UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN.

Tema:

APLICACIÓN DE UNA METODOLOGÍA DE CONTINUIDAD DE NEGOCIO PARA MEJORAR LA SEGURIDAD EN LA IMPLEMENTACIÓN DE UNA PLATAFORMA VIRTUAL MOODLE EN LA UNIDAD EDUCATIVA EMANUEL

Trabajo de Integración Curricular Modalidad: Proyecto de Investigación, presentado previo a la obtención del Título de Ingeniería en Tecnologías de la Información

ÁREA: Tecnologías de la Información

LÍNEA DE INVESTIGACIÓN: Ingeniería de Software

AUTOR: Monserrath Estefanía Acuña Ramos

TUTOR: Ing. David Omar Guevara Aulestia

Ambato – Ecuador

Septiembre - 2022

APROBACION DEL TUTOR

En calidad de tutor del Trabajo de Integración Curricular con el tema: APLICACIÓN DE UNA METODOLOGÍA DE CONTINUIDAD DE NEGOCIO PARA MEJORAR LA SEGURIDAD EN LA IMPLEMENTACIÓN DE UNA PLATAFORMA VIRTUAL MOODLE EN LA UNIDAD EDUCATIVA EMANUEL, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Monserrath Estefanía Acuña Ramos, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 17 del Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado en la Universidad Técnica de Ambato y sus reformas y el numeral 7.4 del respectivo instructivo.

Ambato, septiembre 2022

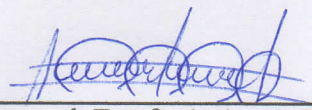
Firmado electrónicamente por:
DAVID OMAR GUEVARA AULESTIA

Ing. David Omar Guevara Aulestia
TUTOR

AUTORÍA

El presente trabajo de Integración Curricular titulado: APLICACIÓN DE UNA METODOLOGÍA DE CONTINUIDAD DE NEGOCIO PARA MEJORAR LA SEGURIDAD EN LA IMPLEMENTACIÓN DE UNA PLATAFORMA VIRTUAL MOODLE EN LA UNIDAD EDUCATIVA EMANUEL, es absolutamente original, auténtico y personal. En virtual, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, septiembre 2022



Monserrath Estefanía Acuña Ramos
CC: 1804366373
AUTORA

APROBACIÓN DEL TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Integración Curricular presentado por la señorita Monserrath Estefanía Acuña Ramos, estudiante de la Carrera de Tecnologías de la Información, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado APLICACIÓN DE UNA METODOLOGÍA DE CONTINUIDAD DE NEGOCIO PARA MEJORAR LA SEGURIDAD EN LA IMPLEMENTACIÓN DE UNA PLATAFORMA VIRTUAL MOODLE EN LA UNIDAD EDUCATIVA EMANUEL, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 19 del Reglamento para la ejecución de la Unidad de Integración Curricular y la obtención del título de tercer nivel, de grado de la Universidad Técnica de Ambato y sus reformas y al numeral 7.6 del respectivo instructivo. Para cuya constancia subscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, septiembre 2022

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
FRANKLIN OSWALDO MAYORGA MAYORGA

Ing. Franklin Mayorga
PROFESOR CALIFICADOR

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Balarezo
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Integración Curricular como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Integración Curricular en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, septiembre 2022

Monserrath Estefanía Acuña Ramos
CC: 1804366373
AUTORA

DEDICATORIA

El presente trabajo investigativo se lo dedico a Dios por darme sabiduría en la trayectoria de mi carrera, a mi madre, padre y hermanos por ser los pilares fundamentales para llegar a alcanzar mis objetivos.

A mis amigos y docentes por el apoyo incondicional que me han brindado durante este proceso de formación profesional.

AGRADECIMIENTO

Agradezco a Dios por darme salud y guiar mi camino en esta trayectoria, a mi madre, padre, hermanos, docentes y amigos por brindarme su apoyo incondicional en el transcurso de mi formación profesional.

A las autoridades de la Unidad Educativa Emanuel, quienes me brindaron la oportunidad de realizar mi proyecto de investigación.

A mi tutor de tesis Ing. David Guevara por la orientación y guía que me brindo en la elaboración del presente trabajo investigativo.

INDICE DE CONTENIDOS

INDICE DE TABLAS

INDICE DE GRÁFICOS

RESUMEN EJECUTIVO

Actualmente las instituciones deben estar preparadas para reaccionar ante eventos inesperados que afecten sus operaciones y su imagen, es importante tener un correcto manejo de riesgos y una visión clara de las actividades a realizar para recuperar las operaciones ante posibles amenazas, por lo tanto, es indispensable contar con un plan que garantice que los procesos continúen después de un desastre.

El presente trabajo tiene como objetivo aplicar una metodología de continuidad de negocio (BCM) para mejorar la seguridad en la instalación de una plataforma virtual, BCM describe la preparación y recuperación de la plataforma ante contingencias, también se recopila información de la situación actual de la institución educativa, identifica activos y procesos críticos, realiza un análisis de impacto de negocio (BIA) y analiza los riesgos para identificar amenazas y vulnerabilidades, además define estrategias de recuperación que brindan la capacidad de resistencia frente a eventos inesperados.

En la implementación de la plataforma virtual se aplica técnicas de hardening para reforzar al máximo la seguridad y reducir las vulnerabilidades que pueden ser provocadas por una falta de control.

Palabras clave: Plan de continuidad de negocio, análisis de impacto de negocio, estrategias de recuperación, hardening.

ABSTRACT

Currently, institutions must be prepared to react to unexpected events that affect their operations and their image, it is important to have a correct risk management and a clear vision of the activities to be carried out to recover operations from possible threats, therefore, it is essential to have a plan that guarantees that the processes continue after a disaster.

The present work aims to apply a methodology of business continuity (BCM) to improve safety in the installation of a virtual platform, BCM describes the preparation and recovery of the platform against the contingencies, information is also collected from the current situation of the educational institution, identifies assets and critical processes, performs an analysis of the impact of business (BIA) and risk analysis to identify threats and vulnerabilities, as well as defined recovery strategies that provide the ability of resistance in the face of unexpected events.

In the implementation of the virtual platform, hardening techniques are applied to maximize security and reduce vulnerabilities that can be caused by a lack of control.

Keywords: Business continuity plan, business impact analysis, recovery strategies, hardening.

CAPITULO I.- MARCO TEORICO

1.1. Tema de Investigación

APLICACIÓN DE UNA METODOLOGÍA DE CONTINUIDAD DE NEGOCIO PARA MEJORAR LA SEGURIDAD EN LA IMPLEMENTACIÓN DE UNA PLATAFORMA VIRTUAL MOODLE EN LA UNIDAD EDUCATIVA EMANUEL.

1.1.1. Planteamiento del Problema

Actualmente, se vive el fenómeno de la globalización a nivel mundial, con el uso generalizado de las tecnologías de la información y la comunicación, que ha repercutido en las actividades diarias y en el seguimiento de una sociedad en la red [1], por lo que es imprescindible que los cambios estructurales de las políticas de educación también, analicen y utilicen los nuevos modelos de educación a distancia para cambiar la forma de capacitar a los docentes y estudiantes creando un nuevo perfil de enseñanza-aprendizaje para elevar su formación académica.

En Ecuador las Tecnologías de la Información y Comunicación (TIC) ha supuesto un gran avance en cuanto al acceso de la información mediante el uso del internet, sobre todo en el ámbito educativo, donde se experimentan nuevos escenarios formativos que apuestan al intercambio de conocimiento inmediato entre docentes y estudiantes, permitiendo que se construya nuevos aprendizajes en forma colaborativa, reflexiva y crítica, en un ambiente amigable, flexible, dinámico, pluripersonal y pluridimensional [2].

En Ambato, en la Unidad Educativa Emanuel se ha podido determinar dificultades en el momento de almacenar la información de los estudiantes debido a que no posee una metodología de continuidad de negocio para mitigar las fallas de seguridad y de esta manera no se puede hacer el análisis, detección y tratamiento de vulnerabilidades de seguridad, periódicamente para prevenir ataques en los puntos más débiles de la institución.

1.2. Antecedentes Investigativos

Revisando la investigación bibliográfica en algunas universidades se han encontrado trabajos que servirán como apoyo en el trabajo investigativo:

En el trabajo de investigación de Klever Patricio Morales Guamán [3] con el tema "Metodologías de evaluación de riesgos Moodle PUCE Ambato" realizado en la Pontificia Universidad Católica del Ecuador en el año 2020 se pudo determinar que:

- Se valida, la factibilidad de aplicación, así como, la eficiencia de la metodología de evaluación de riesgos, misma que arrojo tener un nivel de riesgo bajo, los valores críticos de las oportunidades y amenazas obtenidas del cruce de los criterios realizados de la mejora continua con la metodología, misma que optimiza los recursos de la plataforma Moodle.
- La adopción de la metodología para evaluar los riesgos, motivo de la investigación, mantener un seguimiento documentado, y que, a través de la capacitación y el mantenimiento de la metodología se mantenga vigente y actualizada.

En el trabajo de investigación de José Oswaldo Mendoza García [4] con el tema "Diseño e implementación de un Aula Virtual del Moodle, para fortalecer el proceso de enseñanza aprendizaje en la Unidad Educativa Pablo Hannibal Vela de la ciudad de Portoviejo" en el año 2017 se pudo determinar que:

- Las características de Moodle como plataforma de aprendizaje virtual, se ajustan de tal forma que potencian el aprendizaje de los estudiantes en una forma interactiva, convirtiéndose de este modo en un canal de retroalimentación significativa, motivando la búsqueda de contenidos, independientes de donde se encuentre físicamente el estudiante.

En el trabajo de investigación de Ada Herrera, Laura Ocaña Jackelin Palomino e Iván Zamora [5] con el tema "Plan de negocio para la implementación de una plataforma virtual de clases académicas particulares" realizada en la Universidad ESAN de Lima en el año 2018 donde se pudo determinar que:

- Para el desarrollo de la presente tesis se ha seguido una metodología que comprende el estudio de mercado, determinación del modelo de negocio, diseño de las estrategias y análisis de la viabilidad del negocio considerando los flujos proyectados de ingresos y costos en un horizonte de diez años.
- Se propone una idea de negocio innovadora y escalable para la enseñanza personalizada, convirtiendo a los distractores tecnológicos tales como tablets, laptops, desktop y celulares en herramientas de enseñanza. Es así como se diseña el modelo de una plataforma virtual segura y monitoreada.

1.3. Fundamentación teórica

1.3.1. Plan de Continuidad de Negocio (BCP)

El plan de continuidad es un conjunto de actividades preventivas para minimizar los riesgos en caso de algún desastre de origen natural o humano , manteniendo la operatividad de las actividades a un mínimo nivel hasta recuperar la totalidad de los sistemas y recursos; este, se encuentra conformado por tres acciones fundamentales que son: prevención (acciones para prevenir efectos) , detección (acciones durante o después del desastre)y recuperación (restauración de los equipos y actividades) [6].

Los principales beneficios que brinda un plan de continuidad de negocio son los siguientes:

- Identificación de procesos crítico de la empresa.
- Definición de un cronograma de recuperación.
- Prevención y minimización de pérdidas financieras.
- Clasificación de activos de la empresa otorgando prioridad a su protección.
- Es aplicable a empresas de cualquier tamaño.

Gestión de la continuidad del negocio

La GCN busca sostener en niveles previamente definidos y aceptados, los productos y servicios críticos del negocio a través de la estructuración de procedimientos, tecnología e información, los cuales desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre, con el fin de proteger los intereses de las partes interesadas, la reputación, los activos críticos y otros aspectos generadores de valor [7].

La GCN está principalmente relacionada con las siguientes actividades:

- Identificar productos y servicios críticos.
- Priorizar actividades y recursos.
- Evaluar riesgos de continuidad.
- Contar con procedimientos de recuperación.
- Verificar la efectividad de los procedimientos.

1.3.2. Gestión de Continuidad del Negocio (BCM)

La Gestión de Continuidad de Negocio, más conocida por BCM (Business Continuity Management) es difícil de definir ya que incluye elementos de planificación, valoración de riesgo, respuesta a emergencias, gestión de crisis y recuperación de negocio. El Business Continuity Institute la define del modo siguiente: *"*BCM consiste en la actuación que permite anticipar incidentes que pueden afectar a las funciones y procesos claves para la organización y que asegura una respuesta a dichos incidentes de forma planeada y ensayada [8].

El BCM define el modo más efectivo de abordar las repercusiones inmediatas de un acontecimiento, para alcanzar la operación normal lo más rápidamente posible. No se trata de seguir lo que se dice en unas plantillas, sino de conocer la respuesta específica que requiere una organización dinámica, lo cual supone a menudo delegar autoridad y controlar las interferencias internas [8].

1.3.3. Plataforma Virtual Moodle LMS

La plataforma Moodle es un sistema de enseñanza diseñado para crear y gestionar espacios de aprendizaje online adaptados a las necesidades de profesores, estudiantes y administradores, sirve para crear espacios de enseñanza online y administrar, distribuir y controlar todas las actividades de formación no presencial de una entidad educativa u organización [9].

El carácter gratuito y abierto de Moodle lo convierten en una herramienta muy atractiva, que además cuenta con muchas más ventajas:

- Herramienta estable y de confianza

Todo tipo de organizaciones de todos los tamaños confían en ella para desarrollar sus proyectos de formación online.

- Intuitiva y fácil de usar

Aprender a gestionarla y utilizarla es muy sencillo. El panel de usuario tiene una interfaz simple, características de arrastrar y soltar, y recursos bien documentados.

- Siempre actualizada

Moodle es continuamente revisado y mejorado para adaptarse a las necesidades de los usuarios a lo largo del tiempo. En su desarrollo están implicados miles de usuarios de todo el mundo que se organizan en torno a comunidades online.

- Flexible y personalizable

Al ser un software de código abierto, Moodle puede ser personalizarse y adaptarse a las necesidades individuales gracias a su estructura de funcionamiento modular.

- Escalable a cualquier tamaño

Es una plataforma que puede dar servicio desde unos cuantos estudiantes a miles de ellos, tanto en organizaciones pequeñas como en grandes.

- Ubicua y accesible desde cualquier dispositivo

El acceso a Moodle se realiza desde la web, por lo que puede accederse a él desde cualquier lugar del mundo, en cualquier momento y desde cualquier dispositivo. Su interfaz es compatible con móviles y todos los navegadores de internet.

- Robusta, segura y privada

Los desarrolladores de Moodle están comprometidos con la seguridad de los datos y la privacidad del usuario, por eso los controles de seguridad de la plataforma son actualizados constantemente. Moodle cuenta con sistemas que dan protección frente al acceso no autorizado, la pérdida de datos y el mal uso.

- Con funcionalidades ampliables

Las posibilidades de Moodle son ilimitadas. Sus funcionalidades pueden extenderse gracias a la instalación de plugins y complementos, fruto de la colaboración de una gran comunidad global.

- En tu propio idioma

Moodle está traducido a más de 120 idiomas. Su capacidad multilingüe es otra de sus características más apreciadas.

1.3.4. Técnicas de Endurecimiento (Hardening)

El endurecimiento o hardening son un conjunto de medidas que se toma para reducir los riesgos y vulnerabilidades asociados a sistemas informáticos. El objetivo es reducir la superficie de vulnerabilidad para evitar posibles ataques [10].

El hardening de sistemas trata de encontrar un punto de equilibrio entre la protección y hermetismo y libertad de uso, creando un entorno seguro y cómodo de trabajo donde el usuario pueda realizar sus funciones sin estar bajo amenaza de continuos ataques informáticos [10].

1.3.5. Servicios

Los servicios se encargan de todo lo referente a la estructura de las empresas. Una organización que contrata un servicio informático va a disponer de profesionales que están cualificados para llevar a cabo la asistencia técnica a nivel de hardware y software, sobre la infraestructura IT. Entre las principales funciones que los servicios informáticos realizan se tiene [11] :

- **Pruebas de funcionalidad**: comprenden las tareas de testeo de los distintos softwares de la organización, para garantizar su buen funcionamiento y adaptabilidad a los procesos de la empresa.
- **Implementación y Documentación:** se ayudará a implementar y actualizar todo lo referente de la empresa para tratar de asegurar el crecimiento de la empresa y el aumento de la eficiencia de sus procesos.

1.3.6. Riesgos

Es todo elemento o acción capaz de atentar contra la seguridad de la información. Surgen a partir de la existencia de una vulnerabilidad que puedan ser aprovechada e independientemente de que se comprometa o no la seguridad de un sistema de información [12].

Los riesgos pueden clasificarse en dos tipos:

- Intencionales: en caso de que deliberadamente se intente producir un daño (por ejemplo, el robo de la información, código malicioso).
- No intencionales: en donde se producen acciones que no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo, riesgos relacionados con fenómenos naturales).

1.3.7. Vulnerabilidades

Es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad. Las vulnerabilidades pueden ser de varios tipos, pueden ser de tipo hardware, software, procedimentales o humanas y pueden ser explotadas o utilizadas por intrusos o atacantes [13].

1.3.8. Políticas de seguridad

Las políticas de seguridad consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. Debe estar basada en una identificación y análisis previo de los riesgos a los que está expuesta la información y debe incluir todos los procesos, sistemas y personal de la organización [14].

1.4. Objetivos

1.4.1. Objetivo General

- Establecer una metodología de continuidad de negocio para mejorar la seguridad en la implementación de una plataforma virtual Moodle en la Unidad Educativa Emanuel.

1.4.2. Objetivos Específicos

- Analizar el hardware base, servicios, riesgos y vulnerabilidades que requiere la instalación de una plataforma virtual.
- Determinar una metodología de continuidad del negocio para el mantenimiento y puesta en marcha de la plataforma virtual.
- Implementar la plataforma virtual Moodle aplicando técnicas de endurecimiento y continuidad de negocio para la Unidad Educativa Emanuel.

CAPITULO II.- METODOLOGÍA

2.1. Materiales

Para el desarrollo del presente proyecto se utilizó dos encuestas para docentes (ver Anexo A.1) y personal administrativo y tecnología (ver Anexo A.2) de la Unidad Educativa Emanuel, también se usó una guía de observación, con la finalidad de recolectar información sobre el hardware y riesgos que requiere la instalación de una plataforma virtual.

2.2 Métodos

2.2.1. Modalidad de la Investigación

Investigación de campo

La presente investigación tiene como objeto solventar diversas necesidades educativas por ello se acudió al lugar de los hechos, a la Unidad Educativa Emanuel porque permite estar en contacto directo con el problema, con el propósito de descubrir y explicar sus causas y efectos para la obtención verídica de los datos, para la cual la técnica a aplicarse es la encuesta con su respectivo instrumento como es el cuestionario que está dirigida a los (as), docentes y personal administrativo y tecnología con la finalidad de obtener una información confiable.

Investigación Bibliográfica

Para buscar la mejor forma de sobrellevar la problemática, se vio en la necesidad de ampliar, profundizar y analizar el conocimiento e información en documentos escritos como: libros, revistas, periódicos y otras publicaciones relacionadas con el tema para sustentar el marco teórico de la investigación.

2.2.2. Población y Muestra

En la presente investigación se tomó como objeto de investigación a los docentes y personal administrativo y de tecnología de la Unidad Educativa Emanuel.

Tabla 2.1: Población Docentes

Elaborado por: Monserrath Acuña

POBLACIÓN	FRECUENCIA	PORCENTAJE(%)
Docentes	16	100,00
Total	16	100,00

Tabla 2.2: Población personal Administrativo y Tecnología

Elaborado por: Monserrath Acuña

POBLACIÓN	FRECUENCIA	PORCENTAJE(%)
Personal administrativo y de tecnología	4	100,00
Total	4	100,00

2.2.3. Recolección de Información

La recolección de la información para el desarrollo del presente proyecto se realizó a través de encuestas y una guía de observación.

2.2.3.1. Resultados de las encuestas aplicadas a los docentes

La encuesta fue dirigida a 16 docentes de la Unidad Educativa Emanuel, en donde se obtuvo los siguientes resultados.

Pregunta 1: ¿Conoce de la existencia de un entorno virtual que da soporte al proceso de enseñanza aprendizaje?

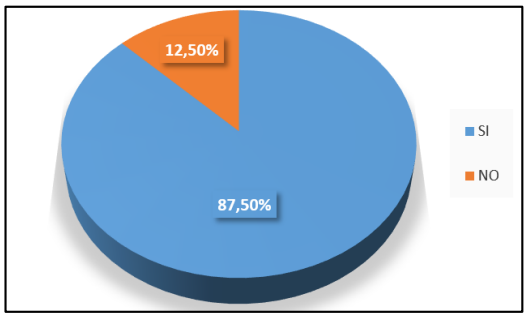


Grafico 2.1: Existencia de un entorno virtual

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 87,50% de docentes si conocen sobre la existencia de un entorno virtual que da soporte al proceso de enseñanza aprendizaje, mientras que el 12,50% no los conoce. Indicando que la mayoría de docentes si conocen y han utilizado entornos virtuales los cuales les han facilitado su proceso de enseñanza.

Pregunta 2: ¿Estaría de acuerdo con la implementación de un aula virtual en su unidad educativa?

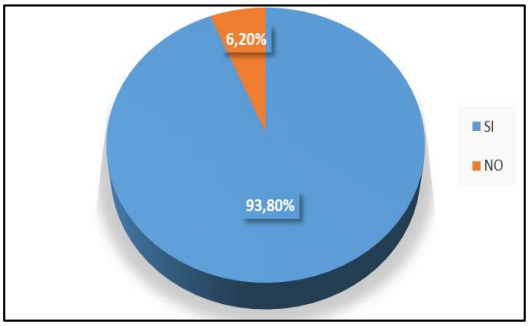


Grafico 2.2: Implementación de un aula virtual

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 97,80% de docentes están de acuerdo con la implementación de un aula virtual en su unidad educativa, mientas que el 6,20 % no está de acuerdo. Por lo tanto, la mayoría está de acuerdo en implementar el aula virtual para mejorar el proceso de enseñanza aprendizaje.

Pregunta 3: ¿La unidad educativa cuenta con un servicio de internet estable?

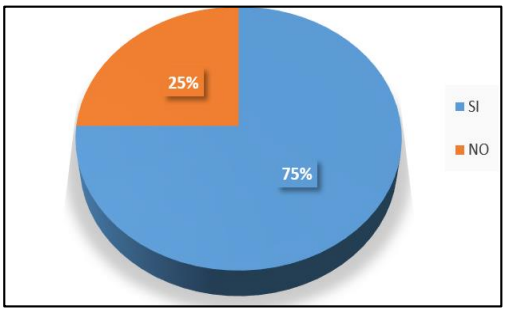


Grafico 2.3: Servicio de internet estable

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 75 % de docentes mencionan que la unidad educativa si cuenta con un servicio de internet estable, mientras que el 25 % mencionan que no. Por lo que la mayoría de docentes están de acuerdo que si hay un internet estable para poder realizar sus actividades sin ningún problema.

Pregunta 4: ¿Cree necesario capacitar a los docentes en creación y manejo de aulas virtuales?

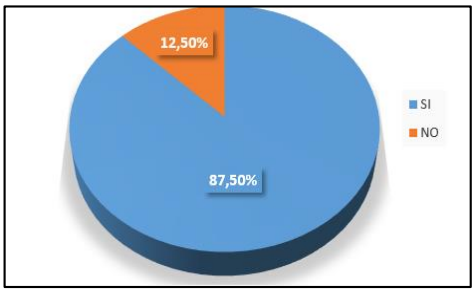


Grafico 2.4: Capacitación a los docentes

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 87,50% de los docentes creen que es necesario capacitar a los docentes en creación y manejo de aulas virtuales y un 12,50% cree que no es necesario. Indicando que la mayoría de docentes si están de acuerdo con una capacitación, siendo esto la base para un resultado óptimo en la educación en línea junto con la metodología correspondiente.

Pregunta 5: ¿Los recursos tecnológicos que el instituto ofrece (internet, computadoras, software) son suficientes y correctos para el aprendizaje virtual?

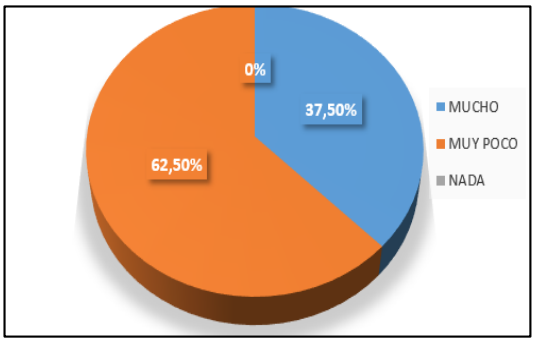


Grafico 2.5: Recursos tecnológicos

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 62,50% de docentes consideran que los recursos que ofrece la institución son muy poco suficiente para el aprendizaje virtual y el 37,50% están de acuerdo los recursos son suficientes y correctos. La mayoría de docentes indican que la institución no cuenta con los recursos suficientes para implantar un aprendizaje virtual.

Pregunta 6: ¿Considera usted que Moodle al ser una plataforma libre también le asegura estabilidad?

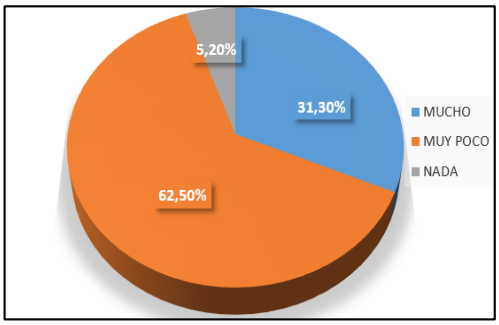


Grafico 2.6: Plataforma Moodle

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 62,50% de docentes consideran muy poco que la plataforma Moodle al ser libre asegura estabilidad, el 31,30% consideran que da mucha estabilidad y el 5,20% nada. Por lo tanto, la mayoría de docentes mencionan que Moodle es una plataforma que no les asegura mucha estabilidad en el proceso de enseñanza aprendizaje.

Pregunta 7: ¿Le parece bien tener la opción de recuperación de contraseña por medio del uso de correo electrónico le da un beneficio adicional en el caso de olvido de contraseña?

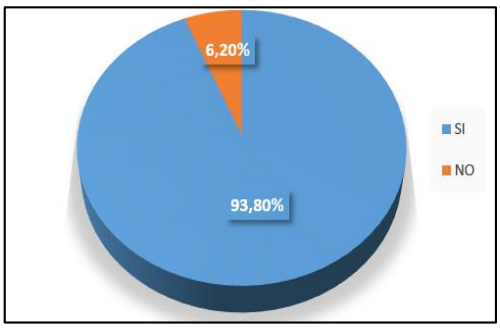


Grafico 2.7: Recuperación de contraseña

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 93,38 % de docentes les parece bien tener la opción de recuperación de contraseña por medio del uso del correo electrónico en el caso de olvido de recuperación y el 6,20 % piensan que no es necesario. Por lo tanto, la mayoría de docentes están de acuerdo de tener una opción de recuperación de contraseña ya que les puede brindar mayor seguridad.

Pregunta 8: ¿Ha tenido algún tipo de afectación a la infraestructura tecnológica?

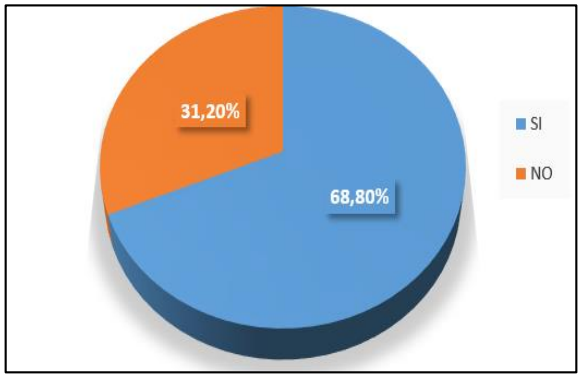


Grafico 2.8: Afectación a la infraestructura

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 68,80% de docentes si han tenido algún tipo de afección a la infraestructura tecnológica y el 31,20% no lo han tenido. Por lo tanto, la mayoría de docentes en algún momento si han sido afectados en la infraestructura tecnológica.

2.2.3.2. Resultados de las encuestas aplicadas al personal administrativo y tecnología

La encuesta fue dirigida a 4 personal administrativo y tecnología de la Unidad Educativa Emanuel, en donde se obtuvo los siguientes resultados.

Pregunta 1: ¿Tiene usted conocimiento de la metodología que se usa en un aula virtual?

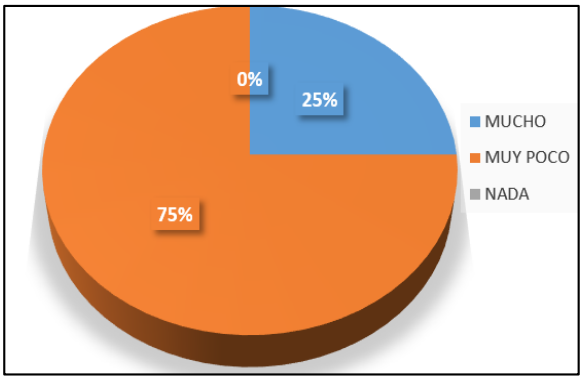


Grafico 2.9: Metodología que usa un aula virtual

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 75% de personal administrativo tiene muy poco conocimiento de la metodología que se usa en un aula virtual y el 25% tiene mucho conocimiento. Indicando que la mayoría del personal tiene muy poco conocimiento sobre la metodología que se utiliza en un aula virtual.

Pregunta 2: ¿Considera que es necesario la implementación de un aula virtual?

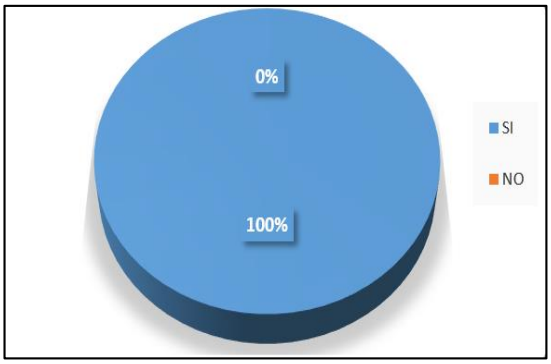


Grafico 2.10: Implementación de un aula virtual

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 100% del personal administrativo considera que si es necesario la implementación de un aula virtual para poder mejorar el proceso de enseñanza aprendizaje.

Pregunta 3: ¿Ha tenido alguna experiencia con el uso de algún entorno virtual?

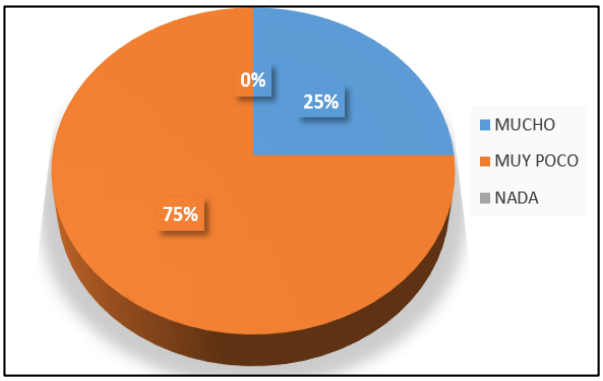


Grafico 2.11: Experiencia con el uso de un entorno virtual

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 75% del personal administrativo ha tenido muy poca experiencia con el uso de algún entorno virtual y el 25% si ha tenido mucha experiencia. Por lo tanto, la mayoría de personal no tiene mucho conocimiento en el uso de alguna plataforma virtual.

Pregunta 4: ¿La institución cuenta con el hardware necesario para la instalación de una plataforma virtual?

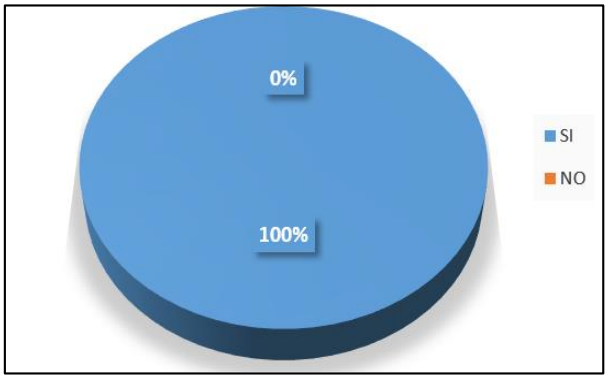


Grafico 2.12: Hardware necesario para la instalación

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 100% del personal administrativo menciona que la institución si cuenta con el hardware necesario el cual facilitara la instalación de una plataforma virtual.

Pregunta 5: ¿Considera que la implementación de un entorno virtual en la institución es una buena inversión?

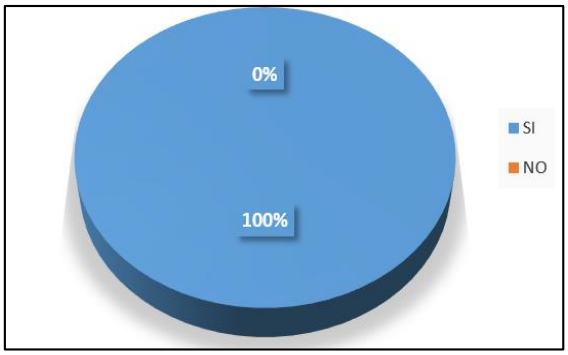


Grafico 2.13: La implementación de un entorno virtual es buena inversión

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 100% de personal administrativo si considera que la implementación de un entorno virtual en la institución en una buena inversión ya que les ayudara mucho en un futuro para poder mejorar el proceso de enseñanza aprendizaje.

Pregunta 6: ¿Tiene una persona capacitada para el manejo administrativo del entorno virtual Moodle?

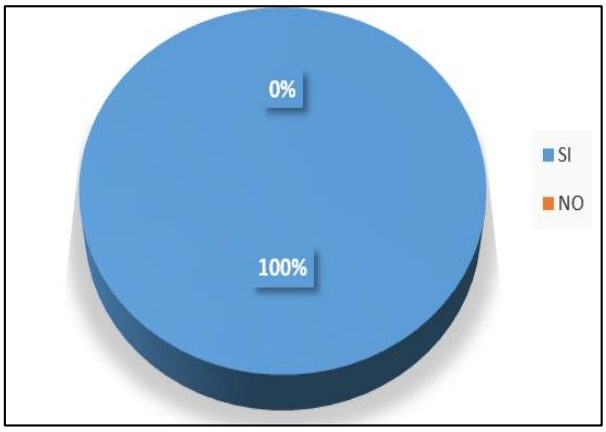


Grafico 2.14: Personal capacitado

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 100% del personal administrativo considera que si se cuenta con una persona capacitada para el manejo administrativo de un entorno virtual Moodle. Por lo que la mayoría del personal no tendrá dificultad en adaptarse a esta plataforma.

Pregunta 7: ¿Cree que es necesario que el sistema sugiera el cambio de contraseña periódicamente, utilizando estándares de seguridad de contraseñas?

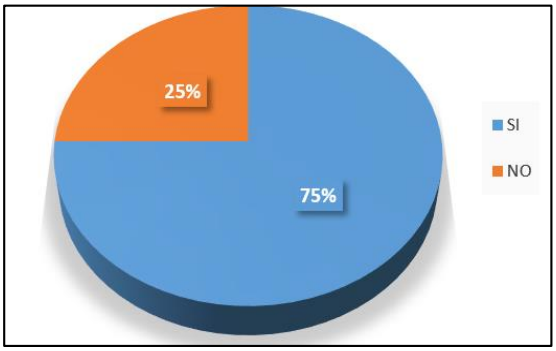


Grafico 2.15: Cambios de contraseña periódicamente

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 75% del personal administrativo si cree que es necesario que el sistema sugiera el cambio de contraseña periódicamente y el 25% no cree que sea muy necesario. Por lo tanto, la mayoría del personal está de acuerdo que el sistema sugiera cambio de contraseña utilizando estándares de seguridad.

Pregunta 8: ¿Tienen la capacidad económica para la adquisición de un Hosting y Dominio para la implementación de un entorno virtual?

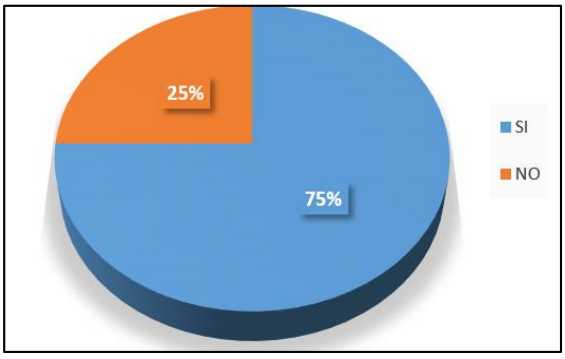


Grafico 2.16: Capacidad económica

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 75% del personal administrativo menciona que la institución si tiene la capacidad económica para la adquisición de un Hosting y dominio para la implementación de un entorno virtual y el 25% menciona que no cuenta con la capacidad necesaria. Por lo tanto, la mayoría del personal está de acuerdo que la institución si cuenta con la capacidad económica para adquirir los servicios y recursos necesarios para la implementación.

Pregunta 9: ¿Cree que es necesario implementar un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales, elaborada a partir de recomendaciones, normativas y estándares?

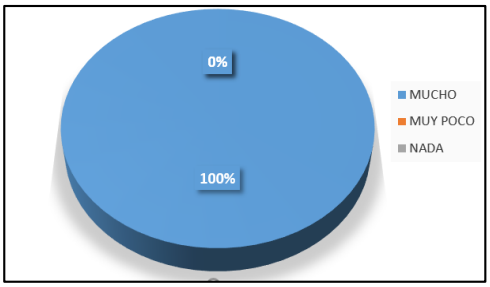


Grafico 2.17: Conjunto de buenas practicas

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 100% del personal administrativo si cree que es necesario implementar un conjunto de buenas prácticas de seguridad para la información se las actividades académicas virtuales las cuales están elaboradas a partir de recomendaciones, normativas y estándares.

Pregunta 10: ¿Cuál cree usted que es la principal amenaza a la que puede estar expuesto una plataforma virtual?

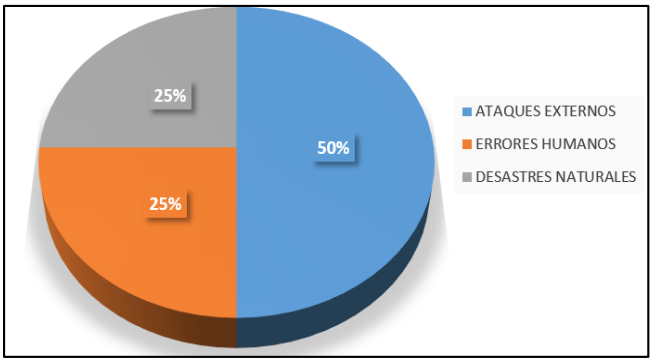


Grafico 2.18: Principal amenaza

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 50% del personal administrativo cree que los ataques externos es la principal amenaza a la que puede estar expuesto una plataforma virtual, el 25% piensa que los errores humanos y el 25% por desastre naturales. Indicando la mayoría del personal administrativo que la principal amenaza a la que puede estar expuesto son los ataques externos.

Pregunta 11: ¿Cree usted que es prudente realizar copias de seguridad frecuentemente en una plataforma virtual?

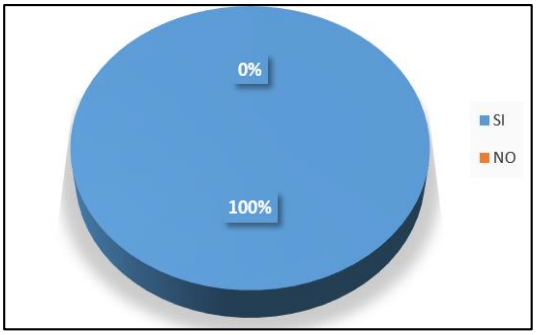


Grafico 2.19: Copias de seguridad

Elaborado por: Monserrath Acuña

Fuente: Encuesta aplicada

Análisis e Interpretación de resultados:

Según la encuesta aplicada el 100% del personal administrativo si cree que es prudente realizar copias de seguridad frecuentemente en una plataforma virtual para evitar la pérdida de información.

Análisis General:

Mediante los datos obtenidos en las encuestas se puede observar que la institución no cuenta con el hardware y software necesarios para implementar la plataforma virtual, el personal está de acuerdo que es importante realizar copias de seguridad de la información para evitar la pérdida de la misma, además están de acuerdo en que se aplique una metodología de continuidad de negocio para estar preparados ante cualquier desastre inesperado y tener una recuperación inmediata de la plataforma.

2.2.3.3. Ficha de Observación

Al aplicar la observación en la Unidad Educativa Emanuel se obtuvo los siguientes resultados.

Tabla 2.3: Ficha de Observación

Elaborado por: Monserrath Acuña

INDICADORES	SI	NO	OBSERVACIONES
1. Posee el hardware necesario para la instalación	**X**		Tiene una computadora disponible que se lo pude adecuar como servidor.

2. Posee el software necesario para la instalación		**X**	No cuenta con el software necesario
3. Posee servicio de internet	**X**		Posee un internet estable y fijo
4. Existe un espacio de trabajo adecuado para la implementación.		**X**	Se puede adecuar un espacio de trabajo para la implementación
5. Posee alguna metodología para almacenar la información de los estudiantes	**X**		Utiliza la plataforma Idukay en donde guardan los datos y calificaciones de los estudiantes.

CONCLUSION:

La Unidad Educativa no cuenta con el espacio de trabajo ni el software adecuado para la implantación de la plataforma virtual, pero la rectora y el personal administrativo están dispuestos en brindar los recursos necesarios para facilitar el desarrollo del mismo.

2.2.4. Procesamiento y Análisis de Datos

- Los docentes y el personal administrativo están de acuerdo con la implementación de una plataforma virtual con políticas de seguridad ya que les servirá como un complemento para poder mejorar el proceso de enseñanza aprendizaje.

- La unidad educativa no cuenta con el hardware y servicios necesarios para poder implementar una plataforma virtual.

- Los docentes y el personal administrativo están capacitados con el uso y manejo de la plataforma virtual Moodle por lo que se podrán adaptar con facilidad.

- El personal administrativo cree que es importante realizar copias de seguridad en la plataforma para evitar la pérdida de la información.

- El personal administrativo está de acuerdo en que se aplique una metodología de continuidad del negocio para estar preparado ante cualquier riesgo y poder solucionarlo de una manera adecuada para evitar el fallo de la plataforma virtual y la perdida de la información.

Del análisis obtenido de las encuestas y ficha de observación se debe recalcar que es muy importante realizar copias de seguridad de todos los datos para poder recuperar la información de una manera más fácil rápida, además no se puede definir si no cuenta con el hardware y servicios necesario debido a que se necesita determinar cuáles son los requerimientos mínimos para que funcione con la carga que va a tener la plataforma virtual.

CAPITULO III.-RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

3.1.1. Hardware base

Los requisitos básicos de hardware para poder instalar una plataforma virtual Moodle son los siguientes [15]:

- Espacio de disco: 200MB para el código de Moodle, más lo que necesite para contenidos, 8GB es el mínimo para correr un sitio de producción.
- Procesador: 1GHz(mínimo) se recomienda 2 GHz de doble núcleo o más.
- Memoria: 512 MB (mínimo), se recomienda 1GB o más. En un servidor de producción debe pensarse en al menos 8GB. Al aumentar la memoria primaria se reducirá la necesidad para que el procesador intercambie a disco y le permita a su servidor manejar a más usuarios.
- Servidor para el frente en web y la base de datos para optimizar el ambiente.

Todos los requisitos anteriores varían dependiendo de las combinaciones del hardware y software específicos, además del tipo de uso y la carga [16].

Tabla 3.1: Requerimientos mínimos de hardware

Elaborado por: Monserrath Acuña

Fuente:[16]

HARDWARE	REQUERIMIENTO MÍNIMO	DIMENSIONAMIENTO
Memoria	8GB	1GB por cada 50 usuarios
Procesador	1 núcleo	1 núcleo por cada 400 usuarios
Disco Duro	2 x 250 GB	500 Mb por usuario
Ancho de banda	10 Mbps	Depende del usuario

3.1.2. Servicios

Los servicios principales que se van a utilizar son [17]:

- Internet
- Servidor web (apache) 2.4
- Servidor de base de datos (Mariadb) 15.1
- Servidor de la Plataforma Virtual Moodle 4.0

3.1.3. Riesgos y Vulnerabilidades

Para poder implementar una plataforma virtual se debe tomar en cuenta varios riesgos y vulnerabilidades, a continuación, se muestran los más importantes.

Tabla 3.2: Riesgos y Vulnerabilidades

Elaborado por: Monserrath Acuña

RIESGOS	VULNERABILIDADES
• Perdida de datos por fallas humanas • Daños en el hardware • Desastres naturales • Fallas eléctricas • Falta de actualización de software • Manejo inadecuado de la información • Falta de capacitación • Falta de mantenimiento • Falta de software • Virus • Pandemia	• Manejo insuficiente de medidas de seguridad • Recursos insuficientes • Incompatibilidad en hardware y software • Capacitación inadecuada • Acceso no autorizado • Falta de aplicación de políticas en las contraseñas • Falta de documentación • Control inadecuado de base de datos

3.1.4. Metodologías de Continuidad del Negocio

A continuación, se muestra un cuadro comparativo entre tres metodologías de continuidad del negocio: Plan de continuidad del negocio (BCP) [18], Gestión de continuidad de negocio (BCM) [8] y Gestión de la continuidad del negocio (GCN) [7], con el objetivo de analizar sus principales características y elegir cual se ajusta mejor para el desarrollo del proyecto.

Tabla 3.3: Metodologías de continuidad del Negocio

Elaborado por: Monserrath Acuña

METODOLOGIAS DE CONTINUIDAD DEL NEGOCIO			
Características	**Plan de continuidad del negocio (BCP)**	**Gestión de continuidad de negocio (BCM)**	**Gestión de la continuidad del negocio (GCN)**
OBJETIVO	Establecer las funciones esenciales de la empresa, identificar que sistemas y procesos deben mantenerse y detallar como mantenerlos.	Permite anticipar incidentes que pueden afectar a las funciones y procesos claves para la organización y que asegura una respuesta a dichos incidentes de forma planeada y ensayada.	Proteger los interese de las partes interesadas, la reputación, las finanzas, los activos críticos y otros aspectos generadores de valor.
BENEFICIOS	- Gestión de riesgos - Mejora de todos los procesos - Mayor madurez organizacional	- Aumenta la probabilidad de supervivencia de la empresa tras un siniestro	- Se puede identificar los riesgos a los que puede estar expuestos

	- Mayor disponibilidad y confiabilidad - Ventaja de mercado	- Mantener e incluso mejorar la reputación de la empresa - Evita errores costosos tanto antes como después del siniestro - Optimiza los recursos, canalizándolos allí donde resultan más útiles	- Contar con las respuestas adecuadas al momento de enfrentar una crisis - Valor agregado frente a la competencia - Ahorro en costos y tiempo
IMPORTANCIA	- Proteger el personal, negocio, los clientes y los accionistas - Puede prevenir y resolver posibles interrupciones - Aumenta el conocimiento y las habilidades de los empleados - Tener una ventaja competitiva en una crisis	- Administrar una respuesta coordinada frente a un incidente - Maximizar la protección personal - Reducir el riesgo de pérdida de datos - Supervisar las actividades de recuperación definidas por las necesidades criticas de negocio - Un aprendizaje de la experiencia y la mejora continua	- Permite la coordinación entre los empleados - Tener la capacidad para recuperarse rápidamente - Contribuye a mejorar la reputación - Generar confianza ante los clientes y nuevos prospectos

ESTANDARES	ISO 22301: 2012 ISO 22313 ISO 22317 ISO 223118 ISO 22398 ISO 22399	ISO 22301:2019 ISO 9001 ISO 14001 ISO 45001	ISO 22301:2012 ISO 9001 ISO 14001 ISO 27001 ISO 20000
FASES	FASE 1 - Definición de roles - Funciones - Competencias FASE 2 - Definición de políticas BCP - Esquema documental - Procedimiento BCP - Esquema de medición	- Preparación del proyecto - Identificación y análisis de riesgos - Respuesta ante emergencias - Manejo de crisis - Continuidad del negocio BCP - Capacitación, sensibilización y mantenimiento.	- Inicio del proyecto - Definir políticas - Compromiso de la alta gerencia - Contexto de la organización - Análisis del impacto del negocio BIA - Gestión del riesgo - Estrategias de continuidad y recursos - Estructura de respuesta inmediata

	FASE 3 - Análisis BIA - Análisis de riesgos –BCP - Diseño estratégico FASE 4 - Planes BCP x proceso - Diseño plan de prueba de escritorio - Documento pre-auditoria al BCP		- Revisión, mantenimiento y mejoras
PLANES COMPLEMENTARIOS	- Plan de recuperación ante desastres - Plan de emergencia - Plan de comunicación de crisis	- Análisis de impacto del negocio - Plan de recuperación ante desastres - Plan de continuidad del negocio	- Plan de recuperación ante desastres - Plan de comunicación de crisis - Plan de evaluación por edificios - Respuesta a ciber-incidentes - Plan de contingencia

De acuerdo con los resultados obtenidos para el desarrollo del presente proyecto se ha seleccionado la metodología Gestión de Continuidad del negocio (BCM). Puesto que anticipa de cualquier incidente que pueda afectar las funciones y procesos de la organización. Además, optimiza los recursos y reduce el riesgo de pérdida de datos.

3.1.5. Técnicas de endurecimiento o Hardening

Entre las actividades propias de un proceso hardening para aumentar nuestra confidencialidad e integridad de nuestro sistema se tiene las siguientes [19]:

- Actualizar los sistemas operativos para obtener los parches de seguridad.
- Generar las particiones del servidor pensando en la seguridad.
- Cambiar todas las claves que se tenga por defecto.
- Desinstalar todo software que sea innecesario.
- Deshabilitar todos los servicios innecesarios en segundo plano.
- Asegurar de que el firewall este correctamente configurado.
- Configurar correctamente los protocolos de red.
- Aumentar la seguridad de los servicios o procesos que si tengan que ser utilizados.
- Cerrar puertos que se encuentren sin uso.
- Utilizar backup (copias de seguridad) como respaldo de datos importantes.
- Utilizar el control de acceso y los permisos para limitar lo que los usuarios pueden hacer en una base de datos.
- Eliminar a los usuarios que no tengan los permisos necesarios.
- Aplicar las políticas de contraseñas.

3.2. Desarrollo de la Propuesta

3.2.1. Fase 1: Comprensión de la Organización

A. Objetivos

- Disminuir la posibilidad de pérdida y divulgación de la información.
- Garantizar y optimizar acciones a desarrollar ante una amenaza.
- Garantizar una recuperación rápida en las amenazas que se presenten.
- Realizar una evaluación de riesgos.

B. Alcance

El alcance del presente proyecto es preparar a la institución ante cualquier interrupción del servicio ya sea de forma natural o provocada, a fin de minimizar el impacto negativo de interrupciones y mejorar la seguridad en la plataforma virtual.

La Plataforma virtual ofrece las ventajas necesarias para mantener continuidad al proceso formativo las 24 horas y los 7 días a la semana, pudiendo acceder docentes y estudiantes.

C. Obligaciones de los stakeholders

Los stakeholders son aquellos individuos o grupos que tienen interés e impacto en una organización y en los resultados de sus acciones [20].

Están involucrados directamente en ir alimentando la plataforma constantemente con actividades y el ingreso de usuarios con los respectivos permisos de uso.

Los tipos de usuarios son los siguientes:

Estudiante: Es el tipo de usuario más básico en Moodle y solo podría acceder a los contenidos creados asignados a su perfil, además de participar en por ejemplo foros creados.

Docente: Tendrá el control total sobre el curso asignado, pudiendo marcar eventos en el calendario, asignar calificaciones, etc.

Administrador: Este usuario tendrá todos los permisos y privilegios, pudiendo crear cursos, asignar profesores a dichos cursos, gestionar y modificar los diferentes módulos que se pueden crear en las diferentes vistas para personalizar el entorno.

D. Políticas

Las políticas del plan de continuidad del negocio consisten en definir acuerdos con los miembros de la institución para la elaboración del plan de continuidad de tal manera que el desarrollo pueda darse con total normalidad rigiéndose en los acuerdos realizados.

E. Análisis de impacto del negocio BIA (Bussiness Impact Analysis)

Tabla 3.4: Escala de Probabilidad
Elaborado por: Monserrath Acuña

PROBABILIDAD	
Bajo	1
Media	2
Alta	3

Tabla 3.5: Análisis de riesgos

Elaborado por: Monserrath Acuña

ANALISIS DE RIESGOS			
Código	**Amenaza**	**Probabilidad**	**Tiempo máximo de recuperación**
A001	Perdida de datos por fallas humanas	Media	2 HORAS
A002	Daños en el hardware	Baja	8 HORAS
A003	Desastre naturales	Baja	8 HORAS
A004	Fallas eléctricas	Baja	4 HORAS
A005	Falta de actualización de software	Media	2 HORAS
A006	Manejo inadecuado de la información	Media	2 HORAS
A007	Falta de capacitación	Media	1 SEMANA
A008	Falta de mantenimiento	Media	4 HORAS
A009	Falta de software	Baja	2 HORAS
A010	Virus	Media	2 HORAS
A011	Pandemia	Baja	N/A

3.2.2. Fase 2: Determinar la estrategia de continuidad o recuperación

Una vez identificados los recursos y servicios se pueden continuar con la evaluación y definición de las estrategias que permitan cumplir con la continuidad del negocio.

Para la determinación de una correcta estrategia, se debe considerar que se cubran los dos puntos:

- Que la estrategia garantice un nivel aceptable de la operación en un escenario de contingencia.
- El tiempo para implementar la estrategia debe ser aceptable.

En las estrategias se deben considerar diferentes recursos:

A. Personal

Como una estrategia para el personal administrativo y de tecnología, se sugiere dar una capacitación sobre continuidad de negocio para asegurar el conocimiento en este tema, también se debe sugerir que conozcan las actividades que realizan sus otros compañeros.

Es necesario definir la mejor estrategia para mantener las principales habilidades y conocimiento de cada persona y asignar un encargado para cada plan.

B. Instalaciones

Se debe verificar que las instalaciones permitan llevar a cabo las actividades que apoyen las operaciones de la organización, deben contar con una infraestructura necesaria que permita continuar a un nivel aceptable.

También se puede tomar la medida para trabajar desde casa o vía remota.

C. Información

Se debe comprobar que se tenga la información necesaria para dar continuidad a las operaciones del negocio, esta información debe cumplir con las características de seguridad indispensables, integridad, disponibilidad y confidencialidad.

Es necesario tomar medidas desde las personas que son responsables de elaborar los respaldos de la información, en que horario, con qué recursos, las medidas de seguridad que se deben tomar en cuenta para llevar a cabo esta tarea.

D. Tecnología

Se debe verificar que la tecnología disponible sea adecuada para realizar operaciones a un nivel aceptable en una emergencia. Para esta estrategia, la infraestructura debe elegirse en función de las necesidades y el presupuesto de la institución.

Para una mejor implementación, se recomienda elaborar una lista de verificación de todo lo relacionado con: sistemas de información, hardware, redes, servidores, usuarios con el fin de entender lo que hay en la institución.

También se debe contar con un sistema de alimentación ininterrumpida (UPS) para evitar que se detenga su función por un problema causado por una interrupción eléctrica, esto daría como resultado problemas que incluyen grandes cantidades de dinero y de tiempo debido a la perdida de información y el daño de sus componentes.

Se debe verificar que la institución cuente con medidas contra incendios apropiadas para reducir al mínimo el riesgo de pérdida de recursos tecnológicos o personal.

3.2.3. Fase 3: Desarrollo e implementación de la respuesta BCM

Durante esta fase, se desarrolla un plan para garantizar la continuidad de las actividades críticas y la gestión de incidentes.

La institución debe definir una estructura de respuesta a incidentes para identificar la naturaleza del mismo, controlar la situación y notificar a las partes interesadas. Estos equipos deben contar con planes, procesos y procedimientos para la gestión de incidentes.

Todos los planes deben tener al menos:

- Qué actividades clave se deben retomar y en qué circunstancias se debe aplicar el plan.
- Priorización de actividades críticas por periodo de tiempo y nivel de recuperación requerido.
- Roles y responsabilidades durante el incidente.
- Iniciar procedimientos para la gestión de incidentes, la continuidad del negocio o la recuperación.
- Responsable de actualizar cada plan.

3.2.3.1. Plan de continuidad del negocio

Para poder comenzar con el plan es necesario haber definido la valoración de los riegos que pueden afectar el funcionamiento del mismo y la estrategia de continuidad más adecuada para el negocio.

A. Organización de los equipos

Los equipos de emergencia están formados por el personal clave necesario para activar y desarrollar el plan de manera continua. Cada equipo tiene funciones y acciones que debe realizar durante las diferentes fases del plan.

Se han conformado los siguientes equipos que pueden formar parte del Plan de continuidad:

- **Equipo de crisis**

Esta encargado de dirigir las acciones durante la contingencia y recuperación.

El objetivo de este equipo es reducir al máximo el riesgo y la incertidumbre en la dirección de la situación. Debe tomar las decisiones importantes durante los incidentes, además de mantener informados a los otros equipos de la situación.

Las principales tareas y responsabilidades son:

- Análisis de la situación.
- Decidir si activar el Plan de continuidad.
- Iniciar el proceso de notificación al personal a través de los diferentes responsables.
- Realizar un seguimiento de la recuperación en función de los tiempos estimados.

El siguiente cuadro muestra al líder del equipo de crisis:

Tabla 3.6: Equipo de crisis

Elaborado por: Monserrath Acuña

Equipo de Crisis	**Nombre:** Pamela Izurieta **Teléfono:** 0985656078 **Cargo:** Rectora

Cuando ocurre un incidente el equipo de crisis debe reunirse y tomar una decisión para afrontar la situación. Deben estar continuamente informados de la situación y determinar si es necesario iniciar con el plan y mantener comunicación con los líderes de los demás grupos según lo planeado.

- **Equipo de recuperación**

Su función es establecer todos los sistemas necesarios. Es responsable de preparar la infraestructura requerida para la recuperación, esto incluye todos los servidores, hardware software y cualquier otro elemento necesario para restaurar la plataforma virtual.

Las principales tareas y responsabilidades son:

- Dirigirse al servidor si no se presenta ningún riesgo.
- Dirigirse al servidor alterno, contactando a la persona responsable para que le proporcione todo lo necesario para que pueda solucionar dicho problema.

El siguiente cuadro muestra el equipo de recuperación.

Tabla 3.7: Equipo de Recuperación

Elaborado por: Monserrath Acuña

Equipo de Recuperación	**Nombre:** María José Revelo **Teléfono:** 0987344322 **Cargo:** Personal de Tecnología **Nombre:** Mishell Tonato **Teléfono:** 0991037563 **Cargo:** Personal de Tecnología

Este equipo se encarga de realizar las actividades de recuperación con el fin de poner en marcha los servicios críticos afectados, ya sea activando el plan de contingencia o desde el servidor ubicado en la oficina de la rectora.

3.2.3.2. Identificación de escenarios

Se han tomado los principales escenarios que pueden afectar la continuidad de la plataforma virtual y establecido los posibles riesgos asociados a estos escenarios.

Tabla 3.8: Incendio

Elaborado por: Monserrath Acuña

Riesgo	Desastre natural /Incendio
Escenario	En el caso de incendio que suceda en la institución o en las oficinas de la misma, las pérdidas que se generarían serían: humanas, información, servicios, activos. Además, este provocaría la destrucción del servidor que está ubicado en el primer piso en la oficina de la rectora, el cual se dañaría completamente provocando la perdida de información y los servicios prestados y con ello todo su contenido dando como resultado una pérdida total.
Acción	Implementar extintores para inhibir la combustión del servidor y así poder proteger los equipos tecnológicos y personal.

Tabla 3.9: Terremoto

Elaborado por: Monserrath Acuña

Riesgo	Desastre natural/Terremoto
Escenario	En caso de producirse un terremoto dependiendo de la magnitud podría producir la pérdida parcial o total de la institución, puede existir pérdidas humanas y bienes materiales entre ellos hardware y otros recursos en donde se encuentra almacenada la información, puede presentar daños provocando así la perdida de continuidad de los mismos.

Acción	La persona a cargo debe ayudar en la evacuación de la instalación y, si es posible, los equipos tecnológicos (hardware).

Tabla 3.10: Fallas eléctricas

Elaborado por: Monserrath Acuña

Riesgo	Fallas eléctricas
Escenario	En la institución no existe una planta de energía la cual es utilizada como contingencia en caso de la suspensión normal del servicio eléctrico. Las fallas eléctricas afectan directamente al hardware de la institución, pueden ocurrir fallas que provoquen corto circuito y generar incendios el cual llevaría a que el servidor se dañe y la plataforma deje de funcionar.
Acción	Se pueden implementar transformadores especiales que soporten la carga de energía para que no haya fallas en el servidor ni impacto.

Tabla 3.11: Manejo inadecuado de la información

Elaborado por: Monserrath Acuña

Riesgo	Manejo inadecuado de la información
Escenario	Para la institución mantener integra la información de los estudiantes y docentes es muy importante, por lo cual los datos que se almacenan en la plataforma no pueden ser alterados por personas que no tienen los permisos necesarios.
Acción	Se debe controlar en la plataforma a quien se les da los privilegios para que puedan modificar la información sin ocasionar ningún daño.

Tabla 3.12: Fallos en la red

Elaborado por: Monserrath Acuña

Riesgo	Fallos en la red
Escenario	Existen varias causas por las que puede ocurrir una falla en la red: • Mala conexión • Rupturas de cables • Exceso de ruido Al tener una falla de red pude suscitarse perdida de la información ya que si los servidores están haciendo rutinas automáticas de respaldos puede generar datos erróneos almacenados que cuando deban ser utilizados no estarán disponibles o estarán equivocados.
Acción	Protección de servidores y mantenimiento de equipos para reducir el impacto cuando ocurren problemas.

3.2.3.3. Plan de Recuperación

A. Objetivos

- Determinar los procedimientos de recuperación en caso de falla del servidor y de la red.
- Mayor atención y enfoque en la recuperación ordenada y la reanudación de las operaciones críticas de las instalaciones, incluido el soporte para todos los servicios basados en la infraestructura de TI.

B. Servicios críticos

Para la preservación del servidor es importante para tener continuidad en cuanto a los servicios que posee la institución se deben resguardar los siguientes:

- Comunicaciones de redes, conectividad
- Servicio de Internet
- Servicio de dominio
- Respaldos de la información
- Servicio de la plataforma virtual Moodle

C. Incidente y Contingencia

Este plan de recuperación se activará bajo una de estas circunstancias:

- Una interrupción puede inhabilitar parcial o completamente las operaciones del servidor de la plataforma virtual durante 24 horas.
- Un problema que afectó a los dispositivos ya la red como consecuencia de circunstancias ajenas a la capacidad diaria de afrontarlo.
- Las situaciones generales que pueden destruir o deshabilitar los servidores generalmente se clasifican en las siguientes categorías principales: cortes de energía, incendios, agua, desastres naturales, robo y virus.

3.2.4. Implementación de la plataforma virtual Moodle

La implementación se va a realizar en maquinar virtuales Para poder instalar Moodle primero se debe configurar el servidor.

Sistema Operativo: Almalinux

Memoria: 8 GB

Disco duro: 20 GB

Procesador: 2GHz

Se va a configurar otro servidor de réplica con las mismas características del servidor principal.

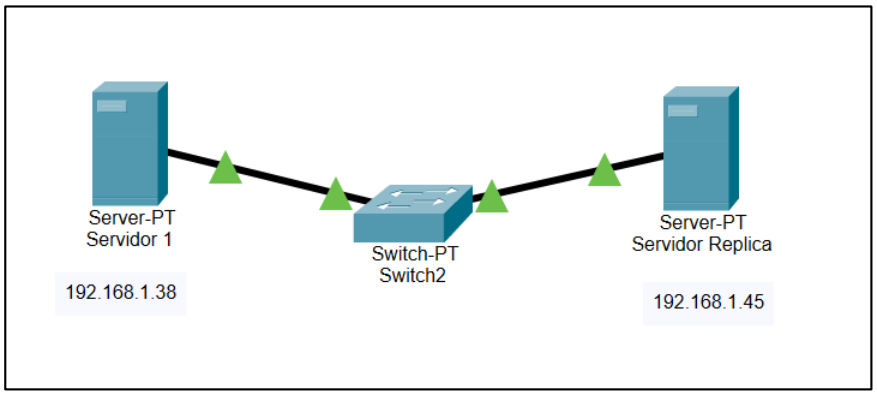


Gráfico 3.1: Diagrama Lógico

Elaborado por: Monserrath Acuña

El sistema operativo que se va a utilizar es Alma Linux debido a que es de código abierto, utiliza el modelo tradicional de soporte y actualizaciones a largo plazo, también brinda estabilidad y seguridad para los usuarios [21].

La política de seguridad que se va a utilizar es ANSSI-BP-028 porque contiene configuraciones de endurecimiento para estar protegido contra ciberataques, también presenta ajustes de configuración relevantes para la seguridad de la información y proporciona una capacidad de verificación automática. Es una recomendación de configuración para sistemas GNU/Linux [22].

Además, proporciona a los administradores información sobre como configurar de forma segura los sistemas bajo su control en una variedad de roles. Los requisitos para la comprobación de la integridad pueden depender del entorno en el que va a utilizar el sistema [23].

1. Instalar Alma Linux y configurar la red y nombre de equipo.

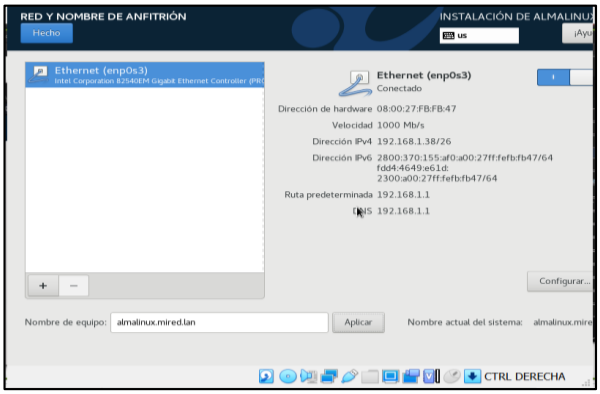


Gráfico 3.2: Configuración de red

Elaborado por: Monserrath Acuña

2. El servidor se va a configurar con políticas de seguridad porque permite garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afecten.

Gráfico 3.3: Políticas de seguridad

Elaborado por: Monserrath Acuña

3. Crear puntos de montaje para la instalación.

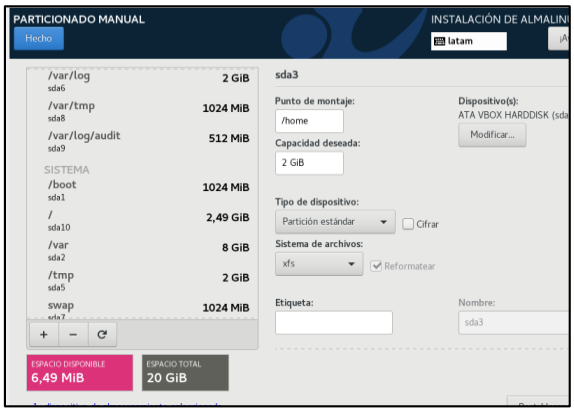


Gráfico 3.4: Particionado manual

Elaborado por: Monserrath Acuña

4. Seleccionar el tipo de software en este caso será un servidor.

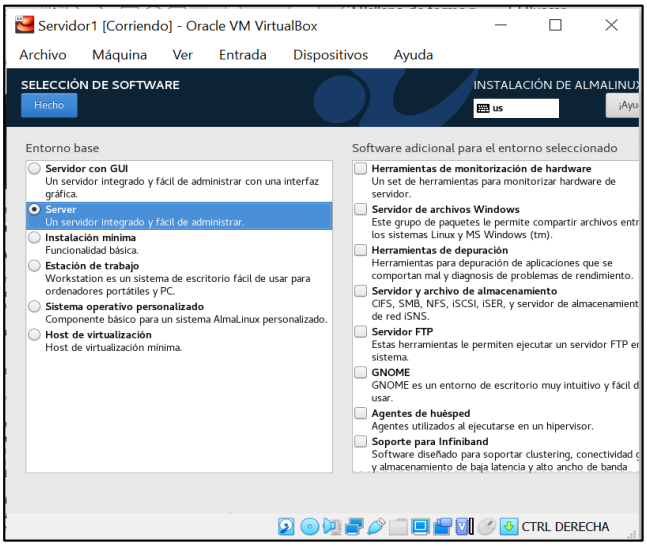


Gráfico 3.5: Selección de software

Elaborado por: Monserrath Acuña

5. Cambiar el hostname de nuestro servidor.

```
[root@emanuel /]# hostnamectl set-hostname evirtual.ueemanuel.com
[root@emanuel /]#
```

Gráfico 3.6: Hostname

Elaborado por: Monserrath Acuña

6. Uno de los pasos importantes antes de ejecutar los programas de instalación es actualizar el sistema, esto ayudara a asegurarse de que todos los paquetes estén actualizados y a reconstruir la memoria cache del sistema para que los servicios funcionen sin problema.

Gráfico 3.7: Actualizar el sistema

Elaborado por: Monserrath Acuña

7. Actualizar las reglas de firewall para abrir los puertos 80(http) y 443(https).

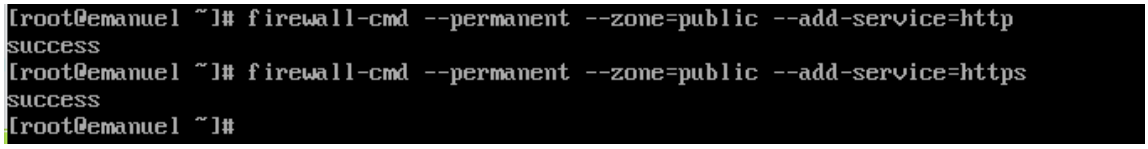


Gráfico 3.8: reglas firewall

Elaborado por: Monserrath Acuña

8. Recargar el firewall para realizar los cambios.

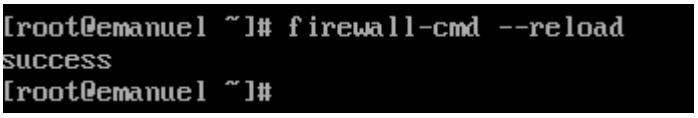


Gráfico 3.9: Recargar firewall

Elaborado por: Monserrath Acuña

9. Instalar los servicios que se va a utilizar para servidor web (http) y base de datos(mariadb).

Grafico 3.10: Servicios

Elaborado por: Monserrath Acuña

10. Configurar el dns para eso se debe cambiar el archivo hosts, agregar la ip de nuestro servidor y el hostname.

```
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.38  evirtual.ueemanuel.com  evirtual
```

Gráfico 3.11: Configurar dns

Elaborado por: Monserrath Acuña

11. Iniciar los servicios de http.

```
[root@emanuel named]# systemctl start httpd
[root@emanuel named]# systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/
httpd.service.
[root@emanuel named]# _
```

Gráfico 3.12: Iniciar los servicios http

Elaborado por: Monserrath Acuña

12. Crear un certificado ssl para mantener la conexión segura y proteger la información.

```
[root@emanuel certs]# make server.key
umask 77 ; \
/usr/bin/openssl genrsa -aes128 2048 > server.key
Generating RSA private key, 2048 bit long modulus
.....................................................................+++
.....+++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:
[root@emanuel certs]# _
```

Gráfico 3.13: archivo. key

Elaborado por: Monserrath Acuña

13. Generar el certificado y escribir una clave.

```
[root@emanuel certs]# openssl rsa -in server.key -out server.key
Enter pass phrase for server.key:
writing RSA key
[root@emanuel certs]#
```

Gráfico 3.14: Generar el certificado ssl

Elaborado por: Monserrath Acuña

14. Crear el archivo. csr y completar la información.

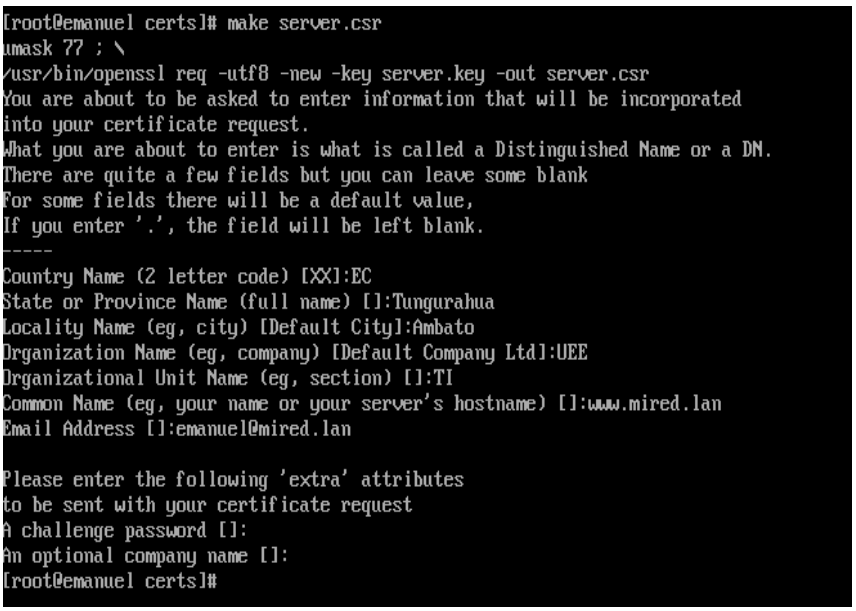


Gráfico 3.15: Archivo. csr

Elaborado por: Monserrath Acuña

15. Firmar el certificado creado.

Gráfico 3.16: Firmar el certificado

Elaborado por: Monserrath Acuña

16. Cambiar a la ruta /etc/httpd/conf.d y modificar el archivo ssl.conf.

Gráfico 3.17: Modificar archivo de configuración

Elaborado por: Monserrath Acuña

17. Reiniciar el servicio de httpd.

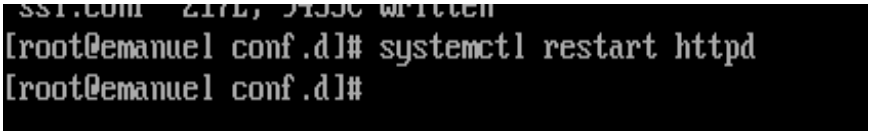


Gráfico 3.18: Reiniciar servicio httpd

Elaborado por: Monserrath Acuña

18. Levantar y habilitar los servicios de mariadb.

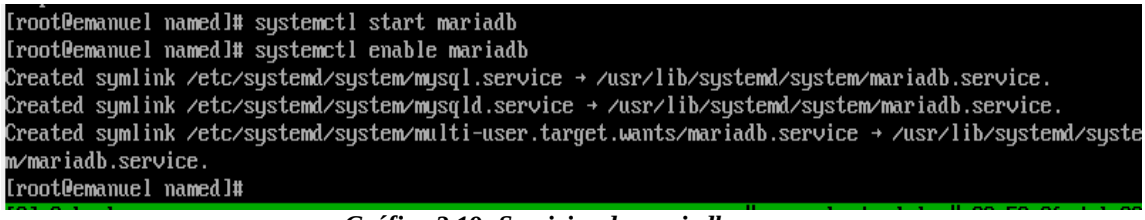


Gráfico 3.19: Servicios de mariadb

Elaborado por: Monserrath Acuña

19. Asignar una contraseña al motor de base de datos para que la conexión sea más segura y no se pueda hacer un ataque externo.

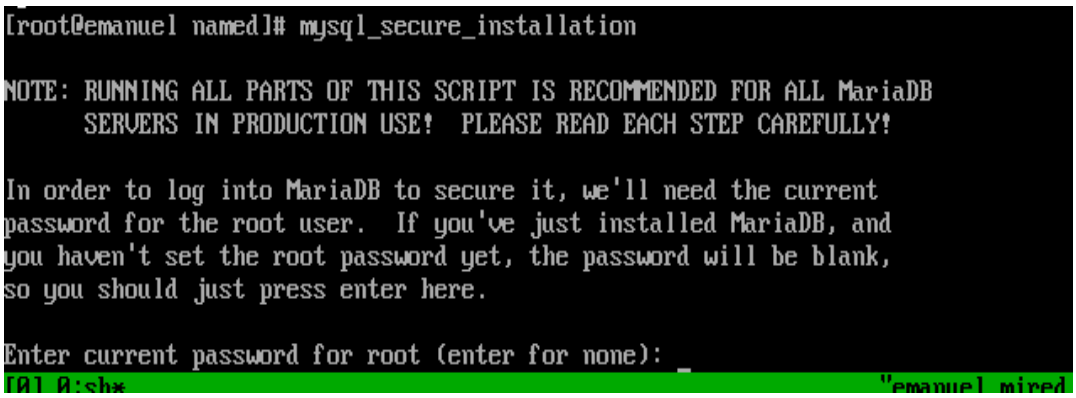


Gráfico 3.20: Contraseña base de datos

Elaborado por: Monserrath Acuña

20. Modificar el archivo php.ini en donde se puede encontrar la configuración.

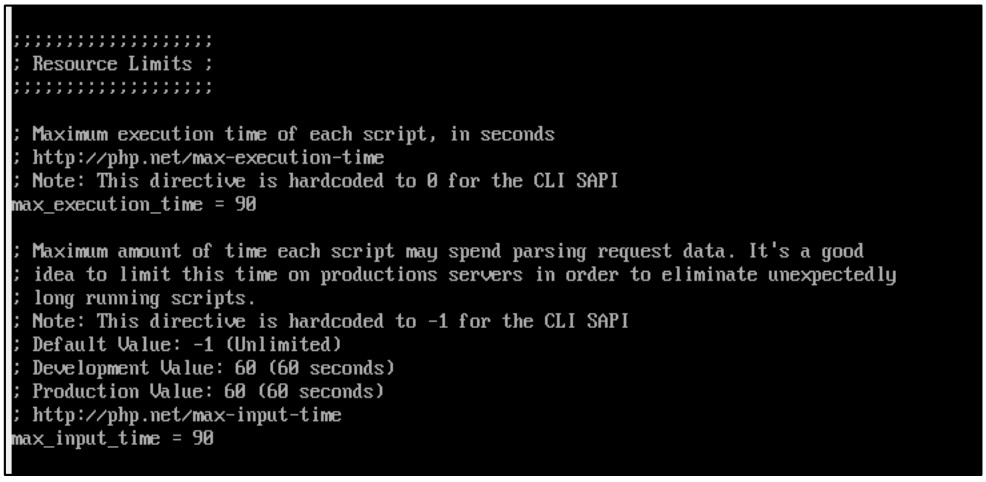


Gráfico 3.21: Configurar php

Elaborado por: Monserrath Acuña

21. Restaurar el servicio de http para que se aplique los cambios realizados.

Gráfico 3.22: Restaurar http

Elaborado por: Monserrath Acuña

22. Configurar las actualizaciones automáticas para mejorar el rendimiento y la seguridad del servidor.

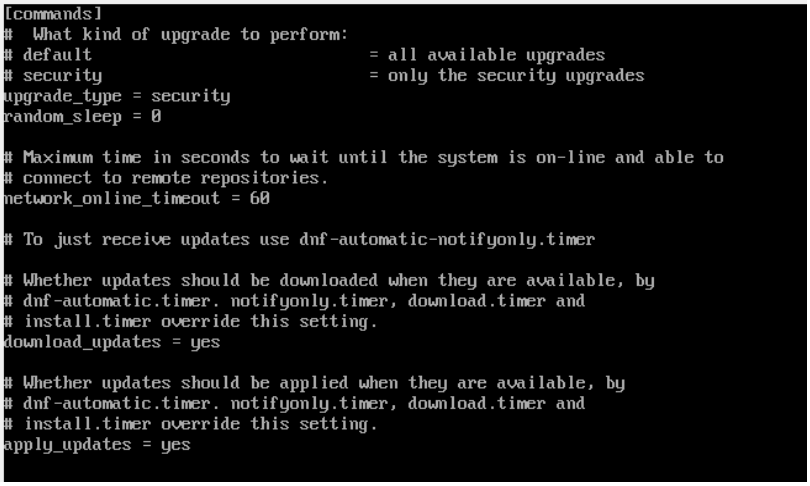


Gráfico 3.23: Actualización automática

Elaborado por: Monserrath Acuña

23. Habilitar e iniciar el temporizador del sistema.

Gráfico 3.24: Temporizador del sistema

Elaborado por: Monserrath Acuña

24. Configurar las políticas de contraseñas para proteger la información y evitar la pérdida de la misma.

```
# Configuration for systemwide password quality limits
# Defaults:
#
# La nueva contrase;a debe tener 4 nuevos caracteres versus la anterior
# old password.
difok = 4
#
# Debera tener por lo menos 10 caracteres de longitud
# credits are not disabled which is the default). (See pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 10
#
# Requiere por lo menos un digito
# it is the minimum number of digits in the new password.
dcredit = -1
#
# Requiere por lo menos 1 letra mayuscula
# If less than 0 it is the minimum number of uppercase characters in the new
# password.
ucredit = -1
#
# Requiere por lo menos una letra minuscula
# If less than 0 it is the minimum number of lowercase characters in the new
# password.
lcredit = -1
#
# The maximum credit for having other characters in the new password.
# If less than 0 it is the minimum number of other characters in the new
# password.
ocredit = -1
#
# The minimum number of required classes of characters for the new
# password (digits, uppercase, lowercase, others).
minclass = 4
#
```

Gráfico 3.25: políticas de contraseñas

Elaborado por: Monserrath Acuña

25. Comprobar los puertos abiertos.

```
[root@evirtual ~]# netstat -lntu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.1.38:53         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp6       0      0 :::3306                 :::*                    LISTEN
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 ::1:53                  :::*                    LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 ::1:953                 :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
udp        0      0 192.168.1.38:53         0.0.0.0:*
udp        0      0 127.0.0.1:53            0.0.0.0:*
udp6       0      0 ::1:53                  :::*
udp6       0      0 fe80::a00:27ff:fefb:546 :::*
```

Gráfico 3.26: Puertos abiertos

Elaborado por: Monserrath Acuña

26. Descargar el archivo comprimido de Moodle.

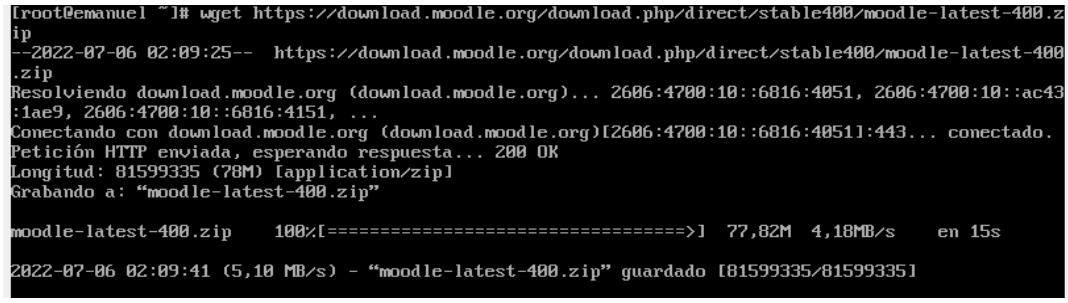


Gráfico 3.27: Archivo comprimido Moodle

Elaborado por: Monserrath Acuña

27. Descomprimir el archivo y mover la carpeta a la ruta /var/www/html.

Gráfico 3.28: Descomprimir archivo

Elaborado por: Monserrath Acuña

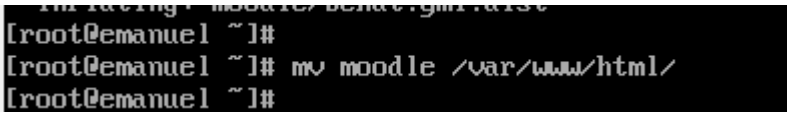


Gráfico 3.29: Mover la carpeta

Elaborado por: Monserrath Acuña

28. Ingresar a un navegador para comenzar con la configuración de Moodle.

Grafico 3.30: Escoger el idioma de Moodle

Elaborado por: Monserrath Acuña

29. Crear el archivo moodledata y dar los permisos al usuario apache.

```
[root@emanuel www]# mkdir moodledata
[root@emanuel www]# ll
total 4
drwxr-xr-x 2 root   root      6 jun 22 06:26 cgi-bin
drwxr-xr-x 6 apache apache 4096 jul  6 02:24 html
drwxr-x--- 2 root   root      6 jul  6 02:24 moodledata
[root@emanuel www]# chown apache:apache moodledata/
[root@emanuel www]#
```

Gráfico 3.31: Creación del archivo moodledata

Elaborado por: Monserrath Acuña

30. Confirmar las rutas en donde se va a instalar Moodle.

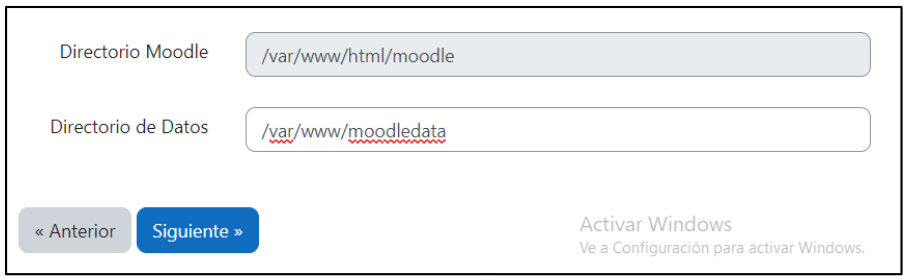


Gráfico 3.32: Confirmación de rutas

Elaborado por: Monserrath Acuña

31. Elegir el motor de base de datos que se va a utilizar.

Gráfico 3.33: Motor de base de datos

Elaborado por: Monserrath Acuña

32. Configurar la base de datos en donde se almacenará toda la información.

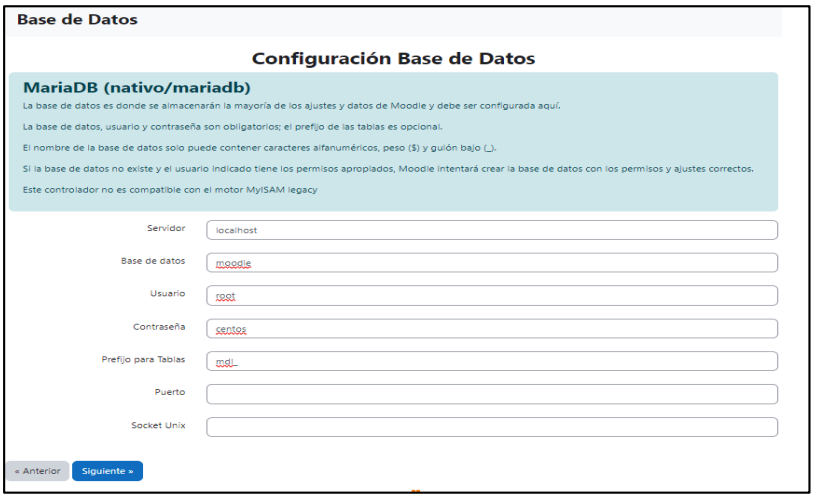


Gráfico 3.34: Configuración base de datos

Elaborado por: Monserrath Acuña

33. Configurar la información del usuario que va a administrar la base de datos.

Gráfico 3.35: Información administrador

Elaborado por: Monserrath Acuña

34. Configurar los ajustes de la página principal.

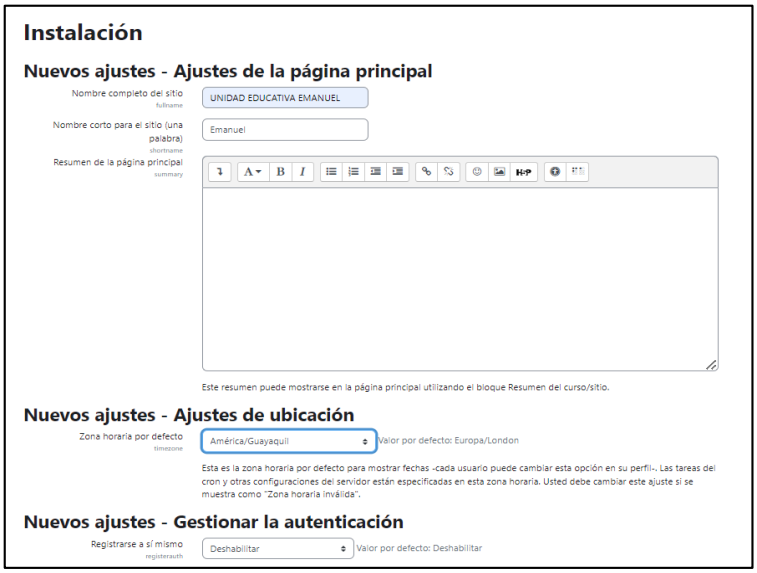


Gráfico 3.36: Página principal

Elaborado por: Monserrath Acuña

35. Ajustar la apariencia según los requerimientos de la Institución.

Gráfico 3.37: Apariencia

Elaborado por: Monserrath Acuña

36. Ingresar a los docentes y estudiantes de la Unidad Educativa Emanuel.

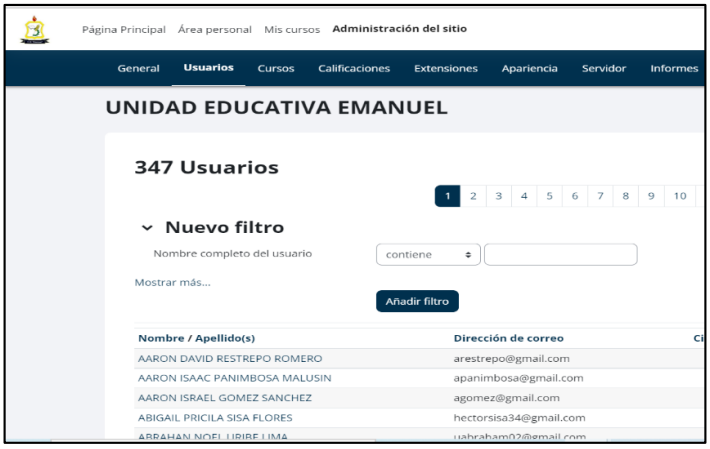


Gráfico 3.38: Ingreso de usuarios

Elaborado por: Monserrath Acuña

37. Crear los cursos correspondientes.

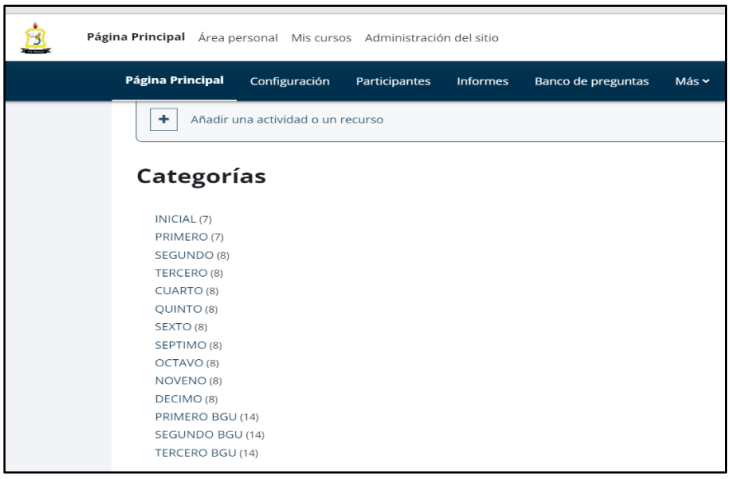


Gráfico 3.39: Creación de los cursos

Elaborado por: Monserrath Acuña

38. Realizar un respaldo de toda la base de datos.

```
[root@emanuel ~]# mysqldump -u root -p --all-databases --lock-all-tables --events > mysql_dump.sql
Enter password:
[root@emanuel ~]# ll
total 103220
-rw-------. 1 root root     2249 jul  5 00:09 anaconda-ks.cfg
-rw-r-----  1 root root 21941005 may 25 00:00 latest-es_EC.tar.gz
-rw-r-----  1 root root 81599335 jul  1 05:28 moodle-latest-400.zip
-rw-r-----  1 root root  2149206 jul  9 23:14 mysql_dump.sql
```

Gráfico 3.40: Respaldo base de datos

Elaborado por: Monserrath Acuña

39. Sacar una copia de seguridad de Moodle para evitar la pérdida de información en caso de que ocurra una contingencia.

En caso de ocurra una contingencia se debe sacar copias de seguridad diariamente para poder recuperar los datos de forma fácil y tener mejor disponibilidad de la información.

El impacto puede ser menor cuando se cuenta con un servidor de réplica.

Un sistema con Moodle se compone de tres partes [24] :

- Los datos almacenados en la base de datos
- Los archivos cargados (archivos del sitio, cursos)
- El Moodle code

La base de datos y los archivos cargados son los más importantes ya que contienen la información que cambiara más a menudo. El Moodle code es menos importante ya que solo cambiará cuando el código real cambie con las actualizaciones.

40. Crear una tarea programada para que diariamente se genere una copia de seguridad y se almacene en otro servidor y generar una réplica del mismo.

Esta tarea sacará un respaldo todos los dias a las 23:59 porque constantemente se estará subiendo y bajando información de la plataforma.

```
59 23    * * *  rsync -avz root@192.168.1.38:/var/www/html/moodle /var/www/html
59 23    * * *  rsync -avz root@192.168.1.38:/var/www/moodledata  /var/www
59 23    * * *  rsync -avz root@192.168.1.38:/root/moodle-latest-400.zip /root
~
```

Gráfico 3.41: Tarea Programada

Elaborado por: Monserrath Acuña

3.2.5. Ejecución del Plan de Recuperación

En caso de que ocurra un ataque o daño en el servidor principal se debe hacer lo siguiente para poder restaurar el servidor:

- El líder del equipo de crisis debe activar el plan de continuidad del negocio.
- Informar a los responsables del equipo de recuperación sobre el servidor de réplica para poner en marcha la utilización del mismo.
- Se debe tomar en cuenta los tiempos máximos de recuperación dependiendo del tipo de riesgo que ocurra.
- Ingresar al servidor de réplica y ver la última copia de seguridad que se ha generado.
- Restaurar los archivos php, base de datos y archivos de datos.
- Si se ejecuta Mysql el respaldo de la base de datos debe estar en un archivo.tar.gz, es necesario extraerlo hasta que sea un archivo con extensión .sql.
- Si ya se está ejecutando mysql mover el archivo SQL en una nueva base de datos en el servidor de réplica.
- Cambiar el archivo config.php para conectarse a esta nueva base de datos (de esta manera usted todavía tiene la base de datos original.
- Levantar los servicios de http y mariadb para que pueda seguir funcionando correctamente la plataforma.
- Notificar a los usuarios que por seguridad deben cambiar de contraseñas.
- Comprobar que la recuperación de la información de los usuarios sea correcta.
- Revisar las políticas de seguridad existentes en el servidor.
- Asegurarse de quien tiene los permisos de acceso al servidor web y la base de datos para evitar la pérdida de información.
- Verificar que el servidor este actualizado a la versión más reciente para maximizar la información.
- Revisar el código y asegúrese de no añadir ninguna vulnerabilidad.

3.2.5.1 Restauración de una máquina virtual

Otra forma de tener un respaldo del servidor es sacando una copia de seguridad de toda la máquina virtual para eso se debe hacer lo siguiente:

1. Ingresar a la parte de archivo y escoger la opción de exportar servicio virtualizado.

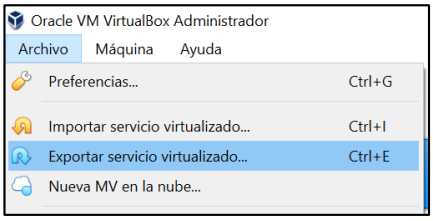


Gráfico 3.42: Exportar servicio virtualizado

Elaborado por: Monserrath Acuña

2. Se creará un archivo. ova en donde se almacenará todos los archivos configurados en la máquina virtual.

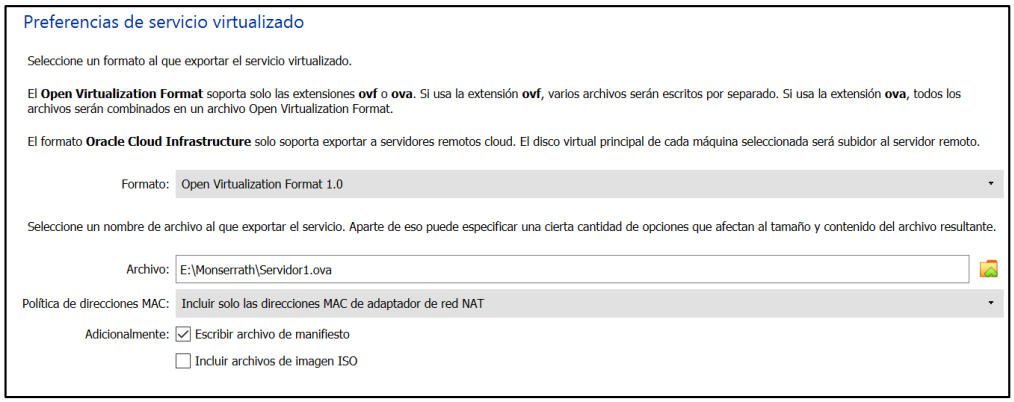


Gráfico 3.43: Preferencias de servicio virtualizado

Elaborado por: Monserrath Acuña

3. Se mostrará toda la información que se va a guardar.

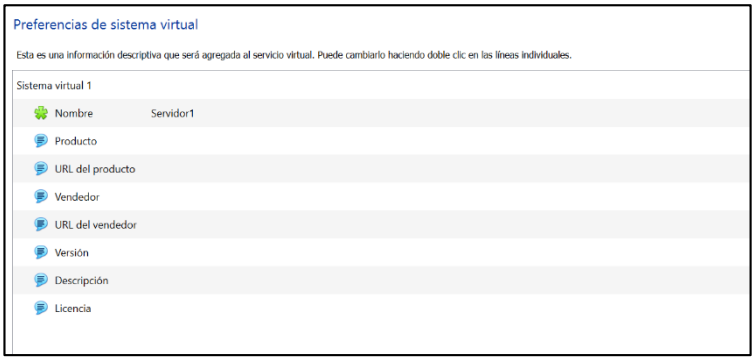


Gráfico 3.43: Preferencias de sistema virtual

Elaborado por: Monserrath Acuña

4. Seleccione exportar y se guardara en donde se escogió anteriormente.

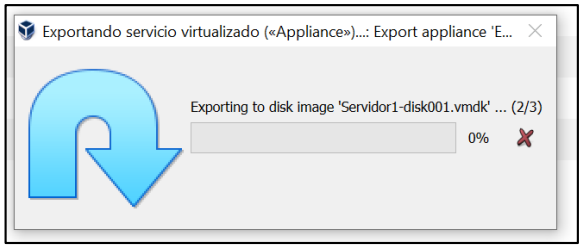


Gráfico 3.44: Exportando servicio virtualizado

Elaborado por: Monserrath Acuña

5. Para poder restaurar la máquina virtual se tiene que escoger la opción de importar y seleccionar la ova ya creada a si ya se tendrá la máquina virtual con todos los datos guardados en la misma.

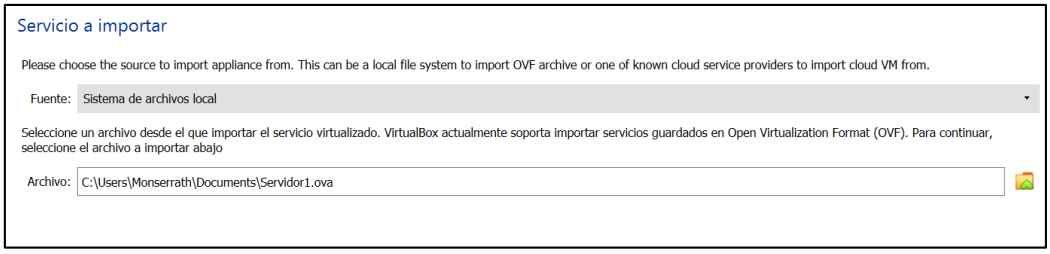


Gráfico 3.45: Servicio de importar

Elaborado por: Monserrath Acuña

CAPITULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

- Se analizó que por medio de la metodología de continuidad BCM se ha identificado los riesgos que se pueden presentar en la unidad educativa al momento de implementar una plataforma virtual Moodle, el cual se puede dar solución a cualquier tipo de incidente reduciendo impactos y minimizando riesgos para que pueda tener un buen funcionamiento.

- Tener claros los objetivos del plan de continuidad del negocio con el fin de llegar a determina los factores críticos, y así cumplir con las estrategias para que la plataforma virtual siga operando con éxito y estar prevenido ante cualquier evento negativo para evitar la pérdida de información.

- Con la aplicación de políticas de seguridad en la información cualquier tipo de amenaza puede ser mitigada y se pueda mantener la integridad y confidencialidad de la información.

4.2. Recomendaciones

- Realizar una capacitación al personal administrativo y de tecnología para que cada uno pueda asumir sus roles y responsabilidades en caso de eventos no previstos de interrupción con la finalidad de garantizar la continuidad de la plataforma virtual Moodle.

- Evaluar periódicamente el BCM para mantener actualizado y en mejora continua, para que la plataforma siga funcionando correctamente.

- Realizar pruebas periódicas y restauración de la información para comprobar el correcto funcionamiento de la plataforma y evitar la pérdida de la misma.

- Se recomienda la participación de todo el personal administrativo y de tecnología quienes deciden las prioridades, los procesos y los recursos involucrados ya que la falta de participación de cualquiera puede hacer fracasar el proyecto.

- Es importante realizar copias de seguridad para recuperar los datos de una forma fácil y rápida después de un desastre, se deben de realizar periódicamente para tener disponibilidad inmediata de la información.

C.MATERIALES DE REFERENCIA

Referencias Bibliográficas

[1] R. Navarro Edel and Y. Navarro Rangel, “Entornos Virtuales de Aprendizaje 2002-2011,” no. September, p. 212, 2015.

[2] “Información y la Comunicación aplicadas a la educación Tecnologías de la.”

[3] K. P. M. Guaman, “Metodologia de evaluacion de riesgos Moodle PUCE Ambato,” vol. 2507, no. February, pp. 1–9, 2020.

[4] J. O. M. García, “Diseño e implementación de un Aula Virtual del Moodle, para fortalecer el proceso de enseñanza aprendizaje en la Unidad Educativa Pablo Hannibal Vela de la ciudad de Portoviejo,” 2017.

[5] I. Z. Ada Herrera, Laura Ocaña, Jackelin Palomino, “Plan de negocio para la implementacion de una plataforma virtual de clases academicas particulares,” *J. Mater. Process. Technol.*, vol. 1, no. 1, pp. 1–8, 2018.

[6] “ISO 22301 Plan de Continuidad de negocio | GSS.” https://www.globalsuitesolutions.com/ec/continuidad-negocio-iso-22301/?gclid=CjwKCAiAxJSPBhAoEiwAeO_fP-TEixfelQZd4nrUc0shRJ1LEVsI4PWQHI57Euv37X9YbrPliIYaUBoCZYgQAvD_BwE (accessed Jan. 17, 2022).

[7] R. Ferrer, “Metodología para la Gestión de la Continuidad del Negocio.”

[8] “BCM Gestión de continuidad de negocio | ACSE.” https://www.acseteruel.com/servicios-bcm-estion-de-continuidad-de-negocio/ (accessed May 31, 2022).

[9] “¿Qué es la plataforma Moodle y para qué sirve? | Maxima Formacion.” https://www.maximaformacion.es/e-learn/que-es-moodle-y-para-que-sirve/ (accessed Jul. 05, 2021).

[10] “Hardering, qué es | Blog SEAS.” https://www.seas.es/blog/informatica/hardening-que-es-y-como-endurecer-las-medidas-de-seguridad-informaticas/ (accessed Jan. 17, 2022).

[11] “Servicios Informáticos: funciones y beneficios - Tuyú Technology.” https://www.tuyu.es/servicios-informaticos-funciones-beneficios/ (accessed Jun. 08, 2022).

[12] “Amenazas a la Seguridad de la Información | Departamento de Seguridad Informática.” http://www.seguridadinformatica.unlu.edu.ar/?q=node/12 (accessed Jun. 08, 2022).

[13] “Qué es una vulnerabilidad informática - Banco Santander.” https://www.bancosantander.es/glosario/vulnerabilidad-informatica (accessed Jun. 08, 2022).

[14] “Políticas de seguridad informática, ¿qué son? | UNIR.” https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/ (accessed Aug. 01, 2022).

[15] “35/Instalación de Moodle - MoodleDocs.” https://docs.moodle.org/all/es/35/Instalación_de_Moodle#Hardware (accessed Jul. 17, 2022).

[16] “Requerimientos de Hardware para Servidor de Moodle | PDF | Moodle | Servidor web.” https://es.scribd.com/document/317483191/Requerimientos-de-Hardware-Para-Servidor-de-Moodle (accessed Jul. 22, 2022).

[17] “Recomendaciones sobre desempeño - MoodleDocs.” https://docs.moodle.org/all/es/Recomendaciones_sobre_desempeño#Configuraci.C3.B3n_del_hardware (accessed Jul. 17, 2022).

[18] F. Y. Revisiones, “PLAN DE CONTINUIDAD DEL NEGOCIO BCP CONTROL DE CAMBIOS NOMBRE VERSIÓN AUTOR FECHA PLAN DE CONTINUIDAD DEL NEGOCIO BCP 1.0 Oficina de Sistemas e,” 2018.

[19] “Guía para el ‘endurecimiento’ de los sistemas y la reducción de los riesgos informáticos.” https://www.ninjaone.com/es/blog/complete-guide-to-systems-hardening-in-2022/ (accessed May 31, 2022).

[20] “Stakeholders: quiénes son, por qué son importantes y cómo gestionarlos.” https://www.iebschool.com/blog/stakeholders-quienes-son-digital-business/ (accessed Jul. 24, 2022).

[21] “AlmaLinux: todo sobre el sistema operativo - IONOS.” https://www.ionos.es/digitalguide/servidores/configuracion/almalinux-que-ofrece-la-nueva-distribucion-de-linux/ (accessed Jul. 18, 2022).

[22] “Guide to the Secure Configuration of Red Hat Enterprise Linux 8 | OpenSCAP Security Guide.” https://static.open-scap.org/ssg-guides/ssg-rhel8-guide-anssi_bp28_minimal.html (accessed Aug. 01, 2022).

[23] “Guide to the Secure Configuration of Oracle Linux 7 | OpenSCAP Security Guide.” http://static.open-scap.org/ssg-guides/ssg-ol7-guide-anssi_nt28_enhanced.html (accessed Aug. 03, 2022).

[24] “Respaldo del sitio - MoodleDocs.” https://docs.moodle.org/all/es/Respaldo_del_sitio (accessed Jul. 10, 2022).

Anexos

A.1 Encuesta aplicada a los docentes

1. **¿Conoce de la existencia de un entorno virtual que da soporte al proceso enseñanza aprendizaje?**

SI ☐ NO ☐

2. **¿Estaría usted de acuerdo con la implementación de un aula virtual en su unidad educativa?**

SI ☐ NO ☐

3. **¿La unidad educativa cuenta con un servicio de internet estable?**

SI ☐ NO ☐

4. **¿Cree necesario capacitar a los docentes en creación y manejo de aulas virtuales?**

SI ☐ NO ☐

5. **¿Los recursos tecnológicos que el instituto ofrece (internet, computadoras, software) son suficientes y correctos para el aprendizaje virtual?**

MUCHO ☐ MUY POCO ☐ NADA ☐

6. **¿Considera usted que Moodle al ser una plataforma libre también le asegura estabilidad?**

MUCHO ☐ MUY POCO ☐ NADA ☐

7. **¿Le parece bien tener la opción de recuperación de contraseña por medio del uso de correo electrónico le da un beneficio adicional en el caso de olvido de contraseña?**

SI ☐ NO ☐

8. **¿Ha tenido algún tipo de afectación a la infraestructura tecnológica?**

SI ☐ NO ☐

A.2 Encuesta aplicada al personal administrativo y de tecnología

1. **¿Tiene usted conocimiento de la metodología que se usa en un aula virtual?**

MUCHO ☐ MUY POCO ☐ NADA ☐

2. **¿Considera que es necesario la implementación de un aula virtual?**

SI ☐ NO ☐

3. **¿Ha tenido alguna experiencia con el uso de algún entorno virtual?**

MUCHO ☐ MUY POCO ☐ NADA ☐

4. **¿La institución cuenta con el hardware necesario para la instalación de una plataforma virtual?**

SI ☐ NO ☐

5. **¿Considera que la implementación de un entorno virtual en la institución es una buena inversión?**

SI ☐ NO ☐

6. **¿Tiene una persona capacitada para el manejo administrativo del entorno virtual Moodle?**

SI ☐ NO ☐

7. **¿Cree que es necesario que el sistema sugiera el cambio de contraseña periódicamente, utilizando estándares de seguridad de contraseñas?**

SI ☐ NO ☐

8. **¿Tienen la capacidad económica para la adquisición de un Hosting y Dominio para la implementación de un entorno virtual?**

SI ☐ NO ☐

9. **¿Cree que es necesario implementar un conjunto de buenas prácticas de seguridad para la información de las actividades académicas virtuales, elaborada a partir de recomendaciones, normativas y estándares?**

MUCHO ☐ MUY POCO ☐ NADA ☐

10. **¿Cuál cree usted que es la principal amenaza a la que puede estar expuesto una plataforma virtual?**

ATAQUES EXTERNOS ☐ ERRORES HUMANOS ☐ DESASTRES NATURALES ☐

11. **¿Cree usted que es prudente realizar copias de seguridad frecuentemente en una plataforma virtual?**

SI ☐ NO ☐