



Pontificia Universidad  
Católica del Ecuador | Sede  
Ambato

**UNIDAD ACADÉMICA**  
OFICINA DE POSTGRADOS

**TEMA:**

METODOLOGÍA DE EVALUACIÓN DE RIESGOS MOODLE PUCE AMBATO

**Proyecto de Investigación previo a la obtención del título de  
Magister en Gerencia Informática**

**Línea de Investigación, Innovación y Desarrollo principal:**

Sistemas de Información y/o Nuevas Tecnologías de la Información y  
Comunicación y sus aplicaciones.

**Caracterización técnica del trabajo:**

Desarrollo

**Autor:**

Ing. Klever Patricio Morales Guamán Mg.

**Director:**

Ing. José Marcelo Balseca Manzano Mg.

Ambato – Ecuador

Diciembre 2020

# METODOLOGÍA DE EVALUACIÓN DE RIESGOS MOODLE

## PUCE AMBATO

Informe de trabajo de titulación  
presentado ante la  
Pontificia Universidad Católica del  
Ecuador Sede Ambato por

Ing. Klever Patricio Morales Guamán Mg.

En cumplimiento parcial de los  
requisitos para el Grado de  
Magister en Gerencia  
Informática.



**Oficina de Postgrados**  
Diciembre 2020

# METODOLOGÍA DE EVALUACIÓN DE RIESGOS MOODLE PUCE AMBATO

Aprobado por:



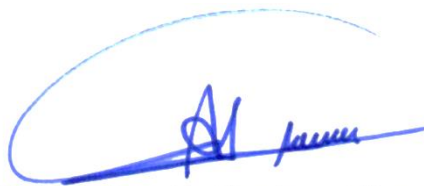
Juan Carlos Acosta Teneda, MSc.  
Presidente del Comité Calificador  
Coordinador de la Oficina de Postgrados



Ing. Galo Mauricio López Sevilla, Mg.  
Miembro Calificador



Ing. José Marcelo Balseca Manzano, Mg.  
Miembro Calificador  
Director de Proyecto



Dr. Hugo Rogelio Altamirano Villarroel, Mg.  
Secretario General



Ing. Santiago Alejandro Acurio Maldonado, Mg.  
Miembro Calificador

Fecha de Aprobación:

## **Ficha Técnica**

**Programa:** Magister en Gerencia Informática

**Tema:** Metodología de evaluación de riesgos MOODLE PUCE Ambato

**Tipo de trabajo:** Proyecto de Investigación y Desarrollo

**Clasificación Técnica del Trabajo:** Desarrollo

**Autor:** Klever Patricio Morales Guamán

**Director:** José Marcelo Balseca Manzano, Ing. Mg.

### **Líneas de Investigación, Innovación y Desarrollo**

Principal: Sistema de Información y/o Nuevas tecnología de la información y comunicación y sus aplicaciones

### **Resumen Ejecutivo**

El problema en sí radica en las frecuentes y comunes caídas de la plataforma, pérdidas de recursos, alteración de contenidos, substracción de medios y contenidos, entre otros debido a la falta de una metodología de evaluación de riesgos para plataformas Moodle que sirva de referencia de actuación ante un evento o ataque producido por internos o externos a la organización.

La forma de gestión y administración de plataformas de educación virtual en instituciones de Educación Superior se desarrolla con conocimientos básicos y hasta empíricos, no se cuenta con el respaldo de una metodología de evaluación de riesgos con lineamientos claros que permita brindar oportuna gestión en un posible evento, lo que ocasiona varios problemas en procesos estratégicos, tecnológicos y hasta financieros institucionales.

Para la PUCE Ambato en la actualidad es necesario contar con una metodología de evaluación de riesgos para su plataforma Moodle cargada en la nube que guíen y se conviertan en un marco de referencia, guía de apoyo y mediante la segmentación de procesos se pueda administrar de manera más efectiva al riesgo que enfrenta la administración de Plataformas Moodle, garantiza así operatividad 24-7, incrementa el control sobre los eventos o amenazas, que se activarían, permite a través de la plataforma aportar a la consecución de objetivos institucionales que apoye el desarrollo académico con recursos y medios a disposición de los usuarios, se logra así incrementar la solución a los problemas de tiempo y espacio, desarrolla interacción entre los participantes del proceso educativo y mejorar la calidad de los servicios educativos brindados a los usuarios por parte de la institución.

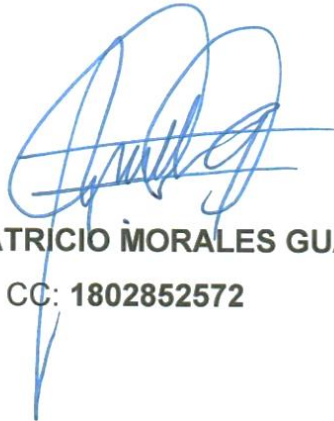
Palabras Clave: ISO 27017, Cloud, AWS, Metodología, Riesgos, ITIL

## Declaración y Autorización

Yo: **Klever Patricio Morales Guamán**, con CC. **1802852572**, autor del trabajo de graduación intitulado: “Metodología de Evaluación De Riesgos MOODLE PUCE Ambato”, previa a la obtención del título profesional de **Magister en Gerencia Informática**, en la Oficina de **Postgrados**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través de sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, diciembre 2020



**KLEVER PATRICIO MORALES GUAMÁN**

CC: **1802852572**

## **Dedicatoria**

*A mis padres Pedro y Victorita.*

## **Reconocimientos**

A todos los distinguidos docentes que aportaron para mi formación y perfeccionamiento profesional, de manera especial al Ing. Mg. Marcelo Balseca que con su calidad personal y orientación metodológica permitió que avance en el trabajo y culmine satisfactoriamente esta etapa estudiantil.

Un agradecimiento a los ingenieros revisores y a todo el personal que de forma directa o indirectamente contribuyeron a que este trabajo de investigación se pudiera llevar a cabo y aprobar.

Finalmente, deseo agradecer a un gran ser humano que conocí como compañero de la maestría y que me brindó su amistad y permanente apoyo, al Ing. Mg. Gabriel Altamirano Ibarra.

## Resumen

El permanente y vertiginoso avance tecnológico en el que convivimos genera la necesidad en las instituciones educativas que incursionen en la utilización de herramientas informáticas para complementar, brindar un valor adicional o potencializar a su oferta académica, lo cual, conlleva la configuración de infraestructura para plataformas de educación virtual como alternativa eficiente al requerimiento.

Sin embargo, la implementación de este tipo de servicios conlleva a que los Departamentos de Tecnologías de la Información y Comunicaciones (DTIC) en las instituciones educativas realicen una planificación alineada a los objetivos institucionales, que considere todos los elementos críticos a superar, entre ellos prever eventos o amenazas que generen riesgos para la entrega del servicio.

Con este antecedente, esta investigación se enfoca en estudiar los elementos inherentes a los riesgos en las plataformas Moodle, así como, también, Cloud Computing que es la tecnología utilizada para hospedar a la plataforma, se realiza un análisis situacional donde se utiliza la Norma ISO 27017:2015 que es la encargada de evaluar riesgos en Cloud, se desarrolla un análisis basado en las mejores prácticas de los marcos de referencia *Information Technology Infrastructure Library* (ITIL) para la gestión administrativa entre la DTI de la PUCE Ambato e IT Era que provee del servicio cloud al ser partner certificado de *Amazon Web Services* (AWS); estudio que permite construir y proponer una metodología para evaluar los riesgos que incurra la plataforma Moodle sobre una nube privada.

**Palabras Clave:** ISO 27017, Cloud, AWS, Metodología, Riesgos, ITIL

## **Abstract**

The permanent and vertiginous technological advance in which society develops generates the need in the educational institutions to incur in the use of computer tools. Therefore, it complements and provides an additional value to education. In addition, it enhances their academic offerings, which leads to the implementation of virtual education platforms as an efficient alternative. Therefore, the implementation of this type of services leads to the Departments of Information Technology and Communications (DTIC) in educational institutions to make a planning aligned with institutional objectives. These consider all the critical elements to be overcome, among them, anticipating events or threats that generate risks in the delivery of the service. Currently, the management and administration of the virtual education platform is done with basic knowledge for its implementation. However, risk management is not considered a transversal element of the project. Consequently, it leads to incidents or problems generated by its non-observance. With this background, the research is focused on studying the elements inherent to risks in Moodle and Cloud Computing platforms, which is the technology used to host the platform. A situational analysis based on the ISO 27017:2015 standard will be carried out, which evaluates risks in the Cloud. Also, an analysis based on the best practices of the Information Technology Infrastructure Library (ITIL) reference frameworks for the administrative management between PUCE Ambato's DITIC and TI Era, which provides the cloud service, as it is an authorized distributor of Amazon Web Services (AWS). In conclusion, the study allows us to build and propose a methodology that assesses the risks incurred by the Moodle platform on a private cloud.

**Keywords:** ISO 27017, Cloud, AWS, Methodology, Risks, ITIL

## Tabla de Contenidos

Ficha Técnica .....	iii
Declaración y Autorización .....	iv
Dedicatoria .....	v
Reconocimientos .....	vi
Resumen .....	vii
Abstract .....	viii
Tabla de Contenidos .....	ix
Lista de tablas .....	xii
Lista de gráficos .....	xiv
INTRODUCCIÓN .....	1
Antecedentes teóricos y prácticos .....	2
Situación problemática .....	4
Planteamiento del problema .....	5
Idea a defender .....	5
Objetivos de la investigación .....	5
Objetivo general .....	5
Objetivos específicos .....	6
Metodología .....	6
Justificación de la investigación .....	6
Capítulo I .....	8
Marco Teórico .....	8
1.1 Definición y conceptos .....	8
1.1.1. Plataformas virtuales .....	8
1.1.2. Tipos de plataformas E-Learning .....	9

1.1.3. Software como Servicio (SaaS).....	18
1.1.4. Plataforma como Servicio (PaaS).....	18
1.1.5. Infraestructura como Servicio (IaaS) .....	19
1.1.6. Seguridad informática.....	19
1.1.7. Metodologías existentes.....	24
Capítulo II.....	27
Metodología.....	27
2.1. Tipo de Investigación y Enfoque de investigación.....	27
2.1.1. Tipo de Investigación.....	27
2.1.2. Enfoque de la investigación .....	28
2.1.3. Tipo de recolección de la información .....	28
• Fuentes Primarias .....	28
• Fuentes secundarias .....	29
• Método deductivo .....	29
• Técnicas.....	30
• Instrumentos .....	30
2.1.4. Análisis de la información sobre el diagnóstico realizado.....	30
2.2. Caracterización de la empresa o institución.....	31
2.2.2 Arquitectura funcional PUCESA – ITERA - AWS .....	37
2.2.1. Análisis de las variables que actúan en Moodle sobre una nube.....	44
2.2.3 Arquitectura Moodle de alta disponibilidad .....	45
2.3. Propuesta de la Investigación .....	51
2.4. Metodología de Evaluación de Riesgos para Plataformas Moodle .....	53
2.4.1. Introducción .....	54
2.4.2. Objetivo metodológico .....	56

2.4.3. Objeto .....	56
2.4.4. Alcance.....	57
2.4.5. Documentos Recomendados.....	57
2.4.6. Desarrollo de las fases de la metodología para evaluación del riesgo ..	58
2.4.6.1. Fase I. Identificación de activos de información de Moodle .....	58
2.4.6.2. Fase II. Determinación de las amenazas, vulnerabilidades e impactos sobre los activos relacionados .....	59
2.4.6.3. Fase III. Análisis del riesgo y del impacto.....	61
2.4.6.4. Fase IV. Gestión de riesgos .....	67
Capítulo III.....	71
Análisis de los resultados de la investigación.....	71
3.1 FASE I. Identificación de activos de información de Moodle.....	71
de la PUCE AMBATO .....	71
Virtual Private Cloud.....	76
3.2. FASE II Determinación de las amenazas, vulnerabilidades e impactos sobre los activos relacionados .....	77
3.2.4. Evaluación de las amenazas.....	88
3.2.5. Evaluación de vulnerabilidades .....	90
3.3. FASE III Análisis del riesgo e impacto.....	92
3.3.1. Calificación del riesgo.....	92
3.4. FASE IV Gestión de riesgos.....	93
Conclusiones.....	95
Recomendaciones.....	96
Bibliografía .....	98
ANEXOS .....	107

## Lista de tablas

Tabla N° 1: Comparación entre plataformas educativas .....	10
Tabla N° 2: Niveles de seguridad Moodle .....	20
Tabla N° 3: Áreas de control de una Matriz de Control de Nube (CCM) .....	23
Tabla N° 4. Recolección de información .....	31
Tabla No. 5 Créditos por servicio AWS .....	38
Tabla N° 6: Calificación valorativa de la amenaza .....	60
Tabla N° 7: Calificación valorativa de la vulnerabilidad .....	61
Tabla N° 8: Caracterización valorativa del riesgo.....	65
Tabla N° 9: Calificación del Impacto.....	66
Tabla N° 10: Calificación crítico de los niveles de riesgos .....	66
Tabla N° 11: Plan de acción para minimizar el riesgo.....	67
Tabla N° 12: Componentes de control interno .....	69
Tabla N° 13: Servicios AWS Certificados ISO/IEC 27017:2015 .....	74
Tabla N° 14. Identificación de los recursos AWS implementados en la arquitectura Cloud [AWS-PUCESA].....	75
Tabla N° 15. Descripción de los recursos críticos AWS implementados certificados ISO 27017 .....	76
Tabla N° 16: Análisis de la situación actual de la nube privada [AWS-PUCESA] .	78
Tabla N° 17. Tiempos de 1era. Respuesta .....	83
Tabla N° 18. Solicitudes de soporte de 2do. nivel .....	84
Tabla N° 19. Soporte y Servicio IT Era.....	84
Tabla N° 20 Reglas de Supresión a Amenazas detectadas .....	86
Tabla N° 21: Análisis descriptivo de amenaza .....	89
Tabla N° 22: Valor crítico de la amenaza .....	89

Tabla N° 23: Análisis descriptivo de las vulnerabilidades.....	91
Tabla N° 24: Calificación valorativa de la vulnerabilidad .....	91
Tabla N° 25: Calificación crítico de los riesgos Moodle en nubes privadas.....	92
Tabla N° 26: valoración del Impacto.....	92
Tabla N° 27: Plan de acción para minimizar el riesgo .....	93

## Lista de gráficos

Gráfico N° 1: Estructura orgánica funcional de la PUCE Ambato .....	32
Gráfico N° 2: Orgánico Estructural DTI PUCE Ambato .....	33
Gráfico N° 3: Estructura PUCESA – ITERA - AWS .....	37
Gráfico N° 4: Arquitectura Moodle de Alta Disponibilidad .....	45
Gráfico N° 5: Diseño de fases y procesos de la nueva metodología de evaluación de riesgos.....	52
Gráfico N° 6: Relación causa efecto entre activos .....	61
Gráfico N° 7: Ciclo de Vida del Servicio según ITIL .....	64
Gráfico N° 8: Resultados del Cloud Security Alliance .....	79
Gráfico N° 9: Análisis del desarrollo filosófico de ITIL.....	80
Gráfico N° 10: Evaluación de amenazas.....	88
Gráfico N° 11: Valoración de las oportunidades.....	90

## Lista de imágenes

Imagen No.1 Pantalla de acceso.....	39
Imagen No.2 Análisis de seguridad.....	40
Imagen No.3 Análisis de rendimiento.....	41
Imagen No.4 Análisis de tecnologías utilizadas .....	42
Imagen No.5 Análisis de construcción de marca.....	43
Imagen No.6 Análisis de disponibilidad de dominios.....	43

# INTRODUCCIÓN

En la actualidad existen diferentes maneras que permiten expandir los conocimientos de profesionales y no profesionales, el conocimiento y aprendizaje hoy en día son beneficiarios de los progresos tecnológicos, mediante la creación de plataformas *E-learning*, la realidad virtual, la educación en teléfonos inteligentes, inteligencia artificial, entre otros avances tecnológicos incorporados en los procesos formativos con la utilización de las Tecnologías de la Información y la Comunicación (TICs) que las instituciones educativas han optado por implementar y fortalecer su oferta académica. La sociedad de mercados competitivos que actualmente, se presenta en la comunidad impulsa a profesionales y no profesionales en adquirir o actualizar sus conocimientos que poseen mediante la educación a distancia o virtual, esto ha llevado a las instituciones de educación pública y privadas a adquirir o implementar su campus virtual para fortalecer su oferta y calidad académica.

Como resultado a lo expuesto anteriormente, se crea la necesidad en las universidades de implementar plataformas de educación virtual como la oportunidad de brindar el soporte efectivo en el proceso de enseñanza-aprendizaje, educación continua y educación a distancia, las plataformas garantizarán la seguridad de la información, así como, también, prestar la garantía de continuidad del servicio ofertado.

Cabe señalar que en el progreso del presente trabajo de investigación, se presentan varios fundamentos teóricos indispensables para el desarrollo del estudio, mismo que evidencia que en la actualidad la mayor parte de toda la información generada por la universidad como en la empresa, se sustenta en procesos automatizados a través de la intervención de las TICs, debido a este motivo la tendencia o la necesidad de advertir riesgos o amenazas para establecer controles y estrategias para atenuar o minimizar dichos peligros.

Es el caso de la Pontificia Universidad Católica del Ecuador Ambato (PUCE Ambato) con la colaboración del Departamento de Tecnología de la Información (DTI), los cuales han integrado el uso de la plataforma Moodle, sin embargo, este tipo de tecnologías requiere procesos metodológicos implementados que logren identificar distintos factores de riesgo como: amenazas, vulnerabilidades y ataques que afectarían al funcionamiento del sistema, provoca dificultad, inconformidad y hasta molestia en los usuarios de la plataforma *e-learning*.

El objetivo principal de E-Learning Virtual (VLE) es proporcionar el aprendizaje electrónico de forma eficiente a un gran número de comunidades estudiantiles para proporcionar el ambiente ideal en el aula virtual. Hay muchos términos que son muy similares al entorno de aprendizaje virtual. Son el sistema de gestión de aprendizaje (LMS), el sistema de gestión de contenido (CMS), el aprendizaje sistema de gestión de contenido (LCMS), entorno de aprendizaje gestionado (MLE), aprendizaje sistema de soporte (LSS), centro de aprendizaje en línea (OLC), software de curso abierto (OCW), plataforma de aprendizaje (LP). El entorno de aprendizaje virtual básicamente funciona con la ayuda de internet, abastece de los materiales y herramientas de aprendizaje a los usuarios de *e-learning* para realizar actividades como el cargar archivos, chatear, acceder a conferencias web, entre otras. También, brinda información sobre los sistemas de gestión de grupos de usuarios.

El presente trabajo de investigación persigue su principal objetivo, en el cual, se propone el diseño de una metodología de evaluación de riesgos para la plataforma Moodle de la PUCE Ambato, los rasgos que abarca la metodología de riesgos que, se propone en el estudio abarca temas de: Gestión de seguridad, eficiencia y confianza para los usuarios.

### **Antecedentes teóricos y prácticos**

Moodle, se considera un programa aplicativo para instituciones de educación públicas, privadas, y mixtas, considerado como un software de código abierto, que

permite tener los beneficios y optimización de recursos. Los gerentes no tienen que preocuparse por honorarios de licencia, y no enfrentan requisitos para contratar a alguien de una empresa para realizar actualizaciones, la capacitación no es problema porque es una aplicación simple y fácil de utilizar, etcétera. Los altos costos y permanentes actualizaciones son condiciones que han obligado a muchas empresas e instituciones a rescindir los productos de licencia, pero eso no ha sido un problema para el software de código abierto (Carneiro, Toscano, C., & Tamara, 2013).

Moodle es una aplicación a la que, se accede por medio de un navegador web o browser Mozilla Firefox, Microsoft Internet Explorer, Google Chrome, Safari, Opera entre otros. Esto significa que para utilizar Moodle, se necesita un computador con un navegador web instalado y con conexión a Internet. Por supuesto, también, se necesita conocer la dirección web del servidor donde Moodle, se encuentre alojado; además, dicha aplicación utiliza un interfaz fácil e intuitivo con el que resulta sencillo familiarizarse rápidamente. Por lo general la información más relevante es mostrada en el centro de la pantalla mientras que a la izquierda y a la derecha, se muestran los llamados bloques de Moodle (Castro E. , 2017).

Al ofrecer cursos de buena calidad e instruir a los usuarios sobre cómo usar Moodle, se los prepara para ambientarse y a desarrollar habilidades necesarias para la gestión académica en la institución educativa. Las herramientas de Moodle son tan diversas que al aprender cómo usarlas de manera efectiva en un entorno académico, desarrollará habilidades que lo llevará a su próximo nivel de formación. Estas habilidades serán útiles si continúa en educación formal o necesita tomar créditos de educación continua o a distancia. Permite desarrollar habilidades web 2.0 el uso de las herramientas que Moodle pone a disposición de los instructores y usuarios en general (Watson, 2018).

Esta es una preocupación realista que todos los instructores y personal de apoyo del departamento de TI de las instituciones u organizaciones, si tienen que

implementar cualquier nuevo software. Sin embargo, existen varios argumentos sólidos por los cuales Moodle es una plataforma de soporte educativo y comercial inteligente para las organizaciones. Por ende, la importancia de evaluar los riesgos oportunamente mediante una metodología adecuada.

### **Situación problemática**

El problema, se evidencia en la gestión que desarrolla el personal de TI encargado de la Plataforma de Educación Virtual Moodle en las Instituciones de Educación Superior (IES), si, se genera problemas que impiden la accesibilidad, gestión de medios y recursos necesarios para el desarrollo de las actividades académicas, lo cual conlleva a la generación de quejas en la entrega del servicio que afecta el prestigio del DTIC, así como, también, a la institución, y al posterior deterioro de la calidad de servicios brindados por la institución.

En muchas universidades e instituciones de educación superior los DTI no cuentan con el efectivo respaldo de la autoridad pertinente para implantar estrategias de seguridad necesarias, así como para destinar recursos definidos para gestionar la seguridad de las plataformas institucionales. (Gómez Á. , 2011).

En estas circunstancias, muchos de los responsables y técnicos realizan estas tareas como actividades adicionales o marginales, se percibe erróneamente que no resulta productiva para la institución.

El problema, se origina por la falta de una metodología de evaluación de riesgos para Plataformas Moodle que sirvan de referencia y actuación ante un evento, complementado con la falta de formación especializada en aspectos de seguridad del personal que trabaja en el departamento de TI en las organizaciones, que desencadena en inconvenientes en los procesos estratégicos institucionales.

El no contar con una metodología de evaluación de riesgos que sirva de marco de referencia para la correcta gestión del riesgo originado en la administración de plataformas Moodle.

### **Planteamiento del problema**

¿De qué manera, se diseñaría una Metodología de Evaluación de Riesgos para Plataformas Moodle?

### **Idea a defender**

La metodología de evaluación de riesgos para plataformas Moodle logrará:

- Servir de marco de referencia para la administración plataformas de educación virtual Moodle.
- Externalizar la evaluación de riesgos en plataformas de educación virtual mediante el servicio de outsourcing.
- Contribuir en la identificación los puntos críticos dentro de las instituciones de educación relacionados a la gestión de riesgos con sus plataformas de educación virtual Moodle.
- Gestionar la información obtenida mediante la metodología de modelo de evaluación, con reportes oportunos y con información íntegra para la toma de decisiones de la dirección de TI.

### **Objetivos de la investigación**

#### **Objetivo general**

Diseñar una Metodología de Evaluación de Riesgos para Plataformas Moodle.

## **Objetivos específicos**

- Fundamentar teóricamente la importancia de la implementación de metodologías de evaluación de riesgos para las plataformas de educación virtual Moodle.
- Diagnosticar la situación actual, necesidades más relevantes y aspectos críticos del departamento de TI de la PUCE Ambato en relación a las metodologías empleadas para identificar oportunamente los riesgos en la administración de plataformas de educación virtual Moodle.
- Desarrollar una metodología de evaluación de riesgos para la administración de la plataforma Moodle de la PUCE Ambato.
- Validar la aplicación y la eficiencia de la metodología de evaluación de riesgos para la plataforma Moodle en el departamento de TI de la PUCE Ambato.

## **Metodología**

La metodología de la investigación, se basa en análisis mixto cualitativo y cuantitativo que, se requiere conocer las cualidades que mantiene el riesgo de la plataforma Moodle; y cuantitativo porque conlleva a un análisis estadístico con frecuencias de los instrumentos aplicados para obtener resultados objetivos, así mismo, se presentará una investigación bibliográfica porque, se requiere indagar los criterios teóricos de los autores que ha realizado estudios similares; y de campo, indagamos la situación actual de la plataforma Moodle; de la PUCE de la ciudad de Ambato.

## **Justificación de la investigación**

La finalidad del presente proyecto, se direcciona en proponer una metodología que permita evaluar los riesgos para la plataforma Moodle de la PUCE Ambato, se parte de que, al ser los proveedores del servicio, se proporcionará controles de seguridad

de la información, controles relacionados al servicio, guías de implementación de advertencias o alertas que contribuyan a mitigar los riesgos que están asociados al eficiente funcionamiento de la plataforma *e-learning*.

Es importante porque, se desarrolla de tecnologías y su aplicación en las instituciones de educación superior requiere más allá de las herramientas básicas para la implementación de sistemas, es decir, acceso a internet, adquisición de implementos tecnológicos, talento humano capacitado para su administración y diferentes mecanismos de control que permitan alcanzar el uso seguro y eficiente de la plataforma Moodle.

Los beneficiarios del presente estudio son el departamento de TI de la PUCE Ambato, así como, también, el autor, que al cumplir los requisitos establecidos por la universidad podrá obtener el título de magister; este documento, también, servirá como material científico para otras investigaciones, además, de ser guía para salvaguardar principalmente la información que gestiona la plataforma de educación virtual de la PUCE Ambato.

El interés que presenta el estudio, es desarrollar una metodología para la evaluación de riesgos en plataformas Moodle sobre infraestructura *Cloud* privada, misma que estará socializada con las personas interesadas, que involucre a los docentes que conocen y manejan entornos virtuales de aprendizaje, y, se fortalecerse con la aplicación de la metodología.

## Capítulo I

# Marco Teórico

### 1.1 Definición y conceptos

En el presente estudio, se indaga las fuentes de información primaria y secundarias que, se encuentran en libros, papers, artículos científicos e incluso repositorios de universidades y escuelas politécnicas, con la finalidad de fundamentar teóricamente la investigación planteada.

#### 1.1.1. Plataformas virtuales

A partir de los años 90, se da inicio a la necesidad de crear materiales didácticos dentro de la web, los cuales, se puedan localizar y, se encuentren disponibles para los usuarios en cualquier parte del mundo mediante el acceso a internet, esto debido a que la existencia de los recursos eran limitados y su localización dificultaba su acceso al material didáctico (Laura, Arano, Vela, & González, 2019), sin embargo, el desarrollo tecnológico el cual permite la evolución en varios campos tales como: académicos, laborales, científicos y de entretenimiento, ha generado grandes progresos en el campo educativo específicamente, el avance tecnológico permite que el aprendizaje, se traslade desde el aula de clases (Becerra & Vegas, 2015), y, se encuentren dentro de plataformas virtuales, los cuales contienen diferentes tipos de materiales didácticos (videos, audios, textos, foros, etcétera), además, de otros elementos complementarios y en total disponibilidad del usuario.

Se entiende como plataforma de educación virtual a una aplicación web misma que, se compone por un conjunto de herramientas utilizadas en el proceso de enseñanza-aprendizaje donde, se genera la educación no presencial o mixta, es por ello que las instituciones educativas, se adaptan al uso de estas herramientas tecnológicas, los beneficios que presenta el uso de plataformas *e-learning* en el

proceso educativo “es la organización y la distribución de contenidos, el seguimiento y responsabilidad del estudiante, un soporte no presencial, o la compatibilidad con experiencias previas de uso de las TIC en la docencia” (Nácher, Ribera, Torrijos, Ballesteros, & Cebadera, 2018, pág. 72). Así mismo, el uso de las plataformas virtuales “permiten el aprendizaje colaborativo, por tanto, el proceso educativo, se corresponde con las habilidades, necesidades y disponibilidad de cada docente y alumno” (Verdezoto Rodríguez & Chávez Vaca, 2018, pág. 4).

Las TIC, se ven afianzadas en la implementación de infraestructura para aportar en el quehacer de la comunidad educativa como soporte a la comunicación interna y externa, tecnologías de soporte administrativo, de las plataformas virtuales y de educación *OnLine* implementadas para la gestión académica universitaria.

El aprendizaje electrónico *e-learning* en la actualidad presenta varios desafíos que, se atenderán para garantizar su calidad, es necesario establecer estándares y buenas prácticas que faciliten y sustancialmente mejoren las condiciones bajo las cuales funcionan, así como el valor que entregan.

### **1.1.2. Tipos de plataformas E-Learning**

Las plataformas de educación virtual se clasifican en tres tipos: plataformas de pago o plataformas propietarias, plataformas de código abierto y plataformas de desarrollo propio, las cuales cuentan con diferentes ventajas y desventajas que, se detallan, a continuación.

Los programas de código abierto, se caracterizan por la autonomía de utilizar el programa, bajo los propósitos de estudiar el funcionamiento del programa, y apropiar a las diferentes necesidades, es decir, poseer el acceso al código fuente, la libertad de distribuir copias, la libertad de mejorar el programa y hacer públicas las mejoras a los demás (Valverde, 2015, pág. 3). Caso contrario a los programas de pago, los cuales no poseen acceso al código fuente del programa ni la

comprensión del funcionamiento del programa y, se caracteriza principalmente por el pago de cierto valor para el uso de dicho programa.

**Tabla N° 1: Comparación entre plataformas educativas**

	<b>Plataformas propietarias</b>	<b>Plataformas de código abierto</b>	<b>Plataformas de desarrollo propio</b>
Características	Son plataformas por las que hay que pagar para tener derecho a la instalación y al mantenimiento, este valor varía según el número de usuarios.	1. La libertad de usar el programa con cualquier propósito. 2. La libertad de estudiar cómo funciona el programa y adaptarlo a las necesidades. 3. La libertad de distribuir copias del programa. 4. La libertad de mejorar el programa y hacer públicas las mejoras a los demás.	No están dirigidas a su comercialización como las comerciales ni pretende una distribución masiva a un conjunto de organizaciones como las de software libre. Surgen en instituciones y grupos de investigación, con el objetivo de responder a necesidades Educativas concretas.
Ventajas	Facilidad de instalación, intuitiva Servicio de asistencia y soporte. Actualizaciones permanentes. Calidad de software. Alta fiabilidad y estabilidad de la plataforma. Módulos específicos	Confiable en diseño e implementación. Costo, no, se paga por licencia o actualización. Versiones escalables. Calidad pues es bastante estable. Personalización, bastante modular.	A la medida. Independencia total. Minimiza costos. Actualizaciones no condicionadas. Aplicaciones propias. Formación de personal experto. Ajustado a la Institución.
Desventajas	Costo de implementación. Poca alternativa de compra. Restricción por requerimientos técnicos.	Aplicaciones con menos funciones que las plataformas propietarias.	Inconvenientes del proceso de diseño, creación, mantenimiento, modificación y costos de una plataforma propia. Todo estará desarrollado por personal propio
Ejemplo	First Class, WebCT, eCollege, Almagesto, BlackBoard	Claroline, Dokeos, Moodle, Sakai	Ágora Virtual (AUM).

**Fuente:** Chamorro & Pazos (2017)

A continuación, se analizan las características principales de algunas plataformas educativas más representativas:

- **First class**

La plataforma FirstClass, se considera como una de las poderosas herramientas de ayuda, prestada por la empresa Open Text, adaptables a todos los ejemplos de mecanismos y efectiva para el entorno educativo, como empresariales, que, se utilizan con los sistemas operativos Windows, Mac OS X y Linux y, además, instala de aplicaciones cliente para iPhone, BlackBerry y Android es un cliente /servidor de groupware<sup>1</sup>, correo electrónico, conferencias en línea de voz, servicios de fax y, a bordo del sistema de anuncios para Windows, Macintosh y Linux es una compañía de software con sede en Denver, EE. UU. Fundada en 1996, eCollege, se formó como una empresa proveedora de "software como servicio" (Software As a Service, o SaaS) inicialmente con el nombre de "Real Educación INC". WEBCT BLACKBOARD es una compañía de software con sede en Washington, DC, EE. UU. Fundada en 1997, Blackboard, se formó como firma consultora con un contrato con la organización sin fines de lucro IMS Global Learning Consortium (Web Course Tools, o Herramientas para Cursos Web) es un sistema comercial de aprendizaje virtual online, el cual es usado principalmente por instituciones educativas para el aprendizaje a través de Internet (Sedeño, 2016).

Dentro de las principales funciones está el desarrollo de contenidos y cursos. Compatibilidad tecnológica y posibilidades de integración. Rapidez en el proceso de implantación. Compatibilidad con los estándares internacionales. Integración de herramientas de administración y gestión. Desarrollo de contenidos y cursos. Integración de Herramientas de Comunicación. Herramientas de apoyo al seguimiento de un curso (Sedeño, 2016).

---

<sup>1</sup> El **groupware** es cualquier tecnología usada específicamente para hacer los grupos más productivos.

- **WebCT**

La plataforma WebCT (*Web Course Tools*), se considera como uno de los entornos de teleformación que alberga contenidos y los organiza para su uso en educación universitaria. Gestiona 500.000 cursos en todo el mundo. Cuenta con más de 200.000 profesores y con unos 6 millones de alumnos. Es utilizada en más de 3.500 organizaciones de 83 países diferentes. Sólo en España es usada por más de 50 instituciones, en su mayoría universidades (fuente: OCU). WebCT, se crea en 1995 y, se pone en marcha en la Universidad British Columbia de Canadá como proyecto de investigación. Esta plataforma, se fundamenta en el uso de una serie de herramientas formativas que, se clasifican en varios tipos: las de comunicación son los foros, los chats y la pizarra virtual; las de evaluación son los exámenes en línea y los ejercicios de autoevaluación; las de contenido son los materiales de consulta, de investigación y las referencias bibliográficas; las de seguimiento sirven para controlar el avance y desarrollo de los cursos (Caballero, 2014)

La plataforma WebCT contribuye a completar el ciclo formativo de los estudiantes de una manera más eficaz.

- **eCollage**

La eCollege, se considera como una plataforma de aprendizaje (LMS) que brinda a docentes y administradores las herramientas, el contenido y el apoyo que necesitan para crear, gestionar y medir experiencias de aprendizaje atractivas con una estructura adecuada para que el estudiante de educación media y superior, se sienta cómodo y sobre todo motivado para aprender, reduce así el riesgo de deserción y mayor probabilidad de lograr excelentes resultados académicos (Pearson Company, 2011).

- **Almagesto**

Los creadores de la plataforma Almagesto (2015) afirman que “es un sistema informático que permite gestionar las etapas de un proyecto de aprendizaje a través de Internet, suministrando la tecnología y el soporte necesario para su puesta en marcha de forma rápida, simple y profesional”.

Plataforma de pago Almagesto fue creada por la empresa Alhambra-Eidos, establece sus beneficios en la presentación de una arquitectura flexible, escalabilidad y alto grado de personalización que posee la plataforma, aporta varias ventajas para el usuario, tal es el ejemplo de fácil usabilidad, rápida adopción, flexibilidad pedagógica y proporcionan experiencias de uso intuitivo (Moreno, 2017).

- **Blackboard**

La plataforma estadounidense fundada en el año de 1997 dedicada a la administración de aprendizaje en línea, utilizada en varias Universidades de Estados Unidos de América, cumple con las normas propuestas por *World Wide Web*. Uno de los mayores beneficios a implantar por sus creadores es la posibilidad de integrarse con otras plataformas de aprendizaje, en adición, existe la posibilidad de complementarse con las redes sociales de los usuarios (Moreno, 2017),

Blackboard Platform fue diseñada específicamente para desarrollar el acceso a programas de enseñanza y aprendizaje, enriquece la calidad de la instrucción, se consideraba una de las mejores plataformas educativas principalmente debido a su flexibilidad y facilidad de uso (Uziak, Oladiran, Lorencowicz, & Becker, 2018).

Una de las debilidades reportadas por los usuarios sobre la plataforma blackboard es la dificultad que presenta al gestionar los chats entre los usuarios, sin embargo,

Blackboard ha sido denominada como una de las plataformas de aprendizaje más apropiadas para el aprendizaje.

- **Claroline**

A Claroline, se considera una plataforma gratuita de libre distribución y código abierto, completamente desarrollada con lenguaje PHP cuyos datos son administrados por una base de datos MySQL. Integra un paquete software de libre distribución que facilita a las instituciones de educación la generación de sistemas educativos a distancia basados en la aplicación de las tecnologías de la información y las comunicaciones (Chiarani, 2017).

- **Dokeos**

La plataforma Dokeos fue desarrollada bajo el lenguaje de programación PHP y el manejo de base de datos creados por MySQL, brinda su funcionamiento las 24 horas del día, presenta una interfaz más atractiva que otras plataformas, además, añaden nuevas herramientas que benefician al proceso de aprendizaje como, por ejemplo, la posibilidad de realizar videos conferencia en línea, pizarra virtual entre otras posibilidades agregadas dentro de esta plataforma (Moreno, 2017).

- **Sakai**

Se da origen en las universidades de Michigan y la Universidad de Indiana, a partir de ello, se les uniría varias universidades de gran prestigio tales como el MIT y Stanford, Sakai es una plataforma educativa de software libre, posee estabilidad al ser desarrollada bajo el lenguaje de programación Java permite sumar varias extensiones por ser de código abierto (Moreno, 2017).

- **Moodle**

Moodle acrónimo de *Modular Object-Oriented Dynamic Learning Environment* (Entorno de Aprendizaje Dinámico Orientado a Objetos y Modular) es una plataforma virtual de software libre. Moodle está diseñado para apoyar un estilo de aprendizaje denominado “Construcción Social”, dicho estilo manifiesta que existe un mejor aprendizaje en un ambiente que posea la interacción con compañeros y material de aprendizaje (Yáñez, 2013). “Moodle inició en el año 2002 con el aporte diferentes combinaciones de gestión de archivos y recursos didácticos, tales como, foros o espacios wiki” (Gómez, 2017, pág. 251).

Para González (2015) las principales características que presenta Moodle es la presencia de una interfaz de navegación sencilla e intuitiva, permite a los profesores editar la información que, se presenta y añadir nuevos bloques, promover el desarrollo de actividades colaborativas, es una plataforma segura, eficaz y utilizada en muchos países en diferentes idiomas.

Según (Miratia, 2010) es un “entorno Modular de Aprendizaje Dinámico Orientado a Objetos” [Object-Oriented Dynamic Learning Environment], lo que fundamentalmente útil para programadores y teóricos de la Moodle es un sistema de gestión de contenidos (CMS), un de software diseñado para ayudar al profesor a crear fácilmente cursos en línea de calidad”.

Moodle esta compuesto por 12 diferentes actividades las cuales son: Asignación, elección, base de datos, comentarios, foro, glosario, lección, cuestionario, paquete scorm, encuesta, wiki y talleres. Obtener varias alternativas para el aprendizaje del estudiante.

Como, se a presentado la plataforma Moodle la cual posee varias actividades con las cuales los estudiantes adquieren o mejoran sus conocimientos, permite una mayor comunicación entre ellos como con el profesorado, se logra la comunicación

individual con el personal docente o, se trata difetentes temas a debatir por todos los miembros que acceden a la plataforma.

- **Hosting**

Se entiende a hosting como “un servicio que, se ofrece por internet a usuarios y empresas que almacenan información y servicios asociados a la misma” (Calvo M. , 2014), es decir, “en un espacio que el proveedor del servicio de internet contratado pone a disposición en sus servidores parte de su capacidad de almacenamiento la cual es rentada y cuyos costes son variados” (Corral, 2017).

- **Cloud Computing**

El *cloud computing* o computación en la nube como lo define Van (2012) “es un modelo para habilitar un acceso de red desde cualquier ubicación, conveniente y bajo demanda a un grupo de recursos de computación configurables (redes, servidores, almacenamiento, aplicaciones y servicio) que serán provisionados y liberados rápidamente en un esfuerzo de administración o interacción con el proveedor de servicios mínimos (MINTIC, 2017).

En otras palabras, el *cloud computing*, es un modelo de computación que permite al proveedor tecnológico ofrecer servicios informáticos a través de internet, este modelo permite a la empresa ofrecer servicios bajo demanda esto como resultado a los recursos compartidos disponibles los cuales serán liberados y asignados con mínima gestión por parte del proveedor (Instituto Nacional de Ciberseguridad, 2017).

La solución que permite la mejor forma de utilizar efectiva y eficientemente la tecnología es mediante la implementación de procesos que garanticen el valor del servicio, esta necesidad, se subsana con el soporte bajo el modelo de servicio en la nube (*Cloud Services*) o *Cloud Computing* (CC), la cual ha llevado a la revolución

de la implementación de la infraestructura tecnológica basada en la credibilidad, disponibilidad y capacidad que en la actualidad tiene el internet. *Cloud Computing* entre las características y beneficios que le ha permitido posicionarse como una efectiva alternativa para los Departamentos de Tecnologías de la Información y Comunicación (DTIC) es que no importa donde reside la infraestructura, así como su manejo porque son de plena responsabilidad del proveedor, que sea “bajo demanda”, es decir, si, se requiere y con la capacidad basada en la necesidad.

En tal sentido, se coincide con (León-Velandia, Alberto, & Rosero-Muñoz, 2014) cuando afirman que *Cloud Computing*, se trata un nuevo modelo de prestación de servicios de negocio y tecnología que permite al usuario acceder a un catálogo de servicios estandarizados y responder con ellos a las necesidades de su negocio de forma flexible y adaptativa, en caso de demandas de carga de trabajo computacional no previsible o de picos de trabajo, se paga únicamente por el consumo efectuado, o incluso gratuitamente, en caso de proveedores que, se financian mediante publicidad o de organizaciones sin ánimo de lucro.

El actual impulso detrás de la aparición de *Cloud Computing* es la excesiva demanda de capacidad de la data *centers* de las instituciones y más organizaciones. Las instituciones buscan minimizar los costos y mayor eficiencia, y extender la eficiencia y eficacia de los DTIC, y pasar de las inversiones en esquemas de aplicación *On Premise* a gastos de operación variables como pago por servicios *Cloud*.

La transformación digital ha sido impulsada por el importante incremento del uso de la computación en la nube como ninguna otra disrupción tecnológica lo había logrado. *Forrester*, una de las consultoras más influyentes a nivel global en 2018 predijo que más del 50% de las empresas basarán al menos en una plataforma en la nube para afianzar su transformación digital (WebDox, 2018).

### **1.1.3. Software como Servicio (SaaS)**

El software como servicio le proporciona un producto completo que el proveedor del servicio ejecuta y administra. En la mayoría de los casos, quienes hablan de software como servicio en realidad, se refieren a aplicaciones de usuario final (Amazon, 2019).

El administrador de sistemas no estará preocupado por mantener el servicio y mucho menos por la infraestructura necesaria para mantener los servicios levantados, tan sólo utilizar el software instalado o contratado.

### **1.1.4. Plataforma como Servicio (PaaS)**

Las plataformas como servicio eliminan la necesidad de las compañías de administrar la infraestructura subyacente (normalmente hardware y sistemas operativos) y le permiten centrarse en la implementación y la administración de sus aplicaciones (Amazon, 2019).

Este tipo de servicio permite mejorar en niveles de eficiencia al departamento de TI de las organizaciones pues ya no, se preocuparán de temas como aprovisionamiento de recursos, cálculo de capacidad, mantenimiento del software instalado, parches o actualizaciones, y nada más que implique la ejecución de su aplicación.

Esto contribuye a mejorar su eficacia, pues no tiene que preocuparse del aprovisionamiento de recursos, la planificación de la capacidad, el mantenimiento de software, los parches ni ninguna de las demás arduas tareas que conlleva la ejecución de su aplicación.

Como lo expone Intel (2014) las plataformas como servicio PaaS “están basado en servicios en la nube que proporcionan a los equipos de desarrolladores la capacidad

de aprovisionar, desarrollar, construir, probar, e implementar aplicaciones en la nube”. “Las plataformas como servicio permiten integrar múltiples aplicaciones en la nube y en las instalaciones, aumenta la flexibilidad y permite obtener un mayor valor comercial de TI” (Oracle, 2019, págs. 1-2).

#### **1.1.5. Infraestructura como Servicio (IaaS)**

La infraestructura como servicio, contiene los bloques de creación fundamentales para la TI en la nube. Por lo general, permite acceder a las características de conexión en red, a los equipos (virtuales o en software dedicado) y al espacio de almacenamiento de datos. La infraestructura como servicio le ofrece el mayor nivel de flexibilidad y control de la administración en torno a sus recursos de TI y guarda el mayor parecido con los recursos de TI existentes con los que muchos departamentos de TI y desarrolladores están familiarizados (Amazon, 2019).

#### **1.1.6. Seguridad informática**

Como, se ha mencionado anteriormente las plataformas educativas actualmente, se han convertido en una herramienta fundamental para la formación académica, sin embargo, es necesario para profesores y estudiantes poseer la seguridad de la información depositados en la plataforma, se encuentren debidamente protegidos.

Se entiende como seguridad de la información a la protección de la información en relación con varios tipos de amenazas, a fin de garantizar la continuidad del negocio, minimiza los riesgos que puedan comprometerlo, y maximiza el retorno sobre las inversiones y las oportunidades de la organización. La seguridad de la información, se logra mediante la implementación de un conjunto de controles: políticas, procesos, procedimientos, estructuras organizacionales y funciones de hardware y software (Kowask, Alcántara, Cesar, & Boca, 2018).

La evaluación de cada uno de los niveles de seguridad, que se utiliza en la plataforma desde el usuario hasta la correcta administración de los servidores los

cuales cuentan con varias configuraciones clave que brindan un nivel aceptable de confiabilidad, las cuales, se representan en el siguiente cuadro:

**Tabla N° 2: Niveles de seguridad Moodle**

<b>SEGURIDAD</b>	<b>NIVEL DE GESTIÓN</b>	<b>NIVEL OPERATIVO</b>
En servidores	La responsabilidad del correcto funcionamiento de los servidores en los cuales, se encuentra levantada la plataforma educativa recae en el administrador Moodle designado por TI.	Manejo actualizado de antivirus. Mantener sistemas operativos actualizados, principalmente control de rootkis (software para esconderse a sí mismo y a otros programas) y exploits (softwares desarrollado para automatizar errores). Cierre de puertos de internet no usados. Control de usuarios y contraseñas complejas para MySQL, administrador de sistemas y administrador de plataformas. Separar la carpeta de datos Moodle y la plataforma principal e imposibilidad vía web. Limitar el acceso a IP desconocidas mediante la configuración de los servidores Apache, IIS, etcétera.
En autenticación	Existen varios métodos de autenticación desde la creación de un nuevo usuario o usar autenticadores por defecto de Moodle.	Plantear de una manera clara el proceso de autenticación del usuario y la construcción de una correcta contraseña de usuario Bloquear dominios de correos de tipo sospechoso Bloquear campos de usuario que considere importantes Regular los invitados no autenticados, definir bien su rol y los permisos asignados.
Con las contraseñas	Es necesario a los usuarios solicitar la autenticación, para ello es necesario la construcción de una contraseña segura para sí inicio de sesión, para evitar el robo de concentrada.	Una longitud mínima de 8 caracteres Incluir letras, números y caracteres especiales Incluir mayúsculas.
En definición de roles	Permite la gestión de los permisos de los usuarios autenticados y de la seguridad general.	Establecer un único usuario con permisos de administrador. Asignar roles globales únicamente al administrador y creador del curso No dar privilegios al rol de invitado Evitar en lo posible asignar roles a los usuarios.

Fuente: Elaboración propia.

## Ciberseguridad en la nube

En la PUCE Ambato al igual que en muchas instituciones y empresas líderes globales, se ha considerado la visión del departamento de TI para migrar hacia la utilización de Infraestructura como Servicio en la nube de tipo privada, para mantener los servicios disponibles 24/7 y optimizar así los recursos disponibles.

La tendencia adoptada por las instituciones, trae consigo considerar la seguridad como un factor relevante, y es por ello que las empresas líderes proveedoras de servicio *cloud* como *Amazon Web Service (AWS)*, *Google Cloud Platform (GCP)* y *Microsoft Azure* han desarrollado ofrecer servicios con estándares de seguridad de clase mundial, pero, también, se consideran medidas de seguridad para ofrecer máxima seguridad en las plataformas (WebDox, 2018).

(Perkins, 2017) durante la Cumbre de Gestión de Riesgos y Seguridad de Gartner, hizo referencia a las tendencias de la ciberseguridad en la nube; advierte que serán los grandes y crecientes volúmenes de información. Un fenómeno que conllevará a desarrollar nuevas competencias en los especialistas como la ciencia de datos, y a la inteligencia artificial como algo imprescindible, así como el invertir en estrategias de detección y respuesta como parte del presupuesto previsto para la prevención de riesgos y ataques. “No todo, se puede prevenir, pero sí es posible saber cómo responder” (WebDox, 2018, pág. 7).

Si para la gestión de los sistemas de la universidad, se ha decidido utilizar los servicios *cloud*, la institución implementará controles, operará de forma efectiva los recursos disponibles, reportará de forma oportuna los no cumplimientos, así como evaluará la capacidad de gestión ante los riesgos y vulnerabilidades existentes. Las vulnerabilidades son por lo general fallos de diseño de procedimientos o de recursos, las vulnerabilidades existen no, se fabrican, una vulnerabilidad es cualquier fallo de diseño que permite que una amenaza pueda afectar a un recurso. Si, se habla de recursos informáticos, se suele decir que una vulnerabilidad es un

fallo de diseño de un sistema, un sistema no actualizado o un sistema mal configurado que permite que un agente externo, acceda sin permisos apropiados al recurso o información que dicho sistema gestiona, en función del tipo de recurso al que estemos orientados existen distintas fuentes de información dónde, se busca vulnerabilidades aplicables a los sistemas con que, se cuenta (Romero, Figueroa, & Vera, 2018).

Las vulnerabilidades, se les considera debilidades de seguridad informática que, se asocia a los activos de información de la plataforma Moodle de la PUCE Ambato; sin embargo, hay que considerar que las vulnerabilidades no causan daño. Simplemente son condiciones que posibilitan tener una amenaza que afecte a un activo. Una vulnerabilidad es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información al permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible (INCIBE, 2017).

La clasificación de las vulnerabilidades en base a la ISO 27017, indica lo siguiente:

- Seguridad de los recursos humanos: falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados, entre otros.
- Control de acceso: segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, password sin modificarse.
- Seguridad física y ambiental: control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujeta a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje.

- Gestión de operaciones y comunicación: complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión.
- Mantenimiento, desarrollo y adquisición de sistemas de información: protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos.

Para la evaluación de los niveles de ciberseguridad que, se utiliza en la nube o requiere la institución para hacer frente a los problemas específicos que son críticos para la seguridad de la nube, se evalúan las áreas de control en una *Cloud Control Matriz* (CCM), las mismas que, se representan en el siguiente cuadro:

**Tabla N° 3: Áreas de control de una Matriz de Control de Nube (CCM)**

<b>ZONAS DE CONTROL 3.0.1</b>
1. Aplicación y seguridad en la Interfaz
2. Aseguramiento de Auditoría y Cumplimiento
3. Gestión de Continuidad Operacional y Resiliencia
4. Control de Cambio y Gestión de la Configuración
5. Seguridad de Datos y de Información de Gestión del Ciclo de Vida
6. Centro de datos de seguridad
7. cifrado y gestión de claves
8. Gobernanza y Gestión de Riesgos
9. Recursos Humanos
10. Gestión de identidades y acceso
11. Infraestructura y seguridad de la virtualización
12. La interoperabilidad y portabilidad
13. Mobile Security
14. Gestión de Incidentes de Seguridad, E-Descubrimiento y la nube Forense
15. Gestión de la cadena de suministro, transparencia y responsabilidad
16. gestión de amenazas y vulnerabilidad

**Fuente:** Cloud Security Alliance (CSA, Cloud Security Alliance, 2014).

### 1.1.7. Metodologías existentes

Las plataformas virtuales de aprendizaje, se encuentran evaluadas por marcos normativos que rigen la constitución de páginas web (Becerra & Vegas, 2015). Esto conlleva que para el presente estudio, se considera las normativas, ISO 27001, que describe cómo gestionar la seguridad de la información, así, también, 27017, e ISO 27018, que manejan las guías de buenas prácticas en *Cloud* que monitorea el adecuado funcionamiento de la nube entre otras normas están siguientes:

- **Metodología de Análisis y Gestión de Riesgos de los Sistemas Informáticos (MAGERIT)**

Es la Metodología elaborada y propuesta por el Consejo Superior de Administración Electrónica (CSAE), surge ante el desarrollo y los beneficios tecnológico existentes, pero, también, da lugar a nuevos riesgos latentes que ameritan medidas de seguridad que brinden confianza a los usuarios (Amutio & Candau, 2012). Reconocida por la ENISA (European Network and Information Security Agency).

- **ISO 20000-9**

La norma internacional ISO 20000/ IEC 20000-1 orientada a la gestión con los proveedores de servicios en la nube (*cloud services*), cubre todo tipo de servicios en la nube como son: Servicio IaaS (infraestructura), PaaS (Plataformas), y SaaS (Software). La guía, se muestra como un conjunto de escenarios que abordan un sin número de actividades típicas de un proveedor de servicios *cloud*.

- **ISO 27001**

La norma internacional ISO / IEC 27001 orientada a la gestión de la información confidencial, y de su seguridad que constantemente es noticia por los robos de identidad, infracciones en registros financieros, terrorismo cibernético, entre otros.

Abarca la gestión de personal, procesos y de los sistemas de TI, mantiene la vanguardia en la aplicación de técnicas para afrontar amenazas de la información y a los posibles problemas de seguridad.

Evidentemente la información de una empresa o institución, se encuentra en su mayor parte en los sistemas automatizados o informáticos, por tanto, la ISO 27001 propone un marco que gestiona la información de la empresa, y, también, considera que la misma, se generará del propio conocimiento y experiencia de las personas que serán tratadas como activos de información de ser necesario. Por tanto, es necesario no centrarse solamente en la seguridad de los sistemas informáticos de la organización.

Los riesgos de seguridad de la información, se presentan como una amenaza constante para las organizaciones por la probabilidad de pérdidas financieras, de servicios de red, confianza y hasta reputación institucional, la norma ISO 27001 define a la información como (Normas ISO, 2019).

“La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada...

... la información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Estará protegido adecuadamente cualquiera que sea la forma que tome o los medios por los que, se comporta o almacene” (Gualan, 2015).

- **ISO 27017**

Es un estándar de seguridad que entrega controles para clientes y proveedores de servicios *cloud*, es muy utilizada por la precisión con la que establece las relaciones entre proveedores y clientes, determina exactamente qué exigir el cliente y qué información proporciona el proveedor del servicio.

La ciberseguridad y la gestión del servicio entregado, se ve fortalecido al cumplir la norma, asegura la gestión de arquitectura, medidas de seguridad, tecnología de cifrado, funcionalidades disponibles y localización de los datos. “La norma contempla 37 controles en la nube -basados en la *ISO -27002*, junto a 7 adicionales que permiten fortalecer la seguridad de los servicios *cloud*” (WebDox, 2018, pág. 12).

- **CRAMM (CCTA Risk Analysis and Management Method)**

Para Vanegas & Pardo (2014) el marco normativo CRAMM es una metodología de análisis de riesgos desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones (CCTA), es el método de análisis de riesgos preferido en los organismos de la administración pública, se compone de tres etapas, cada una apoyada por cuestionarios, objetivos y directrices. Las dos primeras, se encargan de identificar y analizar los riesgos para el sistema, y la tercera recomienda la manera en que estos riesgos serán gestionados (pág. 37).

- **NIST 800-30**

El marco normativo NIST 800-30, se elabora con el objetivo de aseguramiento los sistemas de Información que almacenan, procesan y transmiten información, y que gestionan el riesgo.

Las evaluaciones de riesgos son una parte importante de la ciberseguridad. La mayoría de las organizaciones usan al Instituto Nacional de Estándares y Tecnología (NIST) 800-30 como guía para realizar evaluaciones de riesgos, con los estándares de referencia aquí estipulados. Las agencias gubernamentales han utilizado históricamente la guía, pero cada vez más entidades comerciales en el sector privado, también, lo utilizan para desarrollar programas sólidos de gestión de riesgos. Al utilizar guías de evaluación de riesgo, se beneficia a las organizaciones que buscan comprender mejor sus perfiles de riesgo o aquellos asociados con trabajo del gobierno TI. (Tejena, 2018, pág. 237)

## Capítulo II

# Metodología

### 2.1. Tipo de Investigación y Enfoque de investigación

#### 2.1.1. Tipo de Investigación

En esta investigación intervienen dos modalidades, la investigación bibliográfica o documental y la investigación de campo; estas investigaciones suelen ser las más comunes para el entendimiento de las variables de estudio y así descubrir potenciales soluciones y mejores en las organizaciones o departamentos investigados, en este caso resolver el problema relacionado a los factores de riesgos del que, se encuentren presenten para la plataforma Moodle.

La investigación bibliográfica o documental, se considera al levantamiento de conceptualizaciones o información secundaria, esto quiere decir que, a través de la indagación de temas relevantes en normas, libros, revistas, documentos, permite generar conocimiento que aportan al estudio y al entendimiento de los factores de riesgo.

La investigación de campo permite trabajar en la situación actual de la PUCE Ambato del Departamento de Tecnología de la Información y las Comunicaciones, en este caso, la documentación de los riesgos en la administración de la plataforma de educación virtual Moodle, para ello, se utiliza herramientas y técnicas de recolección de información, lo cual una vez que, se someta a análisis y comprobación, se tendrá información primaria. Así mismo la recolección de información realizada en campo o en in-situ bajo procedimientos del levantamiento de información como: recolección, crítica, digitación, tabulación, y validación recolectada en general, se dirá que es muy importante para descubrir y generar

teoría y datos estadísticos que permita a futuras investigaciones ampliar el campo de acción y generar nuevos estudios.

### **2.1.2. Enfoque de la investigación**

El enfoque de la investigación mixto, es decir, que es cualitativo y cuantitativo, el primer enfoque cualitativo, es descriptivo y desarrolla una serie de detalles que darán a entender la administración de la plataforma de educación virtual Moodle, que evidenciará las cualidades de las variables que las interrelacione y así poder entender el problema que, se genera dentro de la plataforma Moodle. Este enfoque es más analítico y permite argumentar y comprobar las variables de análisis, que se lo considera mediante la norma ISO 27017:2015, lo cual los resultados son representados mediante las herramientas estadísticas y matemáticas, consiguiente, proceder a concluir e implementar soluciones respecto al tema en estudio.

El levantamiento de la información, se utilizó la técnica del Check List, con el instrumento lista de verificación dirigido al departamento de TI de la PUCE Ambato, con cuestionamientos que presentan facilidad para el registro de la información.

En el procesamiento de la información, se procedió a la realizar un estudio estadístico de datos obtenidos para representación de resultados; así mismo, se analizó los resultados estadísticos, se destaca tendencias o relaciones fundamentales de acuerdo con los objetivos e interrogantes referentes los riesgos en la administración de plataformas de educación virtual Moodle.

### **2.1.3. Tipo de recolección de la información**

- **Fuentes Primarias**

En esta investigación, se enfoca en las fuentes de información primarias que son la indagación de lineamientos y políticas que mantenga el departamento de TI de la

PUCE Ambato que posea el tema a indagar los riesgos de TI, en este caso de la identidad corporativa y lo relacionado con la misma. Además, se tomará información de exploración en temas relacionados y revistas científicas para complementar la información requerida por el tema.

- **Fuentes secundarias**

La información que respalda el tema de estudio, se buscó a partir de fuentes bibliográficas fidedignas que permitan tener información seria a cerca de la investigación. Se utilizó diferentes técnicas para la obtención de la información requerida para poder complementar lo investigado para que la toma de decisiones posteriormente sea en base a todos los conocimientos obtenidos.

- **Método deductivo**

Este método permite ordenar las características de los factores de riesgos y generar un producto documental para mitigar el riesgo mediante el manual basado en la norma ISO 27005:2015, que, se enfoca en la formación de la investigación que proporciona un campo más específico en donde centrarnos para el análisis del problema y cómo esto ayuda a resolverlo.

Así mismo, se utiliza el método deductivo que necesita apoyarse en el *Check List*, cuyo instrumento es la observación para lograr la recolección de datos, en este caso para conocer la situación actual de las preferencias de la problemática suscitada en el departamento de TI cuya decisión es de elegir un producto que sirva como instrumento para los profesionales y estudiantes de universidad, esto permite plantear la necesidad de desarrollar una Metodología de Evaluación de Riesgos que contribuya a la administración de la plataforma Moodle de la PUCE Ambato.

- **Técnicas**

El *Check List*, se considera como una técnica de recolección de información con la cual, se indaga la situación actual de la institución en el tema de evaluación de riesgos para la administración de la plataforma Moodle, en este caso son cuestionamientos con escalas colorativas de cumplimiento en donde el investigador tienen la finalidad de evaluar subjetivamente con el propósito que la información sea más clara y específica para luego hacer su interpretación y análisis.

- **Instrumentos**

La lista de verificación es un instrumento en base a cuestionamientos basados en la norma ISO 27017:2015, con el fin de obtener información pertinente acorde a los objetivos planteados en la investigación, para lo cual las preguntas fueron formuladas de forma coherente y organizadas.

#### **2.1.4. Procesamiento y análisis de la información sobre el diagnóstico realizado**

La información recolectada mediante el instrumento *Check List*, y la observación como técnica utilizada con la finalidad de depurar información indeseable, permite:

- Realizar un análisis descriptivo de la información recolectada mediante el instrumento empleado.
- Analizar tendencias de comportamiento de distintos factores que involucra las amenaza y oportunidades.
- Ayudar a tomar decisiones sobre aspectos concretos.
- Averiguar posibles relaciones entre diversos factores y variables del fenómeno estudiado que ayuden a comprender de mejor manera los lineamientos de norma ISO 27017.

**Tabla N° 4. Recolección de información**

<b>PREGUNTAS DE INVESTIGACIÓN</b>	<b>RESPUESTAS</b>
<b>1. ¿Para qué?</b>	Diseñar una Metodología de Evaluación de Riesgos para Plataformas Moodle
<b>2. ¿A quién vamos aplicar?</b>	Plataforma Moodle PUCE Ambato
<b>3. ¿Sobre qué aspectos?</b>	Los lineamientos de la norma ISO 27017
<b>4. ¿Quién?</b>	Investigador
<b>5. ¿Cuándo?</b>	Segundo semestre del 2019
<b>6. ¿En qué lugar?</b>	DTI PUCE Ambato
<b>7. ¿Con que técnicas?</b>	Observación
<b>8. ¿Con que instrumentos?</b>	Check List (Lista de verificación)

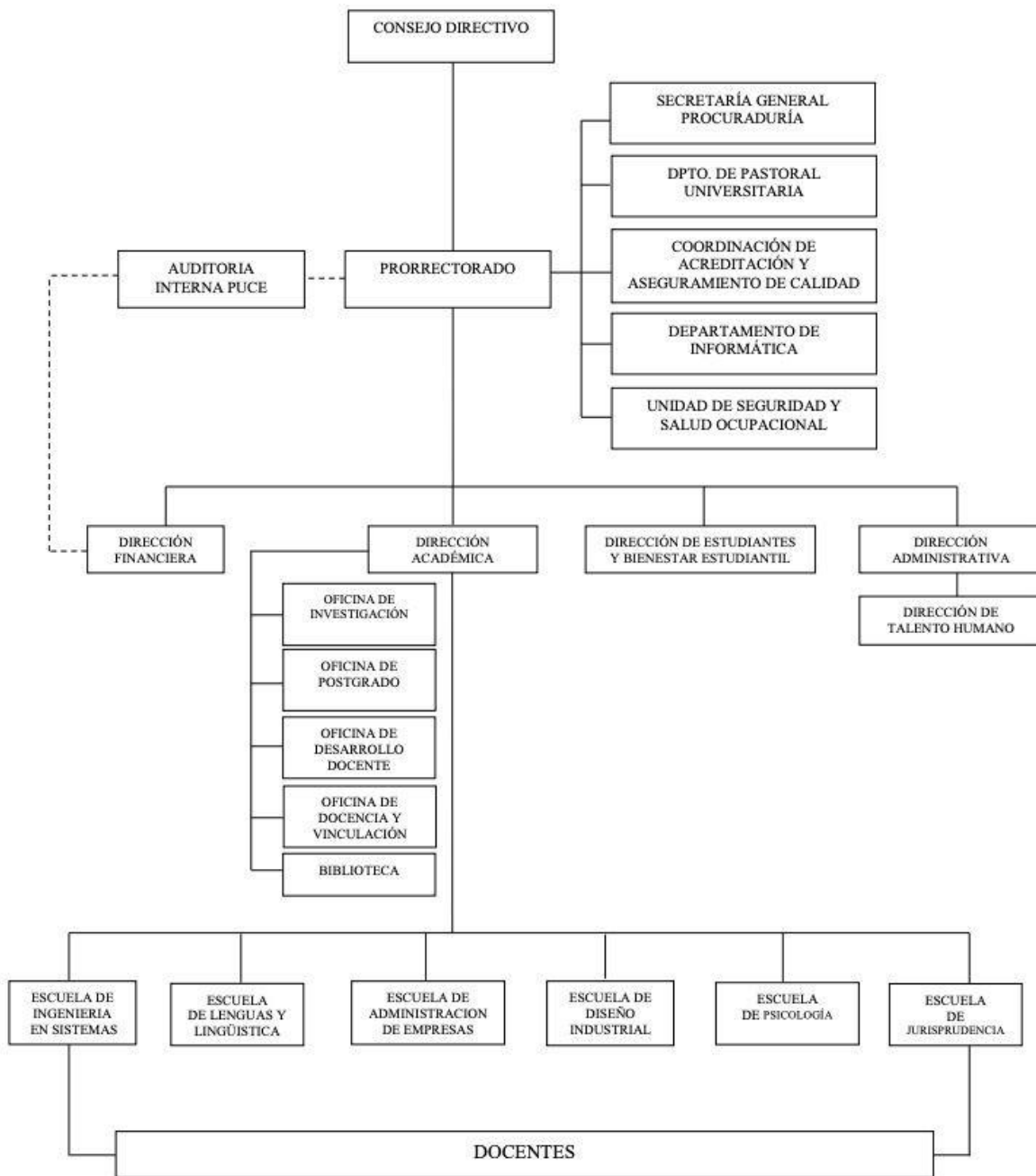
Fuente: Elaboración propia

Por ende, el procesamiento y análisis de la información recolectada en la investigación, se depurará, para que sea adecuada y presentable, y con ello asegurar su fiabilidad. La información depurada, se procesa mediante una hoja electrónica con la cual, se obtiene tablas, gráficos con porcentajes y frecuencias, de donde, se determina los resultados para la viabilidad de la propuesta como, también, la posible solución a la problemática.

## **2.2. Caracterización de la empresa o institución.**

La Pontificia Universidad Católica del Ecuador Sede Ambato (PUCE Ambato) fue creada y aprobada por el Consejo Nacional de Educación Superior (CONESUP) el 26 de septiembre de 1986. Conformada por las escuelas de Administración de Empresas, Jurisprudencia, Lenguas y Lingüística, Psicología, Diseño Industrial y Sistemas. En postgrados ofrece las maestrías en Ciencias de la Educación y Gerencia Informática (Altamirano, 2019, págs. 46-48).

La estructura orgánica de la PUCE Ambato refleja de forma pública en su sitio *web* el “Manual Orgánico Funcional”, como un elemento técnico para el análisis organizacional (ver gráfico 1).



**Gráfico N° 1:** Estructura orgánica funcional de la PUCE Ambato  
**Fuente:** Organigrama General Estructural de la PUCE Ambato (2018)

Con el objetivo de contextualizar al departamento de Tecnologías de la Información de la PUCE Ambato dentro de la estructura institucional, se presenta, a continuación, el Orgánico Estructural del departamento y como anexo el Orgánico funcional del mismo:

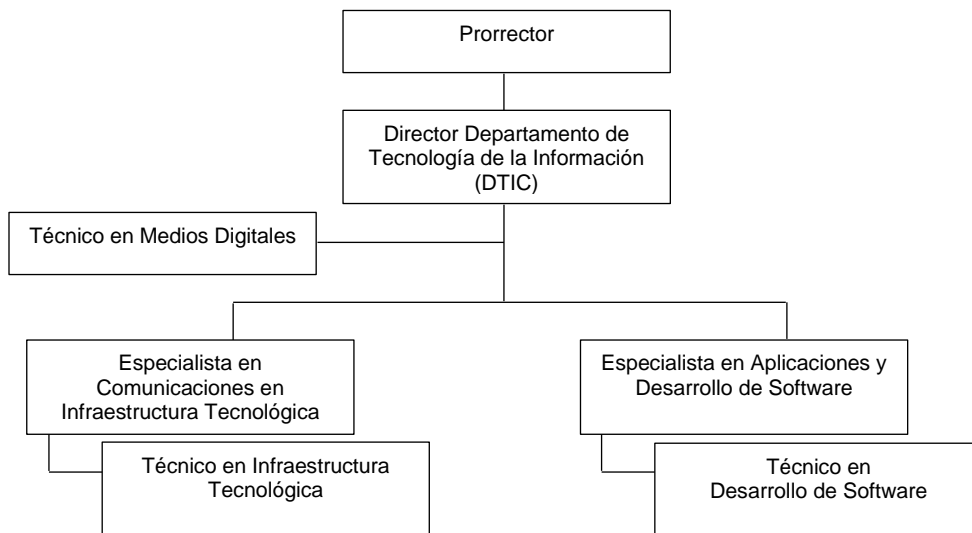


Gráfico N° 2: Orgánico Estructural DTI PUCE Ambato  
**Elaborado por:** DTI PUCE Ambato

La evolución del centro de datos, hacia esquemas más flexibles y la dinámica del mercado tecnológico propician un amplio crecimiento en la adopción de tecnologías que en el caso de computación en la nube han sido exponenciales en el mundo, las instituciones exitosas están encaminadas a migrar a esta nueva y dinámica forma de operar, las que utilizan las TI como un impulsor del negocio, las que buscan tener efectos positivos en los resultados de la organización (Osoreo, 2019).

Según, (Navas, 2016) la computación en la nube es un modelo de prestación y consumo de servicios que ofrece muchas ventajas a las organizaciones (alta disponibilidad, elasticidad, máximo aprovechamiento de recursos, entre otros) que, se traducen en requisitos de calidad que cumple el servicio.

Para acceder a la implementación de una solución *Cloud*, en la organización surgen múltiples dudas, las más comunes el saber dónde, se almacenarán los datos o qué tipo de aplicaciones podemos utilizar, donde la propiedad del servicio, se refiere a quién pertenezcan los recursos empleados y la información almacenada en la nube, así como, también, el tipo de servicio ofrecido, en función de qué nivel de control, se tenga sobre el hardware y software del servicio *Cloud* contratado.

Según la propiedad del servicio, se clasifican en nube pública, privada e híbrida, para el caso de estudio la PUCE Ambato mantiene el servicio de una nube pública

que es ofrecido por una empresa externa como Amazon Web Services (AWS) que, se encarga de su gestión y mantenimiento, que sea pública implica que la información de la universidad, se almacena en servidores de terceros, de los cuales no es propietaria, es decir, los recursos de los servidores, se comparten entre otros clientes de AWS, por lo tanto, los datos de la universidad y de otras instituciones estarían alojados en el mismo equipo, lo que, también, conlleva a que no, se requiere una inversión inicial en infraestructura física, le pertenece a AWS así como, también, la responsabilidad de su mantenimiento y actualización. Sin embargo, la PUCE Ambato mantiene una instancia reservada, lo que, de cierta manera, se considera un ambiente privado en la nube pública.

Según EY CertifyPoint, que es un agente certificador ISO acreditado por el Consejo holandés de acreditación, en octubre del 2015 otorga a Amazon Web Services, Inc. la certificación ISO/IEC 27017:2015 que proporciona orientación sobre los aspectos de seguridad de la información específicos de la nube y recomienda la implementación de controles de seguridad de la información que complementan las directrices de las normas ISO/IEC 27002 e ISO/IEC 27001 (Amazon, 2019).

Según el tipo de servicio ofrecido por empresas dedicadas a servicios “*cloud*”, estos son, *Software as a Service (SaaS)*, *Platform as a Service (PaaS)*, e *Infrastructure as a Service (IaaS)*, el último en mención es el servicio que utiliza la PUCE Ambato, donde mantiene prácticamente total control del servidor, de los recursos asignados, como, también, la instalación del sistema operativo que es algo fundamental.

El Departamento de Tecnología de la Información (DTI) de la PUCE Ambato mantiene el servicio *Cloud* con AWS por medio del canal IT Era y así construir su nube privada a través de una arquitectura IaaS hospedada en la nube pública que para la PUCE Ambato establece físicamente sus servidores en Ohio EEUU, con la denominada Región A (Región de despliegue), donde, se establece una nube privada o en inglés Virtual Private Cloud (VPC) que permite aprovisionar una sección de la nube AWS para la PUCE Ambato y así controlar todos los aspectos

del entorno de red virtual, servidores de aplicaciones o bases de datos, la selección de su propio rango de direcciones IP, la creación de subredes y la configuración de tablas de ruteo y gateways de red, utilizar IPv4 e IPv6 para así asegurar el acceso a recursos y aplicaciones de manera segura y sencilla. Algo muy importante es la implementación de varias capas de seguridad, incluidos grupos de seguridad y listas de control de acceso a la red, para ayudar a controlar el acceso a las instancias de Amazon EC2 en cada subred. Para asegurar la continuidad del servicio de la plataforma Moodle la universidad cuenta con la denominada Región B (Región failover), que, se encuentra ubicada físicamente en Virginia EEUU, así la VPC de contingencia o pasiva, se configura una red multi-región a disposición de la PUCE Ambato.

Y aunque el motivo de este estudio es el análisis de la plataforma Moodle, que para el caso de la PUCE AMBATO, se encuentra en la nube, esta sede universitaria mantiene un entorno *On Premise* o conocida, también, como *in-house* que según (Hashimura, 2013) están asociadas a instituciones que buscan resultados profesionales, ofrecen una gestión controlada de flujo de trabajo definido, además, de una configuración gestionada por los mismos empleados, conformación personalizada al modelo y objetivos institucionales, la clasificación con la que el Centro de Datos de la PUCE Ambato podría contar es TIER 2, por las características técnicas de su implementación, se entiende por TIER de un Data Center a la clasificación ideada por el *Uptime Institute* que, se acoge al estándar ANSI/TIA-942 y que de forma básica establece actualmente 4 categorías, en función del nivel de redundancia de los componentes que soporta el Data Center (Gómez R. , 2012).

El Data Center tiene redundados sistemas vitales, como la refrigeración, cuenta con un único camino de suministro eléctrico, componentes redundantes (N+1), la infraestructura física es de suelo elevado, cuenta con generadores auxiliares *Uninterruptible Power Supply* (UPS) conectados a una única línea de distribución eléctrica y de refrigeración, es decir, mantiene cierto grado de tolerancia a fallos y

que permite al DTI algunas operaciones de mantenimiento “on-line”, cuenta con una disponibilidad de 99.741%.

En el centro de datos de la PUCE Ambato, se establece un *Active Directory* (AD) que según Microsoft hace referencia a una red distribuida de computadores que utilizan distintos protocolos (LDAP, DNS, DHCP y Kerberos), en la DTI crean los usuarios, permisos y asignación de recursos, despliegan programas, direccionan el almacenamiento de la información en una base de datos central, crean equipos o grupos con el objetivo de administrar los inicios de sesión en los equipos conectados a la red, así como, también, la administración de las políticas de acceso de toda la red. El recurso que a través de una *Virtual Private Network* (VPN) obtiene información de la plataforma Moodle que, se encuentra en nube privada [AWS-PUCESA] con dirección <https://moodle.pucesa.edu.ec> es el sistema informático de gestión académica de la PUCE Ambato denominado ACADEMICS.

## 2.2.2 Arquitectura funcional PUCESA – ITERA - AWS

Para la entrega del servicio a los usuarios de los sistemas de la universidad, es necesario que la DITIC coordine y gestione con ITERA los recursos tecnológicos contratados en los Acuerdos de Nivel de Servicios (Service Level Agreement - SLA) que AWS pone a disposición mediante un contrato, que son las políticas que rigen el uso de los servicios incluidos y que aplican de manera independiente a cada cuenta que utiliza.

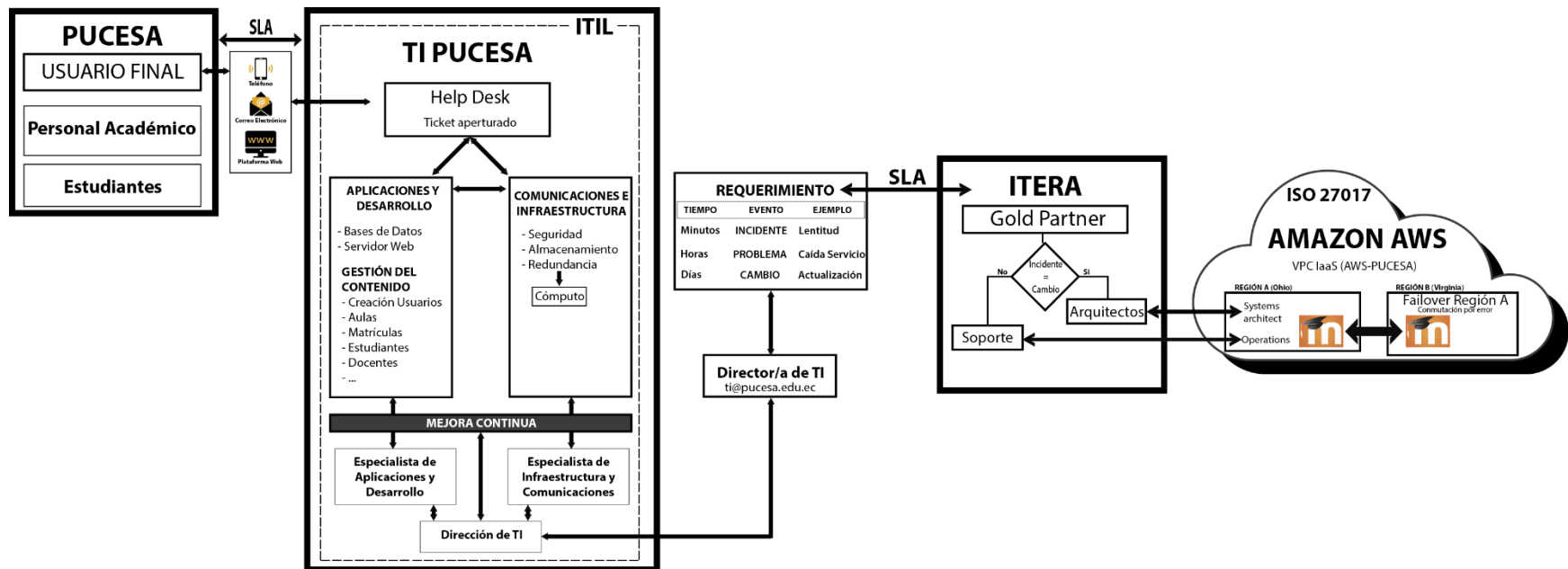


Gráfico N° 3: Estructura PUCESA – ITERA - AWS  
Elaborado por: El Investigador - DTI PUCE Ambato

AWS realizará los esfuerzos para que, los servicios incluidos estén disponibles para cada región con un porcentaje de tiempo de actividad de al menos el 99.99%, en el caso de que cualquiera de los servicios no cumpla con el compromiso la PUCE Ambato será elegible para recibir un crédito por servicio, tal como, se muestra en la tabla siguiente:

**Tabla No. 5 Créditos por servicio AWS**

<b>% de tiempo de actividad mensual</b>	<b>% de crédito por servicio</b>
Menos del 99.99%, pero igual o mayor al 99.0%	10%
Menos del 99.0%, pero igual o mayor a 95.0%	30%
Menos del 95.0%	100%

Fuente: Contrato de Nivel de Servicios Amazon Compute, 22 julio 2019

Para recibir créditos por servicio, la PUCE Ambato presentará un reclamo al abrir un caso en el centro de soporte de ITERA a más tardar al final del segundo ciclo de facturación por medio de la DTIC.

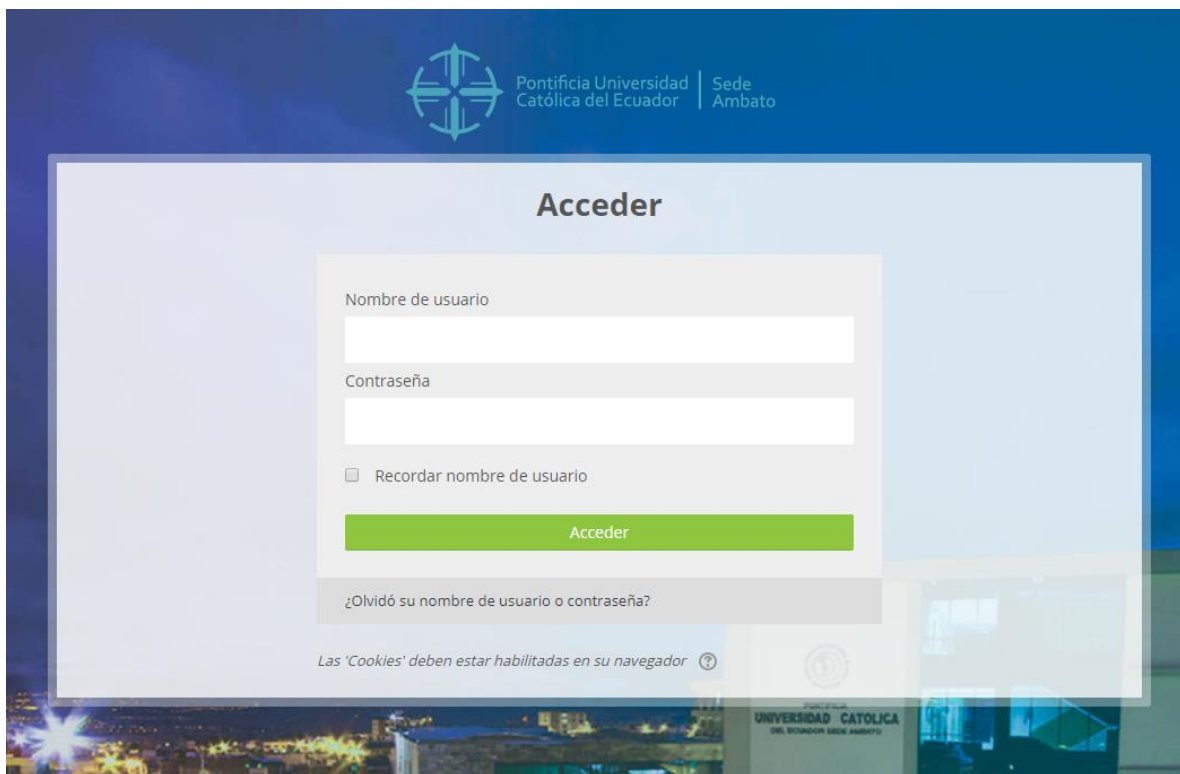
Los principales responsables de evaluar y gestionar los riesgos que, se generen en la plataforma Moodle serán los miembros del departamento TI de la PUCE Ambato, con el afán de evaluar los procedimientos o estrategias empleadas para identificar oportunamente los riesgos en la administración de la plataforma de educación virtual.

Moodle es una plataforma de educación virtual de código abierto bajo la licencia GPL que por tanto siempre está disponible todo lo que produce para descarga, actualización y uso gratuito. La PUCE Ambato tiene instalado Moodle versión 3.5 con fecha de liberación 17 de mayo del 2018, el DTI ha actualizado los problemas del núcleo general en 3.5.x en mayo 2019, se encuentra a la espera de la actualización que soluciona problemas para asuntos de seguridad en 3.5.x que según Moodle.org, se liberará el 10 de mayo del 2021.

En la zona de disponibilidad, se establece la capa de servidores Moodle que almacenan las sesiones *Hypertext Transfer Protocol* (HTTP) en el DynamoDb, zonas que gestionan las transacciones mediante el balanceador de carga y toda la información, se almacena la base de datos principal *Amazon Relational Database Service* (RDS) que optimiza memoria, rendimiento u operaciones de Entrada/Salida (E/S) los respaldos de transacciones, se almacenan en el *Backup Moodle data* (S3) generados tanto en las regiones A y B, la Red de entrega de contenidos (CDN *Cloudfront*) e interactúa con los S3 donde almacena en caché los archivos estáticos de la aplicación y acelera su carga.

Para obtener información de moodle.pucesa.edu.ec y lograr un análisis actual, con fecha 24 de enero del 2020 realiza el corrido de la herramienta woorank.com, se encuentran los siguientes resultados:

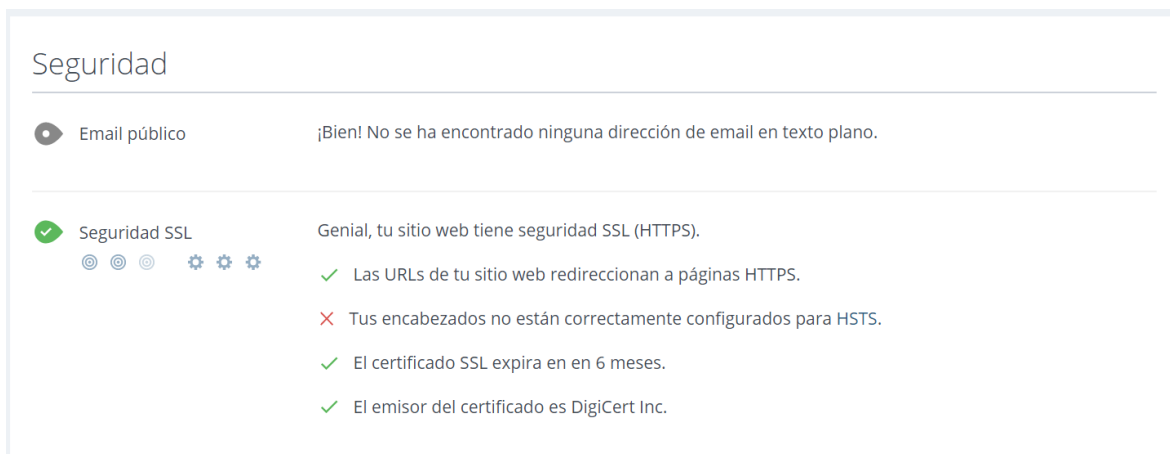
Imagen No.1 Pantalla de acceso



Fuente: <https://www.woorank.com/es/www/moodle.pucesa.edu.ec>

Hay 5 páginas en el dominio puce.edu.ec que enlazan al sitio web de Moodle, el sitio maneja las páginas faltantes con un código de estado HTTP 404, posee codificación GZIP que reduce el tiempo de carga haciéndola eficiente. La visualización para dispositivos móviles como smartphone o tablets, se encuentra optimizada, los enlaces internos están bien definidos lo que ayuda al SEO y a la accesibilidad, en lo referente a la frescura del sitio web, se encuentra que su última actualización, se realizó el 20 de diciembre del 2019 lo que es bueno porque los visitantes perciben actualización y por tanto genera mayor credibilidad.

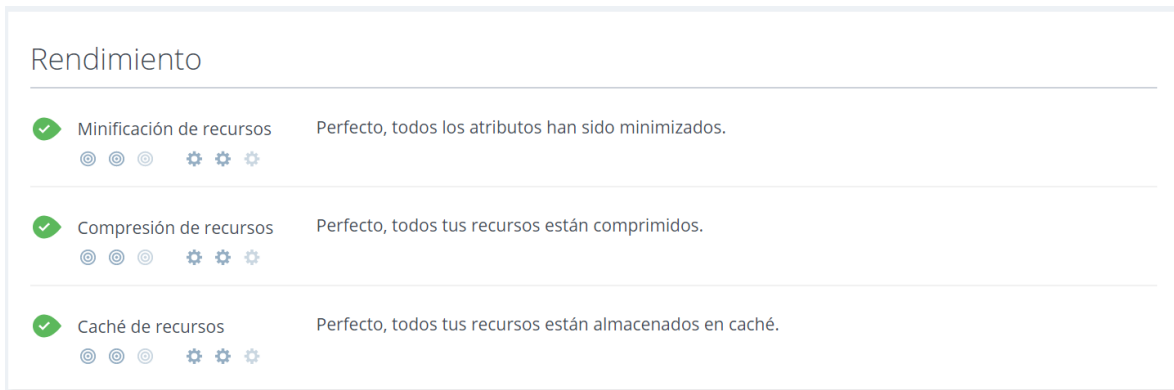
Imagen No.2 Análisis de seguridad



Fuente: <https://www.woorank.com/es/www/moodle.pucesa.edu.ec>

Como, se observa en la Imagen No. 2, el sitio cumple con tres de los cuatro estándares de encriptamiento de la información. No obstante, se aprecia oportunidades de mejora sobre los encabezados HSTS que, según (Fain, 2014) el HTTP *Strict Transport Security* (HSTS) su principal objetivo es impedir que un atacante convierta una conexión HTTPS en HTTP, HSTS envía un mensaje al navegador del usuario que podría ser interpretado como: “¡Hola! Toda nuestra comunicación estará encriptada, caso contrario tendrás que mostrar un mensaje de error.”

### Imagen No.3 Análisis de rendimiento



Fuente: <https://www.woorank.com/es/www/moodle.pucesa.edu.ec>

El indicador de rendimiento en Moodle de la PUCE Ambato es muy alto, el tamaño de la página es 442 Kb, es decir, muy liviano por tanto más rápido, la velocidad de respuesta es 1,8 segundos y cuenta 21 solicitudes de página que es muy aceptable porque mientras más solicitudes HTTP haga el sitio web más lento, se vuelve.

#### Imagen No.4 Análisis de tecnologías utilizadas

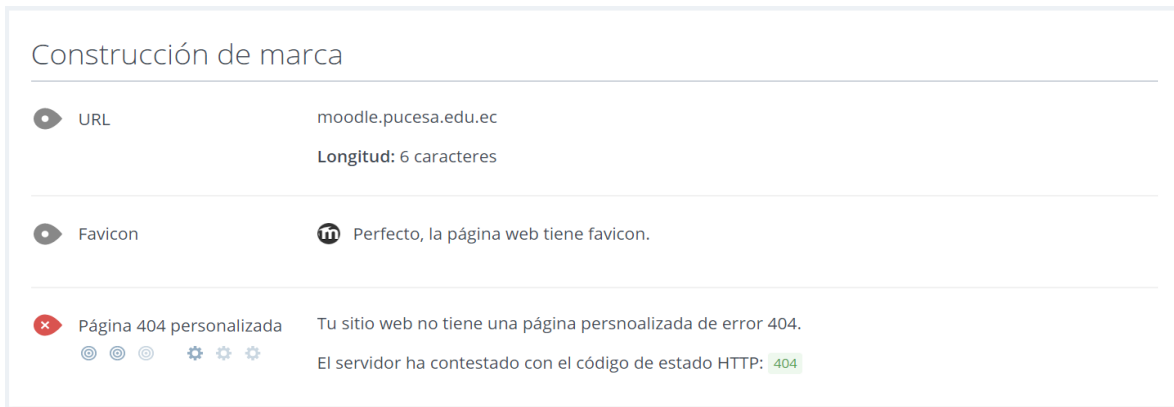
The screenshot displays a 'Tecnologías' (Technologies) analysis page. It features several sections:

- Servidores:** A notification to subscribe for server status updates for moodle.pucesa.edu.ec, with a 'Prueba gratuita' (Free trial) button.
- IP del servidor:** 13.58.170.168, with the location noted as Columbus.
- Tecnologías:** A list of detected technologies:
  - Apache (Web server)
  - Google Font API (Font script)
  - jQuery (JavaScript library)
  - List.js (JavaScript library)
  - Moodle (LMS)
  - RequireJS (JavaScript framework)
  - Ubuntu (Operating system)
- Herramientas de analítica:** A message stating that no analytics tools were found on the website.
- Doctype:** HTML5.
- Codificación:** A message stating that the encoding is correctly specified as utf8.

Fuente: <https://www.woorank.com/es/www/moodle.pucesa.edu.ec>

A nivel de compresión el JavaScript y el CSS están correctamente comprimidos lo que aporta a que el sitio funcione mucho más rápido, se recomienda para ser aún más eficientes renderizar bloqueos, se sugiere eliminar o diferir JavaScript y el CSS que interfiera con la carga de contenido por encima del pliegue, entendiéndose como encima del pliegue, todo lo que aparecerá primero en la pantalla de un visitante. Esto significa que si una función de JavaScript no aparece tan pronto como el visitante carga la página, no, se incluirá en el encabezado de la página del Moodle. Por parte de la DITIC no, se ha implementado ningún sistema de analítica para la plataforma Moodle, el objetivo de usuarios es la comunidad ya establecida en la universidad.

Imagen No.5 Análisis de construcción de marca



Fuente: <https://www.woorank.com/es/www/moodle.pucesa.edu.ec>

Para la marca que identifique a la plataforma, se han tomado en cuenta las sugerencias de eficiencia por ello la longitud es de 6 caracteres y, se ha establecido el correspondiente favicon, se entiende por favicon al muy conocido ícono de la página o imagen asociada. De acuerdo al análisis si es importante establecer una página personalizada por el departamento de comunicación de la universidad para anunciar página no encontrada que sea direccionada al generarse un HTTP:404.

Imagen No.6 Análisis de disponibilidad de dominios



Fuente: <https://www.woorank.com/es/www/moodle.pucesa.edu.ec>

En cuanto a los dominios sería importante que, a pesar del costo, y de su posible falta de uso, el asegurar dominios como el pucesa.net, info, org, biz, podrían ser

adquiridos por cualquier persona u organización y provocar daños o desinformar a los usuarios de los servicios de la PUCE Ambato.

### **2.2.1. Análisis de las variables que actúan en Moodle sobre una nube privada**

La nube privada de la PUCE Ambato [AWS-PUCESA] es la infraestructura Informática en la que soporta el servicio Moodle de la institución, misma que posee la elasticidad y alta disponibilidad, entendiéndose por elasticidad que los recursos, se asignan y liberan rápidamente, muchas veces de forma automática, da la impresión al usuario que los recursos por el contratados son ilimitados y siempre disponibles (Cierco, 2011), así como, también, una recuperación de corto tiempo ante un siniestro informático que según (Villacís, 2016) es un suceso esporádico, accidental y/o planeado que pueden ser ocasionados por terceros y cuyos resultados, generan grandes pérdidas a la empresa.

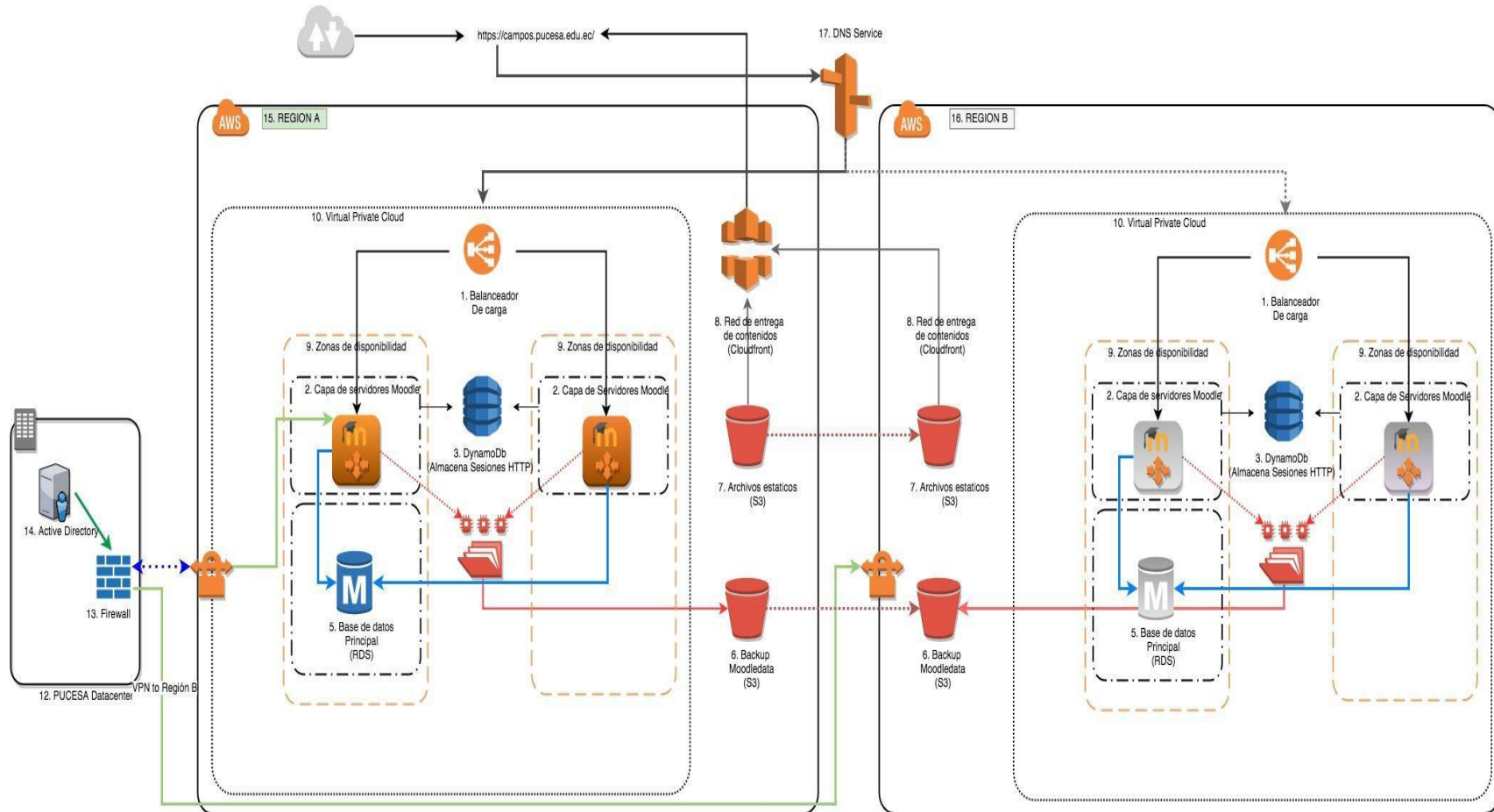
En la plataforma existe el registro de 120 docentes y 1300 estudiantes aproximadamente, se mantiene una concurrencia del hasta 400 usuarios, está dispuesto un servidor Moodle con una capacidad de 24 GB de RAM y 4 cores con una instancia RDS de 15 GB de RAM y 8 cores de una sola zona de disponibilidad.

Se dispone de la facilidad de utilizar la elasticidad de los recursos que ofrece, sabemos que la elasticidad es parte del diseño de la mayoría de los recursos AWS, para implementar esta y todo tipo de arquitectura basada en esta práctica, se necesitó de una preparación adicional que agrega complejidad al diseño e implementación.

Para la PUCE Ambato, la disponibilidad de la plataforma Moodle es crítica, por lo que dispone de una solución basada en una arquitectura escalable y distribuida, capaz de responder a los fallos de cualquier índole o de requerimientos de la infraestructura *cloud*, en este sentido lo dicho, se representa en la gráfica que, a continuación, se presenta.

### 2.2.3 Arquitectura Moodle de alta disponibilidad

Para la implementación de la nube privada de la PUCE Ambato [AWS-PUCESA], se diseña la siguiente arquitectura AWS:



**Gráfico N° 4: Arquitectura Moodle de Alta Disponibilidad**  
**Fuente: DTI PUCE Ambato**

Descripción de los elementos de la arquitectura Moodle de la PUCE Ambato:

1. **Balanceador de carga o Elastic Load Balancing (ELB):** Como la aplicación Moodle de la PUCE Ambato está construida en la red EC2 *Classic*, se utiliza *Classic Load Balancer* que, se encarga de distribuir las peticiones del usuario hacia las instancias que, se encuentren en función en cada zona, así genera alta disponibilidad.
2. **Scaling Group EC2:** La capa de servidores Moodle, se encarga de incrementar o disminuir (*scale in, scale out*) el número de servidores de aplicación. La fluctuación del número de servidores obedece a la carga de peticiones recibidas desde el balanceador de carga y será programado para escalar por hora / fecha o por número de peticiones por segundo durante un periodo continuo de tiempo.
3. **DynamoDB:** Es una base de datos ligera de clave-valor y documentos, pero de gran capacidad de respuesta, ofrece rendimiento en milisegundos de un solo dígito a cualquier escala, tiene el objetivo de centralizar el estado de las sesiones de los usuarios de la plataforma, gestiona más de 10 billones de solicitudes por día y admite picos de más de 20 millones de solicitudes por segundo, cuenta con copia de seguridad, restauración y seguridad integradas, y almacenamiento de caché en memoria para aplicaciones a escala de internet.
4. **EFS:** *Elastic File System* suministra Sistema de Archivos NFS simple, escalable, elástico y totalmente administrado para utilizar con los servicios en la nube de AWS y los recursos locales, está diseñado para ajustar su escala hasta petabytes según, se requiera, sin interrumpir el funcionamiento de las aplicaciones, mediante el aumento y la reducción automática de su

capacidad a medida que elimina o agrega archivos, tiene el objetivo de compartir los archivos de aplicación y de usuarios (moodledata).

5. **Base de datos RDS:** es un servicio de bases de datos relacional en la nube, sencilla de configurar, utilizar y escalar, suministra capacidad rentable y escalable al mismo tiempo que automatiza las tareas administrativas, como el aprovisionamiento de hardware, la configuración de bases de datos, la implementación de parches y la creación de copias de seguridad, administrada con una réplica de lectura sincronizada y que entra en funcionamiento en caso de que la base de datos principal falle, para el caso de Moodle de la PUCE Ambato PostgreSQL.
6. **Almacén de datos S3:** es un sistema de almacenamiento de objetos de alta disponibilidad y durabilidad de costo extremadamente bajo, que ofrece almacenamiento seguro, duradero, flexible para almacenar archivos y copias de respaldo de la plataforma (*Moodle Application* y *Moodle Data*), permite a al DTI de la PUCE Ambato ahorrarse las cargas administrativas de operar y escalar almacenamiento en AWS, para que no tengan que preocuparse por la planificación de la capacidad, el aprovisionamiento de hardware, la replicación de datos, la detección y reparación de errores de hardware o las extensas migraciones de hardware.
7. **Almacén S3:** Almacén de archivos estáticos de la aplicación como *css*, *javascript* e imágenes que ofrece las mismas características, capacidades y bondades que en el numeral 6, y que sirve de Backup o respaldo ubicado estratégicamente en la región B.
8. **Caché de red de entrega de contenido (CDN CloudFront):** Es un componente crítico de casi cualquier aplicación web moderna, almacena en

caché los archivos estáticos de la aplicación y acelera su carga. Para el almacenamiento en caché, un CDN reducirá la carga en el origen de una aplicación y mejorará la experiencia del solicitante al entregar una copia local del contenido desde un borde de caché cercano o Punto de Presencia (PoP). El CDN implementado en infraestructura de la Sede Ambato establece y mantiene conexiones seguras más cercanas al solicitante y, si el CDN está en la misma red que el origen como es el caso de la nube AWS en estudio.

9. **Zonas de disponibilidad (*Availability Zones*):** Cada zona de disponibilidad es un clúster de centros de datos en donde residirán los componentes de la solución, las mejores prácticas de las arquitecturas escalables de la nube sugieren la colocación de un componente en cada zona de disponibilidad con el objetivo de hacerla resistente a la falla, lo cual, se ilustra en el gráfico N° 3. Las zonas de disponibilidad son secciones lógicamente aisladas de una región de AWS. Cada una de las regiones destinadas a soportar la infraestructura de la plataforma Moodle de la PUCE Ambato (A – Ohio y B – Virginia) tiene múltiples zonas de disponibilidad que están diseñadas para operar de manera independiente, estas zonas están separadas en el plano físico por una distancia significativa para protegerse del impacto correlativo con origen en posibles problemas, como rayos, tornados y terremotos. No comparten recursos energéticos ni ninguna otra forma de infraestructura, pero están conectadas entre sí a través de redes privadas de fibra óptica que son rápidas y están cifradas, lo que permite a las aplicaciones realizar una conmutación por error de forma rápida y sin interrupciones. En Amazon han creado AWS de servicios regionales que aprovechan esta independencia entre zonas para alcanzar sus propios objetivos de alta disponibilidad, en el caso PUCE Ambato el servicio regional, se establece en los Estados Unidos de Norteamérica.

10. **Red Privada Virtual (VPC):** Se crearon todos los recursos de infraestructura dentro de la Red Privada Virtual, en inglés *Virtual Private Cloud* (VPC), lo que permite aprovisionar una sección de la nube aislada de forma lógica, en la que, se lanzan recursos AWS en la red virtual que, se ha definido para la PUCE Ambato, donde, se controlan todos los aspectos de una red virtual, incluida la selección de su propio rango de direcciones IP, la creación de subredes, la configuración de tablas de ruteo, gateways de red y otros que el DTI crea necesario.
11. **Sistema PeopleSoft:** Es el sistema que contiene información sobre la gestión, niveles de usuarios, sesiones, docentes, niveles de los estudiantes, entre otras que será transferida con Moodle, esta información sólo le permite realizar la ubicación de los registros correspondientes y hacer una entrega efectiva, hay que señalar que de toda esta información la que, se envía desde la plataforma Moodle al *Active Directory* de la PUCE Ambato son las calificaciones finales por curso al Sistema Informático Academics.
12. **PUCE DataCenter:** Es la red *on Premise* PUCE Ambato, que cuenta con implementación tecnológica de altas características y redundancia en los principales sistemas, contiene los componentes de identidad y datos de la universidad, en su infraestructura física es de suelo elevado (4to. piso) que, se abastece de energía eléctrica por una única línea de distribución, sala de refrigeración, generadores de energía auxiliar (UPS) que abastecen con suficiente holgura la energía necesaria en caso de un evento eléctrico mantiene un cierto grado de tolerancia a dichos fallos, su mantenimiento, se encuentra de forma física por el personal del DTI, que, también, ciertas operaciones las realiza en línea, mantiene un 99.741% de disponibilidad.

13. **Firewall:** El cortafuegos o en inglés *Firewall* del centro de datos PUCE Ambato, proporciona el establecimiento de seguridad de la red, que incluye los nodos que tienen funciones de seguridad que operan en múltiples capas de protocolo, múltiples dispositivos de la red, como son los equipos de acceso remoto, enrutadores, conmutadores, repetidores y tarjetas de red que tienen funciones de seguridad, en el DTI, se ha implementado funciones de firewall distribuido en la red que incluye un componente de definición de políticas que acepta datos de políticas que define cómo, se comportará el cortafuegos.
14. **Active Directory:** Es el Servicio de Directorio para uso en un entorno Windows Server que sincronizará el correspondiente Servicio de Directorios en la nube privada de la PUCE Ambato [AWS-PUCESA], cuenta con funciones de autenticación, autorización y proporciona un framework para otros servicios similares, consiste en una base de datos LDAP que contiene los objetos en red, se crean usuarios, permisos y asignación de recursos, entre otras actividades de administración realizadas por el DTI.
15. **Región A (Ohio):** Amazon Web Services mantiene una Red Global de Regiones que incluye 69 zonas de disponibilidad en 22 regiones geográficas de todo el mundo, según (Amazon, 2019) esta infraestructura de nube global es el entorno de computación en la nube más seguro, extenso y confiable en cualquier lugar, dentro y fuera del planeta. Para la PUCE Ambato, se ha seleccionado la Región de despliegue sugerida e identificada como A, ubicada en Ohio lanzada en el año 2016 con tres zonas de disponibilidad.
16. **Región B (Virginia):** La Región *failover* o conmutación por error, se establece en el Norte de Virginia que al igual que Ohio fue lanzada en el 2016 y cuenta con tres zonas de disponibilidad, se la identifica como la región B y

cumple la misión de ser el respaldo de la zona A, con idénticos atributos de seguridad, disponibilidad, rendimiento, escalabilidad y flexibilidad.

**17. DNS (Route53):** El Servicio de Dominio o en inglés *Domain Name Service* (DNS) Service, es el servicio de internet que traduce los nombres de los dominios, por ejemplo, [www.moodle.pucesa.edu.ec](http://www.moodle.pucesa.edu.ec) en direcciones *Internet Protocol* (IP) que son direcciones numéricas, divididas en 4 octetos que no serán menores a 0 ni mayores a 256, en el caso de la plataforma Moodle de la PUCE Ambato, su IP es 13.58.26.254. Este servicio es imprescindible para poder iniciar cualquier comunicación con otros computadores.

### **2.3. Propuesta de la Investigación**

El uso de las tecnologías de la información en la actualidad son un elemento clave para lograr alto desempeño y entrega de servicios oportunos en la Pontificia Universidad Católica del Ecuador sede Ambato, por ello su departamento de tecnologías de la información, se ha volcado a utilizar y optimizar sistemas que les permitan gestionar y administrar ese preciado recurso que es la información, somos conscientes de que existen ciertos riesgos asociados a su utilización en la plataforma Moodle, y sus posibles consecuencias ya sea por daños provocados, intrusos o causas naturales, que, si no son identificados y evaluados oportunamente, la institución llegaría a quedar seriamente comprometida con sus objetivos y misión.

Para aquello, se aplica las fases de la metodología propuesta, y que a su vez permita aplicarla a la realidad organizacional del DTI de la PUCE Ambato en cuanto a riesgos en la plataforma de educación virtual, se trate.





de gravedad de los resultados encontrados por la herramienta en una escala de alto, medio y bajo.

La tercera fase, se realiza el análisis del riesgo y el impacto al cruzar las variables de vulnerabilidad y amenazas basados en la norma 27017 y con la calificación obtenida, se determina el nivel del impacto inherente que sería crítico, alto, moderado o bajo. Y para finalizar la metodología presenta una cuarta Fase donde se llega a presentar un plan de acción para minimizar el riesgo donde, se sugiere acciones de acuerdo al nivel identificado en la Fase 3 y queda a criterio del DTI de la PUCE Ambato el aplicarlo y gestionar los riesgos de acuerdo a su plan operativo. La eficiencia de la metodología para la evaluación de riesgos Moodle está determinada por la simplicidad que brinda para su aplicación, es muy conocida la cantidad de actividades y procesos que desarrolla un departamento de tecnologías, esta facilidad radica en que, se utilizan estándares o normas conocidas por los profesionales de sistemas como son las normas ISO 27017, ITIL como su fundamento de estructura, solo es necesaria su inclusión dentro del plan de acción anual o semestral de la dirección.

#### **2.4.1. Introducción**

La información y los procesos de la administración de la plataforma Moodle que la apoyan, los sistemas y más recursos, son bienes importantes de la PUCE Ambato, por lo que requieren ser protegidos convenientemente frente a amenazas que pongan en peligro la disponibilidad, la integridad, la confidencialidad de la información, la seguridad de los procesos, los niveles de competitividad, la imagen institucional, y la legalidad, son aspectos necesarios para alcanzar los objetivos de la universidad.

La información generalmente es procesada, intercambiada y conservada en redes de datos, equipos informáticos y soportes de almacenamiento, que son parte de lo que, se conoce como el Data Center o centro de datos de la universidad.

Los sistemas informáticos están sometidos a potenciales amenazas de seguridad de diversa índole, originadas tanto desde dentro de la propia organización, como externa, procedentes de una amplia variedad de fuentes.

Considerado el riesgo como la probabilidad de que ocurra un ataque por parte de la amenaza. (Roldán, 2017) y por otra parte (VOUTSSAS M., 2018) concibe al riesgo como la probabilidad de que un evento nocivo combinado con su impacto, se materializa, es decir, actúa sobre una vulnerabilidad de la plataforma Moodle.

Entre los niveles de riesgos, se encuentra los físicos, entre ellos, accesos no autorizados a la información, catástrofes naturales, sabotajes, incendios, y accidentes; hay que sumarle los riesgos lógicos como contaminación con programas malignos, ataques de denegación de servicio y otros. Fuentes de daños como códigos maliciosos y ataques de intrusos o de denegación de servicios, se presentan cada vez más comunes, ambiciosos y sofisticados.

Con el presente diseño metodológico, se tiene como propósito disminuir o mitigar el nivel de riesgo de forma significativa y con ello la materialización de las amenazas, la reducción del impacto sin necesidad de realizar elevadas inversiones, ni contar con un gran contingente de personal para el departamento.

Elevar los niveles de seguridad en los sistemas informáticos, se consigue mediante un conjunto de controles, que incluyan políticas, procesos, procedimientos, estructuras organizativas y funciones de hardware y software, los que serán establecidos, implementados, supervisados y mejorados en su momento para cumplir los objetivos específicos de seguridad de la organización.

El diseño de la metodología para la evaluación de riesgos está influenciado por las necesidades y objetivos, los requisitos de seguridad y los procesos empleados por la PUCE Ambato, razón por la cual su dimensión y complejidad, se ajusta a lo requerido por la universidad.

El establecimiento de controles generales que, se aplican por igual en todas las áreas y sistemas sin considerar su importancia y particularidades, provocado por la ausencia o ineficiente análisis de riesgos, conduce a que algunas áreas tengan un exceso de protección para las amenazas que enfrentan y otras no estén suficientemente protegidas.

### **2.4.2. Objetivo metodológico**

El objetivo que, se plantea es mantener niveles muy bajos de riesgos sobre los recursos que, se gestionan para la plataforma Moodle, y garantizar la continuidad de las transacciones y operaciones de los usuarios al tiempo que, se administra el riesgo a un costo aceptable, que, se asegure la información de la universidad y mantenga su confiabilidad.

Al entregar la metodología de evaluación de riesgos, se espera que el DTI de la PUCE Ambato haga uso de la herramienta para formalizar sus acciones, y la aplicación dentro de su plan de acción y gestión sea de obligatoriedad, así como su cumplimiento, para así prevenir cualquier amenaza que pudiera generarse y pueda alterar el eficiente servicio que la universidad presta a los usuarios de la plataforma Moodle.

### **2.4.3. Objeto**

La propuesta de la metodología de evaluación de riesgos Moodle PUCE Ambato tiene como objeto de estudio todos los factores que inciden la entrega de valor que produce la plataforma de educación virtual en beneficio de todos sus usuarios.

Tiene un carácter generalizador, que permite su aplicación a otras instituciones educativas que utilicen Moodle como LMS, el acrónimo de *Learning Management System* (Sistema de Gestión de Aprendizaje), y que utilice infraestructura implementada en la Nube con acceso a su administración de tipo IaaS.

Para el estudio de los riesgos a los que, se ve inmersa una plataforma Moodle y al identificar que utiliza *cloud services* como infraestructura para su funcionamiento, se aplica herramientas con los estándares de la ISO 27017 que permite contemplar todos los elementos para evaluar los controles para los proveedores y clientes de servicios de la nube.

#### **2.4.4. Alcance**

El presente documento, se encuentra direccionado a todo el personal académico de la PUCE Ambato, a la Dirección de Tecnologías de la Información de la universidad, que, ya sea por la responsabilidad que tienen asignadas con la gestión de los recursos informáticos, o por las bondades que, por la plataforma educativa, se entrega a los docentes, todos aportan a su efectivo funcionamiento y entrega de valor a la institución.

En cuanto al alcance del presente trabajo investigativo y al tratarse de una metodología de evaluación de riesgos, no, se interviene en la gestión del riesgo y mucho menos el plan de continuidad del negocio, será de utilidad como materia para futuros trabajos de investigación.

#### **2.4.5. Documentos Recomendados**

Se recomienda, que, para profundizar en la materia, se observe la norma ISO/IEC 27017 Controles de seguridad para Servicios Cloud, que proporciona controles para proveedores y clientes de servicios en la nube, aclara las funciones y responsabilidades de ambas partes para ayudar a que los servicios en la nube sean tan seguros como el resto de datos incluidos en un sistema de gestión certificado.

Para la gestión entre el centro de datos y el ambiente *cloud*, se necesaria la participación de personal tanto del DTI de la PUCE Ambato y de IT Era, por tanto esta interacción para la gestión será, también, evaluada porque participa para la entrega del servicio a los usuarios, por tanto, se recomienda como bibliografía necesaria acudir a la Biblioteca de Infraestructura de Tecnologías de la Información o en inglés *Information Technology Infrastructure Library* (ITIL) en su tercera edición, que es un conjunto de conceptos y buenas prácticas usadas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías y las operaciones relacionadas con las TIC's. (Guzmán, 2012). Una mesa de servicio en















































































































# Amazon Web Services, Inc.

## Scope for certificate 2015-015

- ▶ Illinois, United States
- ▶ Indiana, United States
- ▶ Massachusetts, United States
- ▶ Minnesota, United States
- ▶ Missouri, United States
- ▶ Nevada, United States
- ▶ New Jersey, United States
- ▶ New York, United States
- ▶ Ohio, United States
- ▶ Oregon, United States
- ▶ Pennsylvania, United States
- ▶ Texas, United States
- ▶ Virginia, United States
- ▶ Washington, United States



This scope (edition November 5, 2019) is only valid in connection with certificate 2013-015.

## **Funciones del Director del Departamento de Tecnología de la Información**

- Establecer el gobierno de tecnología de la información en la institución.
- Definir la infraestructura tecnológica necesaria para la entrega de servicios tecnológicos sobre actividades académicas y administrativas, en forma adecuada y oportuna.
- Administrar los recursos humanos y tecnológicos para la implementación de proyectos, mantenimiento de equipos y atención de operaciones digitales.
- Diseñar, implementar y controlar procesos que consoliden la estrategia tecnológica institucional.
- Planificar, ejecutar y controlar los planes operativos anuales alineados al plan estratégico de desarrollo institucional.
- Coordinar la adquisición de infraestructura tecnológica con las dependencias correspondientes para el desarrollo de proyectos y garantía de la disponibilidad de los servicios tecnológicos.
- Supervisar la calidad de atención a usuarios por parte de todo el Departamento de Tecnología de la Información.
- Implementar el uso de las mejores prácticas para la gestión de servicios de tecnología de la información para garantizar eficiencia y eficacia en el uso y provisión de recursos tecnológicos.
- Garantizar el mejoramiento continuo de los servicios que son entregados por el área de TI hacia todas las unidades universitarias.
- Asignar responsabilidades a las de áreas de Medios Digitales, Comunicaciones e Infraestructura y Aplicaciones y Desarrollo de Software.

## **Funciones del Técnico en Medios Digitales**

- Administrar el sitio web institucional, su mantenimiento y seguridad.
- Gestionar el hospedaje del portal web institucional.

- Optimizar el sitio web para una ágil navegación y posicionamiento web.
- Monitorear las estadísticas del sitio web institucional a través de analítica y sugerir planes de mejora para optimizar su rendimiento.
- Administrar las redes sociales o medios digitales de la institución.
- Colaborar con el Departamento de Comunicación y Marketing en la elaboración del plan de marketing digital y presupuesto para su ejecución.
- Planificar la agenda de contenidos en coordinación con el Departamento de Comunicación y Marketing.
- Gestionar contenidos digitales generados por el Departamento de Comunicación y Marketing.
- Potenciar los vínculos entre la institución y seguidores en redes sociales.
- Vincular la estrategia social con visitas al sitio web institucional.
- Interactuar con la comunidad digital al ofrecer información institucional de forma oportuna.
- Escalar de forma proactiva las sugerencias, inconformidades y felicitaciones receptadas a través de medios digitales, hacia las unidades correspondientes.
- Evaluar los resultados de la estrategia de marketing digital, sugiere alternativas.
- Administrar la mesa de servicio del Departamento de Tecnología de la Información.

### **Funciones del Especialista en Aplicaciones y Desarrollo**

- Planificar, ejecutar y controlar el área de Aplicaciones y Desarrollo de Software con sus técnicos asignados.
- Gestionar proyectos que sean de Aplicaciones y Desarrollo de Software.
- Diseñar, implementar y controlar procesos y procedimientos correspondientes al área de Aplicaciones y Desarrollo de Software.
- Desarrollar software como soluciones a necesidades que la institución demande para optimizar procesos institucionales.

- Evaluar la calidad del software.
- Administrar las aplicaciones y bases de datos que entreguen servicio a las unidades académicas y administrativas de la universidad.
- Generar reportes personalizados de las bases de datos disponibles.
- Gestionar los servidores web de todas las aplicaciones que provean servicios a la comunidad universitaria.
- Controlar la seguridad de las aplicaciones y bases de datos institucionales.
- Ejecutar los respaldos de aplicaciones y bases de datos operativas.
- Administrar el gestor documental de la institución.
- Capacitar a la comunidad universitaria sobre el uso de aplicaciones.
- Asignar tareas y responsabilidades a Técnicos de Desarrollo de Software.

### **Funciones del Técnico en Desarrollo de Software**

- Cumplir con los procesos y procedimientos correspondiente al área de Aplicaciones y Desarrollo de Software.
- Desarrollar software conforme la supervisión del especialista de Aplicaciones y Desarrollo de Software.
- Gestionar las aplicaciones y bases de datos institucionales.
- Ejecutar reportes a medida solicitados por usuarios finales.
- Atender requerimientos realizados por usuarios finales en torno a aplicaciones y desarrollo de software.
- Capacitar a la comunidad universitaria sobre el uso de aplicaciones.
- Ejecutar las tareas designadas por el Especialista de Aplicaciones y Desarrollo de Software.

### **Funciones del Especialista en Comunicaciones e Infraestructura Tecnológica**

- Administrar el área de Comunicaciones e Infraestructura Tecnológica y sus técnicos asignados.

- Planificar, ejecutar y controlar los proyectos que sean de Comunicaciones e Infraestructura Tecnológica.
- Diseñar, implementar y controlar procesos y procedimientos correspondiente al área de Comunicaciones e Infraestructura Tecnológica.
- Diseñar, implementar, y supervisar comunicaciones y/o redes de datos seguras y eficientes sobre las cuales, se entregan servicios tecnológicos de forma confiable.
- Garantizar un servicio de internet seguro y eficiente.
- Asegurar la disponibilidad de los servicios tecnológicos institucionales.
- Administrar el centro de datos y sus equipos de cómputo, comunicaciones, potencia y acondicionamiento.
- Controlar la seguridad de la información de la sede.
- Dimensionar soluciones tecnológicas a ser adquiridas para la institución.
- Mantener equipos tecnológicos del centro de datos, personal administrativo, docentes y laboratorios de computación,
- Mantener la infraestructura tecnológica de aulas y salas de la institución en óptimas condiciones.
- Suministrar servicios de audio y videoconferencia.
- Proveer software a todos los miembros de la comunidad universitaria.
- Asignar tareas y responsabilidades a Técnicos de Infraestructura Tecnológica.

### **Funciones del Técnico en Infraestructura**

- Cumplir con los procesos y procedimientos correspondiente al área de Comunicaciones e Infraestructura Tecnológica.
- Monitorear y mantener comunicaciones y/o redes de datos y sus equipos.
- Mantener equipos tecnológicos del personal administrativo, docente, laboratorios de computación, aulas y salas de la institución en óptimas condiciones.

- Atender requerimientos realizados por usuarios en torno a infraestructura tecnológica, audio y videoconferencia.
- Elaborar el inventario de equipos tecnológicos de la institución conforme criterios del Departamento de TI.
- Proveer software a todos los miembros de la comunidad universitaria.
- Ejecutar las tareas designadas por el Especialista de Comunicaciones e Infraestructura.