. Además, Azure proporciona una estructura de precios basada en el uso, representando una solución costo-eficiente para empresas que buscan optimizar sus inversiones en tecnología de la información. Finalmente, la escalabilidad es una característica distintiva de Azure, permitiendo a las organizaciones ajustar sus recursos informáticos de acuerdo con sus necesidades actuales, sin incurrir en costos excesivos o comprometer el rendimiento, convirtiendo a Azure en una opción robusta y adaptable para las demandas de computación en la nube de las empresas modernas.

Cuadro Comparativo de Google Cloud Platform (GCP), Amazon Web Services (AWS) y Microsoft Azure

Tabla 1

Comparación tecnologías en la nube

Aspecto	Google Cloud Platform (GCP)	Amazon Web Services (AWS)	Microsoft Azure
Rendimiento de Infraestructura	Red global de alta velocidad, centros de datos avanzados, latencia mínima	Extensa red global de centros de datos, procesamiento rápido y eficiente	Red global de centros de datos, procesamiento de datos veloz y eficiente
Estabilidad	Alta disponibilidad, manejo efectivo de cargas de trabajo fluctuantes	Operatividad constante, manejo efectivo de variaciones en la carga de trabajo	Disponibilidad continua, manejo efectivo de fluctuaciones en la carga de trabajo
Seguridad	Protocolos de seguridad de vanguardia, múltiples estándares de conformidad	Rigurosos protocolos de seguridad, amplio abanico de estándares de conformidad internacionales	Adherencia a protocolos de seguridad rigurosos, estándares de conformidad global
Costo-Eficiencia	Modelo de precios basado en el pago por uso	Estructura de precios flexible, modelo de pago por uso	Estructura de precios basada en el uso
Escalabilidad	Flexibilidad para escalar recursos según la demanda	Ajuste rápido y sencillo de recursos, adaptación a la demanda fluctuante	Capacidad de ajustar recursos informáticos según necesidades actuales

Fuente: Elaboración propia, (2023)

3.1.4 Diferencias geográficas en la presencia de las principales plataformas de computación en la nube

A continuación, se presentan tres mapas visuales. Cada uno de estos mapas muestra las zonas y regiones de Google Cloud Platform (GCP), Amazon Web Services (AWS), y Microsoft Azure respectivamente. Estas representaciones gráficas son fundamentales para comprender cómo cada plataforma ha extendido su infraestructura a nivel mundial, con un enfoque específico en su presencia en América Latina.

La Figura 5 detalla la distribución de GCP, resaltando su amplia cobertura en

América Latina, más allá de Brasil. La Figura 6 y Figura 7 corresponden a AWS y Microsoft Azure, respectivamente, mostrando una concentración de sus servicios principalmente en Brasil para esta región. Estos mapas proporcionan una perspectiva clara de la disponibilidad y el alcance geográfico de cada proveedor de servicios en la nube, un factor crucial para las empresas al tomar decisiones estratégicas sobre infraestructura de TI y servicios en la nube.

Figura 5.

Mapa de ubicaciones de centro de datos de Google Cloud. Fuente: Ubicaciones de Google Cloud

FUENTE: (https://cloud.google.com/about/locations?hl=es#lightbox-regions-map)

Figura 6.

Mapa de ubicaciones de centro de datos de Amazon AWS.

Fuente: Infraestructura global de AWS **(https://aws.amazon.com/es/about-aws/global-infrastructure/?p=ngi&loc=1)**

Figura 7.

Mapa de ubicaciones de centro de datos de Microsoft Azure.

Fuente: Arquitectura y resistencia del servicio Azure (https://learn.microsoft.com/es-es/azure/virtual-desktop/service-architecture-resilience)

Tras un análisis detallado de las principales plataformas de computación en la nube, considerando aspectos como el rendimiento de infraestructura, la estabilidad, la seguridad, la costo-eficiencia y la escalabilidad, la elección de Google Cloud Platform (GCP) se destaca como la más adecuada para las organizaciones ubicadas o con operaciones significativas en América Latina. La amplia presencia de GCP en esta región, con múltiples regiones y zonas más allá de Brasil, la posiciona como una

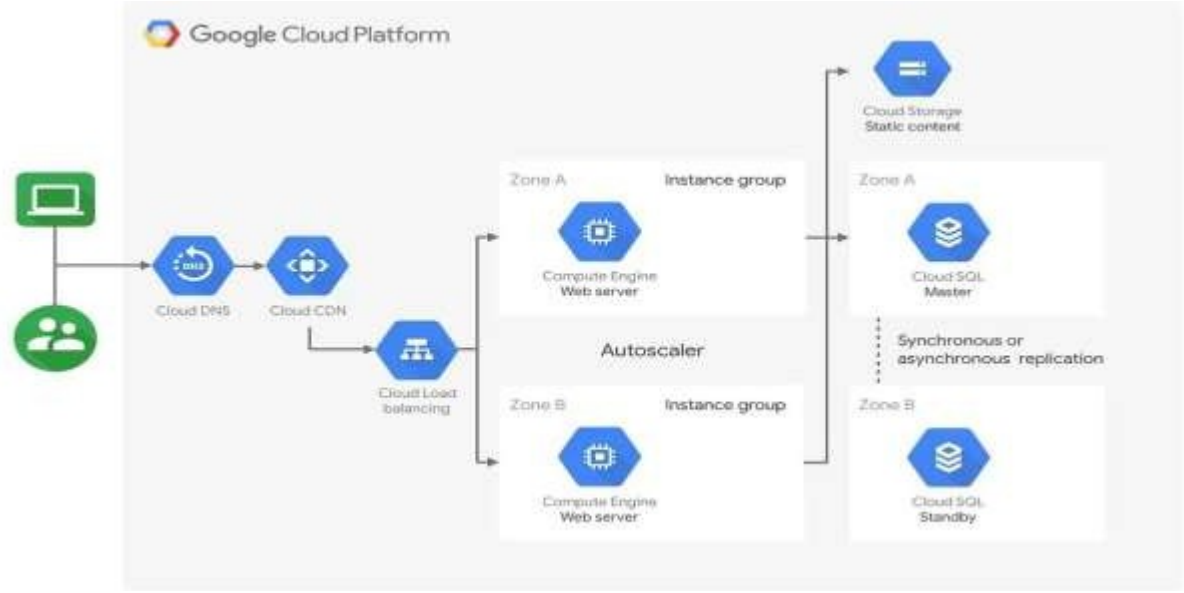
opción superior, especialmente para aquellas empresas que buscan minimizar la latencia y maximizar el rendimiento a nivel local. Esta cobertura geográfica extensa garantiza no solo una mayor proximidad a los centros de datos, lo que se traduce en mejoras en la velocidad y eficiencia de los procesos, sino también asegura una mayor resiliencia y opciones de redundancia en caso de fallos o interrupciones de servicio. Por lo tanto, para las empresas en América Latina o aquellas que sirven a este mercado, GCP no solo cumple con los requisitos técnicos y de seguridad, sino que también ofrece ventajas estratégicas significativas en términos de alcance geográfico y desempeño optimizado en la región.

3.1.6 Diseño de infraestructura de alta disponibilidad en la nube de GCP

El diagrama presentado Figura 8, es una propuesta de arquitectura de sistema web escalable y de alta disponibilidad diseñada para Google Cloud Platform (GCP).

Figura 8.

Fuente propia, Diseño de infraestructura de alta disponibilidad en la nube de GCP.



Fuente: Elaboración propia, (2023)

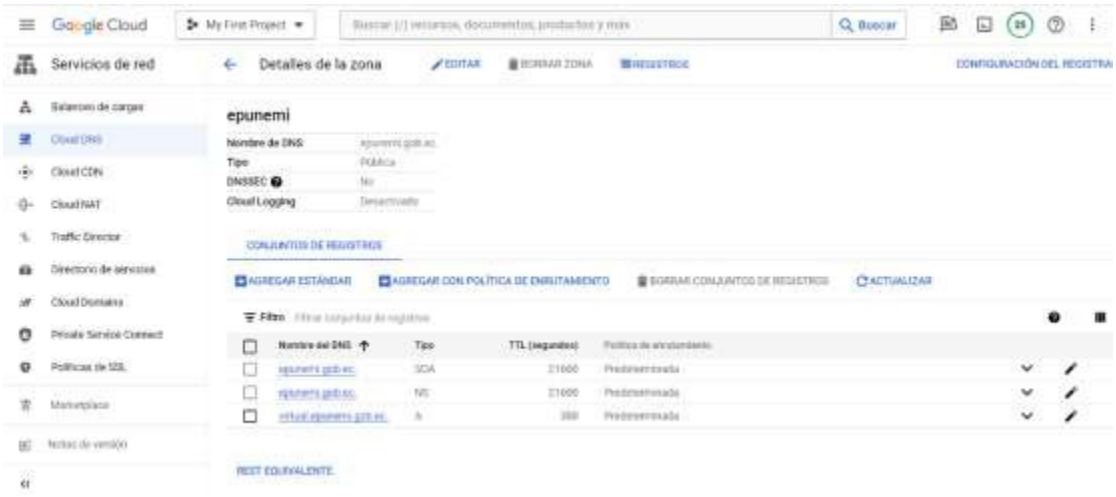
A continuación, desglosaré cada componente y su función dentro del sistema, seguido de los beneficios que aportan a la arquitectura.

3.1.7 Componentes y su Función

Cloud DNS: Este servicio fundamental actúa como un intermediario entre los nombres de dominio humanamente comprensibles y las direcciones IP numéricas requeridas para la comunicación de máquina a máquina. Al interpretar y redirigir las solicitudes de nombres de dominio, como www.example.com, a su correspondiente dirección IP, Cloud DNS es un componente crítico en la resolución de nombres, imprescindible para la funcionalidad y la accesibilidad de las aplicaciones basadas en la web.

Figura 9.

Configuración Cloud DNS para EPUNEMI



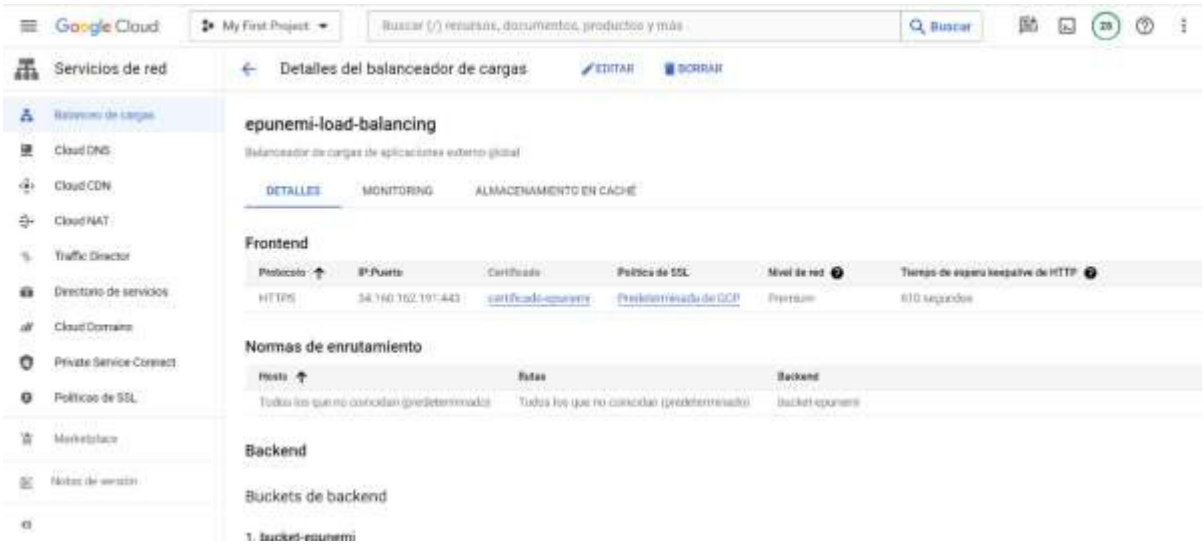
Fuente: Elaboración propia, (2023)

Cloud CDN (Content Delivery Network): La eficiencia en la entrega de contenido estático, tal como imágenes y archivos de JavaScript o CSS, es crucial para optimizar la experiencia del usuario final. Cloud CDN capitaliza la infraestructura global de Google, disminuyendo la latencia y acelerando el acceso al contenido mediante la ubicación estratégica de los datos cerca del usuario, lo que contribuye directamente a la retención y satisfacción del cliente debido a la mejora en los tiempos de carga.

Cloud Load Balancing: Este componente distribuye de manera inteligente las cargas de trabajo entrantes a través de los recursos computacionales disponibles, tales como instancias de máquinas virtuales. La capacidad de gestionar eficazmente el tráfico de red no solo mejora la disponibilidad y la respuesta del sistema, sino que también juega un papel vital en el mantenimiento del rendimiento durante variaciones o picos de demanda.

Figura 10.

Balanceador de cargas EPUNEMI.

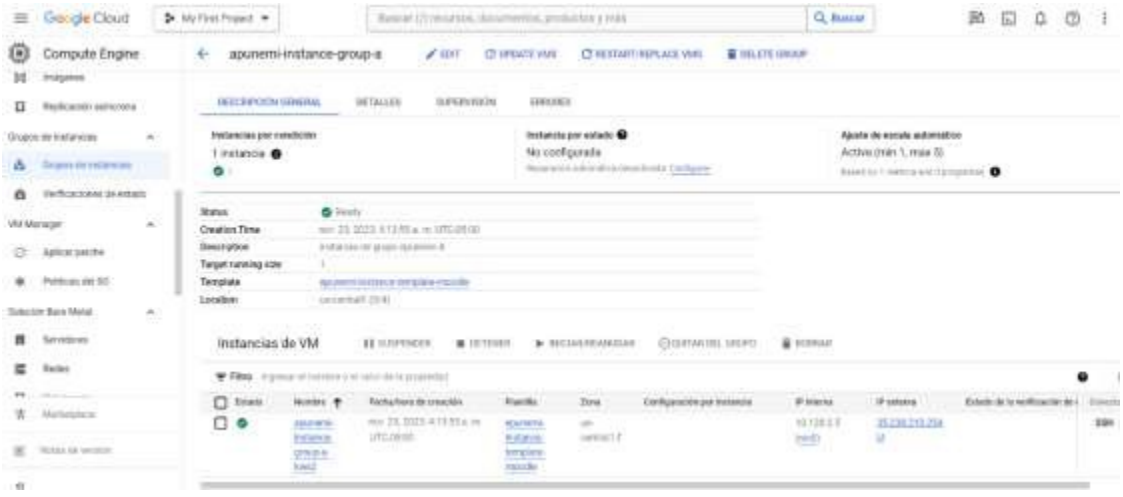


Fuente: Elaboración propia, (2023)

Instance Group: La agrupación de instancias de máquinas virtuales que funcionan como una entidad única permite un manejo simplificado y una distribución equitativa del tráfico hacia la aplicación web o el contenido dinámico, esencial para mantener un servicio coherente y escalable.

Figura 11.

Grupo de instancia para la auto escalabilidad de la VM EPUNEMI



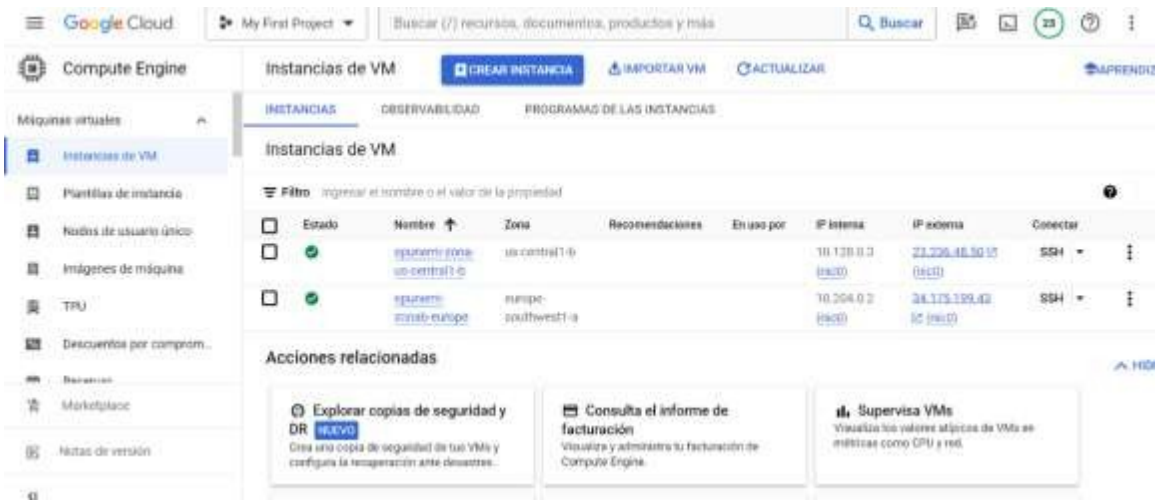
Fuente: Elaboración propia, (2023)

Autoscaler: Este componente dinámico ajusta automáticamente la cantidad de instancias de cómputo dentro de un grupo en respuesta a la carga de trabajo. La capacidad de escalar recursos proporcionalmente a la demanda asegura una gestión de costos eficiente y evita el sobredimensionamiento de recursos, optimizando así la inversión en infraestructura.

Compute Engine: Al brindar máquinas virtuales operativas sobre la infraestructura avanzada de Google, Compute Engine es el pilar donde se alojan los servidores web de las aplicaciones, garantizando el rendimiento y la estabilidad del servicio proporcionado.

Figura 12.

Instancias de Máquinas Virtuales VM.

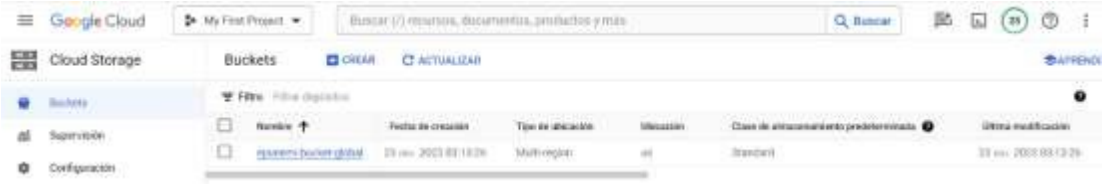


Fuente: Elaboración propia, (2023)

Cloud Storage: El almacenamiento de contenido estático en Cloud Storage, ya sea servido directamente a los usuarios o a través de Cloud CDN, ofrece una solución robusta y escalable para la gestión de datos, crucial para el mantenimiento y la distribución eficiente de los recursos informativos.

Figura 13.

Cloud Storage EPUNEMI



Fuente: Elaboración propia, (2023)

Cloud SQL: Soportando motores como MySQL, PostgreSQL y SQL Server, Cloud SQL es el servicio de base de datos gestionado que opera como el almacén de datos principal. La claridad en la elección entre la replicación síncrona o asincrónica se convierte en un factor decisivo para el diseño de una arquitectura orientada a la disponibilidad y a la coherencia de datos.

Figura 14.

Cloud SQL moodle EPUNEMI

Fuente: Elaboración propia, (2023)

Figura 15.

Copias de seguridad automatizadas

Fuente: Elaboración propia, (2023)

Replicación Síncrona o Asincrónica: La elección de replicación asíncrona, común en Google Cloud SQL, debe reconocerse por su equilibrio entre consistencia eventual y eficiencia operativa. Si bien existe una ventana de latencia donde las últimas transacciones pueden no replicarse inmediatamente en caso de fallo, la replicación asíncrona es suficientemente robusta para aplicaciones empresariales, dada su ventana temporal reducida y su simplificación en la gestión de réplicas.

Zona A y Zona B: La presencia de Compute Engine y Cloud SQL en zonas geográficamente distintas fortalece la infraestructura contra interrupciones y fallos. Esta redundancia geográfica asegura que, ante cualquier contingencia en una zona, las operaciones pueden continuar en la otra sin interrupción del servicio, lo que es fundamental para sistemas que requieren una alta disponibilidad y una estrategia de recuperación ante desastres bien estructurada.

Figura 16.

Replicación de la base de datos en zonas geográficas distintas.

Fuente: Elaboración propia, (2023)

3.1.8 Optimización de Costos mediante el Autoscaler y la Gestión de Recursos

La optimización de costos en infraestructuras de nube es un desafío constante para las organizaciones, y aquí es donde el Autoscaler de Google Cloud Platform desempeña un papel transformador. Este componente dinámico permite que la infraestructura se adapte a la demanda en tiempo real ajustando las instancias de máquinas virtuales automáticamente. Al aumentar o reducir los recursos en función del tráfico y la carga de trabajo actual, se evita la inmovilización de capital en recursos infrautilizados durante los períodos de baja demanda, al tiempo que se garantiza la capacidad de respuesta durante los picos de tráfico. Esto no solo mejora la eficiencia operativa sino que también traduce en ahorros directos, pues se paga estrictamente por el recurso que se consume.

La distribución inteligente de recursos va más allá del simple escalado vertical u horizontal, incorporando la toma de decisiones predictiva basada en tendencias de uso y análisis de tráfico. Esta inteligencia aplicada a la asignación de recursos permite anticipar necesidades y ajustar la infraestructura de forma proactiva, lo que minimiza el riesgo de incurrir en costos excesivos debido a una provisión exagerada. En última instancia, el Autoscaler y una gestión de recursos afinada son esenciales para mantener una estructura de costos variable que refleje con precisión el uso real,

esencial para una gestión financiera prudente en entornos de nube.

3.1.9 Propuesta del Plan de seguridad Informática

Es importante destacar que una infraestructura de TI robusta y confiable debe estar respaldada por un plan de seguridad informática. Dicho plan abarca las políticas, herramientas y procedimientos diseñados para proteger los activos digitales y la infraestructura frente a amenazas internas y externas. Dada la complejidad y el nivel de detalle técnico que involucra este esquema de protección, se ha desarrollado un plan integral de seguridad informática que se adjunta a esta tesis como anexo. Este documento complementario proporciona un desglose detallado de las estrategias de seguridad implementadas, las prácticas de conformidad y las metodologías de respuesta ante incidentes, que juntas forman el escudo contra las vulnerabilidades y los riesgos asociados. La decisión de presentar el plan de seguridad informática en un anexo obedece a la intención de facilitar la consulta detallada de los protocolos de seguridad por parte de los interesados, sin sobrecargar el cuerpo principal de la tesis, permitiendo así una lectura más ágil de los temas centrales expuestos en el documento.

CONCLUSIONES Y TRABAJO FUTURO

Conclusiones

Evaluación de la Infraestructura Tecnológica: Se ha evaluado la infraestructura tecnológica actual de la plataforma MOODLE en la EPUNEMI, identificando métricas clave y eventos críticos que han influido en la experiencia de los usuarios. Esta evaluación ha permitido obtener una comprensión profunda de las necesidades específicas de la plataforma y cómo estas han sido abordadas para mejorar el servicio.

Importancia de la Alta Disponibilidad: Se ha confirmado la importancia crítica de la alta disponibilidad en servidores virtuales para garantizar un acceso ininterrumpido a recursos educativos. Este hallazgo ha resaltado la necesidad de implementar un clúster de alta disponibilidad para optimizar la eficiencia y disponibilidad de la plataforma educativa en línea.

Balanceo de Carga en Sistemas con Tráfico Intenso: Se ha establecido que el balanceo de carga es un mecanismo esencial para asegurar la alta disponibilidad en sistemas con tráfico intenso de usuarios, como Moodle. La implementación de un balanceador de carga adecuado ha sido fundamental para prevenir sobrecargas y garantizar un rendimiento óptimo del sistema.

Mitigación de la Redundancia de Datos: Se ha identificado la necesidad de mitigar la redundancia de datos para mejorar la eficiencia y consistencia del sistema. Este aspecto ha sido crucial para la gestión eficiente de bases de datos y para evitar problemas de almacenamiento y acceso a datos duplicados.

Reconocimiento de la Seguridad Informática: La seguridad informática ha sido reconocida como un requisito principal para alojar aplicaciones críticas en la nube. La protección contra accesos no autorizados y la implementación de restricciones de integridad en la base de datos han sido fundamentales para la seguridad de la plataforma.

Importancia de la Infraestructura Tecnológica Avanzada y Segura: En conjunto, estas conclusiones han subrayado la importancia de una infraestructura

tecnológica avanzada y segura en el ámbito educativo, resaltando la necesidad de adaptaciones y mejoras continuas en las plataformas de aprendizaje en línea para enfrentar los desafíos actuales y futuros en el sector de la educación.

Trabajo futuro

Es esencial llevar a cabo la implementación práctica de las soluciones propuestas para la infraestructura tecnológica, especialmente en lo que respecta a la alta disponibilidad, el balanceo de carga y la redundancia de datos.

Se recomienda realizar una evaluación continua de la infraestructura tecnológica implementada para adaptarse a los cambios en las necesidades y en la tecnología.

Dada la rápida evolución de las TIC, se sugiere mantener una investigación continua en nuevas tecnologías que puedan mejorar aún más la eficiencia y seguridad de la plataforma educativa.

Es importante enfocarse en la formación y capacitación de los usuarios finales, incluyendo tanto a estudiantes como a docentes, para garantizar el uso efectivo de la plataforma y las nuevas tecnologías implementadas.

RECOMENDACIONES

Es esencial continuar con el desarrollo y mejoramiento de la infraestructura tecnológica, especialmente en lo que respecta a la alta disponibilidad y el balanceo de carga. Esto garantizará que la plataforma pueda manejar un aumento en la demanda de manera efectiva y eficiente.

Dada la creciente amenaza de ciberataques, es crucial fortalecer continuamente las medidas de seguridad informática. Esto incluye la actualización regular de software, la implementación de protocolos de seguridad más robustos y la formación de los usuarios en buenas prácticas de seguridad.

Se recomienda realizar evaluaciones periódicas del rendimiento y la funcionalidad de la plataforma para identificar y abordar cualquier problema o área de mejora de manera oportuna.

Fomentar la colaboración con otras instituciones educativas y empresas tecnológicas para compartir conocimientos, experiencias y recursos. Esto podría conducir a innovaciones y mejoras más significativas en la plataforma.

Estas recomendaciones están dirigidas a fortalecer y expandir la eficacia de la infraestructura tecnológica en la EPUNEMI, asegurando su relevancia y utilidad en el cambiante entorno educativo y tecnológico.

BIBLIOGRAFIA

Aguilar Abanto, J. L., Colán Hernández, B. A., Alejos Cuchura, B. G., & Romero Carazas, R. (2022). “Aprendizaje anywhere”: Modelos híbridos en entornos virtuales en educación básica en América Latina. *Horizontes. Revista de Investigación En Ciencias de La Educación*, *6*(26), 1961–1976. https://doi.org/10.33996/revistahorizontes.v6i26.465

Amazon AWS. (2023, November 16). *Welcome to AWS Documentation*. https://docs.aws.amazon.com/?nc2=h_ql_doc_do

Arévalo Cordovilla, F., Arévalo Cordovilla, B., Castillo Salvatierra, L., & Cortez Lara, A. (2021). Gestión de Seguridad en Virtualización de Servidores. *Ecuadorian Science Journal*, *5*(4), 150–163. https://doi.org/10.46480/esj.5.4.178

Digital Guide IONOS. (2023, March 1). *¿Qué es un servidor?* https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-servidor-un-concepto-dos-definiciones/

Google Cloud. (2023, November 15). *Why Google Cloud*. https://cloud.google.com/why-google-cloud?hl=es-419

Mesbahi, M. R., Rahmani, A. M., & Hosseinzadeh, M. (2018). Reliability and high availability in cloud computing environments: a reference roadmap. *Human-Centric Computing and Information Sciences*, *8*(1). https://doi.org/10.1186/s13673-018-0143-8

Microsoft Azure. (2023, November 15). *Get Started Azure*. https://azure.microsoft.com/es-es/get-started/

Mishra, S. K., Sahoo, B., & Parida, P. P. (2020). Load balancing in cloud computing: A big picture. In *Journal of King Saud University - Computer and Information Sciences* (Vol. 32, Issue 2, pp. 149–158). King Saud bin Abdulaziz University. https://doi.org/10.1016/j.jksuci.2018.01.003

Morán-González, M., & Gallegos-Macías, M. R. (2021). Plataformas tecnológicas y su aporte al aprendizaje en línea para la asignatura de matemática. *REVISTA CIENTÍFICA MULTIDISCIPLINARIA ARBITRADA “YACHASUN,” 5*(9 Edición especial

octubre), 119–139. https://doi.org/10.46296/yc.v5i9edespsoct.0115

Olivo García, E., Romero González, R. M., & Olivo Flores, M. A. (2022). Análisis para migración de entornos presenciales a entornos virtuales en educación superior. *EDU REVIEW. International Education and Learning Review / Revista Internacional de Educación y Aprendizaje*, *10*(2), 123–135. https://doi.org/10.37467/gkarevedu.v10.3126

Penna, A. F., Sánchez, I. C., & Delgado, D. D. (2019). Análisis comparativo de las plataformas tecnológicas para el estudio de posgrados en línea en México. *Revista EDaPECI*, *19*(2), 40–51. https://doi.org/10.29276/redapeci.2019.19.211316.40-51

Perafan, H., Guia, N., Rey, D., & Duarte, D. (2018). Diseño de un Cluster de Alta Disponibilidad para un Entorno Educativo Virtual Universitario. *Revista Ingenieria UC*, *25*(1), 108–116. https://www.redalyc.org/articulo.oa?id=70757668014

Ramos Martín, M. J., Ramos Martín, A., & Montero Rodríguez, F. (2006). *Sistemas gestores de bases de datos*. McGraw-Hill, Interamericana de España.

Recalde, H., Baldeón, P., Albuja, P., & Toasa, R. (2022). Integración Moodle con Sistemas de Gestión Académica en las IES, caso de estudio Tecnológica Universidad Israel. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *55*, 77–85.

Wagner, M. N., Kupriyanova, M., Ovezova, U., & Ilina, A. (2021). Distance Learning Courses: New Opportunities for the Development of University Education. *Propósitos y Representaciones*, *9*(SPE3). https://doi.org/10.20511/pyr2021.v9nspe3.1275

ANEXOS

PLAN DE SEGURIDAD INFORMÁTICA

PROPUESTA 2023

ALVARADO GUZMAN

Contenido

PLAN DE SEGURIDAD INFORMÁTICA 1

1. INTRODUCCIÓN 1

2. OBJETIVOS DEL PLAN 2

2.1 Objetivo General 2

2.2 Objetivo General 2

3. JUSTIFICACIÓN 3

4. ALCANCE Y DELIMITACIÓN DEL PLAN 4

5. DISPOSICIONES DE SEGURIDAD 5

5.1 SEGURIDAD FÍSICA 5

5.2 SEGURIDAD LÓGICA 5

6. Gestión de Accesos de Usuarios en la EPUNEMI 8

7. Gestión de Credenciales de Usuario de la EPUNEMI 9

8. CONTROL DE ACCESO A LA INFORMACIÓN 10

8.1 Programas de Control 10

8.2 Contraseñas 10

8.3 Niveles de Acceso 10

9. ANTIVIRUS 12

9.1 Funcionalidades Clave del Sistema Antivirus 12

9.2 Estrategias de Implementación y Mantenimiento 12

10. DISPOSICIÓN DE RESCATE Y CONTINGENCIA 13

10.1 Identificación de Requisitos Operativos Mínimos 13

10.2 Elaboración de Planes de Contingencia 13

10.3 Herramientas de Continuidad del Negocio 13

10.4 Monitoreo y Revisión del Plan de Seguridad Informática 13

10.5 Procedimientos de Respaldos y Restauración 13

10.6 Creación de Imágenes de Servidores 13

10.7 Gestión de Hardware de Servidores 13

10.8 Sincronización de Sistema 14

10.9 Gestión de Activos Críticos 14

10.10 Socialización y Capacitación 14

11. POLÍTICAS DE SEGURIDAD 15

11.1 Política de Acceso 15

11.2 Política de Contraseñas 15

11.3 Política de Gestión de Incidentes 15

11.4 Política de Copias de Seguridad..... 16
11.5 Política de Seguridad Física 16
11.6 Política de Seguridad en la Red 17
11.7 Política de Actualizaciones y Parches 17
11.8 Política de Capacitación y Concienciación 17
11.9 Política de Auditoría y Cumplimiento 18
11.10 Política de Eliminación de Datos 18

PLAN DE SEGURIDAD INFORMÁTICA

1. INTRODUCCIÓN

Empresa Pública de Producción y Desarrollo Estratégico de la Universidad Estatal de Milagro (EPUNEMI), es una institución comprometida con la excelencia en la educación continua, brindando a los estudiantes la oportunidad de avanzar en sus carreras en una variedad de campos especializados.

Dentro de la Dirección de Tecnología de la Información, un equipo especializado está dedicado a la operatividad constante de nuestros sistemas de información y a la prestación de servicios tecnológicos avanzados. Estas herramientas son esenciales no solo para las operaciones diarias sino también para respaldar los objetivos estratégicos de EPUNEMI.

Para asegurar un servicio ininterrumpido y eficiente, es imperativo que desde nuestra dirección tecnológica nos enfoquemos en un proceso de mejora continua.

El mantenimiento de la integridad, disponibilidad y confidencialidad de la información es un pilar en EPUNEMI. A través de la implementación de nuestro Plan de Seguridad Informática (PSI), nos proponemos elevar la gestión de nuestros recursos digitales a niveles óptimos de eficiencia y efectividad.

Además, en la intersección de la tecnología y la pedagogía, nuestros esfuerzos están alineados con el cumplimiento de la normativa aplicable. Este compromiso nos asegura cumplir con los estándares y requerimientos legales, manteniendo nuestra misión educativa al más alto nivel y acorde con las directrices estatales y educativas.

2. OBJETIVOS DEL PLAN

2.1 Objetivo General

Planificar una estrategia integral de seguridad de la información que consolide la alta disponibilidad, confidencialidad e integridad de los datos y activos informáticos en EPUNEMI.

2.2 Objetivo General

Formular un marco de seguridad de la información que se adecúe a las especificidades del Sistema de Información de EPUNEMI, protegiendo contra amenazas y adaptándose a evoluciones tecnológicas.

Instaurar un mecanismo de control de acceso robusto para los activos informativos de EPUNEMI, restringiendo el acceso a información sensible y asegurando la autenticación de usuarios.

Alinear las políticas de gestión y administración de activos informativos de EPUNEMI con la normatividad nacional vigente, garantizando la legalidad y la adecuación regulatoria.

Establecer un conjunto de procedimientos y responsabilidades claras para la seguridad de la información en EPUNEMI, fomentando una cultura de protección de datos.

Proyectar la ejecución del Plan de Seguridad Informática, detallando las actividades, recursos necesarios y documentación asociada, para una implementación efectiva y medible.

3. JUSTIFICACIÓN

La seguridad de la información constituye un eje crítico para EPUNEMI, donde datos precisos y accesibles son indispensables para su misión educativa. En un mundo donde las amenazas cibernéticas evolucionan rápidamente, es vital asegurar la protección de nuestra información contra accesos no autorizados y corrupción de datos.

La interdependencia tecnológica de las instituciones modernas conlleva riesgos inherentes que deben ser mitigados para mantener la confianza y la continuidad operativa. El incremento en la sofisticación de los ataques cibernéticos exige una actualización y fortalecimiento constantes de nuestras políticas y protocolos de seguridad.

El Plan de Seguridad Informática de EPUNEMI busca establecer un marco de actuación robusto, alineado con las directrices nacionales y mejores prácticas internacionales, reforzando así nuestra reputación y competitividad en el ámbito educativo.

Este plan no solo beneficiará a la dirección de EPUNEMI al proveer información segura para la toma de decisiones estratégicas, sino que también resguardará a los usuarios de nuestra plataforma, asegurando la eficiencia y seguridad en el manejo de la información, tanto interna como externa.

La implementación de este plan es un paso esencial para consolidar la confiabilidad y eficacia de nuestros sistemas informativos, garantizando una gestión de información segura y sostenible.

4. ALCANCE Y DELIMITACIÓN DEL PLAN

Este Plan de Seguridad Informática abarca la salvaguarda integral de los activos de información y la infraestructura tecnológica que soporta la plataforma educativa de EPUNEMI, incluyendo el resguardo contra amenazas internas y externas y la prevención de incidentes de seguridad que puedan afectar la continuidad de las operaciones académicas y administrativas.

La ejecución del plan se extenderá hasta el cierre del año académico actual, periodo durante el cual se efectuarán evaluaciones periódicas para su posible actualización, atendiendo a las nuevas regulaciones o cambios organizativos que puedan surgir.

La puesta en marcha de este plan será dirigida por el equipo de Tecnologías de la Información y Comunicaciones, con el apoyo y compromiso de todo el personal académico y administrativo de EPUNEMI, asegurando que la implementación y adherencia a las políticas de seguridad sean aplicadas de manera transversal en la organización.

5. DISPOSICIONES DE SEGURIDAD

Las disposiciones relacionadas a continuación, tendrán aplicabilidad al Inventario de Activos de Información de la Corporación, el cual deberá clasificar los activos a los que se les debe brindar mayor protección, identificando claramente sus características y rol al interior de un proceso.

Las actividades a realizar para obtener el inventario de activos son:

- Definición
- Revisión
- Actualización
- Publicación

5.1 SEGURIDAD FÍSICA

La seguridad física se relaciona con el establecimiento de barreras defensivas y la adopción de protocolos controlados con el objetivo de salvaguardar recursos e información delicada. Dicha seguridad abarca tanto las medidas *in situ* que protegen infraestructura de cómputo y medios de almacenamiento, como los procedimientos para controlar el acceso a distancia a dichos recursos. Estas prácticas son clave para prevenir daños o pérdidas causadas por diversos riesgos.

Entre las principales amenazas que la seguridad física busca mitigar, se incluyen:

- Eventualidades ambientales como incendios, tormentas severas o inundaciones.
- Acciones perjudiciales originadas por individuos.
- Actos de agitación social, así como sabotajes intencionales tanto internos como externos.

5.2 SEGURIDAD LÓGICA

La seguridad lógica se refiere a las medidas que aseguran que solo las personas con autorización puedan acceder a los datos. Esta forma de seguridad implementa la norma de que, si un acto no está explícitamente autorizado, entonces debe estar

prohibido. Los controles de seguridad lógica incluyen limitaciones en el acceso a programas y archivos para que los operadores no necesiten supervisión exhaustiva y no puedan realizar cambios indebidos.

Además, estos controles verifican que los datos se usen correctamente, que la comunicación de información sea segura y dirigida únicamente al destinatario correcto, y que la información no sea alterada durante la transmisión.

Para fortalecer la seguridad, se utilizan métodos como la identificación y autenticación de usuarios, la asignación de roles específicos, restricciones en servicios, controles de acceso tanto internos como externos y administración de dichos accesos en base a factores como la ubicación y el horario. También es crucial establecer procedimientos para acceder a las copias de seguridad de equipos y servidores, asegurando así la integridad de los datos.

Control de Acceso

Para reforzar la seguridad y mitigar riesgos asociados con la pérdida de activos y la exposición indebida de información confidencial, se aplicarán las siguientes medidas en las áreas críticas:

- **Área de Sistemas**

El acceso a esta área se limitará estrictamente al personal con autorización. Excepciones se aplicarán solo cuando la operación lo requiera y sea necesario el apoyo de personal externo.

La entrada al área de sistemas estará protegida por un sistema de seguridad magnético con panel digital. Los códigos de acceso se actualizarán con cada cambio de personal.

- **Cuarto de Redes y Servidores**

El acceso se restringirá a todas las personas no autorizadas. Este espacio se mantendrá seguro en todo momento, salvo cuando esté ocupado por personal autorizado en funciones.

Las llaves de acceso a este cuarto estarán bajo custodia en un lugar seguro, conocido

únicamente por los responsables designados.

- **Acceso a Bases de Datos**

Las credenciales serán de uso exclusivo del administrador de bases de datos y servidores. Se podrán otorgar accesos limitados al equipo de soporte de software o desarrollo cuando proceda, según criterios definidos.

Estas medidas de seguridad están diseñadas para alinearse con los estándares y políticas de la institución, garantizando así la integridad y la continuidad de las operaciones tecnológicas.

- **Acceso a los servidores**

La conexión a los servidores se realizará únicamente a través de conexiones *ssh* dentro de la Red Local (LAN), garantizando que estas conexiones sean administradas directamente por el administrador de bases de datos y servidores. Se podrán conceder accesos restringidos al equipo de soporte técnico o al departamento de desarrollo, bajo determinadas condiciones y necesidades operativas.

Se implementarán medidas adicionales de seguridad que incluyen la autenticación mediante credenciales específicas, la filtración por dirección IP y MAC, así como la obligatoriedad de utilizar conexiones VPN establecidas a través del firewall para cualquier acceso remoto. Esto se hace con el propósito de reforzar la seguridad y proteger la integridad de los datos frente a posibles amenazas o vulnerabilidades.

Se efectuarán regularmente simulacros de ataque, tanto de origen interno como externo, para evaluar la robustez de las medidas de protección de datos. Dichos test serán organizados por el Administrador de Servidores y se llevarán a cabo al menos una vez cada año, comenzando a contar desde la fecha en que se ponga en marcha este plan de seguridad.

6. Gestión de Accesos de Usuarios en la EPUNEMI

Se considera usuario de la EPUNEMI a los miembros de la plantilla fija y todo aquel que tenga un contrato en vigencia, así como a cualquier individuo que haga uso de los recursos, aplicaciones y servicios que provee la EPUNEMI.

La administración de las cuentas de usuario de los dispositivos estará centralizada en el equipo de sistemas de la EPUNEMI. Estas cuentas contarán con una contraseña estándar que será cambiada según se requiera o, como mínimo, dos veces al año.

El equipo de Sistemas de la EPUNEMI tendrá la tarea exclusiva de crear cuentas de usuario para el dominio, el correo electrónico y el acceso a las diferentes aplicaciones institucionales. Estas cuentas se concederán únicamente a quienes presenten documentación oficial que confirme su relación laboral como empleados o contratistas de la EPUNEMI.

El nombre de usuario se generará utilizando la inicial del primer nombre seguido del primer apellido y la inicial del segundo apellido. En casos de duplicidad. Por ejemplo, para Juan Luis Castro Monsalvo, el nombre de usuario sería *jcastrom*, con todos los nombres de usuario en minúsculas. En caso de existir uno repetido existirá una secuencia numérica.

Los usuarios deberán establecer una contraseña en el momento de crear su cuenta. Esta deberá tener un mínimo de ocho caracteres alfanuméricos y se les aconsejará no emplear contraseñas que se relacionen con datos personales predecibles, como fechas de nacimiento o eventos personales significativos.

7. Gestión de Credenciales de Usuario de la EPUNEMI

Para una seguridad óptima, las contraseñas de los usuarios de la EPUNEMI deben incluir al menos una letra en minúscula, una en mayúscula y un número, garantizando así la complejidad y robustez de la misma.

Los nombres de usuario asignados son personales y no deben compartirse; es responsabilidad exclusiva del titular del usuario proteger y mantener la confidencialidad de sus contraseñas.

El acceso a las aplicaciones de la EPUNEMI requiere credenciales personales que se otorgan tras una solicitud formal a través de la intranet o el soporte de aplicaciones y la aprobación del jefe directo, asignando un perfil específico para cada aplicación.

Las cuentas corporativas deben utilizarse exclusivamente para actividades relacionadas con la EPUNEMI, manteniendo la integridad y la profesionalidad en el uso de los recursos de la institución.

Los usuarios tienen la responsabilidad de hacer un uso adecuado del correo electrónico corporativo, asegurando no compartir sus credenciales (usuario y contraseña), ya que no se les solicitarán bajo ninguna circunstancia. Asimismo, deben estar atentos y evitar ser víctimas de técnicas de ingeniería social que buscan la distribución de malware y spam. Ante cualquier correo sospechoso o actividad inusual, es imperativo reportarlo al equipo de sistemas para su análisis y la toma de medidas preventivas correspondientes.

8. CONTROL DE ACCESO A LA INFORMACIÓN

Es crucial mantener la seguridad de los sistemas y bases de datos para prevenir el acceso no autorizado a información confidencial. Para ello, se implementan varias estrategias:

8.1 Programas de Control

Se utilizan programas específicos para administrar y monitorear los derechos de acceso de los usuarios. Estos programas pueden delegar ciertos privilegios, actuando como filtros de información. Un ejemplo inicial de un programa de control es el Antivirus utilizado en la red de la organización.

8.2 Contraseñas

Se requiere que los usuarios introduzcan una contraseña única antes de que puedan realizar cualquier proceso en el sistema. Esto sirve como una barrera inicial para proteger los programas y los datos de intentos de acceso no autorizados.

8.3 Niveles de Acceso

Establecer diferentes niveles de acceso garantiza que los usuarios autorizados solo puedan acceder a la información y las funciones del sistema que están permitidas según su rol, lo que puede incluir permisos de solo lectura o la capacidad de realizar cambios en la información.

Los niveles de acceso a la información se pueden clasificar de la siguiente manera:

- **Consulta de Información No Restringida:** Permite a los usuarios leer datos públicos o no confidenciales sin la capacidad de modificarlos. Cualquier usuario con conocimiento básico del sistema puede acceder a este nivel.
- **Mantenimiento de Información No Restringida:** Concede permisos para agregar nuevos datos sin alterar los existentes.
- **Consulta de Información Restringida:** Otorga acceso para leer información sensible o confidencial, manteniendo la restricción de no modificar los datos.

Mantenimiento de Información Restringida: Incluye varios privilegios como:

- **Ingreso:** Introducir nuevos datos sin cambiar los ya presentes.
- **Actualización:** Modificar datos existentes sin eliminarlos.
- **Borrado:** Eliminar datos del sistema.

La asignación de estos permisos puede ser total, parcial o nula, dependiendo del rol del usuario. Además, la capacidad de alterar el esquema de la base de datos está generalmente reservada para el administrador de bases de datos y servidores, debido a la naturaleza crítica de esta función.

9. ANTIVIRUS

Se destaca la implementación y gestión de un sistema antivirus robusto y eficiente. Este sistema es crucial para proteger nuestra infraestructura de TI de una amplia gama de amenazas digitales, incluyendo virus, gusanos, troyanos, Ransomware y otros tipos de malware.

9.1 Funcionalidades Clave del Sistema Antivirus

- Detección y Eliminación Proactiva de Malware: Capacidad para identificar y eliminar eficazmente una variedad de malware, con actualizaciones automáticas que garantizan una protección continua contra las últimas amenazas.
- Monitoreo Continuo: Vigilancia constante de los sistemas para detectar y responder inmediatamente a cualquier actividad sospechosa o maliciosa.
- Análisis Avanzado: Utilización de técnicas de análisis heurístico y comportamental para identificar malware basado en patrones de comportamiento.
- Integración y Compatibilidad: El antivirus deberá integrarse sin problemas con otras herramientas de seguridad y ser compatible con los sistemas operativos y plataformas de la institución.
- Gestión y Control Centralizado: Una interfaz de administración intuitiva y fácil de usar, que permite una gestión eficiente y configuración personalizable del antivirus.

9.2 Estrategias de Implementación y Mantenimiento

La implementación será realizada por nuestro equipo de TI, asegurando una instalación adecuada y una cobertura completa en todos los dispositivos y servidores.

Se llevarán a cabo evaluaciones periódicas para verificar la efectividad del antivirus y realizar ajustes si es necesario.

El personal de TI recibirá capacitación continua sobre las funcionalidades y el mantenimiento del sistema antivirus para garantizar su eficacia a largo plazo.

10. DISPOSICIÓN DE RESCATE Y CONTINGENCIA

10.1 Identificación de Requisitos Operativos Mínimos

Evaluar y definir los recursos críticos necesarios para mantener las operaciones durante incidentes de contingencia.

10.2 Elaboración de Planes de Contingencia

Formular planes de contingencia en alineación con las políticas de administración de servidores y respaldo de datos.

Asegurar la consistencia con el Procedimiento de Administración de Servidores y la estrategia global de Tecnologías de Información.

10.3 Herramientas de Continuidad del Negocio

Seleccionar o desarrollar soluciones que soporten la continuidad de las operaciones.

Verificar la eficacia del plan mediante pruebas programadas.

10.4 Monitoreo y Revisión del Plan de Seguridad Informática

Mantener un control riguroso del plan de seguridad, ajustándolo conforme a las prácticas de administración de servidores y gestión de copias de seguridad del PETI.

10.5 Procedimientos de Respaldos y Restauración

Implementar procedimientos estandarizados para la administración y restauración de copias de seguridad.

Diseñar guías detalladas para pruebas de restauración de datos en distintas aplicaciones y plataformas.

10.6 Creación de Imágenes de Servidores

Generar imágenes completas de los sistemas operativos de los servidores para una rápida recuperación ante fallos.

10.7 Gestión de Hardware de Servidores

En caso de fallo de hardware, aislar localmente los servidores afectados, retirar y asegurar los discos de almacenamiento en un lugar protegido.

10.8 Sincronización de Sistema

Verificar la sincronización horaria de todos los sistemas de procesamiento de información regularmente.

10.9 Gestión de Activos Críticos

Identificar y asignar responsables para la gestión de los activos críticos de la Corporación.

10.10 Socialización y Capacitación

Difundir los procedimientos, planes y manuales relacionados con la seguridad informática a todos los usuarios.

Promover buenas prácticas en el uso de los recursos tecnológicos disponibles en la Corporación.

Este conjunto de acciones busca minimizar el impacto de cualquier interrupción no planificada, garantizando la resilencia operativa y la seguridad de la información.

11. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad de la información para la EPUNEMI están diseñadas para preservar la confidencialidad, integridad y disponibilidad de los datos. A continuación, se detallan los puntos clave:

11.1 Política de Acceso

Establecer un control riguroso y efectivo sobre el acceso a los recursos informáticos y datos de EPUNEMI, garantizando que solo el personal autorizado tenga acceso a la información relevante.

- **Autenticación y Autorización:** Implementar un sistema de autenticación multifactor para todos los empleados.
- **Roles y Privilegios:** Definir claramente los roles de usuario y asignar privilegios basados en el principio de mínimo privilegio. Cada rol debe tener acceso solo a los recursos necesarios para realizar sus tareas.
- **Revisión y Auditoría:** Realizar revisiones periódicas de los accesos concedidos, asegurando su adecuación y pertinencia. Las auditorías deben registrarse y conservarse para futuras referencias.

11.2 Política de Contraseñas

Asegurar que todas las cuentas de usuario tengan contraseñas fuertes y seguras para proteger contra accesos no autorizados.

- **Complejidad y Longitud:** Las contraseñas deben tener una longitud mínima de 12 caracteres e incluir una combinación de letras mayúsculas, minúsculas, números y símbolos.
- **Cambio y Vencimiento:** Las contraseñas deben ser cambiadas regularmente, con un plazo máximo de 90 días. No se permite la reutilización de las últimas cinco contraseñas.
- **Almacenamiento y Gestión:** Las contraseñas deben almacenarse en un gestor de contraseñas seguro y cifrado, y no se deben compartir entre usuarios ni almacenarse en formatos inseguros.

11.3 Política de Gestión de Incidentes

Establecer un proceso estructurado para la gestión de incidentes de seguridad, minimizando el impacto y recuperando la normalidad operativa lo más pronto posible.

- **Detección y Reporte:** Implementar sistemas de detección de intrusiones y anomalías. Los incidentes deben ser reportados inmediatamente al equipo de seguridad de EPUNEMI.
- **Respuesta y Resolución:** Contar con un equipo de respuesta a incidentes que actúe según un plan preestablecido, incluyendo la contención, erradicación y recuperación.
- **Post-Incidente:** Realizar un análisis post-incidente para identificar las lecciones aprendidas y mejorar las políticas y procedimientos de seguridad.

11.4 Política de Copias de Seguridad

Garantizar la integridad, disponibilidad y confidencialidad de los datos mediante la realización regular de copias de seguridad.

- **Frecuencia y Almacenamiento:** Realizar copias de seguridad diarias de los datos críticos y semanales del resto de los datos. Almacenar las copias de seguridad en ubicaciones físicamente seguras y en la nube.
- **Pruebas de Restauración:** Realizar pruebas de restauración periódicas para asegurar la eficacia y rapidez de la recuperación de datos.
- **Seguridad y Cifrado:** Proteger las copias de seguridad con cifrado fuerte y garantizar que solo el personal autorizado tenga acceso a ellas.

11.5 Política de Seguridad Física

Proteger las instalaciones físicas y el hardware de EPUNEMI contra accesos no autorizados, daños y otras amenazas físicas.

- **Control de Acceso:** Implementar sistemas de control de acceso físico, como tarjetas de acceso y sistemas biométricos, para restringir la entrada a zonas críticas.
- **Monitoreo y Vigilancia:** Usar cámaras de seguridad y sistemas de alarma para monitorear las instalaciones las 24 horas del día.

- **Protección contra Desastres:** Establecer medidas para proteger contra incendios, inundaciones y otros desastres naturales, incluyendo sistemas de supresión de incendios y planes de contingencia.

11.6 Política de Seguridad en la Red

Garantizar la seguridad de la red de EPUNEMI mediante la implementación de medidas para prevenir, detectar y responder a amenazas cibernéticas.

- **Firewalls y Sistemas de Prevención de Intrusiones:** Utilizar firewalls y sistemas de prevención de intrusiones para filtrar el tráfico no deseado y detectar actividades sospechosas.
- **Segmentación de la Red:** Dividir la red en segmentos para controlar el acceso y reducir el alcance de posibles intrusiones.
- **Monitoreo de Red:** Realizar un monitoreo constante de la red para detectar y responder rápidamente a cualquier actividad anómala.

11.7 Política de Actualizaciones y Parches

Mantener los sistemas y aplicaciones de EPUNEMI actualizados para protegerse contra vulnerabilidades conocidas.

- **Programa de Actualizaciones:** Establecer un programa regular para revisar y aplicar actualizaciones y parches de seguridad.
- **Pruebas de Parches:** Probar los parches en un entorno controlado antes de su implementación para evitar interrupciones.
- **Gestión de Vulnerabilidades:** Realizar evaluaciones periódicas de vulnerabilidades para identificar y mitigar riesgos potenciales.

11.8 Política de Capacitación y Concienciación

Asegurar que todos los empleados de EPUNEMI estén informados y educados sobre las mejores prácticas de seguridad informática.

- **Programas de Formación:** Implementar programas de formación y concienciación en seguridad informática para todos los empleados.

- **Actualizaciones Regulares:** Proporcionar actualizaciones periódicas y materiales de formación sobre amenazas emergentes y nuevas políticas.
- **Evaluaciones y Simulacros:** Realizar evaluaciones periódicas y simulacros de phishing para medir la eficacia de la capacitación.

11.9 Política de Auditoría y Cumplimiento

Asegurar el cumplimiento de las políticas y procedimientos de seguridad informática mediante auditorías regulares y un seguimiento exhaustivo.

- **Auditorías Internas y Externas:** Realizar auditorías internas periódicas y contratar auditorías externas para evaluar la eficacia de las políticas de seguridad.
- **Informe de Cumplimiento:** Generar informes periódicos de cumplimiento para la alta dirección, detallando el estado de las medidas de seguridad y cualquier área de mejora.
- **Gestión de Incumplimientos:** Establecer procedimientos claros para abordar y corregir cualquier incumplimiento de las políticas.

11.10 Política de Eliminación de Datos

Garantizar que los datos sensibles y confidenciales de EPUNEMI se eliminen de forma segura y eficaz cuando ya no sea necesarios.

- **Métodos de Eliminación:** Utilizar métodos de eliminación de datos seguros y certificados, como el borrado seguro o la destrucción física de dispositivos de almacenamiento.
- **Registro y Verificación:** Mantener un registro detallado de la eliminación de datos y realizar verificaciones periódicas para asegurar que se ha realizado correctamente.
- **Política de Retención de Datos:** Definir claramente las políticas de retención de datos para determinar cuándo y cómo deben eliminarse los datos.