ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

PROPUESTA METODOLÓGICA PARA UN PLAN DE CONTINUIDAD DEL NEGOCIO ALINEADA A LA NORMA ISO/IEC 22301 Y RECUPERACIÓN ANTE DESASTRES EN CLOUD

TESIS DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN CONECTIVIDAD Y REDES DE TELECOMUNICACIONES

KATYA VERÓNICA VILLACÍS ONOFA
katy_vero16@yahoo.com

DIRECTOR: ANA MARÍA ZAMBRANO VIZUETE
ana.zambrano@epn.edu.ec
CODIRECTOR: JOSÉ ADRIÁN ZAMBRANO MIRANDA
jose.zambrano@epn.edu.ec

Quito, julio 2018

AVAL

Certificamos que el presente trabajo fue desarrollado por Katya Verónica Villacís Onofa, bajo nuestra supervisión.

ANA MARÍA ZAMBRANO VIZUETE
DIRECTOR DEL TRABAJO DE TITULACIÓN

JOSÉ ADRIÁN ZAMBRANO MIRANDA
CODIRECTOR DEL TRABAJO DE TITULACIÓN

DECLARACIÓN DE AUTORÍA

Yo, Katya Verónica Villacís Onofa, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

KATYA VERÓNICA VILLACÍS ONOFA

DEDICATORIA

A mis padres, a quien admiro y son mi mayor ejemplo de superación.

A mi nena preciosa que es mi inspiración y me da mucha fuerza para culminar esta etapa.

AGRADECIMIENTO

A mis padres, a mi hermana y a mi esposo por su apoyo incondicional. Al Centro de Educación Continua de la Escuela Politécnica Nacional, especialmente al Sr. Director por permitirme desarrollar este Trabajo de Titulación.

A mi profesora Dra. Anita Zambrano, por su guía, sus conocimientos y su tiempo brindado para el cumplimiento de los objetivos.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente Trabajo de Titulación se enfoca en lograr una propuesta metodológica para un Plan de Continuidad del Negocio (BCP) alineada a la Norma ISO/IEC 22301 y recuperación ante desastres en *Cloud (DRaaS)* para el Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN) y de manera específica en la Coordinación de Gestión de Tecnologías (CGT) incluyendo para el prototipo a realizar 3 servidores: Servidor de Base de Datos, Servidor de Archivos y Servidor Web.

El **Capítulo 1** realiza una introducción en general del *Cloud Computing*, enfocándose en sus tipos de topología y despliegue; y un estudio arduo de proveedores quienes entregan el servicio de DRaaS. Además se ofrece un análisis de la situación actual del CEC-EPN y de la CGT. Se analiza la norma ISO / IEC 22301 enfocándose en cada una de sus cláusulas.

El **Capítulo 2** presenta el desarrollo del BCP para el CEC-EPN en base a los requerimientos previamente estudiados y siguiendo la norma establecida. Siguiente se detalla la Implementación del prototipo DRaaS, enfocándose en los servicios y configuraciones a realizar.

El **Capítulo 3** presenta las pruebas necesarias para comprobar el cumplimiento del prototipo. Analiza los resultados obtenidos en el prototipo y una comparación de los beneficios conseguidos. Conjunto se detalla una encuesta realizada a los integrantes de la CGT para comprobar su satisfacción.

Finalmente, el **Capítulo 4** presenta las conclusiones y recomendaciones obtenidas de la realización de este trabajo.

PALABRAS CLAVE: *Cloud*, Norma ISO/IEC 22301, BCP, DRaaS, Instancia, pruebas.

ABSTRACT

This thesis project is focused on reaching a methodological proposal for a Business Continuity Plan (BCP) aligned with ISO/IEC Standard 22301 and Cloud (DRaaS) disaster recovery. This shall been done for the Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN) (Center for Continuing Education at the Nacional Polytechnic School), specifically for the Department of Technology Management (CGT). This proposal will also include a prototype for three servers: a Database Server, a File Server and a Web Server.

Chapter 1 provides a general introduction to Cloud Computing, focusing on its types of topology and its use. This chapter will also provide an arduous study on providers that offer DRaaS service. Additionally, an analysis on the current situation at CEC-EPN and CGT will be provided, analyzing ISO/IEC Standard 22301 and focusing on each and every one of its clauses.

Chapter 2 develops the BCP for CEC-EPN based on the previously studied requirements, all the while following the established standard. Following this, the implementation of the DRaaS prototype will be detailed with a focus on the services and settings to be conducted.

Chapter 3 presents the necessary information to prove the prototype's compliance and analyzes the results obtained from the prototype. A comparison of the acquired benefits will also be given. A survey conducted of the members of the CGT will be included to demonstrate their satisfaction.

Chapter 4 presents the conclusions and recommendations obtained from the execution of this project.

KEY WORDS: Cloud, ISO/IEC Standard 22301, BCP, DRaaS, Instance, Proof

1. INTRODUCCIÓN

Actualmente, *Cloud Computing*[1] es una nueva tecnología que apoya el Plan de Continuidad del Negocio por sus siglas en inglés (*BCP Business Continuity Plan*), las cuales son un conjunto de estrategias para asegurar las operaciones de instalación en corto tiempo después de un desastre y que sirven a su vez para definir procedimientos a seguir en caso de un desastre, restablecer la continuidad de negocio en el menor tiempo posible y cómo se restablecería los procedimientos sin tener fallas en el intento.

El Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN) hasta el momento no cuenta con un BCP ni con un Plan de Recuperación de Desastres por sus siglas en inglés (*DRP Disaster Recovery Plan*), el cual no es más que un conjunto de actividades que plasma cómo recuperarse ante un desastre; y al carecer del mismo, ha sido identificado cómo un riesgo crítico, ya que los servicios y aplicaciones deben estar disponibles las 24 horas del día, sin ningún tipo de interrupción. En el caso de que se presente un desastre natural o tecnológico se apagarían todos los servidores y de esta forma no se levantaría ningún servicio informático, viéndose afectados estudiantes y profesores que laboran en la institución, ya que los equipos físicos se encuentran centralizados.

Por otro lado el CEC-EPN al ser una institución pública, se encontraría incumpliendo la Norma de Control Interno 410-11 de la Contraloría General del Estado; plan de contingencias en la que cita "*Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado*" [1].

Por estas razones se ha identificado la necesidad de realizar una propuesta metodológica para un BCP; y un DRP mediante *Cloud* en el CEC-EPN. Por otro lado la principal ventaja sería salvaguardar la información más importante del negocio y realizar copias de seguridad tanto de la información, como de los sistemas informáticos; sería escalable, su almacenamiento sería prácticamente ilimitado; además independiente tanto del tipo de dispositivo como de la ubicación y permitiría la optimización de recursos. Con esta

[1] Cloud Computing.- o computación en la nube, es un conjunto de herramientas que se usan con la finalidad de ofrecer ciertos servicios mediante Internet.

tecnología se estaría protegiendo información crítica, información histórica, registros de información de estudiantes, sistemas informáticos y aplicaciones que son indispensables para el funcionamiento normal del CEC-EPN. Por estas ventajas citadas, la tecnología en la nube se plantea como la mejor solución, ya que es un modelo tecnológico que permite acceder a un conjunto de recursos informáticos tantos de hardware como de software de manera ubicua. La misma posee un sin número de ventajas, siendo una de las más importantes la reducción de costos y la restauración de los servicios en el menor tiempo posible [2].

1.1 Pregunta de Investigación

El presente Trabajo de Titulación busca responder a la siguiente pregunta: *¿Es posible realizar una Propuesta Metodológica que guie un Plan de Continuidad del Negocio alineado a la Norma ISO/IEC 22301 y una Recuperación de Desastres mediante Cloud que mejore el accionar del CEC-EPN en un desastre?*

1.2 Objetivo General

Elaborar una propuesta metodológica para un Plan de Continuidad del Negocio alineada a la norma ISO/IEC 22301 y una recuperación ante desastres en *Cloud*. Caso estudio: Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN).

1.3 Objetivos Específicos

- Analizar la situación actual del CEC-EPN.
- Analizar las tecnologías necesarias que brindan como servicio BCP y DRaaS.
- Desarrollar una propuesta metodológica para un plan de continuidad del negocio y recuperación ante desastres en *Cloud* para el CEC-EPN.
- Implementar un prototipo de recuperación ante desastres en Cloud para un departamento del CEC-EPN.
- Analizar los resultados de las pruebas realizadas.

1.4 Alcance

Esta propuesta metodológica presentará el siguiente alcance con respecto a puntos citados a lo largo del documento:

- Estudiar la situación actual del CEC-EPN y de manera específica de la Coordinación de Gestión de Tecnologías (CGT), departamento en el cual se realizará la implementación del prototipo.

- Estructurar una Propuesta Metodológica para un BCP alineado a la norma ISO/IEC 22301 e investigar tres proveedores *Cloud* que brinden el servicio DRaaS como por ejemplo Amazon, Microsoft y Google; ya que son líderes en el cuadrante de Gartner como servicios públicos de almacenamiento en la nube.
- Implementar un prototipo para la CGT del CEC-EPN; en la que se ejecute el DRaaS para: 3 bases de datos del core del sistema, para un servidor web y para un servidor de archivos (este alcance se encuentra definido en el plan de tesis).

1.5 Marco Teórico

1.5.1 Introducción

El presente capítulo detalla la situación actual del Centro de Educación Continua de la Escuela Politécnica Nacional (CEC-EPN) y de manera especial de la Coordinación de Gestión de Tecnologías (CGT) ya que es el departamento donde se implementará el prototipo. Además, se revisará los aspectos teóricos sobre el *Cloud Computing*, Plan de Continuidad del Negocio (BCP), la Norma ISO/IEC 22301:2012, el Plan de Recuperación de Desastres (DRP), la Recuperación ante Desastres como un Servicio (DRaaS) y un análisis de los proveedores que brindan el servicio de DRaaS.

1.5.2 Antecedentes Centro de Educación Continua (CEC-EPN)

El CEC-EPN fue creado en 1989 ante el Ministerio de Educación con el objetivo primordial de capacitar profesores en nivel de Secundaria. Entre las fechas de 1991 y 1995, el CEC-EPN facilitó varios servicios basado en la capacitación y modernización de las diferentes metodologías de Investigación y Educación a diferentes empresas e instituciones. Sin embargo, desde mayo de 1995 se rige bajo el normativo de la Escuela Politécnica Nacional, con el propósito de ofrecer conocimientos y desarrollar actividades académicas que propendan a la actualización permanente de los miembros de la comunidad de la Escuela Politécnica Nacional, de los egresados de la Institución; además de las empresas que son públicas, privadas y de la comunidad en general. Por tanto, se encarga de ser el nexo con el medio externo, con personas naturales y empresas que requieran servicios de capacitación continua [3].

1.5.3 Descripción de la Información Institucional (CEC-EPN)

La Institución tiene como visión el de "*ser el referente nacional en educación continua, con calidad certificada"* y a su vez tiene como misión *"potenciar el conocimiento del sector productivo del Ecuador*" [7]. De la misma forma con respecto a la Política de Calidad del CEC-EPN es el de "*Mantener permanentemente, en el campo de la Educación Continua, un compromiso de calidad con las partes interesadas, entendiendo sus requerimientos, logrando su satisfacción con oportunidad, mejoramiento continuo, creatividad y visión de país; cumpliendo la legislación pertinente"* [3].

Igualmente el CEC-EPN ha implementado el Sistema de Gestión de Calidad ISO 9001 desde el año 2005, el mismo que cumple con la Norma ISO 9001: 2008. Este centro cada cinco años realiza la planificación estratégica de la organización en la que se revisa la visión, la misión y los objetivos estratégicos. A partir de este análisis interno realizado en dicho centro surge la necesidad de incrementar la seguridad de la información que maneja el CEC-EPN.

En cuanto a la situación actual y análisis de la infraestructura física del CEC-EPN la institución cuenta con ocho áreas y tres sedes; las mismas que se describen a continuación. Las áreas que forman parte del CEC-EPN son [3]:

- Dirección.
- Coordinación de Capacitación y Consultoría.
- Coordinación de Lingüística.
- Coordinación Administrativa Financiera.
- Coordinación de Calidad y Talento Humano.
- **Coordinación de Gestión de Tecnologías (CGT).**
- Coordinación de Marketing.
- Unidad de Educación Virtual.

Sedes que conforman el CEC-EPN [3]:

Sede 1.- Escuela Politécnica Nacional, Edificio Aulas y Relación con el Medio Externo, Etapa I.
Sede 2.- Baquedano 222 y Reina Victoria esquina. Edificio Araucaria.
Sede 3.- Ladrón de Guevara E11-16 y Pasaje España.

1.5.3.1 Coordinación de Gestión de Tecnologías (CGT)

La CGT es un departamento que nace en base a las necesidades de la organización desde el año 2004, cuyo objetivo principal es proveer el soporte tecnológico en base a la infraestructura que se encuentra en los laboratorios y la red de la institución la cual permite el desarrollo normal de las actividades planificadas por todas las unidades del CEC-EPN. Sus objetivos específicos son los siguientes [3]:

- Instalar, administrar y operar las herramientas tecnológicas que son necesarias para garantizar el desarrollo de cada una de las actividades y de la comunicación de manera eficaz.
- Asegurar un manejo óptimo de cada uno de los recursos tecnológicos mediante una apropiada adquisición, asignación, custodia, mantenimiento, actualización, contingencia, adiestramiento y control en base a criterios de costo – beneficio.
- Análisis, diseño e implementación de aplicaciones que permitan la automatización de procesos tanto operativos como manuales.
- Proveer información oportuna y confiable (íntegra y consistente) que proporcione una toma de decisiones de manera eficaz al CEC-EPN.

Es importante indicar que la CGT es un departamento que actualmente (2018) se encuentra formado por 9 personas y a su cargo tiene la responsabilidad de administrar toda la infraestructura tecnológica y todos los servicios necesarios para que el CEC-EPN pueda desarrollar sus actividades con normalidad.

Por otro lado, la CGT es la responsable de:

- Mantener un repositorio de información de la operación del CEC-EPN la misma que es utilizada como insumo para las aplicaciones.
- Disponer de la información de servidores, equipos, aplicaciones y red a nivel de instalación, configuración y operación.
- Autorizar a los usuarios para el acceso a los servicios tecnológicos según su rol.
- Desarrollar aplicaciones y módulos necesarios para el desarrollo del mismo.

Dados los objetivos antes planteados surge la necesidad de estructurar un BCP para la institución y la implementación de un prototipo DRaaS para la CGT, debido a que es un departamento crítico para el funcionamiento adecuado de la institución.

1.5.3.2 Vulnerabilidades y Riesgos

Vulnerabilidad es también conocida como la debilidad de un activo o grupo de activos que puede ser afectada por una amenaza. Generalmente las vulnerabilidades están dadas por determinados errores en la implementación o mala configuración [4].

A continuación en la Tabla 1.1 y en la Tabla 1.2 se presenta el nivel de vulnerabilidad y las vulnerabilidades identificadas en los informes de la consultoría que se realizó en el CEC-EPN en noviembre 2017 por un proveedor externo.

Tabla 1.1. Nivel de Vulnerabilidad [5].

Nivel	Nivel de Vulnerabilidad
3	Alto
2	Medio
1	Bajo

Tabla 1.2. Vulnerabilidades identificadas en el CEC-EPN [6].

Vulnerabilidad	Nivel	
Los profesores divulgan las contraseñas a los estudiantes. No hay un cambio periódico de esta clave.	3	ALTO
No se cuenta con un procedimiento formal y periódico para reorganización del cableado, mantenimiento y reemplazo de los mismos.	3	ALTO
Se cuenta con un anillo de fibra para interconectar las tres sedes; el mismo se encuentra conectado en los postes de cableado eléctrico por lo que es susceptible a cortes, rupturas o daños físicos. (Ha pasado 2 veces en 7 años).	2	MEDIO
El servicio de Internet se lo recibe a través de la EPN, por tanto la administración no depende del personal de la CGT. La mayoría de interrupciones no se deben a problemas del proveedor, sino a situaciones adversas en el funcionamiento de los equipos de conectividad de la EPN.	2	MEDIO
La red está dimensionada para un cierto número de conexiones (100 usuarios por Access Point), sin embargo, se ha revisado que hay más usuarios conectados, puesto que las claves se han filtrado a los estudiantes de forma no autorizada. No se cambia la clave de forma periódica.	3	ALTO
No se cuenta con sistemas de respaldos.	3	ALTO

Por otro lado, el “Riesgo” es la posibilidad de que ocurra un incidente y que éste repercuta negativamente en la organización; es decir es el efecto de la incertidumbre de que suceda algo positivo o negativo. Para el análisis de los mismos, se debe identificar los activos así

como las vulnerabilidades y las amenazas a los que está expuesto; además de la probabilidad de que ocurra y el impacto en la misma, con el objetivo de reducir, trasladar o evadir la ocurrencia.

A continuación se presenta algunos de los riesgos identificados en el contexto externo y en el contexto interno por la consultoría realizada en el CEC-EPN en noviembre 2017.

Tabla 1.3. Riesgos identificados en el contexto externo del CEC-EPN [5].

Factor Externo	Amenazas	Situación de Riesgo
1. Económico		
1.1. Recesión Económica	**1.1.1** Un decrecimiento de la actividad económica en el país, podría generar una disminución de los recursos económicos asignados para el sector de la educación.	Se podría presentar dificultad en la ejecución de proyectos planificados que dependen de recursos económicos asignados a la EPN (tal como construcción de otro edificio).
2. Político		
2.1. Cambio de autoridades de la EPN	**2.1.1** La mayoría de decisiones administrativas son tomadas por las autoridades de la EPN: Consejo Politécnico y el Rector, y no se cuenta con un representante del CEC-EPN en el Consejo Politécnico.	Esto podría ocasionar que las decisiones tomadas por el Rector y el Consejo no favorezcan a los intereses y necesidades del CEC-EPN, impidiendo, retardando o interrumpiendo así la ejecución de proyectos prioritarios.
3. Socio-cultural		
3.1. Expectativa y aceptación de la oferta de capacitación	**3.1.1** Las expectativas y aceptación de la oferta de capacitación del CEC-EPN depende en gran manera de constantes y acertados estudios que tomen en cuenta el rango de edad de los estudiantes, ubicación geográfica, nivel de estudios y especialización.	El CEC-EPN cuenta con este tipo de estudios como parte de sus procesos. Sin esta información podría existir desenfoque de los servicios entregados y por tanto ausencia de clientes interesados en los servicios que oferta.
4. Tecnológico		
4.1. Resistencia a cambios y a nuevas tecnologías	**4.1.1** Las tendencias en educación virtual involucran constantes cambios tecnológicos y nuevas formas de aprendizaje.	Podría existir resistencia en ciertos grupos de clientes, especialmente en el uso de servicios en línea para matrículas y pagos.

Tabla 1.4. Riesgos identificados en el contexto interno del CEC-EPN [5].

Factor Interno	Debilidades	Situación de Riesgo
1. Capacidad Directiva		
1.1. Limitado campo de acción del nivel directivo	**1.1.1** El CEC-EPN tiene una alta dependencia directiva de la EPN, lo cual limita su campo de acción y toma de decisiones.	Se podría afectar la ejecución de estrategias organizacionales establecidas según la misión y visión del CEC-EPN, así como la capacidad de toma de decisiones por parte de la Dirección.
2. Capacidad del Talento Humano		
2.1. Nivel de competencias del talento humano	**2.1.1** La contratación de personal administrativo del CEC-EPN depende en gran parte de la EPN. Esto podría ocasionar que no se contrate el personal suficiente, o que esté acorde con las necesidades, conocimientos y funciones requeridos para el cargo.	Existe el riesgo de prescindir de personal necesario, retrasos en la contratación, o que el personal vinculado no cuente con las competencias apropiadas para sus funciones.
3. Capacidad Tecnológica		
3.1. Sistemas de gestión no integrados ni automatizados	**3.1.1** El CEC-EPN dispone de diversos sistemas de información y aplicaciones, algunas desarrolladas internamente y otras adquiridas, o de uso general y obligatorio por parte de las entidades públicas. Esta tecnología no está totalmente integrada y ciertas funcionalidades se manejan manualmente.	Existe el riesgo de pérdida de la calidad y seguridad de la información (disponibilidad, confidencialidad, integridad); también se podría ver mermada la eficiencia de los procesos que utilizan la información involucrada.
3.2. Falta de estrategias de Continuidad del Negocio	**3.1.2** No se cuenta con un Plan de Continuidad del Negocio que permita mitigar el impacto en caso de interrupción de las operaciones del negocio, especialmente para los procesos críticos del CEC-EPN.	El CEC-EPN corre el riesgo de no poder continuar con sus operaciones normales ante la ocurrencia de eventos que ocasionen la interrupción de las operaciones, la entrega de servicios y/o el procesamiento de la información.
4. Capacidad Financiera		
4.1. Dependencia del Presupuesto del Estado (egresos)	**5.1.1** El CEC-EPN depende financieramente de la EPN (y por medio de ésta, del Estado) para la ejecución de proyectos de gran magnitud.	Existe el riesgo de no poder ejecutar los proyectos anuales planificados, debido a que la EPN podría no aprobar la asignación de recursos financieros para ejecutar los proyectos de mayor magnitud del CEC-EPN.

1.5.3.3 Análisis de Impacto del Negocio

El impacto del negocio es otro elemento que sirve para evaluar la afectación que se produciría en el CEC-EPN en caso de un desastre o incidente de forma desprevenida. Este análisis en vez de ejemplificar cual es la evaluación de los riesgos, se enmarca en el cómo se podría ver afectada la organización, basándose en cada una de sus características, el análisis y toda la valoración de las posibles amenazas en base a la seguridad. Además, se debe medir el impacto de manera crítica y las probabilidades en cuanto a la ocurrencia [7]. Como elemento principal en el análisis de impacto del negocio se debe tomar en cuenta la identificación de los procesos que se consideren críticos en toda la institución y desde ese punto de vista priorizarlos, partiendo de varios criterios y teniendo en cuenta que entre mayor sea el impacto, mayor será la prioridad. A modo de conclusión se puede decir que el análisis del impacto va a determinar las posibles afectaciones que puede tener una organización. Por estas razones se debe crear un BCP para dar respuestas a la misma de manera eficiente y oportuna. Este BCP será desarrollado en el **Capítulo II Apartado 2.1.2.2** con más detalle.

A continuación se presenta los criterios para determinar los niveles de impacto según los informes presentados por la consultoría realizada en el CEC-EPN en noviembre 2017.

En la Tabla 1.5 se presentan los niveles de impacto, los mismos que se encuentran categorizados en cinco niveles y en la Tabla 1.6 se presentan los niveles de impacto en base a las categorías más relevantes identificadas durante el proceso de la consultoría en el CEC-EPN.

Tabla 1.5. Niveles de Impacto.

Niveles	Niveles de Impacto
1	Insignificante
2	Menor
3	Moderado
4	Significativo
5	Extremo

Tabla 1.6. Niveles de Impacto en el CEC-EPN en base a las Categorías [5].

Categoría	Niveles de Impacto				
	1	2	3	4	5
	Insignificante	Menor	Moderado	Significativo	Extremo
1. Servicio al cliente	Sin reclamo de clientes. La competencia no tiene ventajas.	Los reclamos de los clientes son aislados. La ventaja de la competencia es mínima.	Los reclamos de los clientes son importantes; hay pérdida menor de clientes.	Los reclamos de los clientes son masivos; hay pérdida importante de clientes.	Hay pérdida masiva de clientes; se presentan litigios contra las unidades de negocio.
2. Interrupción del servicio u operaciones	El proceso no sufre alteración.	El proceso se interrumpe hasta en un 20%.	El proceso se interrumpe hasta en un 40%.	El proceso se interrumpe hasta en un 60%.	El proceso se interrumpe más del 60%.
3. Seguridad	La información relacionada con el incidente de seguridad se conoce solamente en el área de TI; podría causar disminución en la seguridad, o dificultar la investigación de un incidente.	La información relacionada con el incidente de seguridad se conoce en el área de TI; y podría ser la causa de la disminución en la seguridad, o dificultar la investigación de un incidente.	La información relacionada con el incidente de seguridad se conoce dentro de la organización; probablemente sea causa grave de un incidente de seguridad, o dificultar la investigación de incidentes graves.	La información relacionada con el incidente de seguridad se conoce dentro de la organización; probablemente es causa de un serio incidente de seguridad, o dificultar la investigación de incidentes serios.	La información relacionada con el incidente de seguridad se conoce públicamente; es posible que sea causa de un incidente excepcionalmente serio de seguridad, o dificultar la investigación de incidentes serios.

A continuación se presenta los niveles de probabilidad que no es más que la posibilidad de ocurrencia de un evento.

Tabla 1.7. Niveles de Probabilidad [5].

Probabilidad	Nivel	Frecuencia
Seguro	6	Se puede presentar todos los días y dado que el nivel 6 no se ha presentado nunca, no es considerado.
Casi Seguro	5	Se puede presentar más de una vez al mes, por tanto más de 12 veces en un año.
Muy Probable	4	Se puede presentar entre 7 y 12 veces en el año.
Posible	3	Se puede presentar entre dos (2) y seis (6) veces en el año.
Improbable	2	Se puede presentar máximo una (1) vez en el año.
Raro	1	Se puede presentar máximo (1) vez al año, pero no todos los años. Podría ocurrir rara vez.

1.5.3.3.1 Mapa de Riesgos en el CEC- EPN

El mapa de riesgo es utilizado para indicar los niveles de riesgo, es decir *"consiste en la valoración producto de los niveles de Probabilidad y niveles de Impacto de cada uno de los riesgos; el Nivel de Riesgo es el resultado de multiplicar el impacto por la probabilidad*" [5]. El nivel de riesgo se calcula siguiendo la Ecuación 1.1:

$$NivelRiesgo = \mathrm{Im}\,pacto * \mathrm{Pr}\,obabilidad$$

Ecuación 1.1. Nivel de riesgo

En la Tabla 1.8 se presenta el mapa de riesgo donde se indican los diferentes niveles de riesgo según el impacto y la probabilidad. Este mapa de riesgo fue desarrollado en el proceso de la consultoría informática realizada en el CEC-EPN en noviembre 2017 por un proveedor externo contratado.

Tabla 1.8. Mapa de riesgo del CEC-EPN [5].

Extremo	**5**	5 MEDIO	10 ALTO	15 ALTO	20 CRÍTICO	25 CRÍTICO
Significativo	**4**	4 MEDIO	8 MEDIO	12 ALTO	16 ALTO	20 CRÍTICO
Moderado	**3**	3 MEDIO	6 MEDIO	9 MEDIO	12 ALTO	15 ALTO
Menor	**2**	2 BAJO	4 BAJO	6 MEDIO	8 MEDIO	10 ALTO
Insignificante	**1**	1 RUTINA	2 RUTINA	3 BAJO	4 BAJO	5 MEDIO
Impacto / **Probabilidad**		1	2	3	4	5
		Raro	**Improbable**	**Posible**	**Muy Probable**	**Casi Seguro**

Realizando un análisis cuantitativo de la Tabla 1.8 se puede identificar que cuanto mayor sea el impacto y la probabilidad de ocurrencia, el riesgo crece; así se obtendría un riesgo crítico (25) cuando su impacto sea “extremo” (5) y la probabilidad sea “casi seguro” (5). De la misma manera, si el impacto es “insignificante” (1) y la probabilidad de ocurrencia sea “raro” (1) el riesgo alcanza su nivel más bajo. Una vez analizado el mapa de riesgo, se debe establecer los criterios de tratamiento de los riesgos que serán aplicados; es decir se determinará el tipo de acción que se debe establecer para reducir los riesgos a niveles aceptables para el CEC-EPN.

En la Tabla 1.9 se muestran los tipos de tratamiento de riesgos basado en Costo-Beneficio, en donde el mismo indica el costo que tendría tratar de solventar el riesgo con respecto a los beneficios que tendría evitar o mitigar el riesgo. Además se muestra el tratamiento en base a evitar, reducir, compartir y aceptar.

Tabla 1.9. Tipos de tratamiento de riesgos [5].

Costo-Beneficio	Tratamiento del Riesgo
Cuando el costo del tratamiento del riesgo es muy superior a los beneficios.	**Evitar** el riesgo, dejando de realizar la actividad que lo genera.
Cuando el costo del tratamiento del riesgo es adecuado según los beneficios.	**Reducir** o mitigar el riesgo: seleccionar e implementar los controles adecuados para reducir la probabilidad y/o el impacto.
Si el costo del tratamiento llevado a cabo por terceros es más beneficioso que tratarlo directamente.	**Compartir o Transferir** el riesgo a terceros (a través de la contratación de un seguro o subcontratar el servicio).
Si el nivel de riesgo es menor o igual al nivel de aceptación del riesgo.	**Aceptar** el riesgo. No se requiere tomar ninguna acción, solo se deberá monitorear su conducta.

Tabla 1.10. Criterios para tratamientos de riesgos [5].

RIESGO	ZONA DE RIESGO	TRATAMIENTO
Rutina	Riesgo aceptable	Aceptar / Monitorear
Bajo	Riesgo tolerable	Aceptar / Monitorear
Medio	Riesgo moderado	Reducir el Riesgo Evitar el Riesgo Compartir o Transferir el Riesgo
Alto	Riesgo importante	Reducir el Riesgo Evitar el Riesgo Compartir o Transferir el Riesgo
Crítico	Riesgo inaceptable	Reducir el Riesgo Evitar el Riesgo Compartir o Transferir el Riesgo

Después de haber analizado el mapa de riesgo con su respectivo nivel de riesgo se presenta la Tabla 1.11 con los riesgos identificados a nivel de la CGT por la consultoría realizada en el CEC-EPN en noviembre 2017 por un proveedor externo.

Tabla 1.11. Riesgos identificados en la CGT, según el mapa de Riesgos [8].

DESCRIPCIÓN	NIVEL	RIESGO
Indisponibilidad por saturación de la red inalámbrica WiFi debido a divulgación no autorizada de la clave de acceso de los profesores a los estudiantes; lo que incluso podría poner en riesgo la red interna del CEC-EPN.	9	MEDIO
Que la red LAN sufra desconexión debido a problemas en su cableado o daños en los *switches* y *routers*.	10	ALTO
Que la red de fibra óptica sufra desconexión debido a problemas en su infraestructura física, considerando que está instalada utilizando los postes de la empresa eléctrica Quito y ductos del Municipio de Quito.	10	ALTO
No contar con el servicio de Internet, impidiendo el uso de diferentes servicios que otorga el CEC-EPN.	8	MEDIO
No contar con todos los respaldos de información de las bases de datos, código fuente de aplicaciones y archivos de trabajo del CEC-EPN.	12	Alto
No contar con un esquema que maneje la información por roles y responsabilidades, ya que puede ser conocida/difundida/divulgada, modificada o eliminada sin autorización.	6	Medio

Los riesgos identificados en la Tabla 1.11 serán solventados en el **Capítulo II Apartado 2.1.2.2** como parte del análisis del BCP y el desarrollo del DRaaS.

1.5.4 Cloud Computing

El *Cloud Computing* no es más que un conjunto de herramientas que se usan con la finalidad de ofrecer ciertos servicios mediante la utilización de la red, siendo la más común la Internet. Estas herramientas pueden traer un gran beneficio a cualquier empresa que requiera dar un buen uso y sepa aplicarlo de la manera adecuada [9].

En estudios realizados sobre el uso de la Computación en la Nube, por ejemplo, en la revista FORBES [10], la cual se especializa en todo lo relacionado con el área de finanzas y negocios en el mundo, se ejemplificó que *"en el año 2015 las empresas incrementaron en un 34% la implementación de aplicaciones, en un 27% todo referente a servicios como*

parte de gestión, un 22% de ellas implementaron la planificación de recursos en la empresa, el 20% hicieron uso de almacenamiento en la nube y el 19% hizo uso del mantenimiento de sus aplicaciones que utilizaban como parte de las prioridades para gestionar los gastos que le correspondían". Este resultado fue extraído en base a la encuesta que se aplicó a la empresa *Cowen & Company* [10].

Figura 1.1. *Cloud Computing* [11].

En la actualidad ha crecido el uso de los servicios de computación en la nube, la cual se ha propagado en diferentes ámbitos, uno de ellos es en las organizaciones donde se le da un uso primordial en la manera de trabajar, sobre todo con el tema del almacenamiento; ya que no se necesita dispositivos de almacenamiento o el uso de un computador personal para realizar un determinado trabajo, basta con acceder a la nube en donde se guarda cierta información para realizar el mismo.

Entre las principales ventajas que posee el *Cloud Computing* está [9]:

- Posee un bajo costo, el cual se ve evidenciado en determinados productos gratuitos o con pagos que se realizan mensuales por determinados planes, sin implicar costos adicionales porque no involucra inversión en cuanto a infraestructura ni en licenciamiento.
- Se puede tener acceso de toda la información de manera ubicua, ya que se encuentra alojada en la nube.

- Accesos desde cualquier parte siempre y cuando cuente con acceso a Internet.
- La información solicitada en la nube es en tiempo real, ya que la conexión a la misma es directa.

Como principales desventajas se puede citar:

- La necesidad de contar con una conexión a Internet buena para que se pueda establecer la comunicación y acceder a toda información; caso contrario no se puede acceder a ningún tipo de información que se encuentre en la nube.
- La seguridad, debido a que depende completamente del proveedor y al circular la información por internet corre el riesgo de que sea interceptada por personas maliciosas.

Además, existen actualmente características esenciales de la computación en la nube, las cuales se describen a continuación:

- **Auto-servicio demandado:** El consumidor puede aprovisionar o desprogramar los servicios cuando sea necesario, sin la interacción humana con el proveedor del servicio.
- **Amplio acceso a la red:** Tiene capacidades en la red y se accede a través de un mecanismo estándar.
- **Uso común de Recursos:** Los recursos informáticos del proveedor se agrupan para servir a múltiples consumidores que están utilizando un modelo de múltiples inquilinos, con varios recursos físicos y virtuales dinámicamente asignado, dependiendo de la demanda del consumidor.
- **Elasticidad rápida:** Los servicios se pueden aprovisionar de manera rápida y elástica.
- **Servicio medido:** Los sistemas de *Cloud Computing* controlan y optimizan automáticamente el uso de recursos mediante una capacidad de medición para el tipo de servicio, por ejemplo, almacenamiento, procesamiento, ancho de banda, o cuentas de usuario activas.

1.5.4.1 Modelos de Despliegue

Los modelos de despliegue están formados por cuatro modelos, siendo estos: *Cloud* privado, *Cloud* público, *Cloud* híbrido y *Cloud* comunitario en función de sus características [9]:

1.5.4.1.1 Privado

Son aquellas nubes que han sido creadas y administradas por una sola organización; es decir son los que deciden los procesos a ser ejecutados en la nube. En esta infraestructura se percibe mayor seguridad en cuanto a la información, ya que todos los datos se encuentran dentro de la infraestructura de la organización, las cuales están protegidas por un Firewall. Aquí se controla los usuarios que pueden ingresar a cada servicio en *Cloud*. Con respecto a los costos, estos son altos debido a que mantienen toda la arquitectura tanto de hardware como de software en la misma empresa.

1.5.4.1.2 Público

La infraestructura está disponible a todo el público. En este caso la infraestructura corresponde a una organización que se dedica a vender sus servicios de Computación en la Nube, como pueden ser aplicaciones y almacenamiento. Los servicios de los cuales hace uso el usuario, pueden ser gratuitos o con un costo dependiendo del servicio, capacidad o uso requerido. La administración se realiza por terceros usuarios.

1.5.4.1.3 Comunitario

La infraestructura está disponible a una comunidad cerrada. Dicha comunidad está compartida entre varias organizaciones con intereses similares. En este caso la infraestructura corresponde a una organización que se dedica a vender sus servicios de Computación en la Nube. Los servicios de los cuales hace uso la comunidad o un tercero, poseen un costo operativo ya que es una variación al *Cloud* privado.

1.5.4.1.4 Híbrido

La infraestructura está compuesta por al menos dos tipos de nubes con las que mantienen su misma identidad, ya que por un lado puede usar la nube pública para el acceso a los datos y por otro lado mantiene sus servidores en su nube privada. La diferencia de este modelo con otro es que van a ser unidas ya sea por una tecnología propietaria o por un estándar para facilitar que sean portables los datos y cada una de las aplicaciones [9].

1.5.4.1.5 Comparativo entre los Modelos de Despliegue

Los modelos de despliegue se diferencian principalmente en la administración y el acceso a los usuarios. A continuación en la Tabla 1.12 se cita algunas ventajas y desventajas de cada modelo de despliegue en *Cloud Computing*.

Tabla 1.12. Ventajas y Desventajas de los modelos de despliegue *Cloud Computing* [9].

Cloud	Ventajas	Desventajas
Privado	Se brinda mayor seguridad debido a que la información se encuentra dentro de la propia infraestructura.	El Costo de Implementación es alto.
	Los controles de seguridad son mucho más concretos ya que se posee dispositivos como firewall.	Se debe adquirir tanto hardware como software.
	Mantiene un control total sobre el centro de datos.	
Público	Bajo costo de inversión.	La compartición de recursos que brinda una nube pública, puede conllevar a varios problemas de seguridad.
	Se paga por lo que se usa.	
	Se puede realizar un escalado de las aplicaciones y podrían correr sobre cualquier sistema operativo.	
Híbrido	Ofrece flexibilidad ya que permite que la información de la empresa se mantenga dentro de las instalaciones, mientras que lo menos relevante puede ser alojado en la nube pública.	La implementación de la seguridad, debido a los protocolos que se manejan entre las mismas, debe combinarse y administrarse por dos empresas diferentes.
	Es una solución aplicable si no se cuenta con los recursos necesarios para tener exclusivamente una nube privada con todos los servicios que se piensan brindar a los usuarios.	
Comunitario	Los costos podría ser la ventaja más atractiva que presenta el cómputo en la nube y si no lo es, al menos es la más evidente de todas las que ofrece esta tecnología. Al no tener que adquirir equipos costosos, las pequeñas empresas pueden tener acceso a las más nuevas tecnologías a precios a su alcance pagando únicamente por consumo. De este modo las organizaciones de cualquier tipo podrían competir en igualdad de condiciones en áreas de tecnología de la información con empresas de cualquier tamaño.	Es comprensible la percepción de inseguridad que genera una tecnología que pone la información (sensible en muchos casos), en servidores fuera de la organización, dejando como responsable de los datos al proveedor del servicio.

1.5.4.2 Modelos de Servicio

Existen 3 modelos de servicios para computación en la nube, los mismos que se mencionan a continuación [12]:

1.5.4.2.1 SaaS – Software como Servicio

Software como Servicio o por sus siglas en inglés *(SaaS Software as a Service*) es un modelo de servicio donde el proveedor de dicho servicio es el encargado de hospedar todas las aplicaciones en un servidor con el objetivo de que sus clientes tengan acceso a dichas aplicaciones mediante la conexión a Internet. En este modelo el cliente puede acceder de manera remota sin necesidad de tener presente el hardware y software en las instalaciones, ya que el proveedor se encarga de suministrar y mantenerlo en óptimas condiciones.

1.5.4.2.2 PaaS – Plataforma como Servicio

Plataforma como Servicio o por sus siglas en inglés (*PaaS Platform as a Service*) es un modelo de servicio donde el proveedor entrega al cliente soluciones en las que permita albergar sistemas operativos y aplicaciones que se utilizan para el desarrollo de sistemas y su acceso se realiza mediante un navegador web. La misma facilita que los desarrolladores realicen pruebas, documentos, análisis y ejecución de las aplicaciones con las herramientas ya existentes en *Cloud*, sin tener que instalar alguna herramienta en la computadora. Por lo cual el cliente solo tiene control sobre sus aplicaciones y no sobre dicha plataforma.

1.5.4.2.3 IaaS - Infraestructura como Servicio

Infraestructura como Servicio o por sus siglas en inglés (*IaaS Infrastructure as a Service*) es un modelo de servicio que está compuesto por una distribución propia de la infraestructura que brinda un servicio, la cual se refleja a través de una plataforma de virtualización. Dicha plataforma tiene un costo asociado según los recursos que pone a disposición el proveedor externo [12].

En la Figura 1.2 se presentan los tres modelos de servicios acentuando en sus diferencias:

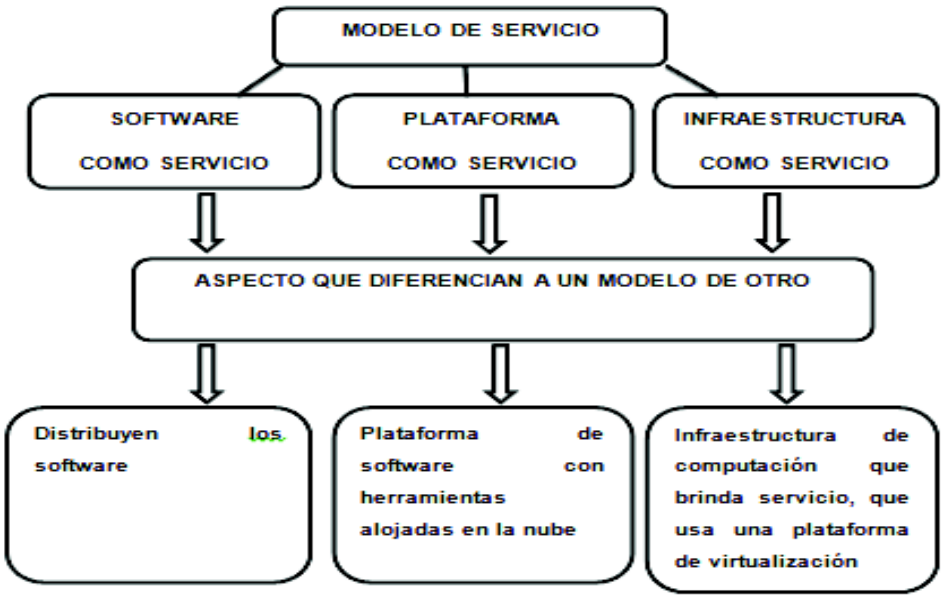

Figura 1.2. Modelos de servicio [13].

1.5.4.2.4 Características primordiales de los Modelos de Servicios

A continuación, se presenta en la Tabla 1.13 las características de cada modelo de servicio.

Tabla 1.13. Características de los modelos de servicios [13].

MODELOS DE SERVICIO	
Software del Servicio	**Características**
SaaS (*Sofware as a Service*)	Puede evidenciar una pérdida de control respecto a los datos, la cual puede estar dada por el acceso no autorizado, cuando no se toman las medidas pertinentes en máquinas locales.
	La importancia de este servicio radica en que se puede implementar de forma rápida el trabajo; facilitando el mismo para las empresas y de manera especial para el departamento de tecnología.
PaaS (*Platform as a Service*)	Mayor cantidad de personas que van a poder desarrollar, mantener y desplegar aplicaciones web. En la actualidad, construir aplicaciones web requiere desarrolladores con habilidades especializadas.
	Desarrollo del *backend* en el servidor (por ejemplo, java/j2EE).
	Desarrollo del *frontend* en el cliente (por ejemplo, JavaspcripDojo).
	Administración de sitios web.
	La importancia radica en la facilidad que le propicia a los programadores en base al entorno de desarrollo, ya que cuenta con un conjunto de herramientas que están pre-configuradas para desarrollar las aplicaciones.
IaaS (*Infrastructure as a Service*)	Es necesario contar con dos centros de datos para la recuperación de desastres, uno que sea propio de la empresa y otro que sea en la nube.
	La importancia del mismo es que permite que se incremente la automatización de tareas, reduciendo los errores humanos y la mejora en la productividad.

1.5.5 Plan de Continuidad del Negocio (BCP)

Un BCP es un plan logístico que facilita que las organizaciones puedan continuar con sus actividades ante cualquier situación que afecte determinadas operaciones, por lo que debe tener en cuenta el antes, el durante y el después que pasa el incidente [14]. Además el BCP se basa en crear un proceso para mantener el negocio y sustentar la información en base a la seguridad de la información [15].

En este Proyecto de Titulación el BCP estará alineado a la norma internacional ISO 22301: 2012 que se refiere a "*Seguridad de la Sociedad: Sistemas de Continuidad del Negocio – Requisitos*" [16]**;** la cual tiene una guía que expone aspectos que pueden garantizar la seguridad de la información si ocurre una anomalía. Esta se centra en el ciclo que mejora de manera continua cada una de las actividades de planear, implementar, operar, revisar y mejorar la gestión de la continuidad del negocio [16]**.** Esto se revisará con más detalle en el **Capítulo II en el Apartado 2.1.2.**

A continuación se expone en la Tabla 1.14, algunos pasos necesarios para crear un BCP.

Tabla 1.14. Pasos para crear un BCP [15].

Pasos	Objetivo
1. Identificar los responsables.	Identifica las personas que participarán en el plan de contingencia.
2. Definir el alcance.	Se define el alcance para dar continuidad del negocio y que responda cómo recuperarse en caso de interrupciones.
3. Contexto en la organización.	Establece cada una de las actividades que son desarrollas en la misma. Se encuentra realizado en el Capítulo I Apartado 1.5.3.
3. Realizar un análisis del impacto en la empresa.	Identificar los procesos que sea críticos en la empresa. Se encuentra realizado en el Capítulo I Apartado 1.5.3.3
4. Realizar el análisis de riesgos.	Identificar los riesgos críticos por lo que puede verse afectada la organización. Se encuentra realizado en el Capítulo I Apartado 1.5.3.2
5. Control del plan.	Controlar de manera continua las actividades definidas. Esto se realizará en el Capítulo II Apartado 2.1.2.2

1.5.5.1 NORMA ISO/IEC 22301: 2012

La norma ISO/IEC 22301 fue creada en el 2012 por el comité técnico ISO/TC 223 [17]. Esta norma ha brindado varios aportes, como la disminución de ocurrencia de incidentes en empresas que la han implementado, como en el caso de originarse un desastre, estar preparados para responder de forma inmediata y de manera adecuada. Esta norma ha servido a países del primer mundo, estando entre ellos EEUU, Alemania, Austria entre otros. Su nombre con la cual fue creada fue "*Seguridad de la Sociedad: Sistema de Continuidad del negocio*" [17].

Existen varios conceptos o definiciones sobre la Norma ISO 22301; sin embargo uno de los conceptos más relevantes se menciona a continuación: "*La Norma ISO 22301 constituye un estándar internacional para la continuidad del negocio en la que especifica requerimientos para planear, establecer, implementar, operar, monitorear, revisar, mantener y continuamente mejorar un sistema de gestión de continuidad documentada para prepararse para responder y recuperarse de interrupciones*" [18].

Una de las características que diferencia este estándar de otros marcos o estándares de continuidad de negocio, es que una organización puede certificarse por un organismo de certificación acreditado y, por lo tanto, podrá demostrar su cumplimiento a sus clientes, socios, propietarios y en el propio entorno en general.

Entre los beneficios que la Norma ISO 22301:2012 posee se encuentran los siguientes [19]:

- Mantener la continuidad de las operaciones comerciales en caso de interrupción del negocio. Una Gestión de la Continuidad de Negocio por sus siglas en inglés (*BCMS Business Continuity Management*) ayuda a una organización a mantener sus niveles de servicio a sus clientes. El BCMS permite a los líderes empresariales evaluar los impactos potenciales de una interrupción operativa, tomar las decisiones correctas rápidamente, implementar una respuesta efectiva y minimizar el impacto general en la organización.

- Proteger servicios e información, lo que significa que la organización puede garantizar la continuidad en la entrega de sus productos y servicios, y realizar actividades que son fundamentales para continuar con éxito sus operaciones. Estas actividades protegen el flujo de ingresos del negocio y reducen el riesgo de mayores pérdidas debido a un incidente o desastre. Además ayuda a proteger los activos de una organización.

- Cumplir con los requisitos legales y reglamentarios el cual proporciona evidencia de que la organización ha tomado las medidas necesarias para cumplir con los requisitos reglamentarios que requieren un programa de gestión de la continuidad del negocio efectivo.

La norma ISO 22301: 2012 se basa en los Sistemas de Gestión, los cuales adoptan una estructura totalmente nueva que se considera de alto nivel, ya que garantiza que haya consistencia con otros estándares de sistemas de gestión; ejemplo de estas se encuentra: *"ISO 9001 (calidad), ISO 14001 (medioambiental) e ISO / IEC 27001 (seguridad de la información)"*.

Este estándar realiza una introducción general, posteriormente específica los requerimientos necesarios para crear y gestionar el BCP, y finalmente estudia todo el proceso en 10 cláusulas que hace referencia al alcance, referencias normativas, términos

y definiciones; conjunto con los requisitos normativos que se muestran en la Tabla 1.15 con su respectiva descripción. Con más detalle se analizará la norma ISO 22301:2012 en el **Capítulo II en el Apartado 2.1.2**, donde se planteará el BCP para el CEC-EPN.

Tabla 1.15. Requisitos normativos de la Norma ISO 22301.

Requisitos normativos	**Descripción**
Contexto de la organización	Es donde se determinan todas las necesidades tanto internas como externas de la organización, con la finalidad de definir bien el alcance. Se establecen todos los requerimientos de los implicados, sin descartar los legales y los reglamentarios que son aplicables.
Liderazgo	Hace referencia a la necesidad de un buen liderazgo que se considere apropiado, con el objetivo de que la alta gerencia establezca todos los recursos que se consideren apropiados, así como las políticas y el responsable de quien la va a implementar y la va a mantener.
Planeación	Se deben identificar objetivos, criterios y riesgos con el fin de medir el éxito.
Operaciones	Se realiza el análisis de la organización y del impacto del negocio desde el punto de vista empresarial, para dicho análisis se requiere de personas que posean una experiencia determinada en esta área. Además se realiza la evaluación de todos los riegos identificados y se buscan estrategias para mitigar los mismos en caso de que sucedan.
Mejoramiento	Se definen las pautas para mejorar el sistema de gestión continua en un periodo de tiempo largo, con el fin de mejorar cada una de las acciones que se consideren correctivas, derivadas de cada una de las auditorías, además de las revisiones entre otros
Evaluación del desempeño	Este se rige bajo el ciclo PDCA (Planificar, Hacer, Controlar y Actuar) ya que la norma ISO 9001 se fundamenta en ellos, y es sólo mediante este paso por el que se puede establecer si el Método de Gestión de la Calidad se encuentra actuando correctamente o si los cambios son inevitables para cumplir con dichos requisitos. En esta se valora la utilidad que va obteniendo de cada función en base al plan, por lo que se efectúa por secciones y mide a través de métricas basadas en el rendimiento que se consideren adaptadas. Esto se revisará a más detalle en el **Capítulo II en el Apartado 2.1.1.3**.
Apoyo	Se debe identificar determinada competencia en busca de encontrar personas que tengan una determinada experiencia, habilidades, además de conocimiento para que apoyen en caso de que ocurra algún incidente.

A continuación se enuncian cada uno de los elementos que se consideran obligatorios en esta norma [20] para formulación del BCP con una pequeña descripción.

- **Fecha:** Fecha que se elabora el BCP.
- **Alcance**: Describe el alcance para dar continuidad al negocio.
- **Términos y definiciones:** Ejemplifica términos y definiciones que son necesarios para que haya un mejor entendimiento por parte del usuario del documento entregado.
- **Contexto en la Organización:** Establece las actividades que son desempeñadas en la empresa por áreas y servicios.
- **Compromiso:** Plantea el compromiso de los líderes y los roles de los coordinadores.
- **Planeación**: Identifica requerimientos, riesgos y oportunidades como elementos esenciales, sin dejar de plantear otros que se consideren importantes para la organización.
- **Apoyo:** Identifica los recursos que van a formar parte de la implementación, mantenimiento y mejora para dar continuidad al plan de negocio**.**
- **Análisis de impacto del negocio:** Realiza el análisis del impacto de negocio en la organización.
- **Estrategias de continuidad de negocios**: Se establece posibles estrategias para dar continuidad al negocio.
- **Estructura de respuesta y finalización de incidentes**: Estructura las respuestas de las funcionalidades y cuáles son los incidentes que se tienen.
- **Plan de mantenimiento y pruebas:** Establece un listado que plasme como se va a realizar el mantenimiento y cuáles son las pruebas a realizarse.
- **Establecimiento de prioridades:** Define las acciones que se consideren prioritarias para la organización.
- **Selección de estrategias de recuperación**: Define las estrategias para la recuperación después del desastre.

- **Análisis de riesgo:** Analiza los posibles riegos que pueden estar asociados a la organización.
- **Control:** Se ejecuta en base a las actividades que estén planificadas, para verificar el avance y el cumplimiento de las mismas.

Después de haber analizado los elementos necesarios, los cuales constituyen la guía del BCP, se presentará en el **Capítulo II en el Apartado 2.1.2.1 y 2.1.2.2** el desarrollo de la misma.

1.5.6 Plan de Recuperación de Desastre (DRP)

Son procesos documentados o conjuntos de procedimientos que sirven para recuperar y proteger una infraestructura de TI comercial en caso de un desastre. Es decir que el plan normalmente documentado por escrito, especifica los procedimientos que una organización debe seguir en caso de un desastre. El desastre podría ser natural, ambiental o provocado por el hombre. Los desastres inducidos por el hombre podrían ser deliberados (por ejemplo, un acto de un terrorista) o involuntarios (es decir, accidentales).

Dada la dependencia de las organizaciones con las Tecnologías de la Información y las Comunicaciones (TIC's) para realizar sus operaciones, es necesario apoyarse en un DRP, el cual garantice el trabajo de las organizaciones para que no sea detenido ante el suceso de un desastre.

Además se asocia cada vez más con la recuperación de datos, información y aplicaciones que forman parte de la infraestructura de las TIC's. El mismo se realiza en base a las precauciones que se toman para determinados efectos que se producen en un desastre, con el objetivo de que la organización sea capaz de restaurar de manera rápida las funciones en una situación crítica.

Lo anteriormente planteado involucra un análisis de todos los procesos inmersos en el negocio y de las necesidades para dar continuidad, el tipo de negocio que se maneje, los procesos que intervengan y el nivel de seguridad que requiera dicha institución.

A continuación en la Tabla 1.16 se muestra las ventajas y las desventajas más relevantes de un DRP.

Tabla 1.16. Ventajas y Desventajas de un DRP [21] [22].

Ventajas	Desventajas
Un DRP permite mantener la continuación de cada uno de los servicios que se relacionan con las TIC's en el negocio.	La integridad de los datos está basada en la confianza apuntada hacia un tercero o empresa externa la cual tiene el destino de los datos en sus manos.
Con un DRP se podrá ahorrar tres elementos importantes: esfuerzo, tiempo y dinero.	Puede tomar mucho tiempo la planificación de una DRP y los costos pueden ser muy elevados.
Se podrá proteger las posibles fallas que puede tener el negocio de manera general en todo lo relacionado con servicios informáticos.	Requiere de una planeación muy detallada y participación de todas las personas de la empresa
Se podrán minimizar gran parte de los riesgos si falta algún servicio.	
Garantiza el acceso a toda la información desde el punto de vista empresarial.	
Mantiene la disponibilidad de cada uno de los recursos del área de informática	
Minimiza todo lo referente a la toma de decisiones equivocadas si se presenta un desastre.	
Posibilita que se recupere el negocio de manera exitosa.	
Brindar una buena atención a todos los implicados de forma continua.	

A modo de conclusión se puede decir que en la medida que una organización esté creciendo desde el punto de vista tecnológico, necesita proteger su información y crear nuevas estrategias mediante un DRP para recuperar la información y así, darle continuidad a cada uno de los servicios. De esta manera se estaría manteniendo la atención a sus clientes en base a las exigencias que propone el mercado.

1.5.6.1 Objetivo de Tiempo de Recuperación (RTO)

Objetivo de Tiempo de Recuperación, por sus siglas en inglés (*RTO Recovery Time Objective*), no es más que el tiempo para recuperar el servicio después de un desastre.

El RTO se ve implícito cuando deja de funcionar determinadas aplicaciones debido a la caída de algún servicio que se encuentra asociada a la misma, siendo el principal objetivo determinar el tiempo para darle continuidad al negocio. Por lo general la respuesta va a depender de la criticidad de la aplicación o de las aplicaciones. Es por eso que se debe analizar cada uno de los casos para saber cómo proceder ante una interrupción. De esta manera, siguiendo el estudio realizado en el CEC-EPN, se ha definido un lapso de tiempo referencial entre 15 minutos a 1 hora, dadas las pruebas realizadas en el prototipo (Ver **Capítulo III, Apartado 3.2.3**), que toma reanudar cada uno de los servicios una vez que haya ocurrido un desastre, para el cual se debe tener en cuenta los últimos backups tanto del sistema como de las aplicaciones que permitirán mantener la puesta en marcha del negocio con un tiempo límite para el funcionamiento. El tiempo de referencia mencionado puede variar dependiendo de la velocidad de la Internet y del tamaño de los archivos o del servidor que se intente recuperar.

1.5.6.2 Objetivo de Punto de Recuperación (RPO)

Objetivo de Punto de Recuperación, por sus siglas en inglés (*RPO Recovery Point Objective*) define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre. Se relaciona directamente con la copia de seguridad de datos, para tener la custodia de todos aquellos que son vulnerables ante una causa inesperada. De esta manera, siguiendo el estudio realizado en el CEC-EPN, se ha definido un lapso de tiempo referencial entre 30 minutos a 1 hora, dadas las pruebas realizadas en el prototipo (Ver **Capítulo III, Apartado 3.1.3**), para ir realizando dichas copias, con la finalidad de mejorar la recuperación una vez que se haya caído el sistema. A modo de resumen no es más que la selección de la copia de seguridad que se utilizará para realizar la recuperación, teniendo en cuenta la última y la penúltima copia.

A continuación se muestra un gráfico que ejemplifica el RTO y RPO tomando en cuenta el punto de contingencia, donde se muestra RPO con el último backup realizado. Una vez que haya una interrupción se procede a realizar la recuperación de los datos y las aplicaciones mediante el último backup. Mientras que el RTO indica el tiempo que tomará la recuperación de los datos.

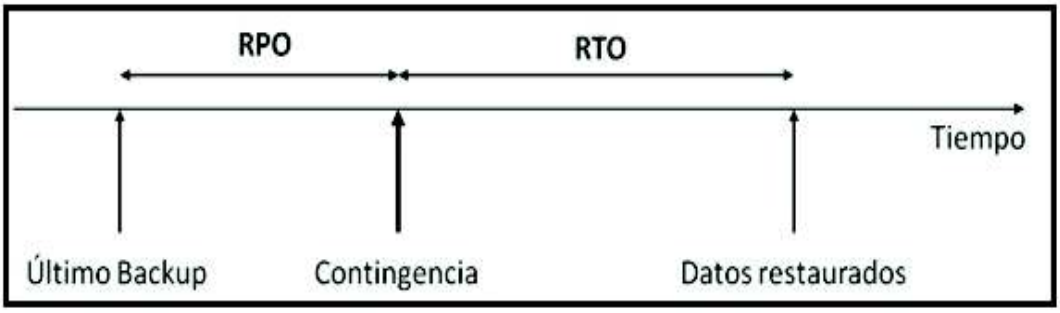

Figura 1.3. RPO y RTO desde un punto de contingencia [23].

1.5.7 Recuperación ante Desastres como Servicio (DRaaS)

Es una estrategia que forma parte de la disponibilidad integral, que se extiende hacia una nube híbrida, la cual propicia tanto el almacenamiento en la nube como de manera local. Actualmente un DRaaS se encuentra poco demandado debido a su implementación, ya que la gran tendencia en cuanto a las opiniones por parte de los usuarios es que es muy difícil de implementar [24]. Es importante que los usuarios dispongan de acceso a estos servicios y a las diferentes aplicaciones en los Centros de Procesamientos de Datos (CPD), donde la prioridad debe ser implementada a través de políticas que balanceen la carga para que se pueda priorizar cada acceso hacia el CPD del cliente [24].

Un DRaaS es la replicación y el alojamiento de servidores físicos o virtuales por parte de un tercero para proporcionar "conmutación por error", que es un modo de funcionamiento de respaldo que cuenta con un componente del sistema principal y un secundario, siendo este último el que se habilita cuando la principal falla en el caso de una catástrofe natural o provocada por el hombre. Normalmente, los requisitos y las expectativas de un DRaaS se documentan en un Acuerdo de Nivel de Servicio por sus siglas en inglés (*SLA Service Level Agreement*) y el proveedor de terceros proporciona "conmutación por error" a un entorno de computación en la nube, ya sea a través de un contrato o de pago por uso. En el caso de un desastre real, un proveedor fuera del sitio es menos propenso que la propia empresa a sufrir los efectos directos e inmediatos, lo que le permite al proveedor implementar el DRP incluso en el caso del peor de los escenarios: cierre total o casi total de la empresa afectada [25].

1.5.7.1 Ventajas y Desventajas de un DRaaS

Con un DRaaS, el tiempo para devolver las aplicaciones a la producción se reduce al tiempo que demore la restauración de los datos a través de Internet. DRaaS puede ser

especialmente útil para las pequeñas y medianas empresas que carecen de la experiencia necesaria para aprovisionar, configurar y probar un plan de recuperación de desastres efectivo. El uso de DRaaS también significa que la organización no tiene que invertir en su propio entorno de DRP. La mayor desventaja que presenta DRaaS es que la empresa debe confiar en un proveedor de servicios para implementar el plan en caso de un desastre y cumplir con los objetivos definidos en el RPO y RTO. Los inconvenientes adicionales incluyen posibles problemas de rendimiento con aplicaciones que se ejecutan en la nube y posibles problemas de migración al devolver aplicaciones al CPD local de un cliente.

Tabla 1.17. Ventajas y Desventajas de DRaaS [26].

Ventajas	Desventajas
Permite la recuperación de manera integrada de todo el entorno crítico, además admite conservarlo en el *Cloud*, el cual espera la disponibilidad integral para cuando sea necesario.	Si no se implementa bien el DRaaS se podrían perder todos los datos.
Realiza la réplica de los datos de manera continua en los sistemas que se encuentren en producción.	La seguridad se verá afectada en cuanto a las copias de seguridad en el caso de que haya un problema en la infraestructura de la empresa.
Facilita la recuperación de todo el servicio a través de las copias de seguridad.	Existe falta de confianza debido al temor de perder la información si no se establece una buena infraestructura que responda a los intereses de la empresa.
Presenta un enfoque híbrido ya que se puede utilizar varios modelos de despliegue.	Puede existir dificultad, si no se logra configurar todo el entorno para la realización de la recuperación de las copias de seguridad.
Se pueden realizar copias de seguridad asentada en imágenes.	
Minimiza los costos, ya que es flexible y el costo depende de las necesidades y el uso que requiera la empresa.	

1.5.7.2 Proveedores de Cloud Computing que Ofrecen DRaaS [27] [28] [29].

Los proveedores de *Cloud Computing* forman parte de todo el proceso de implementación de servicios en la nube, por lo que ellos participan en todo el proceso. La elección del proveedor es un factor determinante para alcanzar el éxito, por lo que se debe escoger el proveedor que más se ajuste al entorno de negocio, en base a lo que ofrece.

A continuación se describen varios servicios, los cuales son parte del DRaaS, siendo estos:

- **Computación:** es el servicio que permite el intercambio de información a través de Internet por medio de las máquinas virtuales.
- **Almacenamiento:** es el servicio que permite almacenar los datos en la nube o en el servidor del proveedor.
- **Migración**: es el servicio que se utiliza para migrar una aplicación o base de datos que se esté utilizando.

Los servicios antes mencionados constituyen el pilar de otros servicios personalizados en diferentes proveedores, tal es el caso de **Amazon, Google y Microsoft**, los cuales presentan un paquete completo para la DRaaS y se les conoce como: ***Amazon Web Services - Disaster Recovery, Google Cloud Platform - Disaster Recovery y Microsoft Azure - Disaster Recovery*** respectivamente [27] [28] [29].

En modo de resumen en la Tabla 1.18 se muestra los tres proveedores y por cada proveedor el servicio DRaaS que ofrecen:

Tabla 1.18. Proveedores y servicios de DRaaS.

Proveedores de DRaaS	Servicios de DRaaS
Amazon	Amazon Web Services - Disaster Recovery
Google	Google Cloud Platform - Disaster Recovery
Microsoft	Microsoft Azure - Disaster Recovery

En la Tabla 1.19 se muestra los servicios básicos (computación, almacenamiento y migración) que son parte de los servicios que brindan los tres proveedores como parte de DRaaS; las cuales ayudarán a documentar y seleccionar el proveedor idóneo, teniendo en cuenta los requerimientos que posea la organización.

Tabla 1.19. Servicios de DRaaS por proveedores.

Servicios básicos	**Proveedores de DRaaS**		
	Amazon	**Google**	**Microsoft**
	Servicios de DRaaS		
	Amazon Web Services - Disaster Recovery	**Google Cloud Platform - Disaster Recovery**	**Microsoft Azure - Disaster Recovery**
Computación	*Amazon Virtual Private Cloud "VPC"*	*Google Compute Engine: Container Engine*	*Virtual Machines*
Almacenamiento	*Amazon Simple Storage Service "S3"*	*Cloud Storage - Disco persistente*	*De Blobs; Archive storage*
Migración	*AWS Database Migration Service*	*Cloud SQL*	*Azure Database for MySQL*

En la Tabla 1.20 se muestran las principales características de los servicios de DRaaS de los tres proveedores, donde se destacan características relacionadas con el acceso, disponibilidad y administración.

Tabla 1.20. Características de los Servicios de DRaaS por proveedor.

CARACTERÍSTICAS		
Amazon Web Services -DRaaS	**Google Cloud Platform – DraaS**	**Microsoft Azure – DRaaS**
Requiere de una identidad para el acceso.	El acceso a la nube se puede realizar desde Visual Studio y otras herramientas que son independientes.	El acceso a los servicios se puede realizar a través de navegadores web.
Ayuda en la práctica de la integración continua y la entrega continua	Este servicio permite que se pueda compilar, implementar, diagnosticar y administrar aplicaciones, lo que posibilita que sea escalable.	Permite la configuración de las tareas como un cron, con la finalidad de mover cada uno de los datos al estándar de Cloud Storage (almacenamiento en la nube). Una vez configurado la tarea en el cron se puede usar Cloud Storage Transfer Service (servicio de transferencia para almacenar en la nube).
Cada servicio está totalmente administrado en la nube.	Utiliza una amplia gama de tecnologías para brindar el servicio, teniendo en cuenta lenguajes de programación, base de datos, sistemas operativos entre otras.	A través del mismo se realiza una configuración desde la aplicación que permite hacer copias de seguridad de los datos en el disco persistente adjunto a la instancia.
Es un servicio que puede ser extensible e independiente	Este servicio diagnostica todas las aplicaciones que se encuentren activas a través de la depuración, generador de perfiles, herramientas específicas para el diagnóstico y exploradores de primer nivel [20].	Brinda suficientes recursos que son escalables. Además brinda soporte con personal calificado con la finalidad de dar mantenimiento y solucionar posibles problemas.

En la Tabla 1.21 se muestra las principales ventajas de los servicios de DRaaS de los tres proveedores.

Tabla 1.21. Ventajas de los servicios de DRaaS [27] [28] [29].

VENTAJAS		
Amazon Web Services - Disaster Recovery	**Google Cloud Platform - Disaster Recovery**	**Microsoft Azure - Disaster Recovery**
Fácil de usar	Posee un servicio de aprendizaje llamado Machine Learning.	Presenta varios servicios fáciles de usar y que se consideran atractivas en todo el tema de análisis.
Presenta control completo de todo el entorno y la infraestructura.	Para las instalaciones presenta una plataforma muy bien consolidada para todo el tema de la gestión de cada uno de los componentes que conforma la nube híbrida	Posee gran velocidad en cuanto a la escalabilidad y el despliegue.
Propicia todo lo que es almacenamiento, redes y comunicación	Propicia funciones para la gestión de nube, además del abastecimiento de la infraestructura y supervisión del comportamiento del rendimiento.	Posee un rápido despliegue en el equilibrador de la carga.
Fácil de aumentar o disminuir el almacenamiento.	Proporciona administradores en la nube para el almacenamiento.	Administración de almacenamiento a través de la nube

Por otro lado, se podría citar en la Tabla 1.22 las desventajas de los servicios de DRaaS de los tres proveedores.

Tabla 1.22. Desventajas de los servicios de DRaaS [27] [28] [29].

DESVENTAJAS		
Amazon Web Services	**Microsoft Azure**	**Google Cloud Platform**
Precio Premium.	Los precios se establecen de manera mensual, por hora o por mes.	Los precios se establecen en un plan basado en una capacidad de almacenamiento.
En la documentación no especifica nada referente a un control de acceso en cuanto a la tecnología subyacente	No posee una amplia documentación para la ejecución y puesta en marcha de los servicios.	No posee documentación que haga referencia al trabajo entre varios usuarios
Tienen funcionalidades limitadas.	Tienen funcionalidades limitadas.	Puede no ser seguro el entorno de trabajo si el usuario no crea una buena contraseña.

En la Tabla 1.23 se presenta los aspectos que son tomados en cuenta para determinar el costo del servicio de DRaaS, el cual va a variar dependiendo del proveedor.

Tabla 1.23. Aspectos relevantes para determinar el precio del servicio [27] [28] [29].

Aspectos relevantes		
Amazon Web Services	**Microsoft Azure**	**Google Cloud**
Presenta una capa gratuita que se puede utilizar por 12 meses con la finalidad de que se obtenga experiencia con la plataforma, los productos y los servicios	Ofrece algunos servicios gratuitos los primeros 12 meses después de inscribirse.	Ofrece algunos servicios gratuitos.
La tarifa de precios se establece por lo que consume y de la región.	Los precios van a depender de la región en que se encuentre y la divisa, haciendo un cálculo que dependerá de la instancia, los núcleos, tamaño de almacenamiento, disco duro, además del tamaño de aplicación y si se usa habitualmente. Por otra parte tendrán otros valores que dependerán aparte de los parámetros antes mencionados de la vCPU (Unidad Central de Procesamiento virtual). Además de si requiere de un disco duro más rápido; y por último para bases de datos grandes.	Pago por uso del servicio que se utilice.
		Brinda descuentos por realizar uso continuado de hasta 30%.
		Presenta planes en dependencia del tipo de servicio que solicite, comenzando por computación y almacenamiento.

En la Tabla 1.24 se presenta los precios en dólares por servicios básicos asociados, el cual varía en dependencia del proveedor.

Tabla 1.24. Precios por servicio básicos de los proveedores DRaaS [27] [28] [29].

Precios por Servicios básicos	Servicios de DRaaS		
	AWS - Disaster Recovery	**Google Cloud Platform - Disaster Recovery**	**Microsoft Azure - Disaster Recovery**
Computación	$ 0,050 por hora de conexión.	Depende del tipo de máquina que se utilice, siendo el costo mínimo de $0,047 y el máximo de $4,560 por hora.	$0,010/hora por máquinas virtuales.
		Por nodos del clúster, mayor a 6 cobra $0.150 por clúster	$0,072/hora por procesos optimizados.
			$0,081/hora por uso general.
			$0,113/hora por memoria optimizada
			$1538,920/mes por 6 vCPU, 112 RAM,
Almacenamiento	50 TB/mes a $0.023 por GB	15GB libre de costo	Primeros 50 TB/mes a $0, 038 por GB.
	450 TB/mes a $0.022 por GB	100GB =$1.990 por mes	Siguientes 50 TB/mes a $0, 037 por GB.
	Más de 500 TB/mes a $0.021 por GB	1TB= $9, 990 por mes	Más de 500 TB/mes a $ 0, 036 por GB
		10TB= $99, 990 por mes	
Migración	El precio varía en dependencia del tipo de instancia, la mínima de cada una de ella es:	Dependiendo de la instancia va a variar desde $0,025 hasta $2,310 por hora.	Para una unidad de proceso de 50 el precio es de $0, 018/hora y para una de 100 es de $0, 035/hora.
	T2= $0,018 por hora. T2 (instancia de desempeño mínimo del CPU)		
	C4= $0,154 por hora. C4 (instancias reservadas por región)		

Se hace notar que el análisis del presente **Apartado 1.5.7.2** (Proveedores de *Cloud Computing* que Ofrecen DRaaS) será fundamental en la elección del Proveedor a utilizar **Capítulo II Apartado 2.2.**

2. METODOLOGÍA

2.1 Diseño

En el presente capítulo se estudiará primeramente las metodologías que se van a utilizar, siendo estas la Investigativa, Exploratoria y el Modelo PDCA, que serán utilizadas para cumplir los objetivos de este Proyecto de Titulación. Seguido, se realizará un análisis de la norma ISO/IEC 22301 para BCP y se presentará una propuesta de guía metodológica de BCP para el CEC-EPN siguiendo esta norma. Además se detallarán los servicios seleccionados para DRaaS y los requerimientos para la migración, que serán tomados en cuenta para el Diseño e Implementación.

2.1.1 Metodologías a Utilizar

2.1.1.1 Metodología Investigativa

La metodología investigativa se basa en el análisis de toda la información que se recopila a través de las bibliografías. Expone que se haga un estudio, en donde se separa todo y se divide en partes los elementos que se desean observar según su causa, naturaleza o efecto y se examina de forma específica [30].

Esta metodología se caracteriza por guiar y orientar la investigación, ya que permite realizar el análisis de manera sistemática de los procedimientos de la investigación [30].

Además se encarga de reunir diferentes elementos que son básicos y aplicables a cualquier investigación, siendo estos los enfoques, la forma o la manera de producción, habilidades, técnicas y sistematicidad de acontecimientos.

Este método ha sido de gran importancia, ya que el mismo ha sido utilizado para describir los procesos que se encuentran en el CEC-EPN, identificando características y aspectos que son relevantes en cada uno de ellos; además del estudio de la norma ISO 22301, con el objetivo de conocer cómo se aplica la misma y lo esencial de cada requisito normativo. Para el diseño eficiente del DRaaS se tuvo en cuenta los diferentes servicios que brindaban varios proveedores, sin embargo se seleccionará solo los servicios necesarios según el prototipo a ser implementado, los cuales servirán para dar solución a la problemática existente en el CEC-EPN. Además, esta metodología ayuda en la selección del proveedor y los servicios que ellos brindan a través de la investigación y el análisis de elementos relevantes como las máquinas virtuales, la migración y el almacenamiento.

2.1.1.2 Metodología Exploratoria

La metodología exploratoria trata de dar un enfoque general de modo que se aproxime a la realidad. Es utilizada cuando el tema de investigación no se ha explorado mucho, es poco reconocido y sobre el cual no se puede generalizar.

Este método permite realizar una exploración en base al objeto de estudio que resulta desconocido, donde se carece de antecedentes para orientar la investigación en base al comportamiento y aspectos que se relacionan con la misma; además responde a la identificación de funcionalidad, clasificación y delimitación del estudio, sin descartar que permite la estimulación en el desarrollo de la investigación y que se obtenga como resultado la producción de cada uno de ellos [30].

Esta exploración permitirá aislar todo lo referente a características, observaciones, comportamientos y elementos que son de gran importancia para la implementación del prototipo. Con esta exploración se obtienen los requerimientos que posteriormente serán implementados como parte del prototipo, teniendo este como objetivo fundamental satisfacer las necesidades que posee el CEC-EPN, en especial la CGT, con la finalidad de recuperarse ante cualquier desastre en el menor tiempo posible.

2.1.1.3 Modelo PDCA

El modelo PDCA es una estrategia de mejora continua de la calidad, el cual está comprendido en cuatro fases fundamentales siendo estas:

- Planificar.
- Hacer.
- Controlar.
- Actuar.

Estas fases son conocidas por sus siglas en inglés (*PDCA Plan, Do, Check and Act),* cuyas fases se establecen de manera cíclica.

A continuación se muestra en la Figura 2.1 la representación de las mismas haciendo énfasis en la relación directa de una con otra:

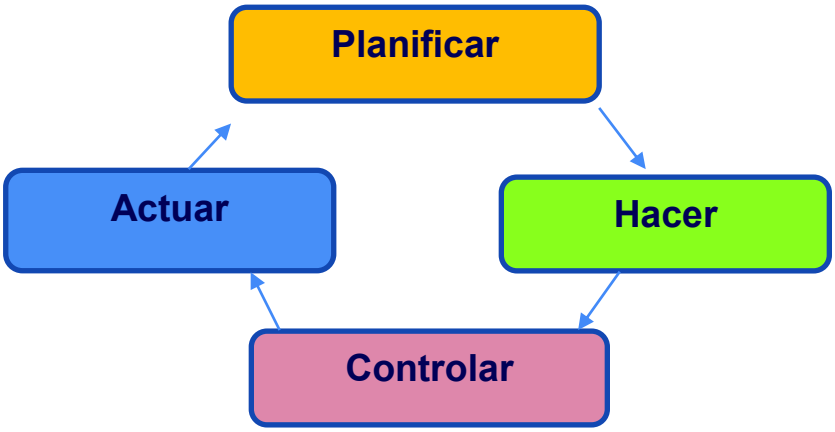

Figura 2.1. Modelos PDCA [31].

Estas 4 fases están enfocadas a lograr de manera sistemática la mejora continua de la calidad, basada en el mejoramiento de lo que se produce, en busca de reducir fallos, aumentar la eficiencia, la eficacia, dar solución a problemas así como la previsión y eliminación de cada uno de los riesgos que se consideren potenciales. Se denomina cíclica porque una vez terminada la última fase vuelve a realizar el ciclo, con la finalidad de que las actividades sean reevaluadas cada cierto periodo de tiempo y se les pueda incorporar nuevas mejoras. La misma está diseñada para que sea aplicada en las empresas y las organizaciones [31], como por ejemplo en el CEC-EPN.

A continuación se muestra cuáles son las actividades que se deben tener en cuenta en la puesta en práctica de cada una de estas fases [31].

- **Planificar**: Se deben identificar las actividades que sean susceptibles a la mejora, además de establecer cada uno de los objetivos que se desean alcanzar.
- **Hacer**: Permite la realización de los cambios que se van a implementar como parte de la mejora para la propuesta.
- **Controlar**: Realiza el control a través de la verificación de los requerimientos con el fin de determinar si están correctos, si es que no cumple entonces se debe modificar y ajustarlo a lo que se esperaba.
- **Actuar**: Una vez que haya terminado todo el proceso de prueba, es imprescindible estudiar cada uno de los resultados y compararlos con las actividades que fueron anteriormente implementadas antes de la mejora. Si el resultado es satisfactorio entonces se implementará la mejora de manera definitiva, en caso contrario se deben estructurar los cambios o desechar el mismo.

2.1.2 Análisis de la Norma ISO/IEC 22301 para BCP

Primeramente se hace notar que, el presente Proyecto de Titulación radica en una Propuesta Metodológica la cual se basa en la definición de un BCP siguiendo la norma ISO/IEC 22301 para el CEC-EPN y por consiguiente, el detalle de un DRaaS, el cual será implementado en el **Capítulo II, Apartado 2.2.3.**

La norma ISO/IEC 22301 para BCP se relaciona con el PDCA, ya que entre su ciclo de actividades se obtiene de manera detallada cada una de las acciones que se van a desarrollar, con las cuales se va a estructurar todo lo referente a la protección de la empresa ante los incidentes o interrupciones que pueden ocurrir. Además se establece cómo podría recuperarse la empresa ante una situación como esta en el menor tiempo posible.

Esta norma establece un control para supervisar un BCP y revisar los resultados de las actividades definidas para el aseguramiento del mismo. Además establece cuáles son las funciones de cada uno de los participantes, verifica el Análisis de Impacto de Negocios por sus siglas en inglés (*BIA Business Impact Analysis*), define los riesgos, monitorea todas las actividades definidas para el aseguramiento de la calidad y resuelve los incidentes que surjan.

Como parte de la norma se debe identificar cada uno de los requerimientos de la empresa, con la finalidad de tener operando cada producto y servicio que se ofrece de manera adecuada y personalizada.

Como un elemento primordial que establece la norma ISO/IEC 22301, es que el BCP debe ser proactivo y asegurar que tanto los productos como los servicios sigan siendo entregados aun cuando haya ocurrido una interrupción que no estaba planeada. Además debe incluir un plan con las medidas y las diferentes disposiciones, con el objetivo de asegurar que entreguen de manera continua lo que se está ofreciendo por parte de la organización. Por otro lado, se debe identificar cuáles son los recursos necesarios que van a ser utilizados para respaldar, lo que dará continuidad al negocio, incluyendo el personal, los archivos, equipos, los recursos financieros, la seguridad y el alojamiento si es necesario.

Tener implementado un BCP en una organización mejora la imagen de la misma ante sus empleados, los accionistas y los clientes, al tener un sustento que demuestra proactividad. El mismo mejora la eficiencia organizacional, entre cada proceso que interviene en la organización.

Ante cualquier interrupción que se presente en la institución se debe cumplir con el alcance que se haya definido en el BCP, siendo esto la clave para la recuperación.

Esta norma está compuesta por 10 cláusulas, siendo las tres primeras las no auditables porque no necesitan interpretación, sino que constituyen una guía para la organización; mientras que las cláusulas de la 4 a la 10 si son auditables. A continuación se menciona una síntesis de cada una de las cláusulas, y se adjunta la norma ISO 22301:2012 con todos sus detalles, en el **Anexo I.**

Cláusula 1: Alcance.
Como parte del alcance se debe establecer qué se va a implementar, mejorar y asegurar la conformidad de la política que está establecida en la empresa, es decir que los involucrados conozcan y acepten lo planteado.

Cláusula 2: Referencias normativas.
Son los documentos que se consideran indispensables como referencia para la aplicación del documento que se está desarrollando.

Cláusula 3: Términos y definiciones.
Son los términos que forman parte del documento, los cuales son definidos para brindar un mejor entendimiento en el contexto que será desarrollado.

Cláusula 4: **Contexto de la Organización.**
Hace referencia a todo lo relacionado con los temas internos y externos que poseen mayor relevancia en la empresa, con la finalidad de que se establezca un buen BCP. En la misma se identifican actividades de la empresa, vínculo con otras organizaciones, necesidades y expectativas.

Cláusula 5: Liderazgo.
A través del liderazgo se debe crear un ambiente que involucre a todos los trabajadores en el BCP, con la finalidad de que se cumplan los objetivos propuestos por la empresa y las tareas asignadas.

Cláusula 6: Planificación.

Se construyen todos los objetivos estratégicos y cada uno de los principios para realizar el BCP. Para dicha planificación se debe tener en cuenta el propósito, los riesgos y los requisitos en base a las necesidades de la empresa. Estos requisitos deben ser aplicables, medibles, controlados y actualizados cada un periodo de tiempo determinado.

Cláusula 7: Soporte.

Para la gestión que se realiza en el BCP se debe destinar recursos para que desarrollen cada una de las actividades.

Cláusula 8: Operación

Una vez realizada la planificación, la organización tiene que poner en marcha el BCP para lo cual debe tener en cuenta el análisis de impacto, valoración de los riesgos, los procedimientos, estrategias para dar continuidad al negocio y planes de continuidad del negocio.

Cláusula 9: **Evaluación del Desempeño.**

Una vez que se haya implementado el BCP se necesario realizar un seguimiento, el cual se debe realizar a través de revisiones paulatinas para mejorarlo continuamente. El seguimiento se les debe dar a las políticas, objetivos, metas, procesos, requerimientos, auditorías antes realizadas.

Cláusula 10: Mejora.

La mejora debe estar definida en cada una de las acciones que se hagan en la organización, para de esta manera aumentar la eficacia y eficiencia en los procesos y en los controles en busca de beneficios para la empresa.

A continuación se muestra la Tabla 2.1 en la que se presenta la relación de las fases del PDCA con las cláusulas asociadas a la norma ISO/IEC 22301:

Tabla 2.1. Relación entre las cláusulas de la norma ISO/IEC 22301 y el ciclo PDCA [32].

Ciclo PDCA	Cláusula	Contenido
Planificar (P)	Cláusula 4	Introduce los requerimientos necesarios para establecer el contexto del Sistema de Gestión de Continuidad del Negocio (SGCN) en la organización.
	Cláusula 5	Resume los requerimientos específicos de la alta gerencia.
	Cláusula 6	Describe los requerimientos en su relación al establecimiento de objetivos estratégicos y principios guías para el SGCN.
	Cláusula 7	Soporta las operaciones de SGCN en su relación al establecimiento de las competencias.
Hacer (D)	Cláusula 8	Define los requerimientos de la Continuidad del Negocio, determina como atenderlos y el desarrollo de procedimientos para atender un evento alternador.
Controlar (C)	Cláusula 9	Hace un resumen de los requerimientos necesarios para medir la gestión del desempeño.
Actuar (A)	Cláusula 10	Identifica y actúa en relación a conformidades detectadas al SGCN tomando acciones correctivas.

2.1.2.1 Guía de un BCP alineado a la Norma ISO 22301

A continuación se presenta la guía de un BCP con sus distintos apartados, en base a la teoría y conceptos que se describe en la norma ISO 22301 (Anexo I) [32]:

1. **Fecha:** Fecha de elaboración del BCP.
2. **Alcance (Cláusula 1)**: Describir el alcance para dar continuidad al negocio, especificando que se va a implementar, mejorar y asegurar en base a las políticas establecidas.
3. **Referencias normativas (Cláusula 2)**: Plasma los documentos que se consideran indispensables para el desarrollo del BCP.

4. **Términos y definiciones (Cláusula 3)**: Se establecen los términos y definiciones necesarias con la finalidad de que entiendan todos los usuarios que interactúen con el documento.

5. **Contexto de la Organización (Cláusula 4)**: Establece cada una de las actividades que se desempeña en la empresa a través de sus áreas y servicios. Hace referencia a temas internos y externos que tengan gran importancia.

6. **Liderazgo (Cláusula 5):** Se especifican los equipos que están subordinados al líder con la finalidad de involucrar a todo el personal.

7. **Planificación (Cláusula 6):** Estable todos los objetivos estratégicos para la estructuración del plan, los mismos deben ser medibles y controlables.

8. **Soporte (Cláusula 7):** Especifican todos los recursos que son necesarios para la realización de las actividades.

9. **Operación (Cláusula 8):** Se pone en marcha el BCP teniendo en cuenta el análisis de impacto, análisis de riesgos, estrategias de continuidad y planes de continuidad del negocio.

10. **Evaluación del desempeño (Cláusula 9):** Se debe realizar un seguimiento a través de revisiones paulatinas para la mejora continua del BCP.

11. **Mejora (Cláusula 10):** Establece las actividades a desarrollar como parte de las acciones para mejorar los procesos en base al PDCA.

    - Antes de la realización del BCP se hizo un análisis de todo el contexto de la organización el cual se encuentra reflejado en el Capítulo I como parte del marco teórico.

    - Durante la realización del mismo se tuvo en cuenta todo lo referente a los requisitos normativos, los cuales se verán explícito en el contexto del BCP.

    - Después del incidente se tendrá en cuenta el RTO el cual mostrará el tiempo de referencia para reanudar el servicio, mientras que el RPO representará la copia que será tomada en cuenta para reanudar el servicio.

Después de haber analizado la guía del BCP, se presenta en el siguiente apartado la formulación del mismo para el CEC-EPN.

2.1.2.2 Formulación Metodológica de un BCP para el CEC-EPN

En este apartado se desarrollará y se explicará el BCP paso a paso según la guía mencionada anteriormente en el **Apartado 2.1.2.1**. La Norma ISO 22301 ha sido considerada la línea base para que el CEC-EPN pueda recuperase ante un desastre, cumpliendo así el objetivo planteado.

Cabe indicar que se entregará al CEC-EPN el documento oficial del BCP, el cual se encuentra como **Anexo II** del Trabajo de Titulación.

1. **Fecha**

   1 de marzo del 2018.

2. **Alcance:**

   Este Proyecto de Titulación, se limita a la continuidad y recuperación en el caso de un desastre que afecte 3 servicios en el departamento de la CGT en el CEC-EPN: servidor web, servidor de base de datos y servidor de archivos. Se hace constancia que este trabajo considera un prototipo, el cual posteriormente se lo puede ampliar para toda la infraestructura y aplicaciones que sean indispensables para el funcionamiento del CEC-EPN.

3. **Referencias normativas**

   Los documentos que se presenta a continuación se consideran indispensables para la estructuración del BCP:

   - Norma ISO/IEC 22301 (**Anexo I**).
   - Contrato del servicio de Internet adquirido por la DGIP (**Anexo II**).
   - Renovación del Dominio "*cec-epn.edu.ec*" adquirido con Nic.ec (**Anexo III**).

4. **Términos y definiciones:**

   Los términos importantes que forman parte del documento se presentan a continuación:

   - BCP: Plan de Continuidad del Negocio.
   - DRP: Plan de Recuperación ante Desastres.
   - DRaaS: Recuperación ante Desastres como Servicio.

- CEC-EPN: Centro de Educación Continua de la Escuela Politécnica Nacional.
- CGT: Coordinación de Gestión de Tecnologías.
- FO: Fibra Óptica
- LAN: Red de Área Local.
- DNS: Sistemas de Nombres de Dominio
- DGIP: Dirección de Gestión de Información y Procesos
- NIC EC: Centro de Información de Red Ecuador

5. Contexto en la Organización:

El CEC-EPN es una unidad ejecutora desconcentrada que maneja procesos administrativos y financieros independientes. Realiza su propia autogestión y genera sus propios recursos mediante los cursos de capacitación que imparte. Las áreas que forman parte del CEC-EPN son las siguientes:

- Dirección.
- Coordinación de Capacitación y Consultoría.
- Coordinación de Lingüística.
- Coordinación Administrativa Financiera.
- Coordinación de Calidad y Talento Humano.
- Coordinación de Gestión de Tecnología.
- Coordinación de Marketing.
- Unidad de Educación Virtual.

Los servicios que brinda el CEC-EPN son cursos de capacitación en modalidad presencial y virtual a la medida de cada requerimiento, los cuales son de idiomas, empresariales y tecnológicos.

La CGT es la encargada de administrar todos los servicios tecnológicos necesarios para el funcionamiento del CEC-EPN los cuales se mencionan a continuación:

- Portal académico.
- Facturación electrónica.
- Matrículas online.
- Sistema SIICECW.
- Sistema SYSNOTE.

Entre las partes interesadas se encuentran: el cliente (participantes que reciben los cursos), el proveedor interno (instructores que imparten los cursos) y proveedores externos (personal que no pertenece a la organización, que provee productos y servicios).

El vínculo con otras organizaciones se estable a través de un grupo representativo de diferentes empresas que asisten por los planes de capacitación establecidos en cada institución.

A pesar de que el CEC-EPN es una unidad ejecutora desconcentrada la CGT trata de alinearse a los procesos y servicios que maneja la DGIP de la EPN para su funcionamiento.

6. Liderazgo:

El Director del CEC-EPN será la persona encargada de liderar a todo el personal; el mismo que se encontrará estructurado en diferentes equipos:

- **Equipo de Gestión de Contingencia:** Realiza la coordinación de las actividades de administración de contingencia y respuesta a emergencias; el mismo está compuesto por el Director y los Coordinadores del CEC-EPN.
- **Líder del Equipo de Gestión de Contingencia:** Es el responsable de velar por la creación del BCP, ejecución del mismo y la revisión. Además debe atestar que todo el personal del CEC-EPN tenga conocimiento del plan, estén en capacidad de reaccionar inmediatamente en caso de un incidente.
- **Coordinador del Equipo de Gestión de Contingencia:** Responsable de asegurar las actualizaciones y mantenimiento del BCP por lo menos una vez al año debido a la alta rotación del personal.
- **Representante Jurídico:** Responsable del asesoramiento político al líder del equipo de gestión y al Apoyo de Comunicaciones externos.
- **Apoyo Comunicaciones (Internas / Externas):** Su objetivo principal es difundir la información mediante mensajes internos y externos que se relacionen con el incidente presentado.
- **Responsabilidades del Equipo de Atención de Contingencia:** Apoya a las actividades de administración de la contingencia y da una contestación ante una incidencia.

- **Líder del Equipo de Atención de Contingencia:** Su objetivo principal es asegurar que haya un correcto entendimiento del BCP.
- **Equipo de Atención de Contingencia:** Son los responsables de dar un mantenimiento adecuado del conocimiento del BCP, además de su revisión y actualización.

7. Planificación:

Para la planificación se establecen los siguientes objetivos estratégicos con el propósito de recuperar los servicios y garantizar una continuidad del negocio:

- Establecer que todos los servicios y aplicaciones se encuentren disponibles las 24 horas del día con el menor tiempo de interrupción.
- Garantizar que los servicios estén disponibles, para que los estudiantes y profesores puedan acceder a las aplicaciones en todo momento.
- Realizar réplica del servidor en la nube con la finalidad de respaldar toda la información crítica, información histórica, registros de información de estudiantes, sistemas informáticos y aplicaciones que son indispensables para el funcionamiento normal del CEC-EPN en caso que se presente un desastre natural o tecnológico.
- Implementar un prototipo en DRaaS que permita recuperar los servicios del CEC-EPN.
- Configurar los servicios necesarios que serán utilizados como parte de la implementación del DRaaS para realizar respaldos periódicos, migración de las bases de datos, migración de las aplicaciones web, creación de máquinas virtuales para replica de servidores, copias de seguridad de información, recuperación de aplicaciones, recuperación de información y realización de pruebas.

También como parte de la planificación se tratarán los requisitos en base a las necesidades de la empresa y los riesgos identificados en el **Capítulo I Apartado 1.5.3.2** (Tabla 1.3, Tabla 1.4 y Tabla 1.11). Además los tipos y criterios de tratamiento de riesgos fueron analizados en el **Capítulo I Apartado 1.5.3.2** (Tabla 1.9 y Tabla 1.10).

- La principal necesidad del CEC-EPN es contar con una guía que les permita continuar con el servicio y recuperarse en el caso de un desastre.
- Otra de las necesidades fundamentales del CEC-EPN es salvaguardar la información más importante del negocio.

De esta información se define que, las acciones a tomar para los planes de tratamientos de los riesgos identificados en la CGT son:

- Al ser considerado un riesgo crítico y por ende inaceptable el no contar con un BCP se ha desarrollará una propuesta del BCP en base a la Norma ISO/IEC 22301 la misma que se presentará como **Anexo IV**.
- Diseñar un procedimiento para la administración de la red Wifi que incluya la reprogramación de cambio de contraseñas periódico.
- Establecer un esquema redundante para la red LAN (equipos activos).
- Implementar el mecanismo de redundancia automática del anillo de fibra óptica.
- Contar con un proveedor de Internet alterno para cuando el enlace principal falle.
- Generar un procedimiento formal y documentado para la gestión de respaldos que incluya pruebas periódicas de recuperación de *backups* en sus diferentes modalidades.
- Establecer un esquema de manejo de la información por roles y responsabilidades para brindar mayor seguridad a la misma.

8. **Soporte:**

Para el soporte se contará con los recursos humanos y tecnológicos que serán utilizados en el BCP ante un desastre. A continuación se menciona algunos de ellos:

- **Recursos Humanos:** principalmente los funcionarios de la CGT ya que son los involucrados directos en el BCP y son los que se encargarán de brindar todo el soporte necesario para recuperar los servicios. El resto de funcionarios de las diferentes áreas del CEC-EPN serán como apoyo para difusión a los usuarios, movilización de equipos, etc.

- **Recursos Tecnológicos:** Internet, servidores, bases de datos, discos externos, switch, routers, laptops, etc.
- **Aplicaciones Tecnológicas:** máquinas virtuales, servicios de *Google Cloud Platform.*

9. Operación:

Como parte de la operación se analizará todo lo referente a:

➢ **Análisis de Impacto del Negocio**

En el caso del CEC-EPN el impacto estará evidenciado cuando se vean afectados los sistemas informáticos, los cuales repercuten en los clientes y actividades del centro, como se analizó en el **Capítulo I Apartado 1.5.3.3** (Tabla 1.5 y Tabla 1.6).

Una vez analizado el impacto del negocio se procede a presentar las acciones a ser ejecutadas para disminuir el impacto del mismo en el caso de la interrupción de un servicio. Estas acciones han sido tomadas en cuenta en base a la infraestructura con la que cuenta la CGT del CEC-EPN:

- Contratar personal con experiencia y que le guste trabajar con clientes directamente para que el servicio sea el adecuado.
- Virtualizar la infraestructura tecnológica de la CGT del CEC-EPN para que en el caso de una interrupción se pueda habilitar los servicios y operaciones en el menor tiempo posible.
- Analizar las normas de manejo de Data Center e implementar las mejoras posibles.
- Realizar un procedimiento formal con respecto a la seguridad de la información y el acceso controlado a la misma.
- Charlas de concientización para el personal del CEC-EPN. Establecer una política para ejecutar una charla de concientización al año.
- Realizar la remediación de los hallazgos identificados en la consultoría con respecto al hackeo ético y a las vulnerabilidades en las IP públicas.

- **Valoración de los Riesgo**

  La valoración de los riesgos fue realizado en el **Capítulo I Apartado 1.5.3.3.1** (Tabla 1.8) a través del mapa de riesgos donde se pudo definir los diferentes niveles de riesgo según el impacto y la probabilidad.

- **Estrategias de Continuidad de Negocio:**
  - Contar con una guía BCP en la que se indique como proceder para mantener la continuidad del negocio.
  - Contar con una guía en la que se explique cómo se procedería en el caso de un desastre.
  - La puesta en práctica del DRaaS haciendo uso de la nube para dar continuidad al negocio.
  - Monitoreo continuo del proyecto creado en *Cloud.*
  - Copias de seguridad cada un cierto periodo de tiempo.
  - Verificación de las copias de seguridad con las que se cuenta.
  - Preparación a todo el personal de la CGT enfocada a la recuperación ante una falla inesperada debido a los distintos horarios que se maneja.
  - Realizar consultorías para determinar mecanismos idóneos para la continuidad del negocio.
  - Realizar un seguimiento continuo.
  - Implementar un Centro de Datos alterno en la sucursal.
  - Implementar redundancia de los equipos que sean críticos para el CEC-EPN.
  - Cambiar la infraestructura de red para contar con una configuración automática que permita salir por el firewall de la sucursal cuando en la matriz se tenga un problema de Internet.
  - Mantener en buen estado los UPS para que se pueda apagar de manera correcta los servidores en el caso de un corte de energía eléctrica.

  Los beneficios que estas estrategias propiciarían, sería la rápida recuperación del negocio ante una catástrofe; propiciando la reducción de tiempo y costo en determinados periodos, sin descartar el costo que tendría al contar con una infraestructura de respaldo.

- **Procedimiento para Continuidad del Negocio:**

El CEC-EPN seguirá los siguientes procedimientos con los que se pretende garantizar la continuidad de las actividades:

- En caso de afectación se utilizarán los medios de comunicación interna y externa que presenta la institución, para informar a todos los involucrados la situación actual del CEC-EPN, pudiendo utilizar la intranet, correo electrónico, reuniones, página web, videoconferencias, llamadas, e incluso, redes sociales.
- Dar a conocer de manera precisa las medidas que se están tomando de forma inmediata para resolver la interrupción o caída de alguno de los servicios.
- Determinar el impacto que provoca la interrupción.
- Analizar todas las posibles causas que provocaron la afectación del o los servicios del CEC-EPN.
- Proceder con las estrategias adecuadas para darle solución a la afectación que se encuentre presente en el CEC-EPN.
- Establecer una estructura de respuesta al incidente que se está tratando, tal como se lo había presentado en la Figura 2.3, relacionada con la estructura de respuesta y finalización de incidente.

- **Planes de Continuidad del Negocio:**

Como primera instancia, es importante el conocimiento y la capacitación de todos y cada una de las personas involucradas en la institución siguiendo el presente BCP. Para lo cual se formarán 2 Equipos, el de Gestión y Atención de Continuidad del Negocio definidos en la Tabla 2.2 y Tabla 2.3.

Estos integrantes han sido definidos desde el contexto actual (2018).

Tabla 2.2. Integrantes del Equipo de Gestión de Continuidad del Negocio

EQUIPO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO	
Integrantes	**Nombres**
Líder de Gestión de Continuidad	Msc. Adrián Zambrano
Coord. Equipo Gestión Continuidad	Msc. Ximena Uchupanta
Apoyo Jurídico	Dr. Pablo Proaño
Apoyo Comunicaciones Int./Ext.	Msc. Janeth Morales
Coordinador Administ-Financiero	Dra. Nathalia Rodríguez
Coordinador de Talento Humano	Ing. Carla Ortiz
Coordinador de Tecnología	Msc. Ximena Uchupanta
Coordinador de Lingüística	Ing. Henry Guy
Coordinador de Educación Virtual	Msc. Gabriela Martínez
Coordinador de Capacitación	Msc. Franklin Guevara

Tabla 2.3. Integrantes del Equipo de Atención de Continuidad del Negocio.

EQUIPO DE ATENCIÓN DE CONTINUIDAD DEL NEGOCIO	
INTEGRANTES	**NOMBRES**
Líder Equipo de Atención de Continuidad	Ing. Emerson Puma
Equipo de Atención de Continuidad	Tnlgo. Christian Gordón
	Ing. Katya Villacís
	Sr. Diego Alvear
	Ing. Edison Logacho
	Ing. Leonardo Medrano
	Msc. Víctor Olalla
	Ing. Bolívar Basantes

Adicional a estos equipos, podrían ser necesarios otros departamentos de la institución como: Lingüística, Capacitación y Consultoría, Educación Virtual, Administrativa Financiera, Marketing, Talento Humano y Calidad. A continuación se muestra el organigrama con los equipos que se conformarán para la atención para brindar continuidad al negocio:

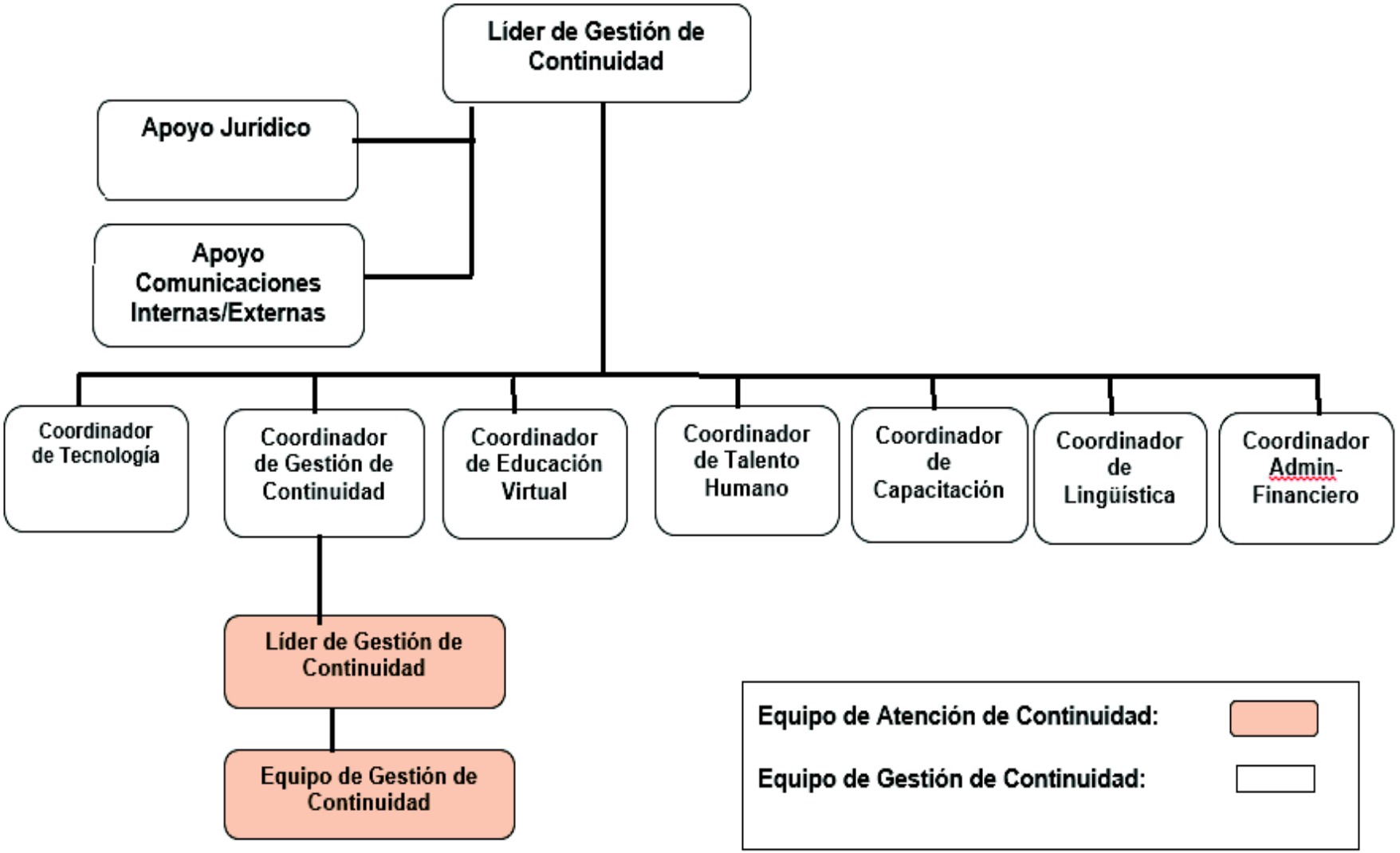

Figura 2.2. Organigrama de Gestión y Atención de Continuidad

- En el caso que se presente un incidente el Líder del **Equipo de Atención de Continuidad** será el encargado de comunicar al Líder del **Equipo de Gestión de Continuidad del Negocio**, con el fin de tomar la mejor decisión con respecto a la comunicación del incidente a los integrantes de la institución.
- En el caso de que el incidente se trate sobre la perdida de alguno de los 3 servicios informáticos mencionados en el Alcance de este documento, se procederá a ejecutar el DRaaS implementado en este Proyecto de Titulación siendo el departamento responsable la CGT.
- Los pasos a seguir para la recuperación del desastre mediante *Cloud*, se explican en el prototipo DRaaS realizado en el **Capítulo III, Apartado 3.2** y se detallan a continuación:

    - Ingresar a la plataforma de *Google Cloud Platform* desde cualquier equipo que cuente con Internet y con una cuenta de correo electrónico registrado en la plataforma.
    - Seleccionar el proyecto que se encuentra creado DRaaS.
    - Verificar la máquina virtual que ha sido replicada y que se encuentra lista para realizar la recuperación de la información.
    - Una vez que se haya restaurado la máquina virtual con toda la información y la aplicación web se procederá a poner en marcha el funcionamiento del servidor web desde *Cloud* siguiendo los pasos que se indican en el **Capítulo III, Apartado 3.2.1**. Dependiendo del tipo de incidente se procederá a variar el TTL cuanto sea necesario. Teniendo en cuenta que su valor mínimo es 5 minutos.
    - Una vez que esté funcionando la aplicación web se procederá a revisar el servidor físico, los errores y las soluciones para el mismo. Una vez que este solventado el problema se procederá nuevamente a levantar el servidor físico, con la previa sincronización de las bases de datos.
    - Al final del incidente se procederá a documentar el mismo con las acciones correctivas realizadas.

- **Pruebas:**

  - Se verificará el correcto funcionamiento del DRaaS levantando los servicios configurados en *Google Cloud Platform.*
  - Se confirmará que el tiempo de recuperación sea en el menor tiempo posible para que esta transición sea transparente para los usuarios.
  - Se identificará la causa del problema para solventar el servidor físico o la aplicación en la que se presentó el incidente.
  - Una vez que este solventado el problema con el servidor físico o la aplicación se procederá a sincronizar toda la información para que no se pierda ningún dato.
  - Finalmente se debe verificar que el incidente presentado haya sido solventado ya sea desde la aplicación web o desde el servidor.

10. Evaluación del Desempeño:

La evaluación se realizará a través de las revisiones periódicas del BCP y DRaaS que permitan perfeccionar su operación, entre las que se menciona a continuación:

- Seguimiento periódico de los objetivos de continuidad del negocio.
- Ejecución de auditorías internas planificadas para validar el cumplimiento del BCP en base a la Norma 22301.
- Contar con los servicios configurados en *Google Cloud Platform.*
- Verificación de las réplicas de información realizada.
- Comprobar que la información que ha sido restaurada sea correcta.
- Evaluación periódica por parte de la máxima autoridad del CEC-EPN.

También es importante tomar en cuenta la estructura de respuesta y finalización ante la presencia de un incidente, la misma que se presenta a través de varios pasos en la Figura 2.3.

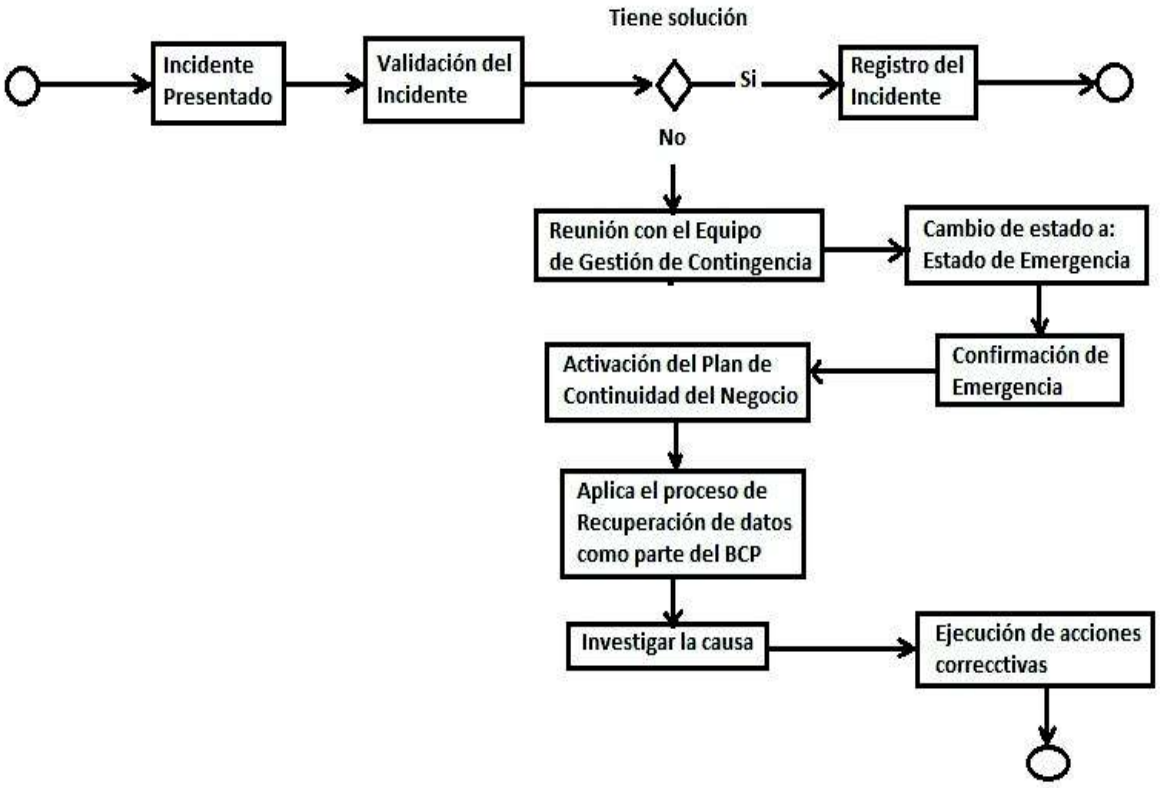

Figura 2.3. Estructura de respuesta y finalización del incidente.

11. Mejora

La mejora continua se realizará a través de acciones que permitan mejorar las actividades y procesos como las que se mencionan a continuación:

- Capacitación periódica a todo el personal sobre BCP y DRaaS debido a que existe rotación continua del personal.
- Plan de mantenimiento preventivo semestral de la infraestructura tecnológica que posee la CGT del CEC-EPN para garantizar un correcto funcionamiento los 365 días del año, las 24 horas del día.
- Renovación anual de licenciamiento del equipo Firewall que permite brindar seguridad tanto a los equipos como a la información del CEC-EPN.
- Renovación anual del certificado que utiliza la aplicación web portal para que sea considerado un sitio web seguro.

- Monitoreo continuo de la capacidad a los servidores del CEC-EPN para repotenciar los mismos de manera oportuna.
- Innovación de los equipos tecnológicos con los que cuenta el CEC-EPN para ser un referente como Centro de estudios.
- Revisar la guía propuesta del BCP y mejorar su alcance.
- Probar el prototipo implementado DRaaS para posteriormente validarlo con otros servicios y aplicaciones.

Este apartado ha sido realizado con un detalle exhaustivo del cumplimiento de cada cláusula bajo los requerimientos del CEC-EPN. Sin embargo, el BCP finalizado y entregado al CEC-EPN, el cual fue aprobado por el Director del mismo se encuentra en el **Anexo IV**.

2.2 Implementación

En esta fase se implementará el prototipo de recuperación de desastres para la CGT del CEC-EPN que es parte de la Propuesta Metodológica propuesta. Para esto primero se seleccionará el proveedor y la plataforma con la que se va a realizar la implementación; después se detallará los servicios seleccionados y en forma general los pasos a seguir para la implementación del DRaaS. Se realizará la creación del proyecto DRaaS en *Google Cloud Platform*, luego se procederá con la configuración de los servicios DRaaS necesarios para la implementación del prototipo según la infraestructura con la que cuenta la CGT**.** Posteriormente se procederá a crear la máquina virtual para migrar las tres bases de datos, la aplicación web portal en *Cloud* y las pruebas de replicación y restauración de la información a través de la máquina virtual, confirmando su correcto funcionamiento a través del RTO y RPO.

Para comenzar con la fase de la implementación y después de haber analizado las características generales de los tres proveedores en el **Capítulo I Apartado 1.5.7.2,** se ha decidido el uso de ***Google Cloud Platform*** dado que:

- ✓ Presenta un almacenaje libre con un límite de uso y espacio, lo que permitirá realizar la implementación del prototipo para la CGT; almacenando una aplicación web, tres bases de datos y archivos.

- ✓ Presenta una estructura que se encuentra de forma integrada, de manera completa, es rápida y segura a la hora de realizar backups, todo esto se evidenciará en la implementación del prototipo para la CGT.
- ✓ Posee una configuración amigable al momento de configurar los servicios y la realización a los backups.
- ✓ Los tiempos de respaldos son configurables según las necesidades de la CGT.

Nota: Los respaldos a ser realizados son en base al alcance definido en el Plan de Tesis como son: 3 bases de datos, servidor web y archivos de información.

De la misma manera, justificando el proveedor escogido se presenta la Tabla 2.4 que representa la matriz de decisiones. Esta matriz de decisiones ha sido elaborada en conjunto con los integrantes de la CGT.

Tabla 2.4. Matriz de Decisiones de Proveedores de DRaaS.

Opciones/Criterios	Amazon	Google	Microsoft
Peso	4	4	4
Almacenaje libre con límite de uso.	3	4	3
Servicios DRaaS según necesidades del CEC-EPN.	3	4	2
Funcionalidades limitadas	4	3	4
Herramienta amigable	1	4	1
Fácil configuración	2	4	2
TOTAL	**17**	**23**	**16**

A continuación en la Tabla 2.5 se presentan las características técnicas de los equipos contemplados para el DRaaS, los cuales fueron definidos en el Alcance de este documento:

Tabla 2.5. Características técnicas de los servidores para el prototipo DRaaS.

Servidores	Características Técnicas	Servicios
Aplicaciones web	Modelo: Proliant BL460C Gen7 Procesador: CPU 1: Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 Cores) CPU 2: Intel(R) Xeon(R) CPU E5620 @ 2.40GHz (4 Cores) Memoria: 4 GB Disco usado: 31.4 GB/ Disco disponible: 136 GB Sistema Operativo: Windows server 2008 R2	Portal de servicio estudiantil
File Server	Modelo: ProLiant SE1220 Procesador: Intel(R) Xeon® CPU E5520 2, 27 Ghz Memoria: 6 GB Disco usado: 2.86 TB Disco disponible: 4.41 TB Sistema Operativo: Windows Server 2003	Servidor de archivos
Base de Datos	Modelo: Proliant DL 360P Gen 8 Procesador: Intel ® Xeon® CPU E5-2630 2, 30GHz Memoria: 16 GB Disco usado: 97.0 GB Disco disponible: 182.0 GB Sistema Operativo: Windows Server(R) 2008 Enterprise	Base de datos SQL: - AUDITORIA - CEC-RECAUDA - SISINFCEC

Para la migración de la información y de la aplicación web al prototipo implementado para la CGT del CEC-EPN es necesario contar con el acceso al Sistema de Nombres de Dominio por sus siglas en inglés (DNS *Domain Name System*).

2.2.1 Servicios Seleccionados para el DRaaS

Dado las necesidades que tiene el CEC-EPN y teniendo en cuenta los riesgos y vulnerabilidades q han sido estudiadas en el **Capítulo I Apartado 1.5.3.2** se ha seleccionado tres servicios de DRaaS los cuales forman parte de los servicios de *Google Cloud Platform* del proveedor *Google,* los mismos que son de gran importancia para dar solución a las necesidades del CEC-EPN, siendo estos: *Computer Engine* (máquina virtual); *Cloud SQL* para todo lo relacionado con la migración de las bases de datos; y *Cloud Storage* para hacer referencia al almacenamiento en la nube.

2.2.1.1 Computer Engine (Computación - Máquina virtual)

Este servicio consiste en ejecutar los centros de datos mediante las máquinas virtuales de manera innovadora y se conecta mediante una red mundial a través de fibras. El mismo permite que se escalen desde las instancias individuales hasta el entorno de *Cloud Computing* para establecer un balance de carga; el mismo se va a utilizar para realizar la replicación de datos entre servidores [27].

2.2.1.2 Cloud SQL - Migración

Este servicio facilita la configuración, mantenimiento y administración de la base de datos desde la nube y permite la integración con *Compute Engine*. En este caso *Cloud SQL* se encuentra incluido como parte de la creación de la instancia de la máquina virtual [27].

2.2.1.3 Cloud Storage - Almacenamiento

Este servicio brinda el establecimiento de una capacidad de almacenaje en la nube, y permite guardar cualquier tipo de archivo y que los mismos sean compartidos y organizados según desee el usuario. Para este trabajo se usará los discos persistentes los cuales están internos en la máquina virtual [27].

Los pasos necesarios para implementar un DRaaS utilizando el servicio *Google Cloud Platform* del proveedor Google son [27]:

- ✓ Cuenta de correo electrónico.
- ✓ Registro del usuario.
- ✓ Creación del proyecto.
- ✓ Requisitos para la migración de la información.
- ✓ Selección de los servicios de DRaaS.
- ✓ Creación de la instancia de la máquina virtual.
- ✓ Configuración de los servicios de DRaaS.

2.2.2 Acuerdo de Nivel de Servicio

El Acuerdo de Nivel de Servicio, por sus siglas en inglés (SLA *Service Level Agreement*), está incluido como parte de *Google Cloud Platform,* citando en resumen:

- El servicio estará disponible en un 99, 9%, para tener un margen de error de 0,1%.

- Si el cliente cumple con todas las obligaciones que solicita el proveedor, entonces el proveedor se debe hacer cargo de cualquier falla que ocurra en cuanto a la disponibilidad.
- Debe tener servicio abierto para todas las instancias que se encuentren guardadas y un equilibrio en cuanto a la carga que se encuentran en el servicio de *Google Compute Engine*.
- Que se hagan actualizaciones de manera ocasionales, sin que la región o la zona sea un impedimento.
- Que las instancias de retorno se encuentren sanas y que respondan de manera afirmativa a todos los controles que se encuentran en el estado de equilibrio de carga.
- En caso de que haya pérdida de información, el cliente debe mostrar el servidor con los datos de registro donde se muestre la fecha y hora que ocurrieron los errores, de no mostrarlo no tiene derecho a ningún tipo de reclamación.
- Para el tema relacionado con la auditoría es necesario que se muestren informes de la monitorización, registros de la configuración y cualquier información que se encuentre disponible y que sea de interés del CEC-EPN.
- La realización soporte que se haga cada 3 o 6 meses.
- Que haya confidencialidad en la información que se encuentra involucrada en el todo el proceso.

2.2.3 Configuración del Proyecto en *Google Cloud Platform* [27]

Para la configuración de este proyecto llamado Drass que representa el prototipo del Trabajo de Titulación, es necesario la creación de una cuenta de correo electrónico con el proveedor seleccionado Google. Además se necesita el registro en *Google Cloud* a través del cual se podrá acceder a *Google Cloud Platform* donde se configurarán los servicios necesarios para el DRaaS.

A continuación se muestran las Figuras 2.4 y 2.5 relacionadas con lo antes mencionado:

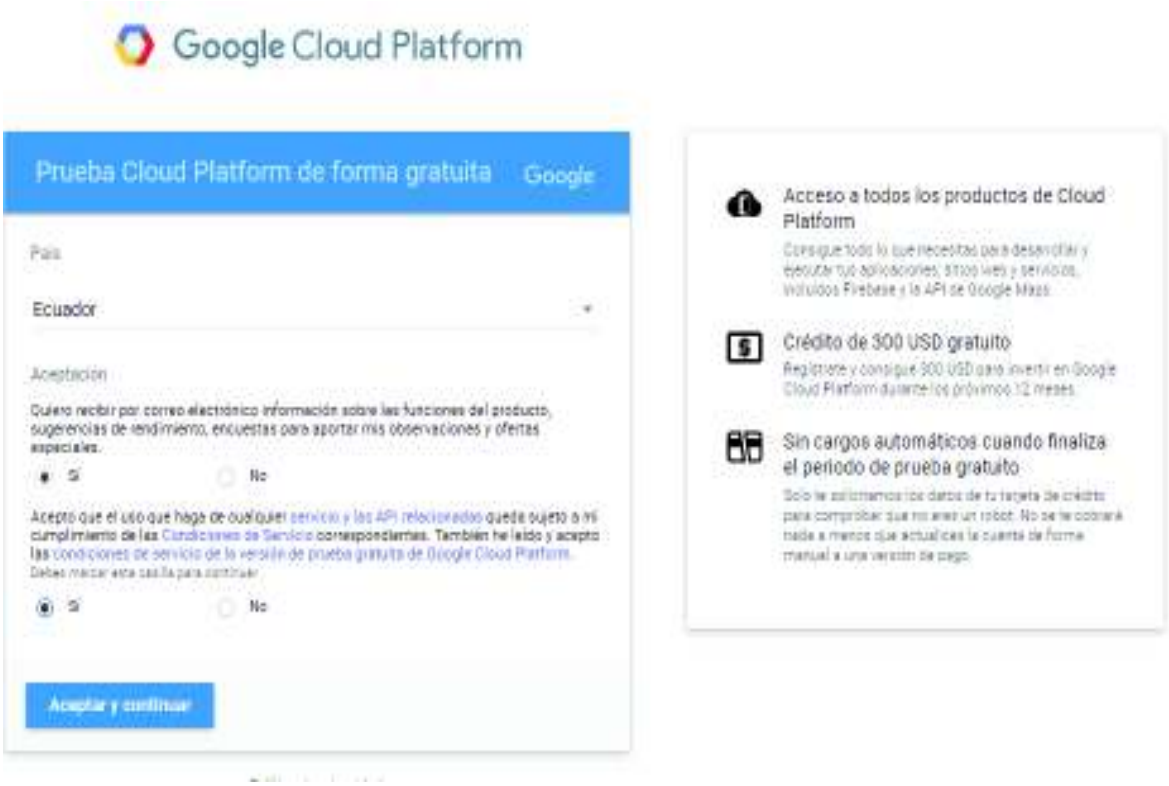

Figura 2.4. Registro en *Google Cloud Platform.*

Figura 2.5. Cartel de bienvenida a *Google Cloud Platform.*

Luego de la bienvenida se muestran todos los elementos que se puede explorar dentro de la plataforma, siendo estos las API, la documentación, la opción de crear un proyecto; además de varios tutoriales para aprender a realizar pruebas con *Compute Engine*, *App*

Engine, Cloud Storage entre otras opciones. A continuación se muestra la Figura 2.6 con la información del proyecto creado y luego la Figura 2.7 con algunos servicios, productos y recursos que ofrece *Google Cloud Platform.*

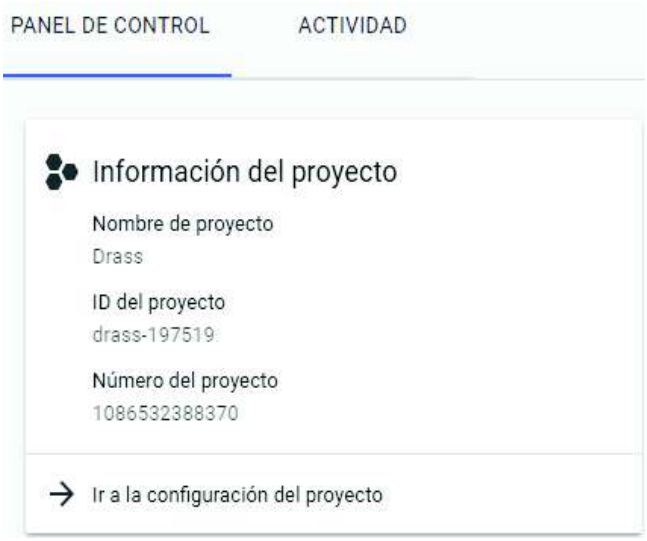

Figura 2.6. Información del proyecto creado en el DRaaS.

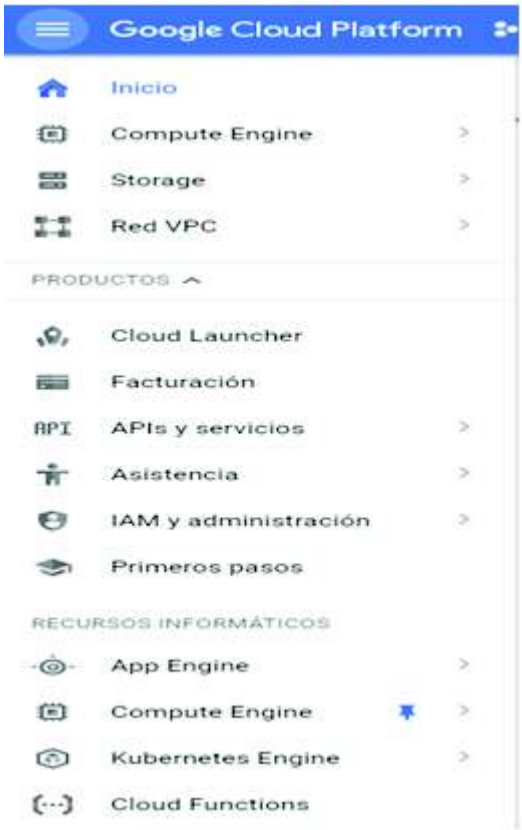

Figura 2.7. Servicios, productos y recursos que ofrece *Google Cloud Platform*.

2.2.4 Configuración de Servicios DRaaS [27]

En este apartado se realizará la configuración de los servicios DRaaS mencionados en el **Capítulo II Apartado 2.2.1.** A continuación se explica el procedimiento necesario para la configuración de dichos servicios.

2.2.4.1 Configuración del Servicio Compute Engine

Para la configuración de este servicio es necesario la creación de la instancia de la Máquina Virtual por sus siglas en inglés (VM *Virtual Machine*). La creación de una instancia VM hace referencia del objeto sobre el cual se crea, en este caso es la creación de una VM que representará al servidor en el cual se copiará las bases de datos y el servidor web con la aplicación portal. Una VM no es más que la simulación del sistema en donde se puede ejecutar todos los programas como si se estuviese en un entorno real de un servidor.

En la Figura 2.8 se presenta la creación de la instancia de VM desde *Google Cloud Platform*:

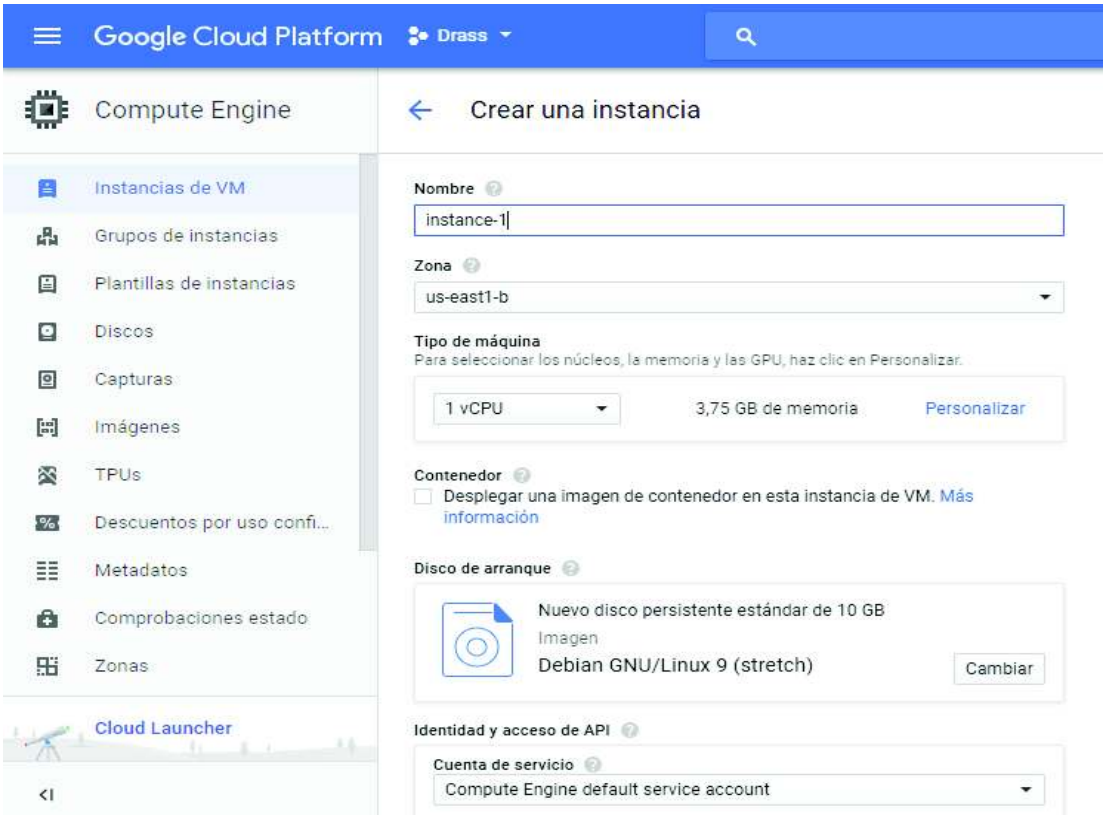

Figura 2.8. Creación de una instancia VM.

Después de haber creado la instancia de VM se procede a seleccionar la opción *Cloud Launcher*, donde se podrá escoger el sistema operativo que se desee instalar. En este caso se seleccionó Windows Server 2012 R2.

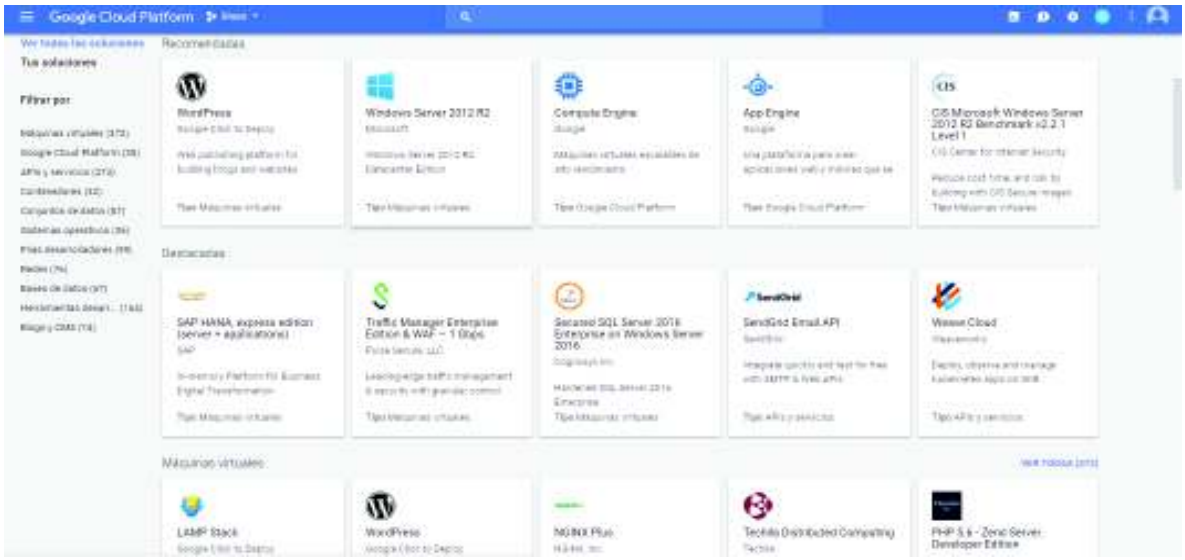

Figura 2.9. Selección del Sistema Operativo.

Una vez seleccionado el sistema operativo se procede a ejecutar la instalación de *Compute Engine*, es decir inicia la creación de la nueva instancia de VM.

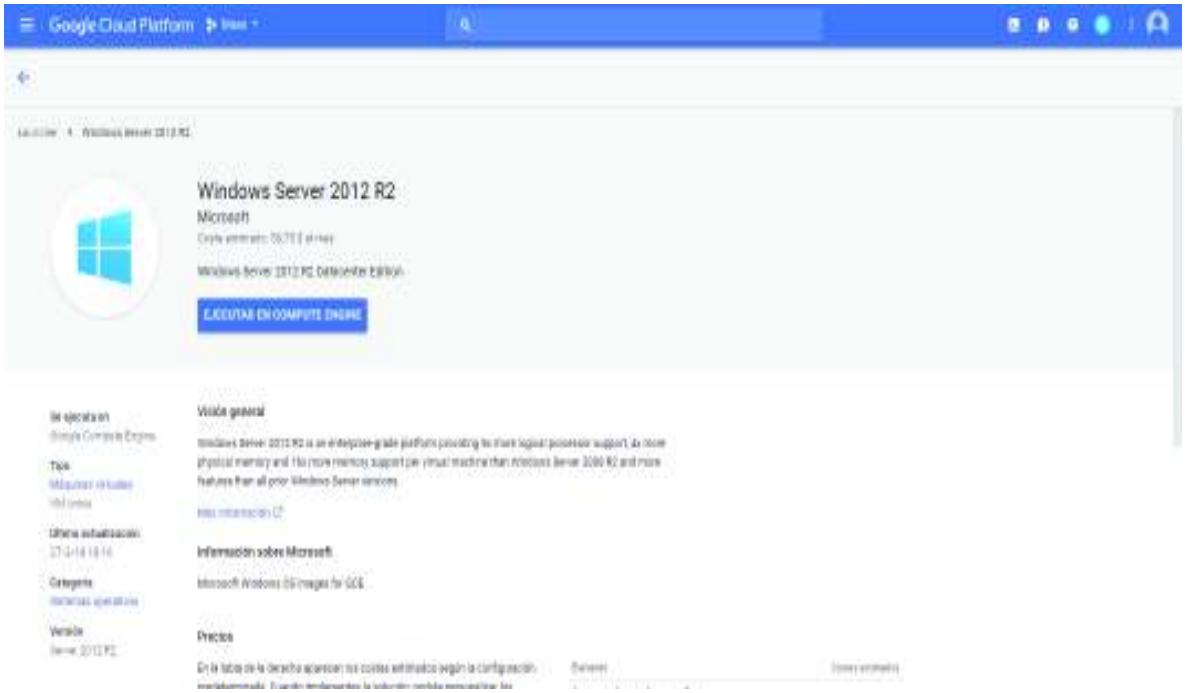

Figura 2.10. Ejecución de la instancia VM con Windows server 2012 R2.

Una vez configurados todos los parámetros necesarios para la creación de la nueva instancia en VM, se muestra el avance de la instalación en la Figura 2.11:

Figura 2.11. Avance de la instalación de la instancia de VM.

Una vez que la instancia de la VM ha sido creada se procede a asignar los recursos que se consideren necesarios como nombre, zona, tipo de CPU, memoria, disco de arranque, cuenta de servicio y alcance del acceso:

Figura 2.12. Asignación de recursos en la instancia de VM.

Después de haber seleccionado los recursos, finalmente se puede observar la instancia de VM creada, la misma que se encuentra con un visto y seleccionada en un recuadro. Además se puede observar elementos relevantes como zona, IP interna y externa, las cuales son asignadas por el proveedor *Google* a la hora de crear la instancia de VM.

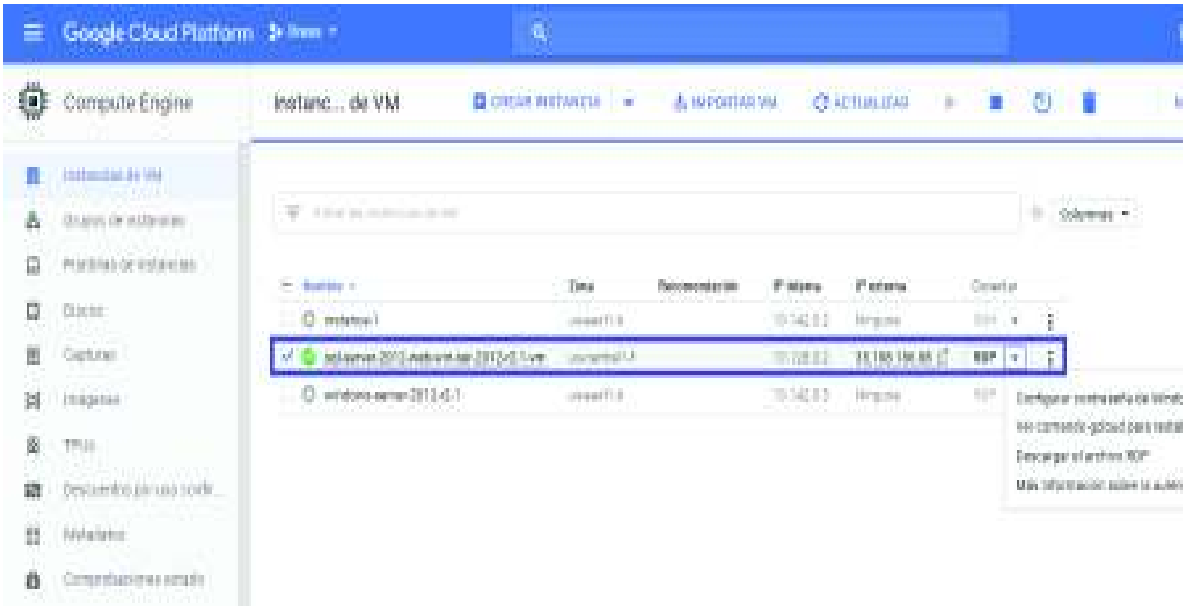

Figura 2.13. Instancia de VM creada.

2.2.4.2 Configuración del Servicio Cloud SQL

El servicio *Cloud SQL* se configura automáticamente al momento de crear la instancia VM; es decir al momento de seleccionar el sistema operativo todos los programas se configuran de manera automática. Es importante mencionar que el servidor web del CEC-EPN necesita que las bases de datos se encuentren en el mismo servidor ya que se encuentran relacionadas para su correcto funcionamiento. Es por esto que se ha creado únicamente una instancia de VM tanto para las tres bases de datos como para el servidor web; siendo esto una ventaja para la recuperación ya que permite que el proceso sea más rápido.

2.2.4.3 Configuración del Servicio Cloud Storage

Este servicio se configura de manera automática cuando se crea la VM, ya que es una parte interna de la misma que tiene como función el almacenamiento de la información que desee el usuario. A través de este servicio es que se realizan las réplicas, las cuales

pueden ser en “caliente”[2] o “frío”[3] dependiendo si el servicio se encuentra activo. La copia en frío no es más que cuando se tiene la información almacenada pero no es utilizada, mientras que en caliente es cuando se está utilizando la información.

A continuación en la Figura 2.14 se muestra una réplica de una copia en frío y en la Figura 2.15 una segmentación automática de *Google* para guardar la información a través de los discos persistentes.

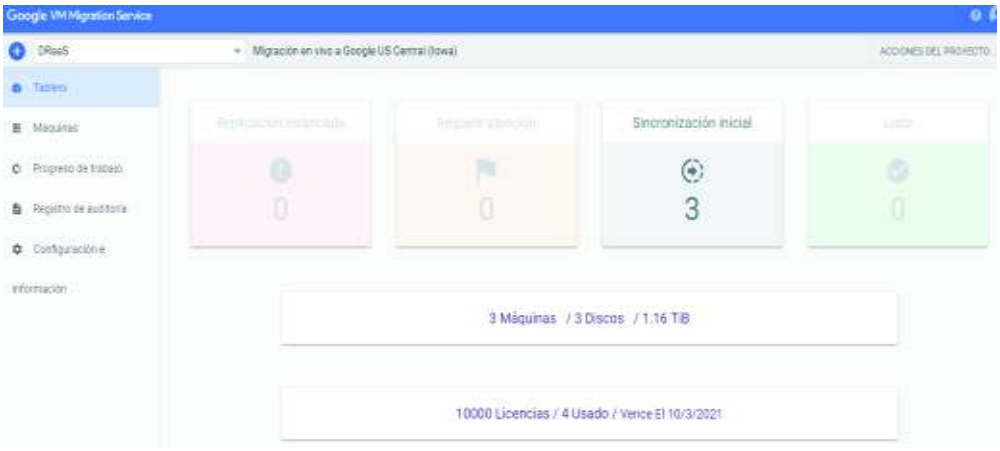

Figura 2.14. Replica de una copia en frío de una instancia de VM.

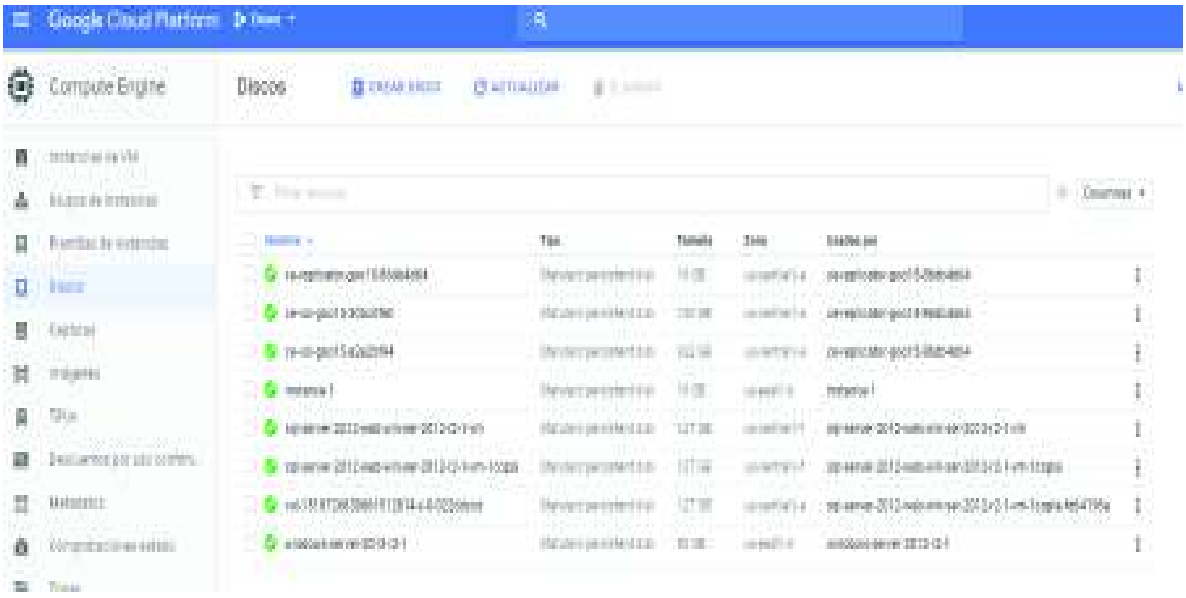

Figura 2.15. Replica en discos persistentes de una instancia de VM en *Cloud.*

[2] La réplica en caliente es cuando se utiliza la información.

[3] La réplica en frío es cuando se tiene la información almacenada pero no es utilizada.

2.2.5 Migración de la Información del CEC-EPN a *Google Cloud*

Este paso es necesario debido a que el prototipo se está realizando a través de una máquina virtual que simule un entorno real. Antes de realizar la migración de las bases de datos y de la aplicación web se debe verificar que la instancia de VM se encuentre creada correctamente, operativa y con los programas necesarios para la migración antes mencionada. En este caso se verificará que se encuentre instalado SQL Server 2012 para las bases de datos y XAMPP, que es un paquete de software libre, desde donde se puede administrar diferentes actividades relacionadas con sus siglas, las cuales significan X(para cualquier sistema operativo), A(Apache), M (MariaDB/MySQL), PP(lenguajes de programación Perl y PHP); en este caso se utilizará XAMPP para ejecutar el servidor web Apache; siendo este un requerimiento propio de la aplicación web que utiliza el CEC-EPN. Para verificar la disponibilidad de la instancia de VM se procede a inicializar y realizar la conexión a través del Protocolo de Escritorio Remoto, por sus siglas en inglés RDP. Para poder conectarse a través de RDP, es necesario crear unas credenciales de administración a través del botón crear o establecer una contraseña de Windows.

Figura 2.16. Restablecimiento de la contraseña para realizar la conexión a la VM.

Con las credenciales generadas se puede acceder a la nueva instancia de VM, tal como si fuera un escritorio remoto. Como se observa en la Figura 2.17.

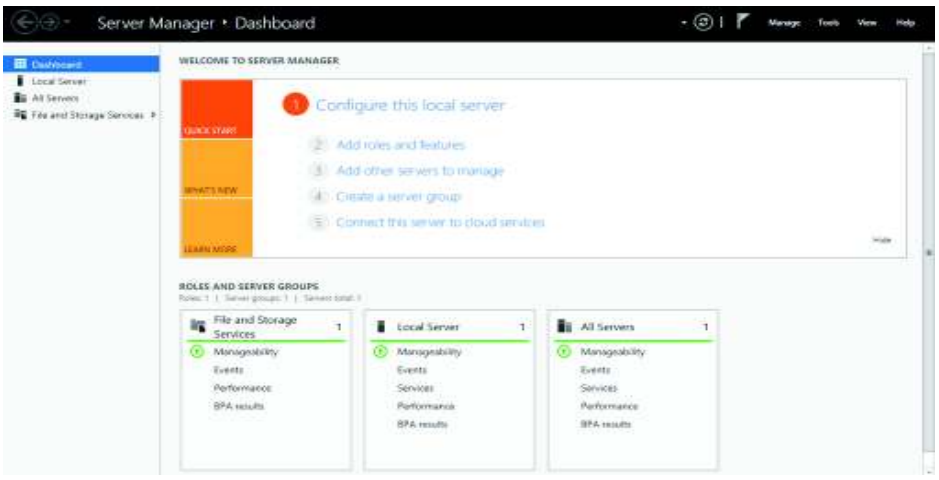

Figura 2.17. Acceso a la nueva instancia VM.

2.2.5.1 Migración de Bases de Datos

Para migrar las bases datos se procede a realizar la extracción de las mismas a través de los respaldos obtenidos del Servidor de BDD de producción de la CGT del CEC-EPN como se encuentra evidenciado en la Figura 2.18.

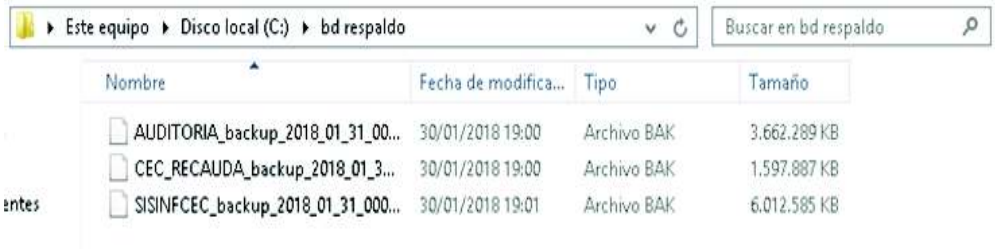

Figura 2.18. Respaldo de las bases de datos de la CGT del CEC-EPN.

Luego se inicializa SQL Server 2008 R2 de la instancia de VM para proceder con la carga de las bases de datos ejemplificadas anteriormente en la Figura 2.19.

Figura 2.19. Inicialización de SQL Server 2008 R2 en la instancia VM.

A continuación en la Figura 2.20, se muestra el explorador con las bases de datos migradas en la instancia VM.

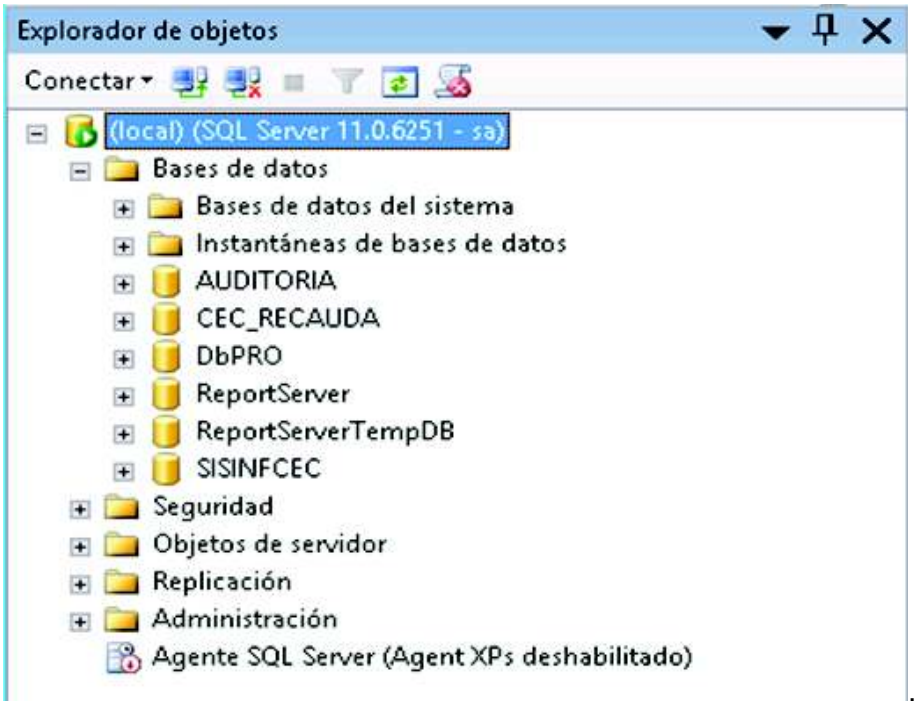

Figura 2.20. Base de Datos en la instancia VM.

Debido a que las bases de datos se encontraban comprimidas se procede a descomprimir y a utilizar la funcionalidad de "Restaurar" como se indica en la Figura 2.21. Posteriormente se debe especificar la ubicación de la copia de seguridad.

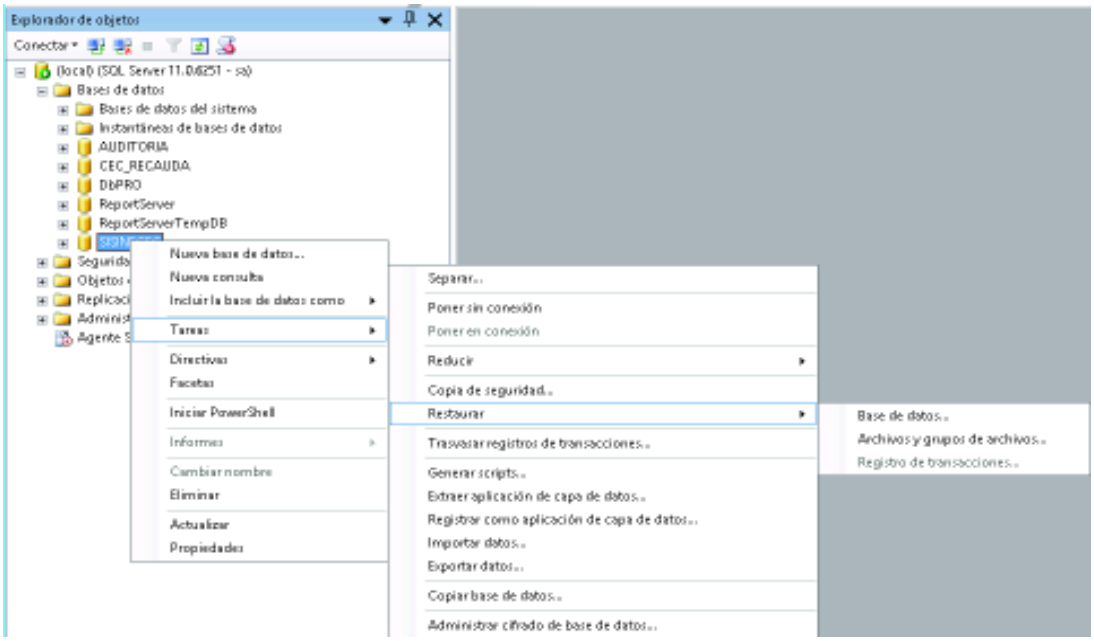

Figura 2.21. Restauración de las Bases de datos migradas en VM.

Luego se selecciona la copia de seguridad que se va a restaurar como se muestra en la Figura 2.22 y se acepta.

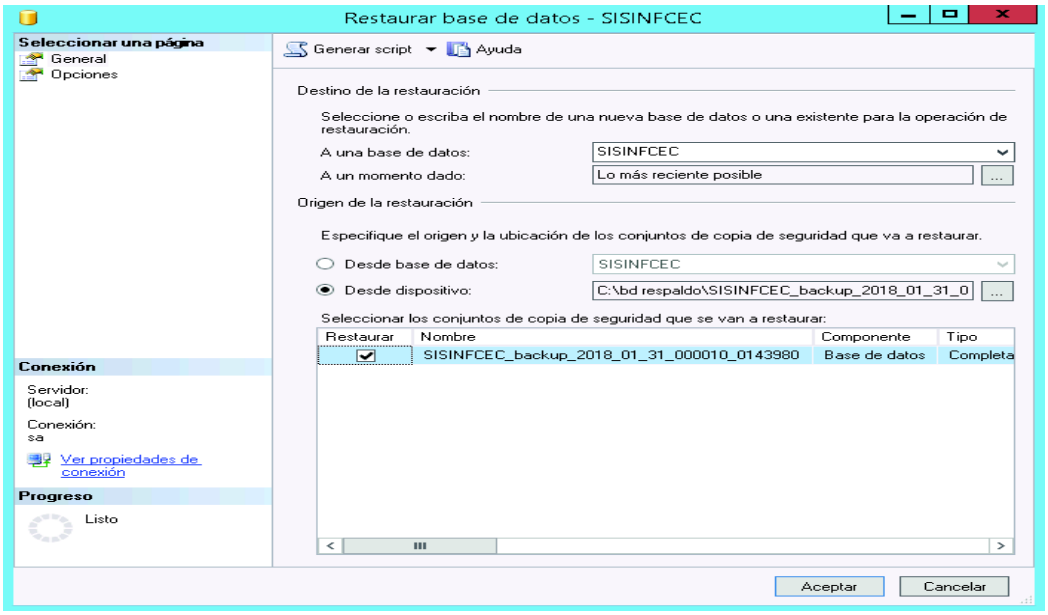

Figura 2.22. Restauración de la Base de datos de la CGT del CEC-EPN.

2.2.5.2 Migración del Servidor Web

Para la migración del servidor web se utilizó XAMPP para Windows como se muestra en la Figura 2.23, el cual constituye un requisito propio de la CGT del CEC-EPN.

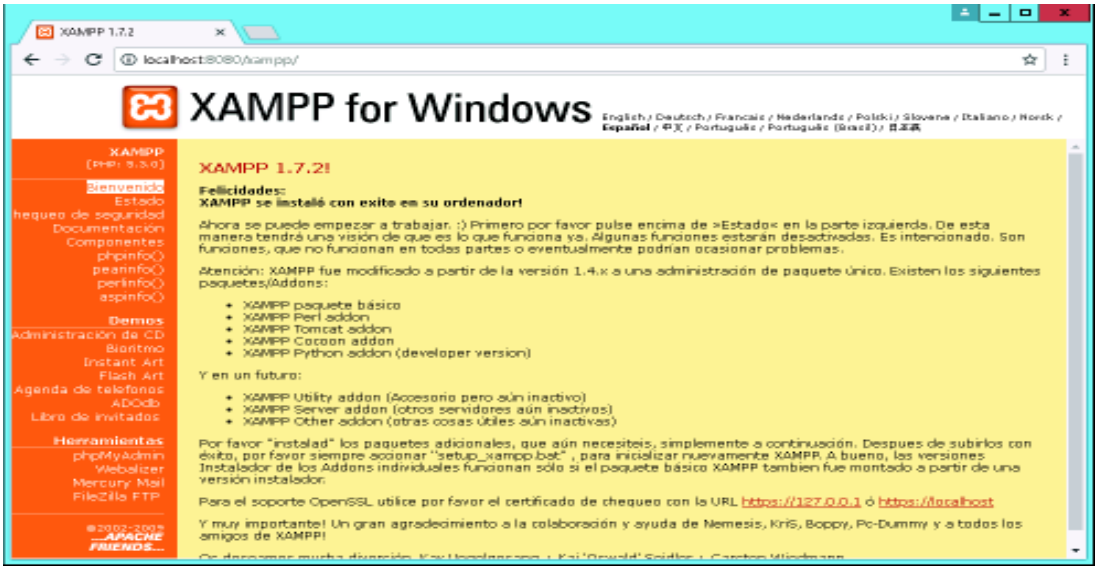

Figura 2.23. Instalación de XAMPP para Windows en la VM.

Luego se procede a copiar la aplicación en la carpeta htdocs (es una carpeta que genera XAMPP en su instalación en la cual se debe copiar todas las aplicaciones que se deseen iniciar desde el servidor, como se muestra en la Figura 2.24.

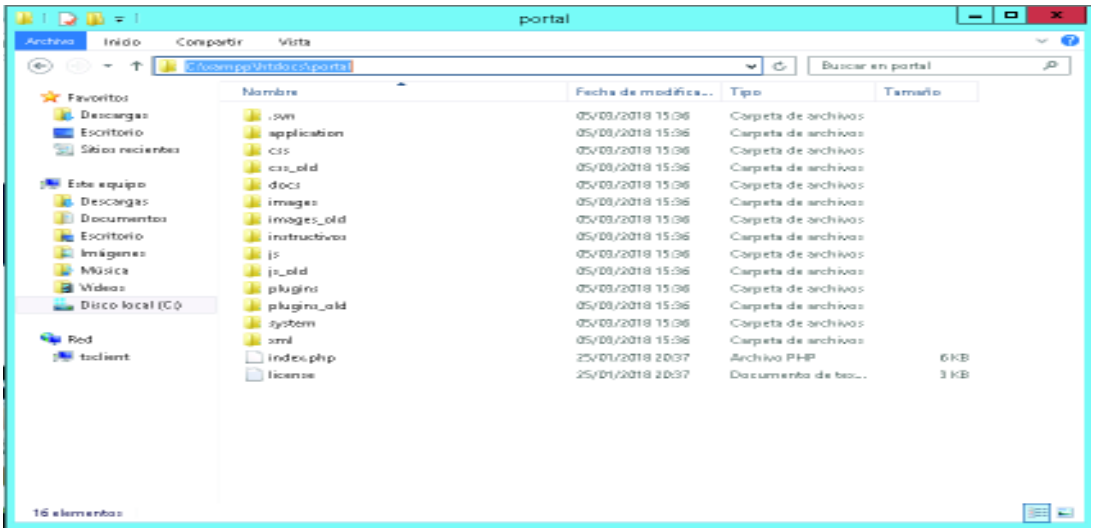

Figura 2.24. Copia de los archivos de la aplicación web en htdocs.

Una vez que están realizadas todas las configuraciones se procede a verificar ejecutando la URL local del servidor: localhost:8080/portal de la instancia de VM en *Cloud*. Como se muestra en la Figura 2.25.

Figura 2.25. Acceso al portal CEC-EPN en el servidor local.

3. RESULTADOS Y DISCUSIÓN

3.1 Pruebas de los Servicios DRaaS en *Cloud*

Para validar el correcto funcionamiento del prototipo implementado para la CGT del CEC-EPN se realizarán las pruebas necesarias mediante la máquina virtual que se encuentra simulado un ambiente real en *Google Cloud Platform*. A continuación se presentan las pruebas realizadas:

3.1.1 Prueba de la Aplicación Web

Para la realización de esta prueba se inicializa la instancia VM la misma que se encuentra simulando al servidor web del CEC-EPN. Posteriormente para que la aplicación web funcione se inicializa el servidor web Apache a través de XAMPP debido a que es un requerimiento propio del CEC-EPN como se lo mencionó anteriormente. Como se observa en Figura 3.1.

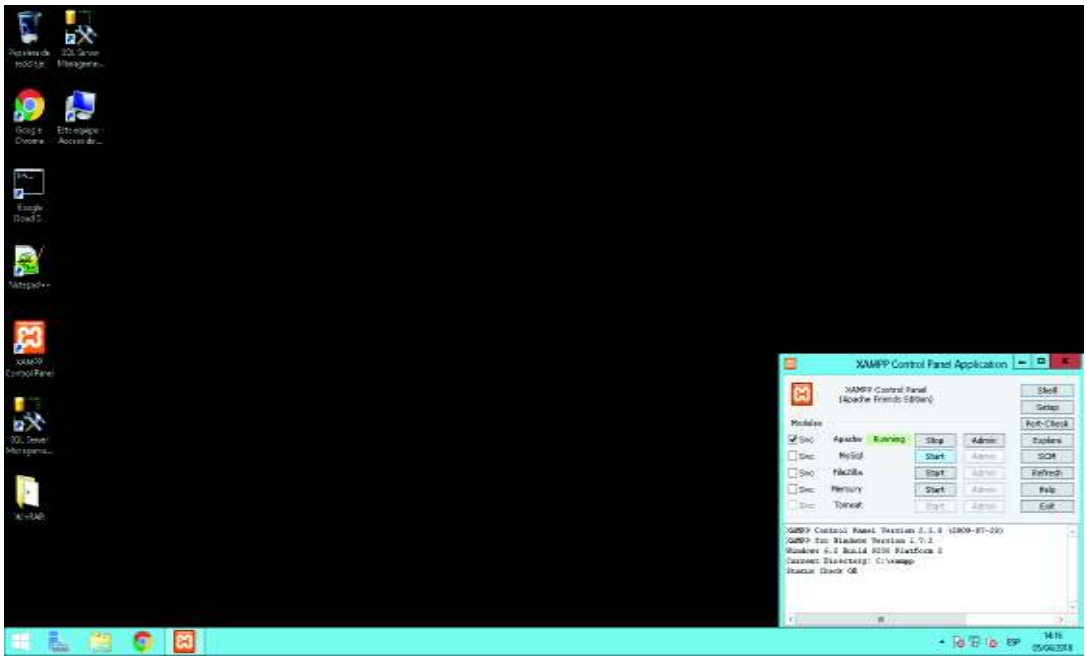

Figura 3.1. Inicialización de Apache a través de XAMPP.

Una vez inicializado el servidor Web Apache en la instancia de VM se procede a ingresar al portal con el usuario, la contraseña generada por el sistema, y el “perfil estudiante” como se muestra en la Figura 3.2.

Figura 3.2. Ingreso de datos de un usuario al portal en línea.

Una vez ingresado los datos se puede observar que el ingreso al portal fue satisfactorio como se indica en la siguiente Figura 3.3.

Figura 3.3. Ingreso satisfactorio al portal en línea.

Como segunda prueba se procede a ingresar los datos de un usuario que si se encuentra en el sistema, pero ingresa mal la contraseña. El resultado de la búsqueda en el sistema será “usuario o contraseña incorrecta” como se evidencia en la Figura 3.4.

Figura 3.4. Ingreso fallido al portal en línea.

Como tercera prueba se procede a ingresar los datos de un usuario que nunca ha tomado un curso en el CEC-EPN, es decir es un cliente nuevo. Al momento de intentar ingresar con sus datos el sistema le emitirá el siguiente mensaje: “sus datos no están registrados en el sistema” como se observa en la Figura 3.5.

Figura 3.5. Usuario no registrado en el sistema.

3.1.2 Prueba de la Réplica del Servidor

Esta prueba será realizada para comprobar el correcto funcionamiento del DRaaS con los servicios de almacenamiento, migración y computación mediante la VM que se encuentra con la información del CEC-EPN. Esta prueba es una réplica completa del equipo, es decir es una copia tanto del sistema operativo, programas, información y aplicaciones. Esta replica se realiza de manera automática y no tiene un tiempo definido ya que depende del tamaño de los archivos, del servidor y de la velocidad de Internet con la que cuente. Mientras la instancia de VM se encuentre inicializada las réplicas o copias de seguridad serán realizadas una a continuación de otra de manera automática, como se observa en la Figura 3.6.

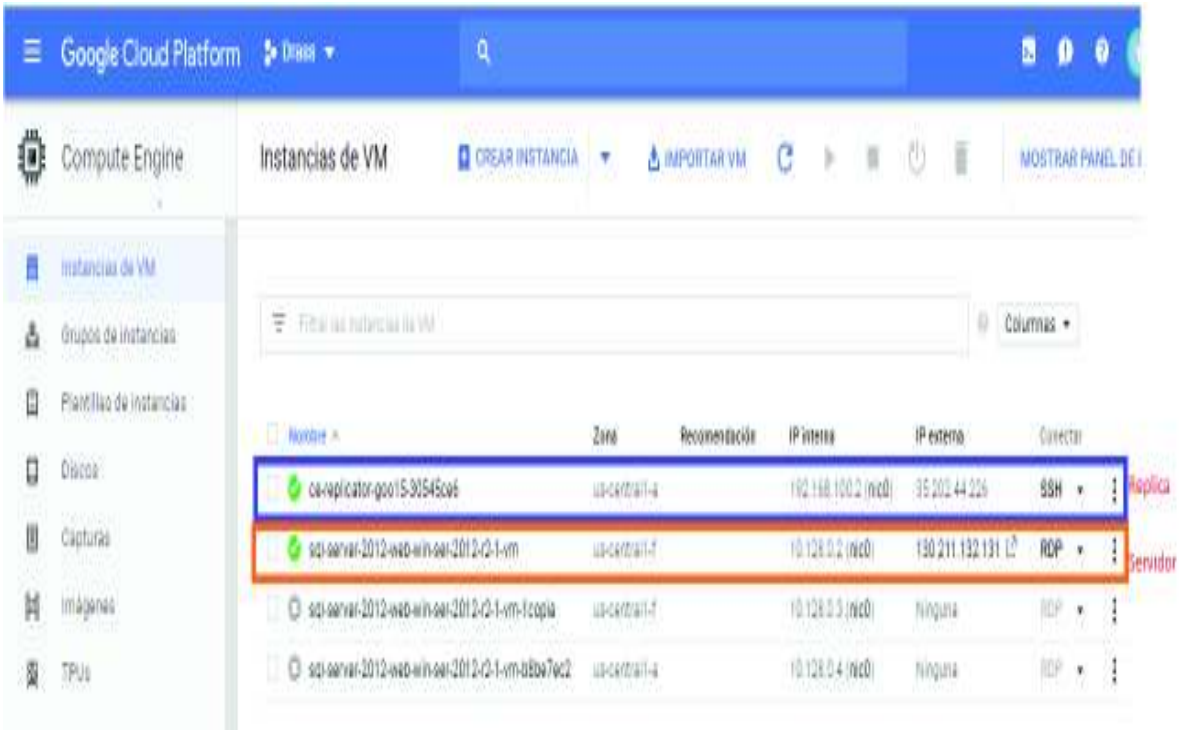

Figura 3.6. Réplica de la instancia de VM.

Una vez finalizada la réplica o la copia de información, inicializa la próxima replica la misma que es generada como un temporal hasta que haya sido finalizada exitosamente y reemplaza a la réplica anterior; es por eso que siempre va a salir en la pantalla una sola copia. Esta copia es almacenada en frio hasta que desee realizar la recuperación de la información como se evidencia en la Figura 3.7.

Figura 3.7. Réplica de la instancia de VM almacenada en frio.

Para verificar las réplicas que han sido realizadas se cuenta con la opción de Audito Log en la que se puede revisar todos los eventos realizados con su respectiva fecha, esto se puede observar en la Figura 3.8.

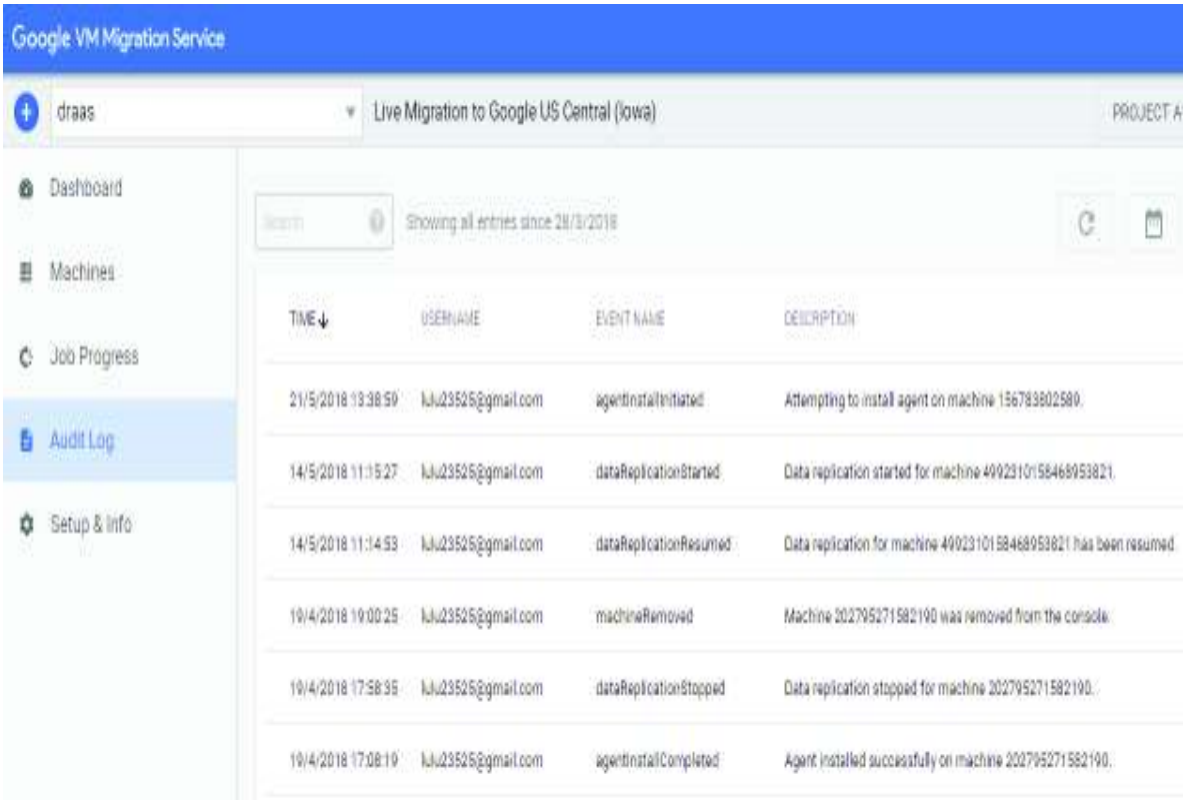

Figura 3.8. Opción *Audit Log* en *Google Cloud Platform*.

3.1.3 Pruebas de Recuperación de Datos

Para el proceso de recuperación de la información de una instancia de VM en la plataforma de *Google Cloud Platform* se debe proceder de la siguiente manera:

Se debe ingresar a *Google* VM *Migration Service* y en la opción *Machines* se debe seleccionar la máquina replicada que está lista para realizar el proceso de recuperación de datos, la cual va a mostrar en su estado un avioncito color azul como se muestra en la Figura 3.9.

Figura 3.9. Recuperación de la información de la VM.

En la sección de instancias de VM se muestran todas las máquinas que están activas y sobre las cuales se hará la recuperación como se muestra en la Figura 3.10.

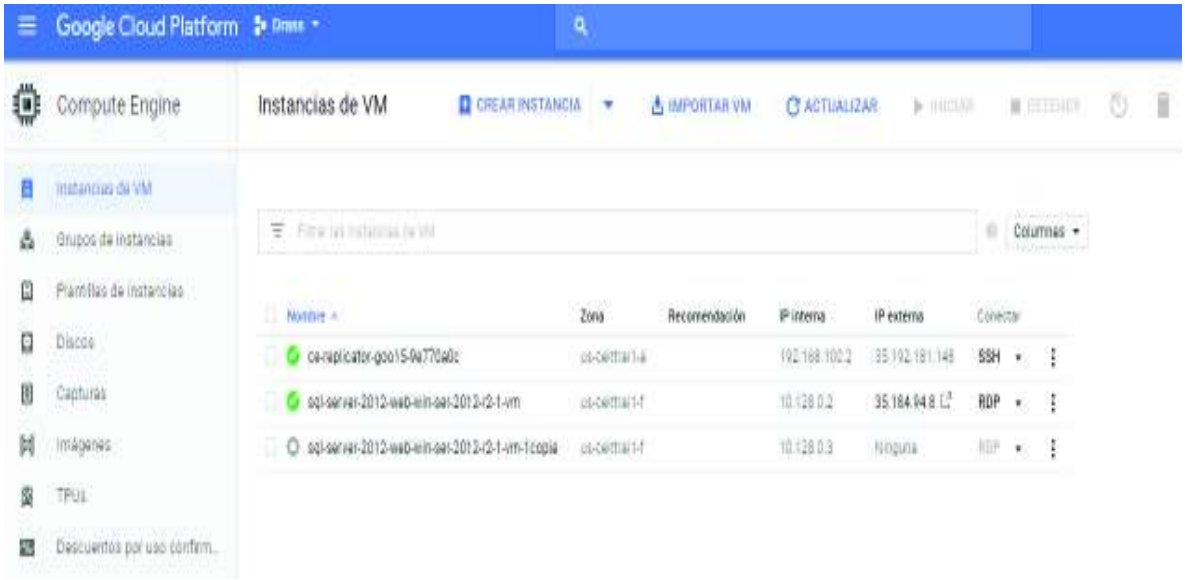

Figura 3.10. Máquinas activas.

Al lanzar la máquina que se encuentra activa se tiene la Figura 3.11 la cual ejemplifica la continuidad del proceso.

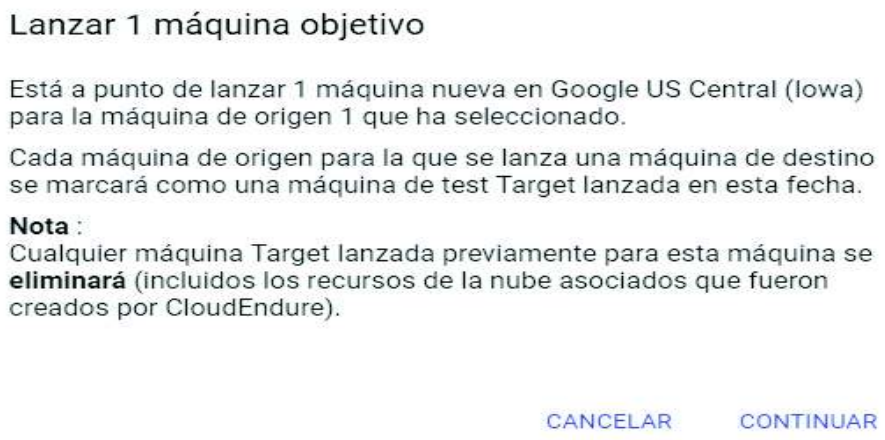

Figura 3.11. Lanzamiento de la máquina activa.

Al lanzar la máquina activa se muestra el progreso de trabajo como se ve en la Figura 3.12 en donde se ejemplifica el tipo, el estado, la fecha y hora de inicialización; además debe mostrar la fecha y hora de terminación cuando termine el proceso.

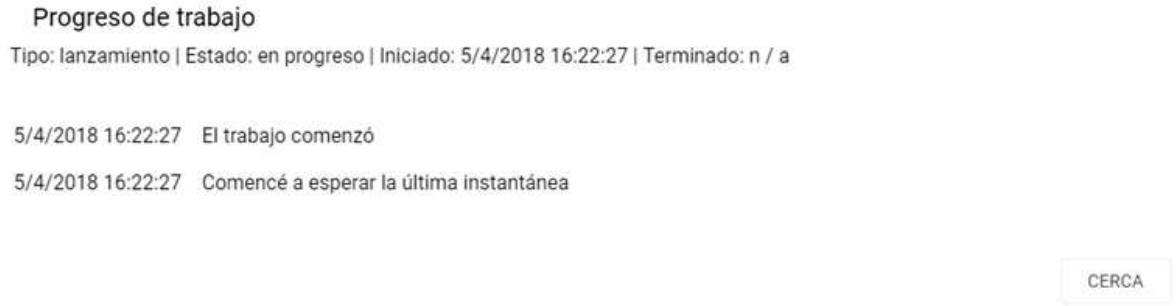

Figura 3.12. Inicialización del proceso.

Finalizado el proceso de recuperación se obtiene la información referente del mismo, en donde se obtuvo como resultado un tiempo de 19 minutos como se muestra en la Figura 3.13, siendo este el resultado del **RTO** (como tiempo tomado para la restauración), este tiempo se obtiene a través de la resta del tiempo de finalización con el tiempo de inicialización del proceso, es válido destacar que ese tiempo puede variar en base al tamaño de los archivos, los diferentes servicios y la velocidad del Internet. Mientras que el

RPO es el último backup con el que se contaba es decir no se perdió ninguna información.

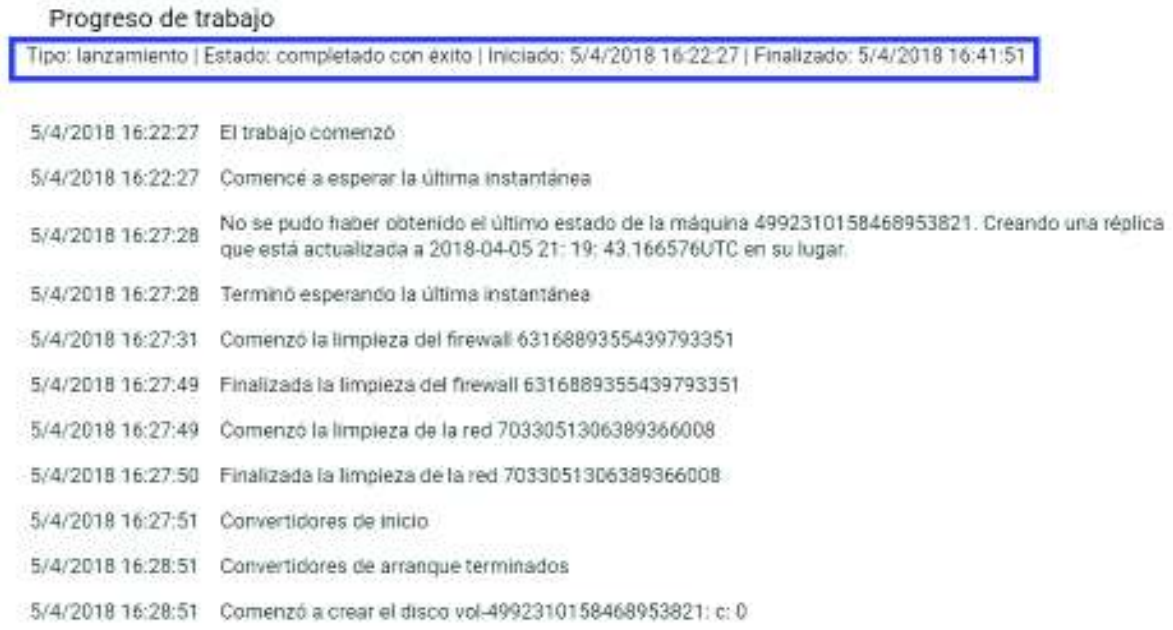

Figura 3.13. Finalización del proceso.

Por último se obtiene una nueva instancia de VM del proceso de recuperación de datos como se muestra en la Figura 3.14.

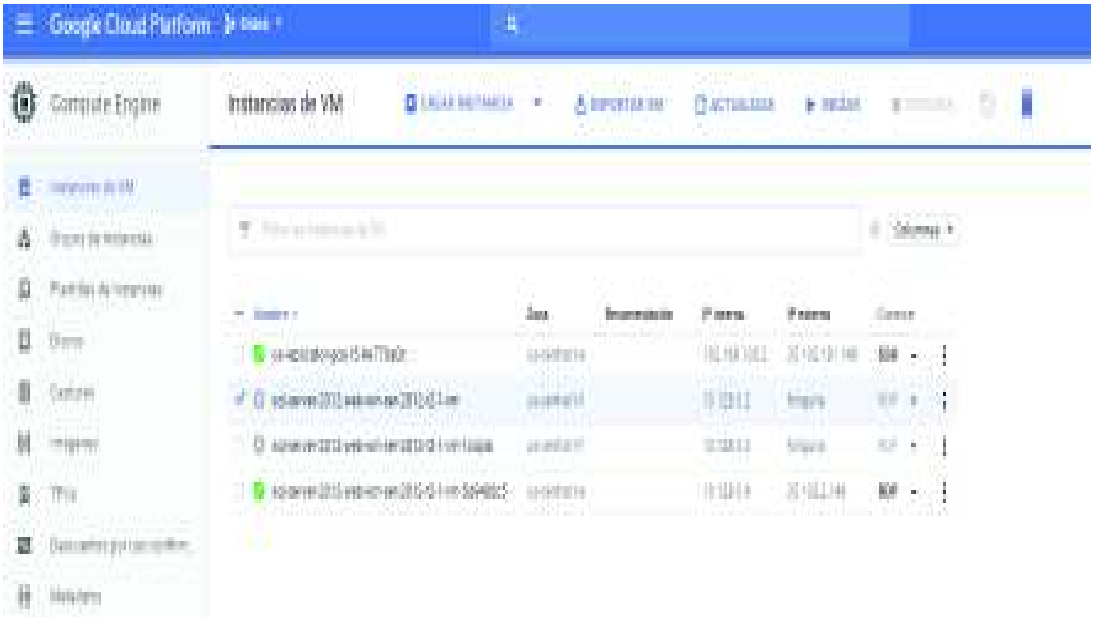

Figura 3.14. Obtención de la instancia VM recuperada.

3.2 Pruebas Simulando un Ambiente Real

Las pruebas simulando un ambiente real consisten en validar el funcionamiento de DRaaS de la Plataforma *Google Gloud Platform* con la información y equipos que se encuentran en producción en el CEC-EPN. Dada la importancia de los servicios que ofrece en el CEC-EPN, y considerando que estos deben estar operativos las 24 horas del día; estas pruebas han sido realizadas una sola vez en una noche previamente programada y analizada por todo el equipo de la CGT. Las Figuras presentadas en este apartado fueron capturadas en este proceso con el fin de comprobar el cumplimiento efectivo del DRaaS y los objetivos de este Trabajo de Titulación.

3.2.1 Prueba de la Aplicación Web

Esta prueba se ha realizado una sola vez debido a que es necesario apagar el servidor de producción con el que trabaja la CGT del CEC-EPN; esta prueba fue realizada en horas de la noche y con la autorización respectiva como ya se mencionó anteriormente; sin embargo no se volverá a realizar dado los problemas que generaría.

Dicha prueba consiste en levantar la instancia VM del servidor web portal que se encuentra implementado en *Google Cloud Platform*; esto es probando un fallo en el servidor de producción que se encuentra en sitio y los usuarios no pierdan su conexión al portal por mucho tiempo, es decir que el cambio sea transparente y el usuario pueda conectarse directamente a través de la misma URL: https://aps.cec-epn.edu.ec/.

Para poner en funcionamiento la instancia VM del servidor web portal que se encuentra en *Cloud* es necesario contar con el acceso a la configuración del DNS del CEC-EPN (cec-epn.edu.ec), el mismo que se encuentra alojado en *Hurricane Electric* (que es el portal de alojamiento que le permite administrar el DNS) [33].

Para ingresar a *Hurricane Electric* o lo que es lo mismo a la administración del dominio se debe ingresar al link: *https://dns.he.net/*. En el mismo se debe ingresar el usuario y la contraseña, como se evidencia en la Figura 3.15.

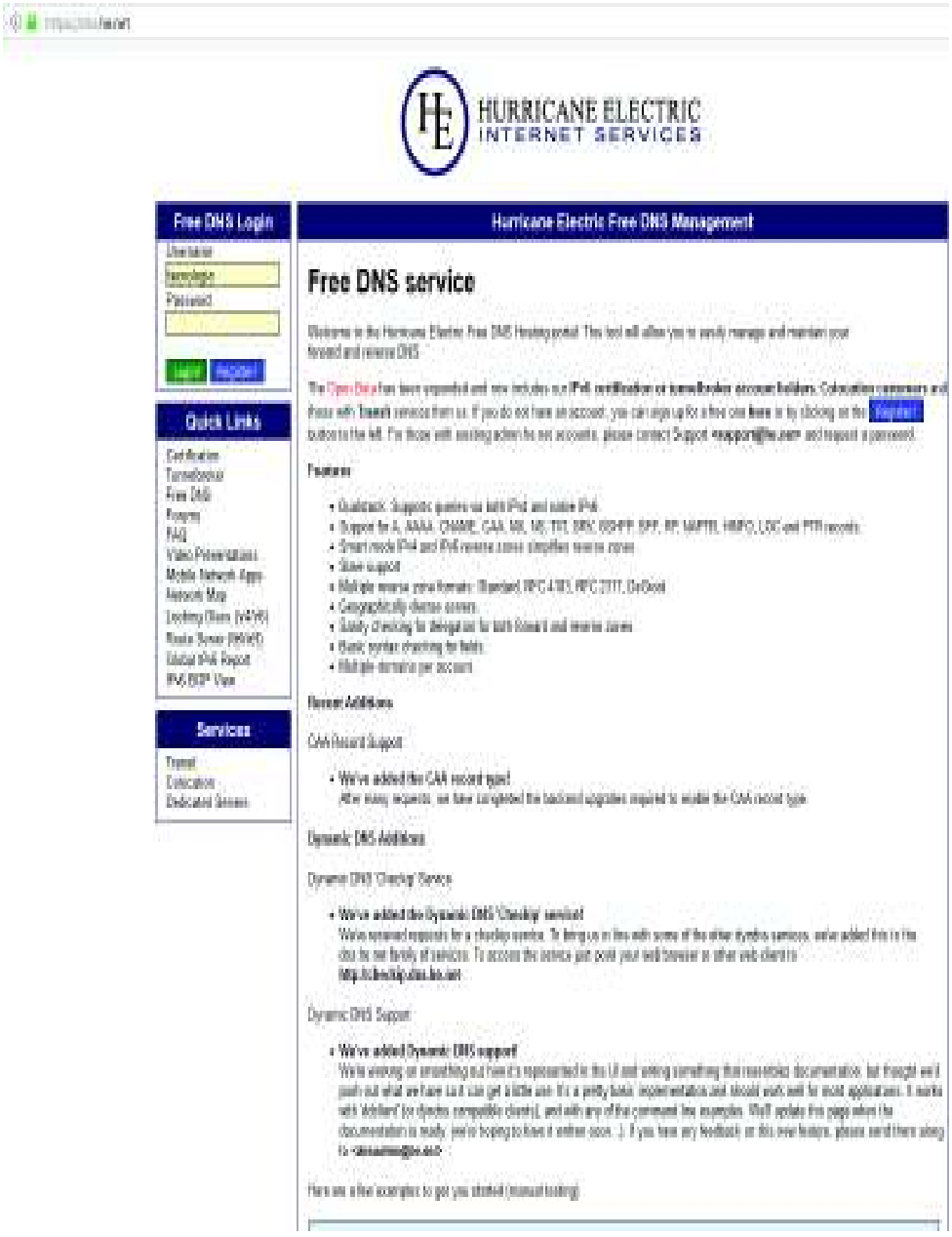

Figura 3.15. Página principal de Hurricane Electric.

Una vez que se haya ingresado a la administración del dominio se procede a seleccionar el dominio del CEC-EPN, en este caso es “cec-epn.edu.ec” como se indica en la Figura 3.16.

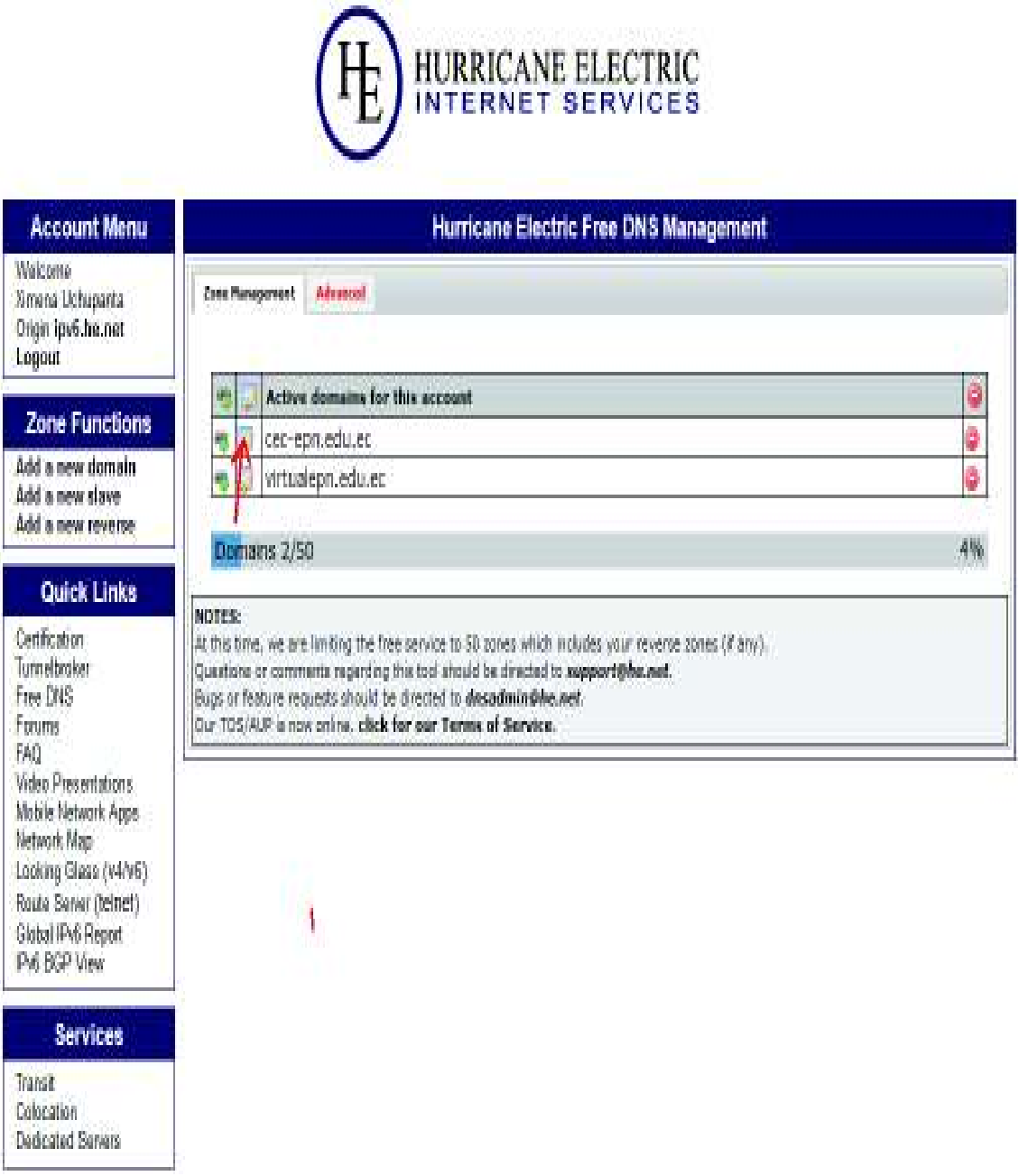

Figura 3.16. Selección del dominio del CEC-EPN.

Al momento de seleccionar el dominio se despliegan todos los subdominios con los que cuenta el CEC-EPN, en este caso el subdominio que nos interesa debido al servidor web portal es el que se encuentra seleccionado en la Figura 3.17 con el nombre “aps.cec-epn.edu.ec”.

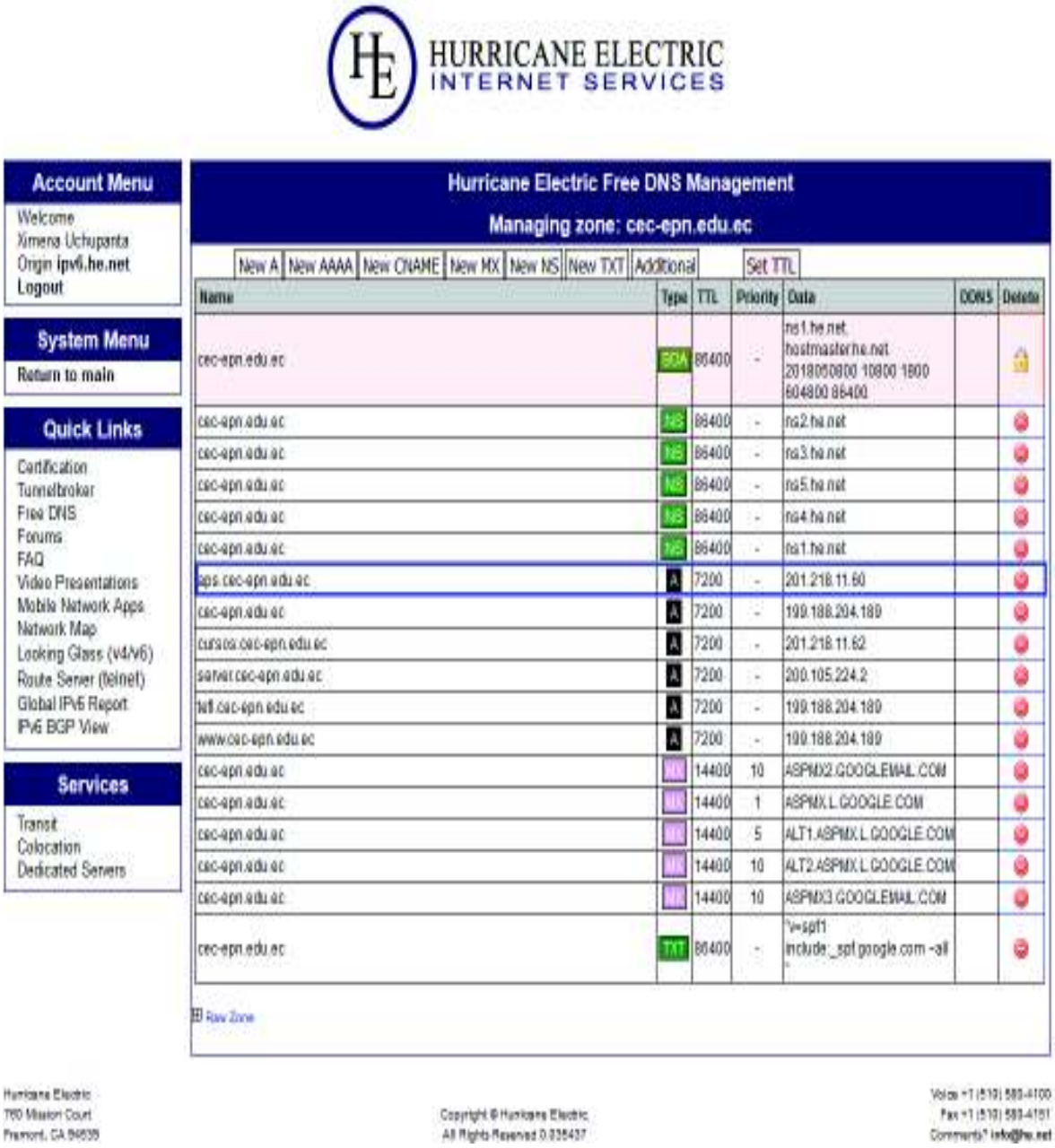

Figura 3.17. Selección del subdominio aps.cec-epn.edu.ec.

Al momento de seleccionar el subdominio “aps.cec-epn.edu.ec” se despliega una ventana en la que se debe realizar el cambio de IP a la nueva IP Pública que en este caso sería la IP externa aleatoria que proporciona *Google Cloud Platform*, esto se evidencia en la Figura 3.18.

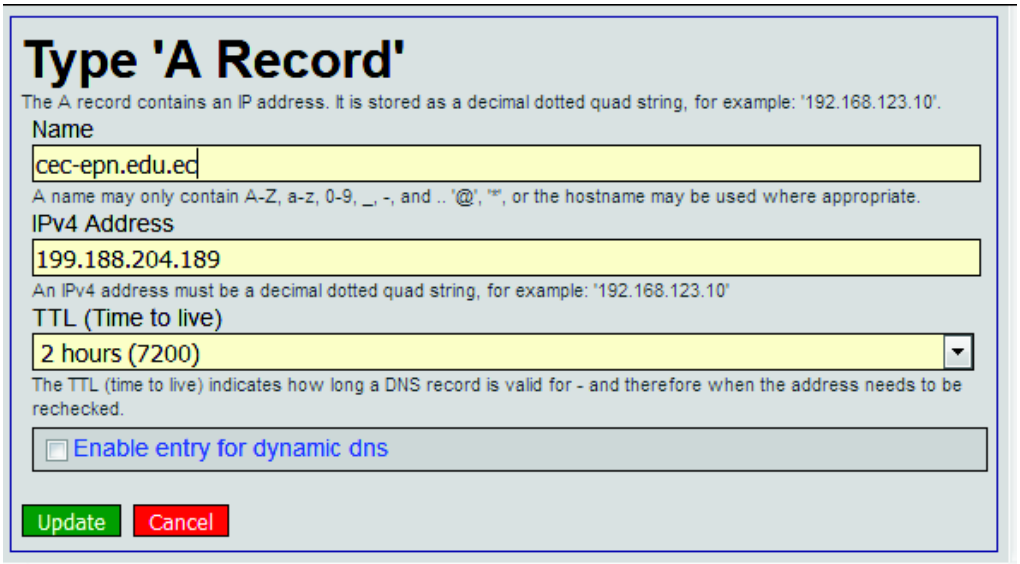

Figura 3.18. Ventana en la que se debe realizar el cambio de IP

Además en la Figura 3.18 se puede observar el Tiempo de Vida por sus siglas en inglés (TTL Time to Live). El tiempo en segundos e indica por cuánto tiempo es válido un registro DNS, y por lo tanto, cuándo es necesario volver a verificar la dirección. Es decir este subdominio necesita 2 horas o 7200 segundos para que el nuevo servidor sea visto en todo el Internet al momento de realizar el cambio de dirección IP externa; este tiempo ha sido establecido como política interna del CEC-EPN; sin embargo en el caso de una emergencia se podría variar el TTL.

Una vez realizado el cambio a la nueva IP pública asignada por *Google* se selecciona "*Update*", se espera las 2 horas del TTL y se verifica la configuración, el funcionamiento del servidor y especialmente el funcionamiento correcto de la aplicación web portal mediante la URL.

3.2.2 Prueba de la Réplica del Servidor

Para esta prueba se realizará la conexión con el servidor físico del CEC-EPN detallando los pasos que se deben seguir para realizar la réplica del mismo.

Primero se debe ingresar a *Google Cloud Platform* desde el servidor que se desea realizar la conexión, se selecciona el proyecto creado > se ingresa a instancias de VM y se selecciona Importar VM como se muestra en la Figura 3.19.

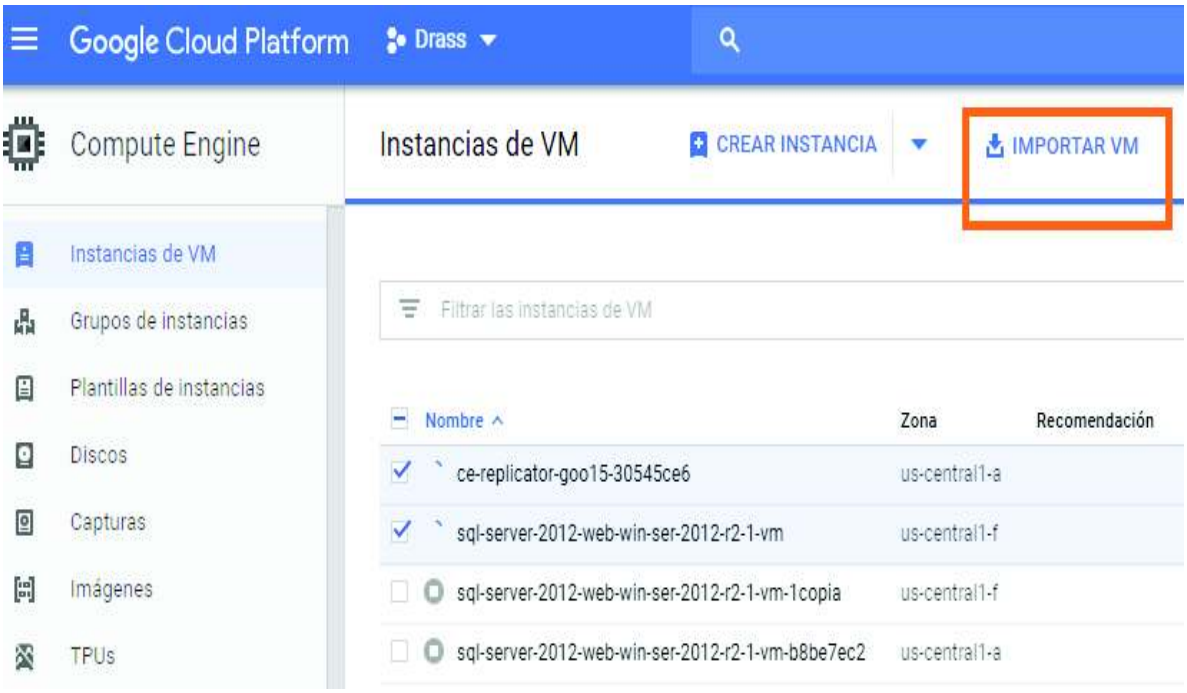

Figura 3.19. Selección de la opción importar VM.

Una vez seleccionada la opción importar VM, se despliega la ventana en la que hay que escoger *CloudEndure* (que es la que proporciona un servicio para migración de VM o servidores físicos) como se indica en la Figura 3.20.

Figura 3.20. Selección de la opción *CloudEndure.*

Una vez que se ingrese a *Google* VM *Migration Service* se debe agregar la maquina como se indica en la Figura 3.21.

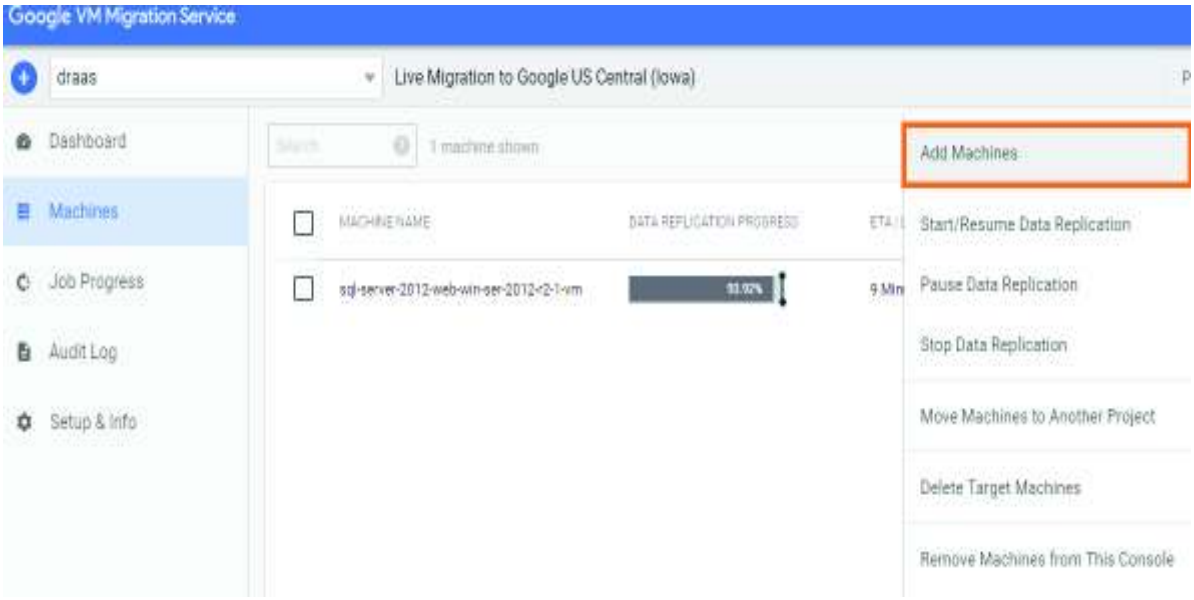

Figura 3.21. Añadir la máquina en *Google* VM *Migration Service.*

Una vez que se ingrese a *Google* VM *Migration Service* se debe agregar la máquina como se indica en la Figura 3.22.

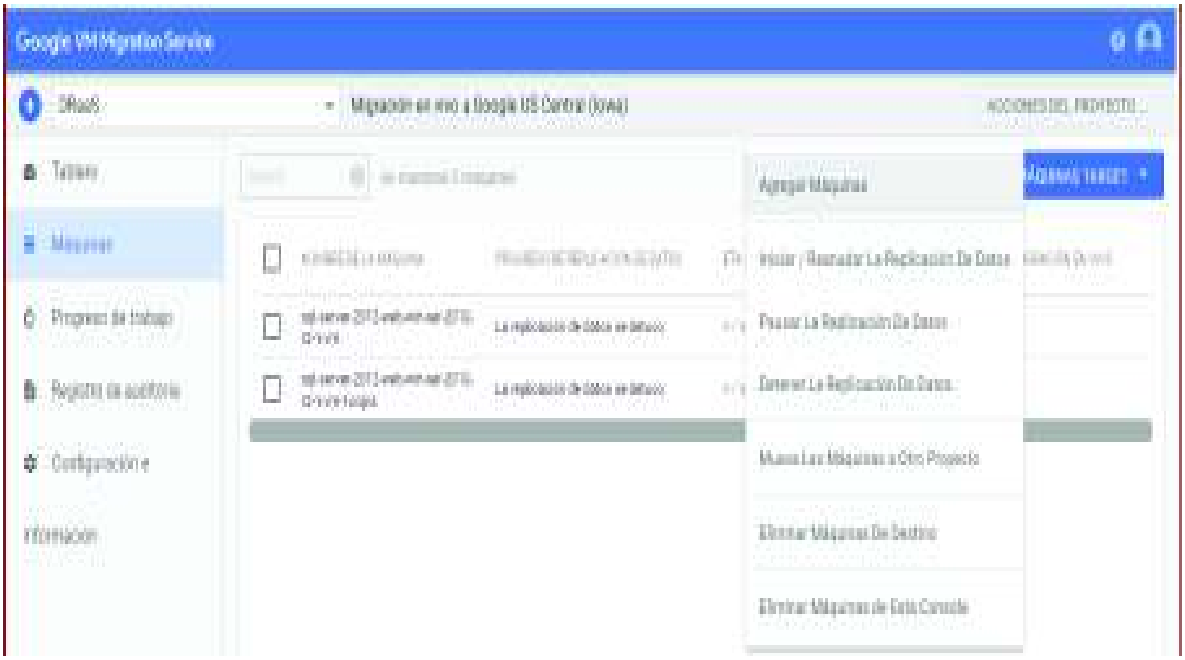

Figura 3.22. Selección de la máquina a ser replicada.

Al momento de seleccionar la máquina se despliega una pantalla con un token donde dice "**Su token de instalación del agente**". Este token debe ser copiado como se evidencia en la Figura 3.23. Este token realiza el vínculo entre *Cloud* y el servidor físico.

Figura 3.23. Token de instalación del agente.

Una vez obtenido el código de instalación de la máquina se procede a descargar el Shell de conexión para la réplica desde el link que dice "**Descargue el instalador de Windows**" como se observa en la Figura 3.24.

Figura 3.24. Descarga de Shell de conexión para la réplica.

Con el Shell descargado se instala y se selecciona click derecho para editar, luego se pega el código de instalación o token que se copió anteriormente, para que se cree las imágenes de los servidores como se indica en la Figura 3.25.

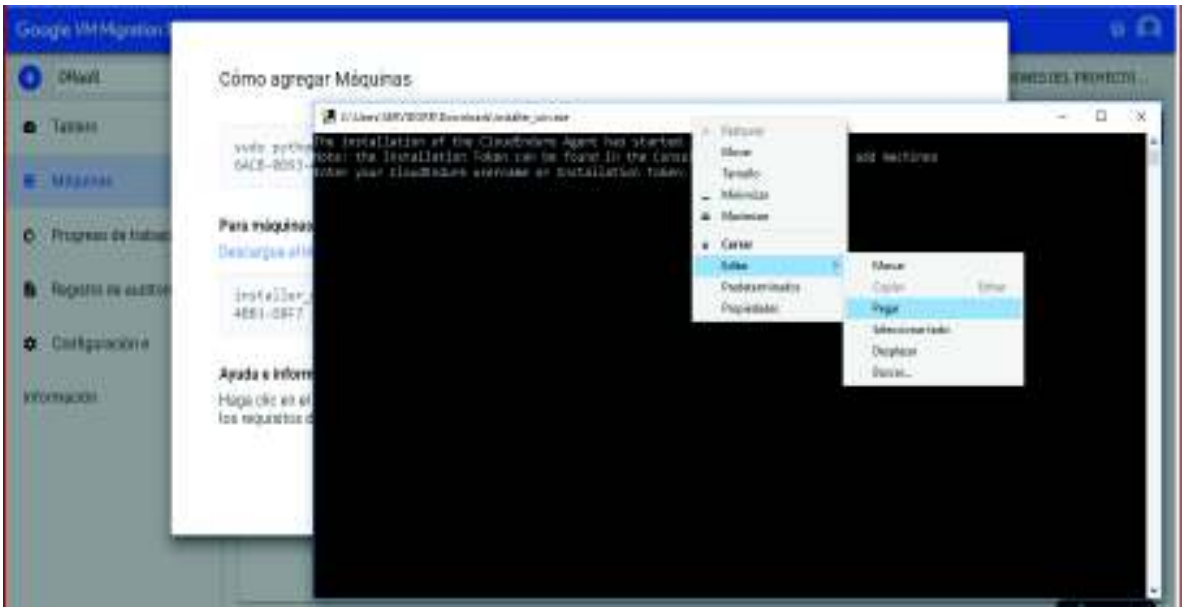

Figura 3.25. Ejecución del Shell de conexión.

Una vez inicializada la réplica se va mostrando la identificación de los discos como se evidencia en la Figura 3.26.

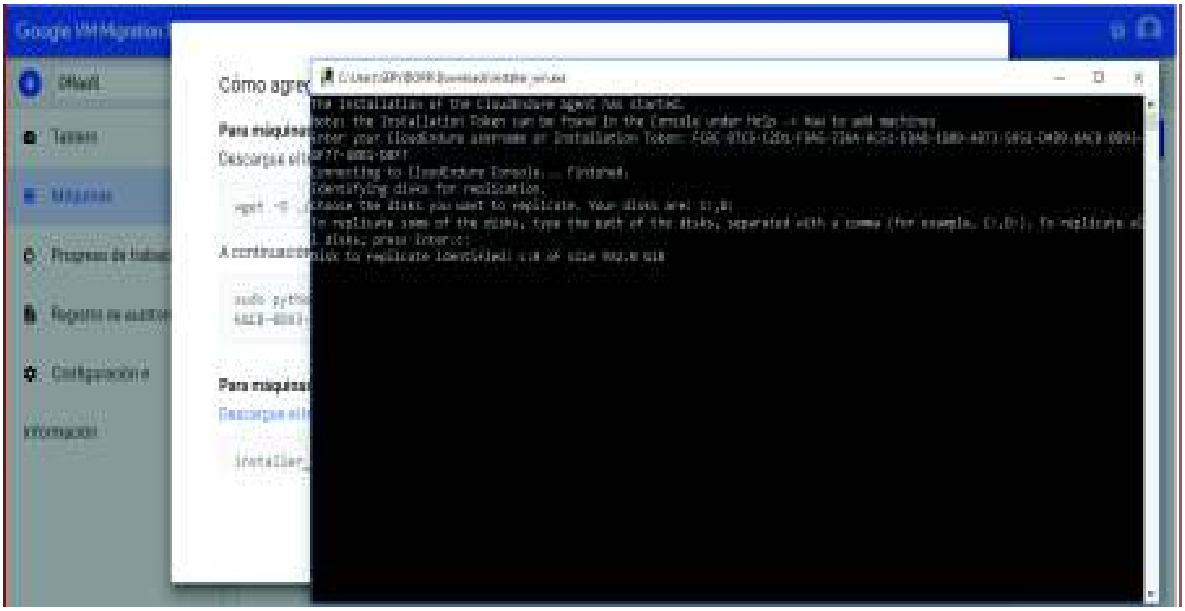

Figura 3.26. Identificación del disco replicado.

Mientras se realiza la réplica se puede ir verificando en *Google* VM *Migration Service* el avance y los detalles como la fecha y la hora de la inicialización del proceso como se muestra en la Figura 3.27.

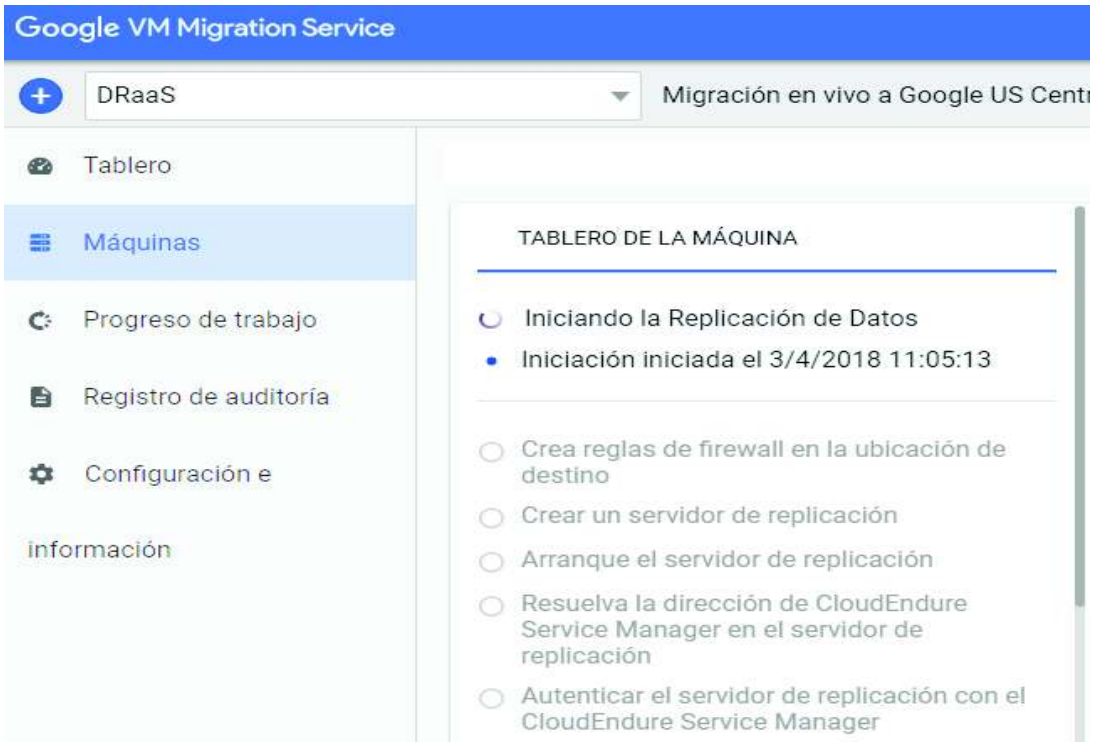

Figura 3.27. Detalles de la réplica

Al terminar la réplica se tiene el siguiente resultado donde no se muestra ningún error y se prueba que la réplica fue un éxito al estar con el icono del avión. Esto se evidencia en la Figura 3.28.

Figura 3.28. Finalización de réplica.

3.2.3 Pruebas de Recuperación de Datos

Para el proceso de recuperación de la información del servidor físico que fue replicado desde *Google Cloud Platform* se debe proceder de la siguiente manera:

Se debe ingresar a *Google* VM *Migration Service* y en la opción *Machines* se debe seleccionar la máquina replicada en este caso es ServidorPrueba. Se selecciona el avioncito color azul como se muestra en la Figura 3.29.

Figura 3.29. Recuperación de la información de la VM.

Inicia la recuperación como se indica en la Figura 3.30.

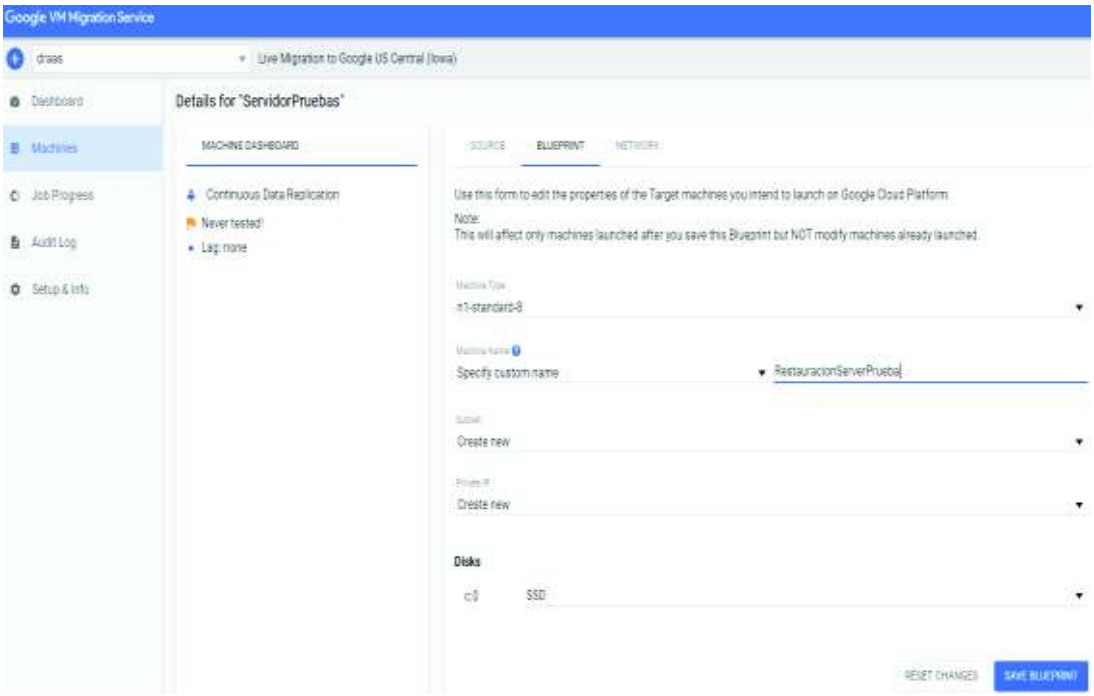

Figura 3.30. Máquinas activas.

Se verifica el avance del proceso de la recuperación de la información de la réplica del servidor físico como se indica en la Figura 3.31.

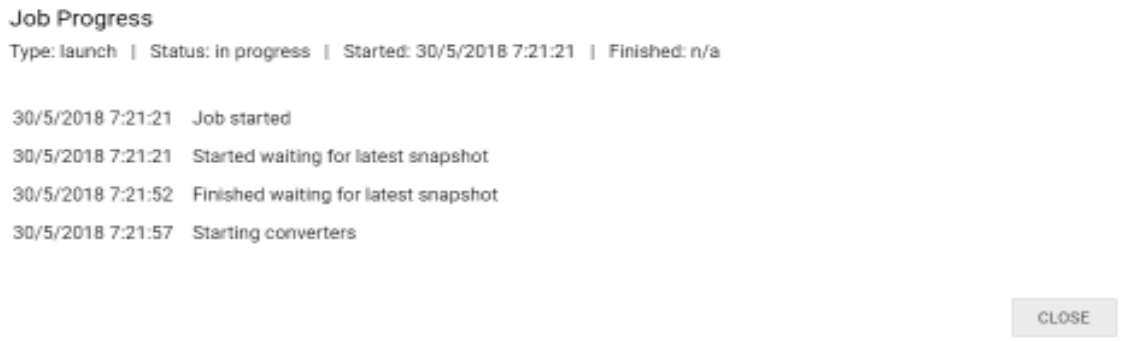

Figura 3.31. Lanzamiento de la máquina activa.

Al finalizar la recuperación de la información se puede observar el progreso con la información de la hora de inicio y la hora de finalización del mismo. Esto se evidencia en la Figura 3.32.

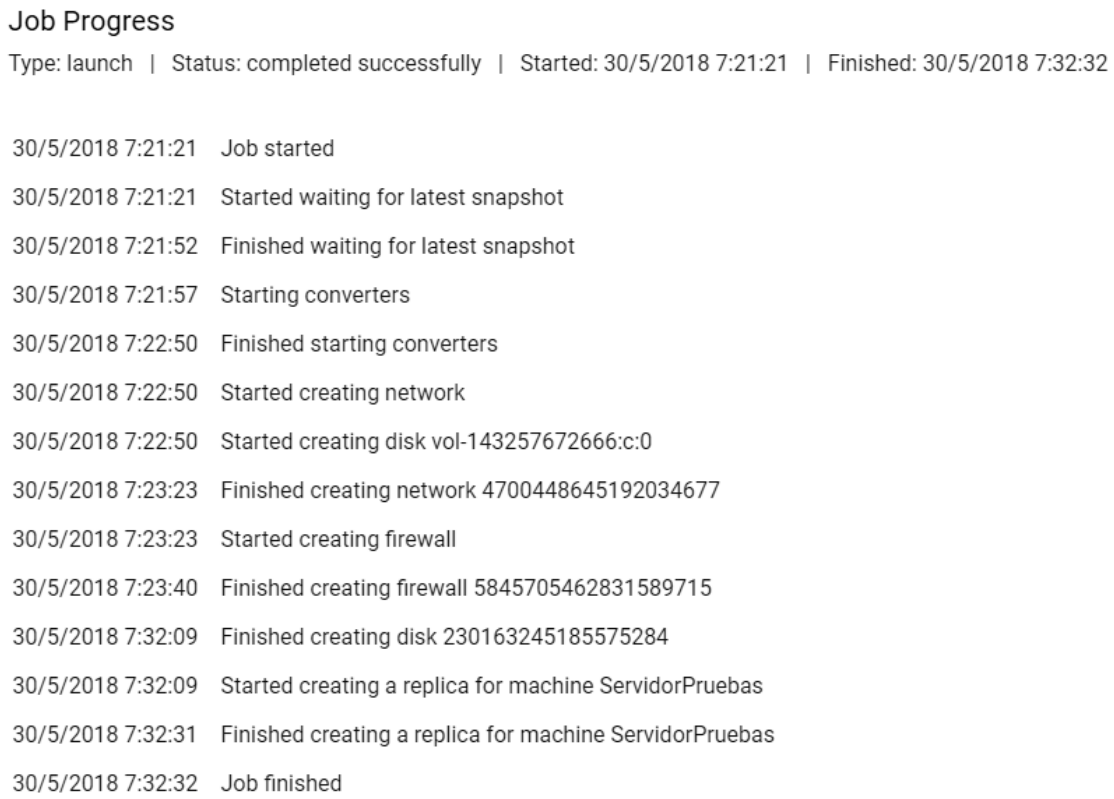

Figura 3.32. Finalización del proceso de recuperación.

Por último se obtiene una nueva instancia de VM del proceso de recuperación de datos como se muestra en la Figura 3.33.

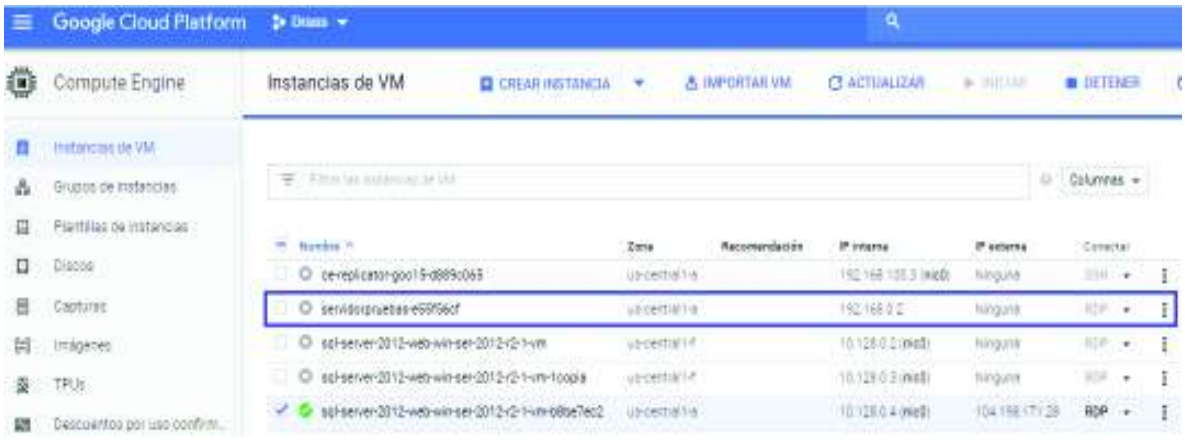

Figura 3.33. ServidorPrueba Recuperado

Finalizado el proceso de recuperación del servidor físico que inicialmente fue replicado y ahora recuperado se concluye que el RTO es decir el tiempo que se demoró en restaurarse el servidor completo en el *Cloud* con toda su información fue de 11 minutos y el RPO es exactamente de 12 horas que tomo en realizar la réplica.

3.3 Análisis de Resultados

3.3.1 Análisis de la Situación Actual

Aunque la situación actual del CEC-EPN ha sido analizada en el **Capítulo I Apartado 1.5.3**, a continuación se presenta las conclusiones de su funcionamiento con el fin de realizar una comparación con las ventajas posteriores al prototipo implementado.

- Actualmente no se cuenta con ningún BCP; es decir cuando se presenta algún problema se desconoce cómo proceder ante el mismo.
- No se cuenta con acciones o tratamientos que se pueda aplicar ante los riesgos y vulnerabilidades con las que se cuenta actualmente.
- No se tiene disponible respaldos completos de las aplicaciones web con las que trabaja la CGT.

- Para restablecer los servicios el RTO como mínimo es de 9 horas ya que se tendría que preparar un servidor, configurar el software necesario, migrar la información y ponerlo en marcha; sin embargo tampoco sería la mejor solución porque no se cuenta con respaldos recientes de los mismos; es decir el RPO también seria alto porque se estaría perdiendo bastante información aproximadamente de 1 mes.

3.3.2 Análisis de la Situación Posterior al Prototipo

Este apartado es el resultado del desarrollo del **Capítulo II,** que incluye la formulación del BCP y la implementación del prototipo DRaaS. A continuación se detallan las ventajas obtenidas en su culminación:

- Se ha culminado la guía del BCP la misma que será entregado al CEC-EPN con la finalidad de disminuir los daños que puede provocar un desastre a la Institución.
- Se identificaron las vulnerabilidades, riesgos y niveles de impacto que pueden afectar a la continuidad del negocio.
- Se han presentado las acciones a ser ejecutadas para disminuir el impacto del negocio, las estrategias de continuidad del negocio y las acciones de tratamiento a los riesgos identificados.
- Mediante un BCP y un DRaaS es posible recuperar los servicios y aplicaciones mejorando los tiempos con los que se ha venido trabajando hasta el momento; es decir mientras se cuente con las réplicas ininterrumpidamente y automáticamente; la recuperación o conocido como el RTO de un servidor físico disminuiría considerablemente.
- Con respecto al RPO la información que será recuperada siempre será la más actual ya que la copia se realiza continuamente.
- Al contar con los servicios de DRaaS en *Google Cloud Platform* las réplicas serían automáticas y en el caso de un desastre el RTO y RPO sería menor como se pudo verificar en las pruebas realizadas.
- Al momento de realizar la réplica simulado un ambiente real mediante una VM con la información del CEC-EPN es decir con las 3 bases de datos, una muestra de

archivos y la aplicación web se pudo confirmar que la réplica es automática y que el tiempo de recuperación de la información es decir el RTO es de 19 minutos.

- En cambio para realizar la réplica de un servidor físico que se encuentra ubicado en el CEC-EPN el tiempo total fue de 12 horas y la recuperación de información es decir el RTO fue de 12 minutos como se indica en las pruebas; este tiempo variará en cada servidor ya que depende de la capacidad de disco y de las aplicaciones que tenga en el mismo.
- Las pruebas de réplica de la instancia de VM y recuperación de la información son exitosas ya que se pudo confirmar que al contar con los servicios de DRaaS en *Googel Cloud Platform* y al realizar la recuperación de la instancia de VM se recupera la VM completa, es decir con todas sus aplicaciones, configuración e información siendo esto un plus que beneficiaría al CEC-EPN al contar con la última tecnología.

3.3.3 Encuesta Realizada a Integrantes de la CGT

Se procede a realizar una encuesta con preguntas cerradas, es decir se establecerán solo 2 alternativas de respuestas (Si/No) y solo en una (Bueno, Regular o Malo); se ha seleccionado este tipo de encuesta ya que es un tema bien definido que admiten estas alternativas como respuesta, son preguntas fáciles de responder y sobre todo de codificar los resultados.

A continuación se presenta la encuesta que fue aplicada al personal de la CGT del CEC-EPN ya que el prototipo implementado es para este departamento; posteriormente se analizan los resultados en base a la guía propuesta del BCP y al prototipo implementado con los servicios DRaaS en *Cloud*.

Encuesta de Satisfacción

1. ¿Tiene conocimientos acerca de Plan de Continuidad del Negocio?

Si_____ No_____.

2. ¿Tiene conocimientos acerca de Plan de Recuperación ante Desastres en Cloud?

Si_____ No_____.

3. ¿Ha interactuado alguna vez con Google Cloud Platform?

Si_____ No_____.

4. ¿Considera la capacitación como un elemento fundamental para el entendimiento de los Servicios de Recuperación ante Desastres en Cloud?

Si_____ No_____.

5. ¿Considera necesario la divulgación de un Plan de Continuidad del Negocio y Recuperación ante desastres en Cloud? dentro de la Institución?

Si_____ No_____.

6. ¿Considera que el Plan de Continuidad del Negocio mejoraría los procesos con los que cuenta la Institución actualmente?

Si_____ No_____.

7. ¿Cree usted que un Plan de Continuidad del Negocio y la puesta en práctica del servicio de Recuperación ante Desastres en Cloud brinde algún beneficio a la Institución?

Si_____ No_____.

8. ¿Se encuentra satisfecho con el resultado obtenido a través de los servicios seleccionados en Google Cloud Platform para la Institución?

Si_____ No_____.

9. ¿Cómo considera la rapidez de los servicios probados?

Bueno_____ Regular_____ Malo_____.

10. ¿En base al resultado obtenido, considera usted que sería una opción viable para que la Institución pueda utilizar esta solución para toda su infraestructura como parte del Plan de Continuidad del Negocio y Recuperación ante Desastres?

Si_____ No_____.

11. ¿Desde su punto de vista cree usted que a través de la implementación de los servicios de Google Cloud Platform se mejorarían los tiempos ante la Recuperación de un Desastre?

Si_____ No_____.

12. ¿Recomendaría el uso de Recuperación ante desastres en Cloud? a otra empresa?

Si_____ No_____.

La encuesta fue aplicada a la CGT, que son 9 personas considerando como la totalidad de la comunidad.

A continuación se muestra el resultado de cada una de las preguntas aplicadas en la encuesta:

Pregunta #1:

Con respecto al conocimiento que poseen acerca de un Plan de Continuidad del Negocio el 88,9% de los encuestados plantean que sí, mientras que el 11,1% plantea lo contrario, este resultado se evidencia en la Figura 3.34.

Figura 3.34. Porcentaje de Conocimiento de Plan de Continuidad de Negocio.

Pregunta #2:

Con respecto a la pregunta #2 relacionada con el conocimiento acerca del Plan de Recuperación ante Desastre *en Cluod* el 67,7% de los encuestados afirman que poseen conocimiento, mientras que un 33,3% lo desconocen, este resultado se muestra en la Figura 3.35.

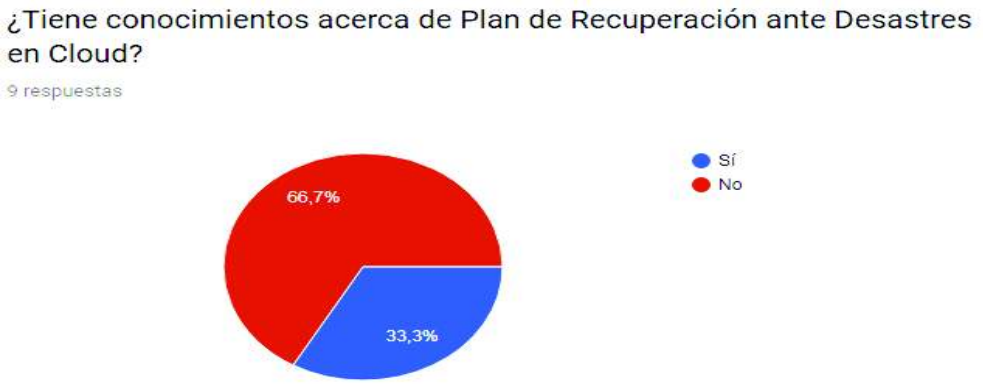

Figura 3.35. Porcentaje de Conocimiento de Plan de Recuperación ante Desastre en *Cloud.*

Pregunta #3:

Con respecto a la pregunta #3 relacionada con la interacción de alguna vez con Google *Cloud Platform* el 44,4% de los encuestados afirman que sí, mientras que un 55,6% plasman lo contrario, este resultado se muestra en la Figura 3.36.

Figura 3.36. Porcentaje de Interacción con *Google Cloud Platform.*

Pregunta #4:

Con respecto a la pregunta #4 relacionada con la consideración de la capacitación como un elemento fundamental para el entendimiento de los Servicios de Recuperación ante Desastres en Cloud el 100% de los encuestados afirman que sí, mostrándose dicho resultado en la Figura 3.37.

Figura 3.37. Porcentaje de necesidad de capacitación sobre Servicios de Recuperación ante Desastre en *Cloud*.

Pregunta #5:

Con respecto a la necesidad de divulgación de un Plan de Continuidad del Negocio y Recuperación ante desastres en Cloud dentro de la Institución el 100% de los encuestados afirman que sí, evidenciándose en la Figura 3.38.

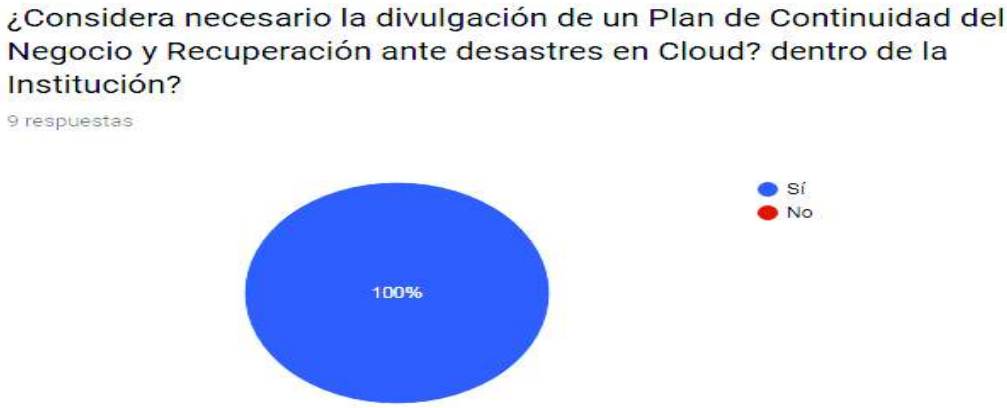

Figura 3.38. Porcentaje de necesidad de divulgación de BCP y Recuperación ante Desastre en Cloud en la Institución.

Pregunta #6:

Con respecto a la consideración de que si el Plan de Continuidad del Negocio mejoraría los procesos con los que cuenta la Institución actualmente, el 100% de los encuestados afirman que sí, evidenciándose en la Figura 3.39.

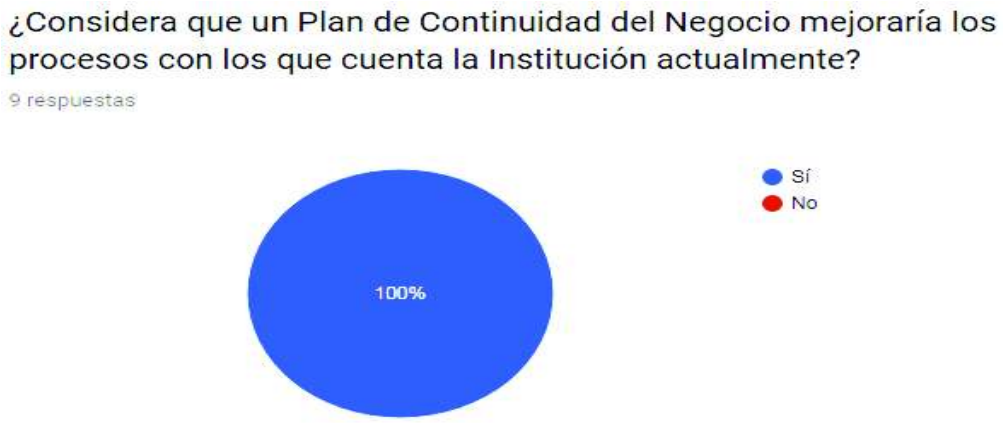

Figura 3.39. Porcentaje de consideración de mejora del BCP en la Institución.

Pregunta #7:

En base a la puesta en práctica del BCP y del servicio de Recuperación ante Desastres en Cloud brinde o no algún beneficio a la Institución, el 100% de los encuestados afirman que sí, evidenciándose en la Figura 3.40.

Figura 3.40. Porcentaje de creencia si BCP y la práctica del servicio de Recuperación ante Desastre en *Cloud* brinda algún beneficio.

Pregunta #8:

Con respecto satisfecho con el resultado obtenido a través de los servicios seleccionados en Google Cloud Platform para la Institución, el 62,5% de los encuestados afirman que sí, mientras que el 37,5% plantea que no, este resultado se muestra en la Figura 3.41.

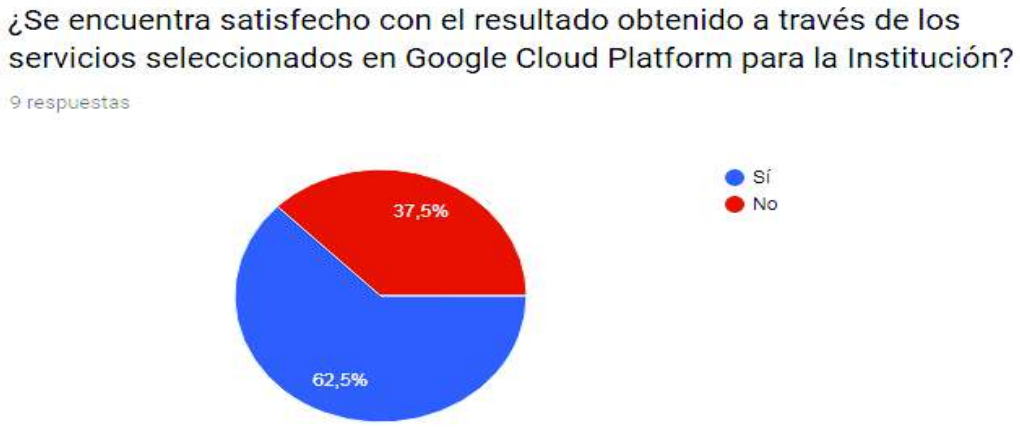

Figura 3.41. Porcentaje de satisfacción del resultado obtenido con los servicios seleccionados de *Google Cloud Platform*.

Pregunta #9:

Con respecto a la consideración la rapidez de los servicios probados, el 88,9% de los encuestados plantea que es bueno, el 11,1% que es regular, mientras que no hay ningún criterio de malo, resultado que se muestra en la Figura 3.42.

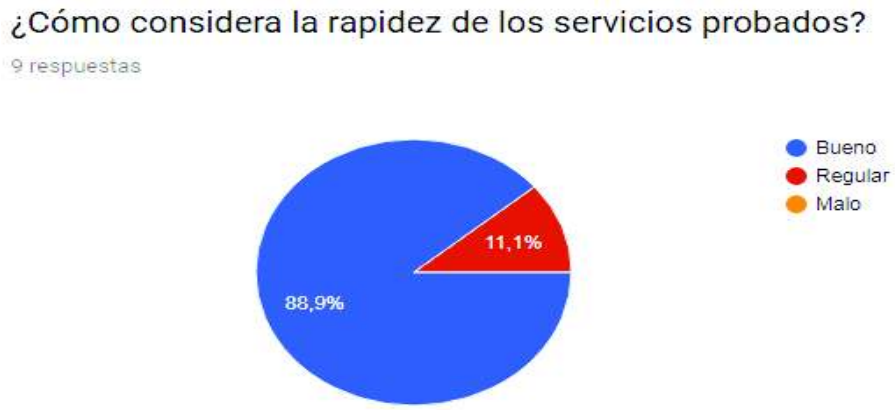

Figura 3.42. Porcentaje de la consideración de la rapidez de los servicios.

Pregunta #10:

En base al resultado obtenido y la consideración de que la opción sería viable para que la Institución pueda utilizar esta solución para toda su infraestructura como parte del Plan de Continuidad del Negocio y Recuperación ante Desastres, el 88,9% plantean que sí, mientras que el 11,1% plantea lo contrario, resultado que se evidencia en la Figura 3.43.

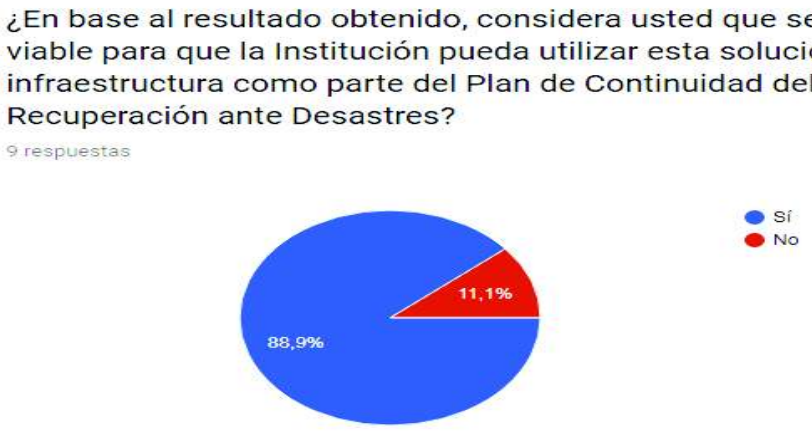

Figura 3.43. Porcentaje de consideración del resultado obtenido es viable para la Institución.

Pregunta #11:

Con respecto a la pregunta #11 relacionada con la implementación de los servicios de Google Cloud Platform puedan o no mejorar los tiempos ante la Recuperación de un Desastre el 88,9% de los encuestados plasman que sí, mientras un 11,1% plantea lo contrario, resultado que se muestra en la Figura 3.44.

Figura 3.44. Porcentaje de mejora de tiempos de Recuperación ante Desastre en Cloud con la implementación de los servicios *Google Cloud Platform.*

Pregunta #12:

Con respecto a la recomendación del uso de Recuperación ante desastres en Cloud a otra empresa, el 100% de los encuestados afirman que sí, evidenciándose en la Figura 3.45.

Figura 3.45. Porcentaje de recomendación del uso de Recuperación ante Desastre en *Cloud*.

4. CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Se realizó el análisis de la situación actual del CEC-EPN con el objetivo de conocer los servicios que brindan, conocer los riesgos y vulnerabilidades actuales; para lo cual se utilizó la metodología investigativa y la metodología exploratoria para definir todo lo relacionado con los requerimientos que posteriormente se implementan.
- Se analizó la Norma ISO/IEC 22301 para construir el BCP y se hizo la selección de *Google* como proveedor DRaaS, seleccionando a su vez los servicios necesarios para darle respuesta a la problemática planteada a través de la migración utilizando las máquinas virtuales, y almacenamiento a través de discos persistentes que se encuentran en la plataforma de *Google*.
- Se desarrolló una Propuesta Metodológica de un plan de continuidad del negocio y recuperación ante desastres en *Cloud* para el CEC-EPN, la cual servirá como guía para mejorar la continuidad del negocio y recuperarse ante cualquier desastre en el menor tiempo posible en el caso de que se presente un incidente.
- Se implementó un prototipo de recuperación ante desastres en *Cloud* para el departamento de la CGT del CEC-EPN mediante una VM consiguiendo que se puedan hacer copias de seguridad automáticamente y que esta pueda ser restaurada en caso de una catástrofe.
- Las pruebas realizadas para comprobar el correcto funcionamiento del prototipo arribaron resultados satisfactorios, ya que se hizo una prueba de manera integral del prototipo, probando la aplicación web del portal, la réplica del servidor y la recuperación de datos.
- La mejora será notablemente al contar el CEC-EPN con un BCP y DRaaS ya que al momento de que se presente un desastre ya contarán con una guía en la que puedan guiarse para proceder con la recuperación de los servicios que se han considerado para el prototipo.
- Finalmente se puede concluir que este Trabajo de Titulación ha cumplido con el alcance, el objetivo general y con los objetivos específicos mencionados en el Plan de Trabajo de Titulación.

4.2 Recomendaciones

- Realizar una capacitación a todos los funcionarios y especialmente al personal de tecnología para explicarles sobre el BCP y el funcionamiento del prototipo.
- Hacer pruebas periódicas en base a la copia y restauración de la información para comprobar el correcto funcionamiento de las máquinas virtuales correspondientes al DRaaS.
- En base a la guía propuesta del BCP el CEC-EPN podrá ampliar el mismo para toda la Institución.
- Si aparecen nuevas problemáticas en el CEC- EPN se debe realizar una revisión del BCP para actualizarlo y agregar nuevas estrategias para dar continuidad al negocio, y que estas sean debatidas entre todos los involucrados.
- Debido a que es solo un prototipo y que tiene un alcance limitado se recomienda verificar la facturación del mismo ya que cuando finalice su versión de prueba o se haya terminado el espacio se podría adquirir la siguiente versión e incluso migrar otras aplicaciones que sean críticas para el CEC-EPN.
- A pesar de que se contaba con la carta de auspicio del CEC-EPN, la fase de implementación del prototipo si se complicó debido a que tanto los servidores como las aplicaciones que se utilizaban para el prototipo están siempre operativas y al momento de realizar la réplica de un ambiente real era necesario bajar los servicios de producción; por esto es que se lo realizó una sola vez en horas de la noche, con autorización y colaboración de la CGT.

5. REFERENCIAS BIBLIOGRÁFICAS

[1] «Registro oficial N. 78,» 1 12 2009. [En línea]. Available: //www.azuay.gob.ec/resoluciones.

[2] P. Rochina, «Continuidad de negocio a través del cloud computing. DRaaS,» 4 10 2016. [En línea]. Available: https: //revistadigital.inesem.es/informatica-y-tics/continuidad-negocio-draas/.

[3] Escuela Nacional Politécnica, «Nuestra Identidad,» 2018. [En línea]. Available: https://www.cec-epn.edu.ec/quienes-somos/nuestra-identidad/.

[4] Diaz Herrera, «VULNERABILIDAD DE LOS SISTEMAS INFORMÁTICOS,» 11 04 2013. [En línea]. Available: http: //vulnerabilidadtisg.blogspot.com/.

[5] C. Montalvo, «Contexto de la organización-CEC,» CEC-EPN, Quito, 2017.

[6] C. Montalvo, «Matriz de vulnerabilidades,» CEC-EPN, Quito, 2017.

[7] A. Villarán, «Planes de Continuidad de negocio,» Bilbao, 2014.

[8] C. Montalvo, «Matriz de Riesgos-CEC,» CEC-EPN, Quito, 2017.

[9] I. Peña López y M. Guillén Solá, «Computación en la Nube,» 2012. [En línea]. Available: http: //ictlogy.net/articles/20120308_ismael_pena-lopez_merce_guillen_sola_-_computacion_en_la_nube.pdf.

[10] M. Moreno, «COMPUTACIÓN EN LA NUBE,» 06 2015. [En línea]. Available: https: //www.econstor.eu/bitstream/10419/130817/1/832556165.pdf.

[11] MyTechlogy, «¿Cuáles son las principales características de la computación en la nube?,» 7 Septiembre 2017. [En línea]. Available: https://www.mytechlogy.com/IT-blogs/18964/what-are-the-main-characteristics-of-cloud-computing/#.WpR4Gehua1s.

[12] Lol Cloud, «Modelos de Servicio Cloud - SaaS, IaaS, PaaS,» 2016. [En línea]. Available: http: //www.licenciasonline.com/ec/es/cloud/modelos-de-servicio.

[13] Evaluando Cloud, «Modelos de servicios de Cloud computing,» 04 08 2015. [En línea]. Available: http: //evaluandocloud.com/modelos-de-servicios-de-cloud-computing/.

[14] A. Villarán, «Planes de Continuidad de negocio,» Bilbao, 2014.

[15] S. COBB, «4 pasos para armar un Plan de Continuidad del Negocio,» 14 05 2014. [En línea]. Available: https: //www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/.

[16] C. GUTIÉRREZ AMAYA, «ISO 22301: 2012 el estándar de la continuidad del negocio,» 4 01 2014. [En línea]. Available: https: //www.welivesecurity.com/la-es/2014/01/06/iso-22301-2012-estandar-continuidad-negocio/.

[17] S. Tangen y A. Dave, «Business continuity - ISO 22301 when things go seriously wrong,» 18 06 2012. [En línea]. Available: https: //www.iso.org/news/2012/06/Ref1602.html.

[18] ESTANDAR INTERNACIONAL ISO22301, «Seguridad de la Sociendad: sistemas de Continuidad de Negocio,» Madrid, 2012.

[19] «ISO 22301 Gestión de la Continuidad de Negocio,» 2017. [En línea]. Available: https: //www.bsigroup.com/es-ES/ISO-22301-continuidad-de-negocio/.

[20] 27001Academy, «Conceptos básicos sobre ISO 22301,» 2017. [En línea]. Available: https: //advisera.com/27001academy/es/que-es-iso-22301/.

[21] S. Bustos Rodríguez, «BENEFICIOS DE IMPLEMENTAR UN DRP (Disaster Recovery Plan) EN LAS ORGANIZACIONES PYMES,» 04 2014. [En línea]. Available: http: //www.grupoalbe.com/beneficios-de-implementar-un-drp-disaster-recovery-plan-en-las-organizaciones-pymes/.

[22] M. Staimer, «Ventajas e inconvenientes de la replicación remota en la recuperación de desastres,» 2015. [En línea]. Available: http: //searchdatacenter.techtarget.com/es/consejo/Ventajas-e-inconvenientes-de-la-replicacion-remota-en-la-recuperacion-de-des.

[23] SW Green House, «Soluciones de Continuidad de Negocios, probadas, estables y sencillas,» 2018. [En línea]. Available: https://www.swgreenhouse.com/conceptos-de-continuidad-de-negocio/rto-rpo.

[24] Grupo Garatu, «DRaaS Gestionado – Recuperación ante desastres,» 2017. [En línea]. Available: https: //garatucloud.com/beneficios-cloud-gestionados-para-empresas/draas-gestionado-disaster-recovery/.

[25] M. Rouse, «¿Qué es Plan de Recuperación de Desastres (DRP)?,» 09 2013. [En línea]. Available: http: //searchdatacenter.techtarget.com/es/definicion/Que-es-Plan-de-Recuperacion-de-Desastres-DRP.

[26] Grupo Garatu, «DRaaS Gestionado – Recuperación ante desastres,» 2017. [En línea]. Available: https: //garatucloud.com/beneficios-cloud-gestionados-para-empresas/draas-gestionado-disaster-recovery/.

[27] Google, «Disaster Recovery Cookbook,» 2017. [En línea]. Available: https: //cloud.google.com/solutions/disaster-recovery-cookbook/.

[28] Microsoft , «Microsoft Azure,» 2017. [En línea]. Available: https://azure.microsoft.com/es-es/solutions/.

[29] Amazon , «Amazon Web Services,» 2017. [En línea]. Available: https://aws.amazon.com/es/.

[30] J. Maldonado «Metodología de la Investigación,» 2015. [En línea]. Available: https://www.gestiopolis.com/la-metodologia-de-la-investigacion/

[31] J. Jimeno Bernal, «Ciclo PDCA,» 08 2013. [En línea]. Available: https://www.pdcahome.com/5202/ciclo-pdca/.

[32] C. Montalvo, «LA NORMA ISO 22301:2012, CONTENIDO DE LA NORMA EN EL CICLO P-D-C-A,» Quito, 2017.

[33] Hurricane Electric;, «Hurricane Electric Internet Services,» 2018. [En línea]. Available: https://dns.he.net/.

[34] «Recuperación de desastres y continuidad del Negocio en pequeñas empresas,» 9

08 2016. [En línea]. Available: http: //normaiso22301.com/recuperacion-de-desastres-y-continuidad-del-negocio-en-pequenas-empresas/..

[35] J. L. Colom Planas, «Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión,» 25 11 2012. [En línea]. Available: http: //www.aspectosprofesionales.info/2012/11.

[36] F. Prieto Bustamante y M. Arias Flórez, «Cloud Computing como ventaja competitiva en las organizaciones,» 2 07 2014. [En línea]. Available: http: //www.laccei.org/LACCEI2014-Guayaquil/RefereedPapers/RP231.pdf.

[37] M. Zamora Barzallo, «Desarrollo de un marco metodológico orientado a la gestión de continuidad del negocio utilizando el modelo de referencia Cobit 5.0, relacionado al procesamineto y administración de los datos en la nube caso de estudio: Metropolitano de Diseño,» 2016. [En línea]. Available: http: //dspace.udla.edu.ec/handle/33000/5318.

[38] D. Mannella Lemos, «Diseño de una guía para la implementación del uso de computación en la nube como mecanismo de recuperación ante desastres tecnológicos en pymes en el DMQ,» 12 11 2012. [En línea]. Available: https: //repositorio.espe.edu.ec/ha.

[39] J. Colom, «Aspectos profesionales: Protección de Datos, Cloud Computing y Sistemas de Gestión,» [En línea]. Available: http: //www.aspectosprofesionales.info/2012/11/.

[40] Google, «10 Características de Google Drive,» 2017. [En línea]. Available: https://www.caracteristicas.co/google-drive/.

[41] C. Montalvo, «Plan de Contingencias-CEC,» CEC-ENP, Quito, 2017.

6. ANEXOS

Anexo I: Norma ISO/IEC 22301.

Anexo II: Contrato del servicio de Internet adquirido por la DGIP.

Anexo IIII: Renovación del Dominio “cec-epn.edu.ec” adquirido con Nic.ec.

Anexo IV: BCP para el CEC-EPN.

Anexo I

Norma ISO/IEC 22301

Anexo II

Contrato del servicio de Internet adquirido por la DGIP

Anexo III

Renovación del Dominio “cec-epn.edu.ec” adquirido con Nic.ec

Anexo IV

BCP para el CEC-EPN