ESCUELA DE INGENIERÍA EN SISTEMAS

Tema:

PLAN DE CONTINUIDAD DE NEGOCIOS PARA LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR - AMBATO

Proyecto de investigación y desarrollo previo a la obtención del título de Ingeniero de sistemas y computación

Línea de Investigación:

Sistemas de información y/o nuevas tecnologías de la información y comunicación y sus aplicaciones

Autor:

César Andrés Granizo Medina

Director:

Ing. Galo Mauricio López Sevilla, Mg.

Ambato - Ecuador

Octubre 2019

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE AMBATO

ESCUELA DE INGENIERÍA EN SISTEMAS

HOJA DE APROBACIÓN

Tema:

Plan de Continuidad de Negocios para la Pontificia Universidad Católica del Ecuador - Ambato

Línea de investigación:

Autor: CÉSAR ANDRES GRANIZO MEDINA

Galo Mauricio Lopez Sevilla, Ing. Mg. f.

CALIFICADOR

Enrique Xavier Garcés Freire, Ing. Mg. f.

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f.

CALIFICADOR

Mónica Patricia Mena Moreno, Ing. Mg. f.

DIRECTORA ESCUELA DE INGENIERÍA EN SISTEMAS

Hugo Rogelio Altamirano Villaroel. Dr. f.

SECRETARIO GENERAL PUCESA

Ambato Ecuador

Octubre - 2019

Declaración de Originalidad y Responsabilidad

Yo, CÉSAR ANDRÉS GRANIZO MEDINA, portador de la cedula de ciudadanía No. 0503470528, declaro que los resultados obtenidos en el proyecto de titulación y presentados en el informe final, previo a la obtención del título de Ingeniero en Sistemas, son absolutamente originales y personales. En tal virtud, declaro que el contenido, las conclusiones y los efectos legales y académicos que se desprenden del trabajo propuesto, y luego de la redacción de este documento, son y serán de mi sola y exclusiva responsabilidad legal y académica.

Dedicatoria

El presente trabajo va dedicado al pilar fundamental en mi vida que es mi familia, sin el apoyo de ellos no sería posible el ningún logro profesional, ellos me han acompañado en los momentos duros en la vida.

A mi hermana Gaby quien ha sido apoyo fundamental durante los últimos semestres universitarios.

No puede faltar el ejemplo y apoyo de mis abuelitos, que gracias al esfuerzo y sacrificios de ellos han sido mi guía y ejemplo que seguir.

Reconocimientos

La realización de este proyecto de investigación fue posible, en primer lugar, a la cooperación brindada por el Departamento de Tecnología de la Información de la Pontificia Universidad Católica del Ecuador – Ambato, al Ing. Gabriel Altamirano por su ayuda constante y por su continuo estimulo durante todo el proceso hasta el final de este.

Se agradece además a la Escuela de Ingeniería en Sistemas y a sus docentes por su dirección y ayuda constante, en especial al Ing. Galo López por su orientación metodológica y su dirección durante la elaboración del siguiente proyecto de investigación.

Resumen

El presente trabajo de investigación tiene como objetivo desarrollar un plan de continuidad de negocio para la Pontificia Universidad Católica del Ecuador – Ambato. A través de diferentes técnicas de investigación cuantitativa, mediante entrevistas y encuestas; para lograr identificar los problemas representativos que la institución presenta al no contar con un plan de contingencia ante desastres. El presente estudio se ha desarrollado debido a la importancia del manejo estratégico de la información y la recuperación ante desastres como servicio (DRaaS), basada en tecnología de recuperación en la nube, que permite albergar una copia de los servicios que provee el departamento de tecnología de la información a la comunidad universitaria en un sitio alterno en caso de desastre del centro de datos o indisponibilidad de los servicios.

En capítulo I, se detalla el estado del arte, donde se definen conceptos generales sobre el desarrollo del presente proyecto de investigación.

En el capítulo II, se identifican las fases de la metodología que propone ITIL para el diseño de plan de continuidad del negocio la cual consta de 4 fases: iniciación, requerimientos y estrategia, implementación y gestión operacional.

En el capítulo III se desarrolla las fases anteriormente mencionadas, además de identificar los servicios críticos que tiene el departamento de tecnología de la información, y poder elaborar una correcta respuesta ante desastres mediante la estrategia de continuidad.

Palabras Clave: plan de contingencia, ITIL, DRaaS.

Abstract

The objective of this research project is to develop a business continuity plan for the Pontifical Catholic University of Ecuador - Ambato. Different techniques of quantitative research, such as interviews and surveys, were used to identify the representative problems that the institution experiences from not having a disaster contingency plan. This study has been developed because of the importance of strategically managing information using disaster recovery as a service (DRaaS) with cloud recovery technology and making it possible to store a copy of the services provided by the Information Technology Department to the university community on an alternate site in case of a disaster in the data center or the unavailability of services. The first chapter describes the state of art and includes the definitions of the general concepts used in the development of this research project. The second chapter identifies the phases of the methodology proposed by ITIL for the design of the business continuity plan, which consists of 4 phases - initiation, requirements and strategy, implementation, and operational management. The third chapter develops the phases in addition to identifying the critical services that the Information Technology Department has and being able to develop a proper disaster response through the continuity strategy.

Keywords: contingency plan, ITIL, DRaaS.

INDICE

Índice de Gráficos

Índice de Cuadros

INTRODUCCIÓN

El plan de continuidad de negocios, tiene como principal objetivo proteger los servicios críticos del negocio, contra desastres, naturales, humanos o tecnológicos y evaluar las posibles secuelas que pueden generarse como perdida de continuidad de los servicios, para ello es importante que la Pontificia Universidad Católica del Ecuador - Ambato la cual maneja información sensible, registro de notas, nómina de estudiantes, matrículas, graduación, repositorio digital , servidores de dominio cuente con un plan de continuidad de negocios para evitar interrupciones en los procesos transaccionales como consecuencia de fallas o catástrofes puesto que actualmente la institución no cuenta con un plan de respuesta y recuperación de servicios el cual permitirá a la Universidad recuperarse de manera óptima ante un evento adverso que ponga en riesgo la continuidad de los servicios.

El presente proyecto de investigación tendrá como objetivo el desarrollo de un plan de continuidad de negocios mediante el paradigma Disaster *Recovery as a Service (DRass)* el cual permitirá a la institución afectada por un desastre natural o antrópico, con la pérdida total de información, que retome sus servicios mediante una asistencia de Cloud *Computing;* y, para esto se apoya en la metodología ITIL la cual permitirá diseñar el plan de continuidad de negocios.

Preguntas científicas:

1. ¿Cómo se fundamenta teórica y metodológicamente un Plan de Continuidad del Negocio?

2. ¿Cómo se identifican las aplicaciones y servicios necesarios que respondan a las necesidades de la institución en caso de existir algún desastre y pérdida total de información ?

4. ¿Cómo se diseñará una propuesta de Recuperación de desastres como servicio, adaptada a las necesidades de Tecnologías de la información de la institución que incorpore las aplicaciones vitales para el funcionamiento de la universidad?

Objetivo General

Desarrollar un Plan de Continuidad de negocios para la Pontificia Universidad Católica del Ecuador – Ambato.

Objetivos Específicos

- Fundamentar teórica y metodológicamente un plan de continuidad de negocios.
- Identificar los servicios que respondan a las necesidades de la institución en caso de existir algún desastre y pérdida total de información.
- Diseñar una propuesta de Recuperación de desastres como servicio, adaptada a las necesidades de Tecnologías de la información de la institución que incorpore las aplicaciones vitales para el funcionamiento de la universidad.

Metodología

Para el desarrollo de la presente investigación se aplicó el método analítico sintético el cual según Ramon Ruiz (2007), se encarga de analizar los elementos constituyentes. Se dice que va de lo abstracto a lo concreto significa que los elementos aislados se reúnen y se obtiene un todo concreto real.

La metodología de desarrollo que se empleara para el proyecto es ITIL, para el desarrollo de planes de continuidad de negocios, es una guía para desarrollar el plan en donde se realizan diferentes fases para la búsqueda de información y así tener una idea clara de lo que se pretende lograr con el proyecto.

Justificación

En la actualidad, la función interrumpida de las aplicaciones informáticas o las pérdidas de datos, causan graves problemas económicos según Mercuriana (2016), las empresas no pueden dejar de entregar sus servicios en ningún momento, ya sea por un periodo de tiempo por la criticidad de sus operaciones

Barahona (2016) afirma que los servicios del *cloud computing* pueden ser de gran ayuda para las empresas porque generan confianza al realizar respaldo de aplicaciones y datos, pero, más allá de ello, pueden ser muy valiosos para apoyar los planes de recuperación ante desastres.

Actualmente la PUCE – Ambato, requiere de una solución tecnológica acorde a las tendencias actuales que le permita estar preparada para responder de forma efectiva, ante cualquier interrupción del servicio o pérdida de la información, se considera la criticidad de la administración de esta y así se busca disminuir la posibilidad de ocurrencia de un incidente de gran impacto para la organización.

Por lo tanto, se eligió este tema de tesis porque el plan de continuidad de negocios el cual utiliza el paradigma DRaas (*Disaster recovery as a service*) se convierte rápidamente, en una excelente alternativa para soportar las necesidades de las organizaciones, como alternativa de solución para la continuidad de negocio.

Como se observa en el grafico 1.1 el DRaas (*Disaster recovery as a service*) permite realizar una copia de seguridad basado en una replicación del sitio dentro de un almacenamiento que proporciona el proveedor del servicio *DRaaS*, y permite restaurar las aplicaciones en un tiempo menor a 24 horas.

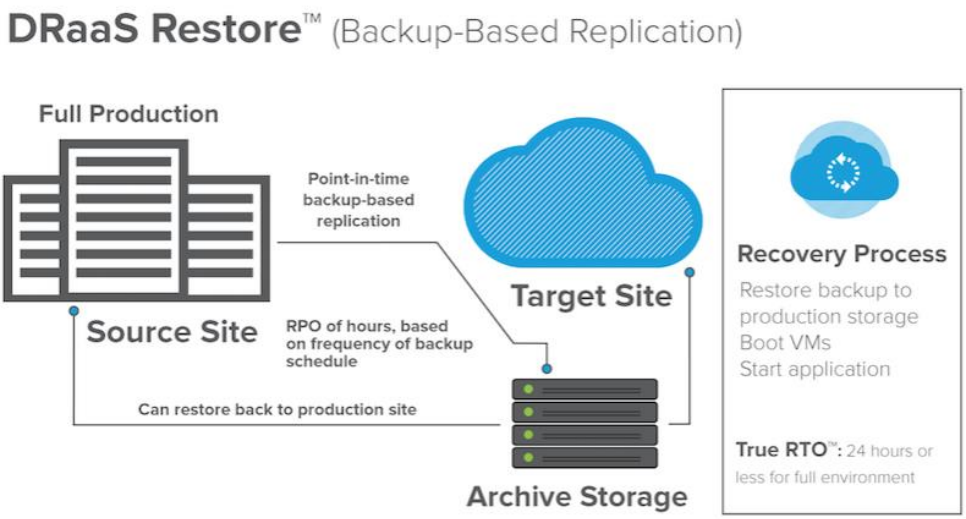


Gráfico: DRasS Restore en funcionamiento

Fuente: Veeam. (2016)

CAPITULO I: ESTADO DEL ARTE Y LA PRÁCTICA

1.1 Seguridad informática

Con respecto a la información que se tiene de lo que es una vulnerabilidad se interpreta los siguientes tres conceptos:

Cuadro 1.1: Definición de seguridad Informática

Referencias:	**Conceptos:**
Pinto, M. G. H., & Sánchez, B. A. N. (2016).	Seguridad Informática son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados
Lara, L. (2006).	La Seguridad de la Información sirve para abrir puertas, no para cerrarlas, evidentemente, la idea es abrir la puerta sólo a quién se le tiene que abrir.
Rodríguez Carrillo, A. M. (2014).	En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema que permite a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.

Fuente: elaboración propia

La integridad de la información asegura que los datos almacenados y aquellos que se intercambian de un punto a otro no han sido modificados de ninguna manera. La disponibilidad significa que la información puede obtenerse por parte de aquellos que están autorizados y la necesitan. Para lograr que la información susceptible esté disponible para su uso o modificación se utilizan mecanismos de autenticación y autorización. La autenticación se encarga de probar que cada usuario es quien dice ser.

1.2 Amenazas

Con respecto a la información que se tiene de lo que es una amenaza, se interpreta los siguientes tres conceptos:

Cuadro 1.2: Definición de Amenazas

Referencias	Conceptos
Gaona Vásquez, K. D. R. (2013)	Se define como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.
Tarazona, T., & Cesar, H. (2007).	Una amenaza en términos simples es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades el cual afecta directamente la información o los sistemas que la procesan.
Albarracín Lazo, C. A. (2011).	Posible peligro del sistema. Pueden provenir de personas (hackers, crackers), de programas, de sucesos naturales. Equivalen a los factores que se aprovechan de las debilidades del sistema.

Fuente: elaboración propia

Las amenazas informáticas se definen como una posible situación u evento en la cual una vulnerabilidad sea aprovechada con el fin de afectar la información, dichos eventos o situaciones pueden provenir de personas o de eventos naturales.

1.3 Análisis de Riesgo

Con respecto a la información que se tiene de lo que es un análisis de riesgo, se interpreta los siguientes tres conceptos:

Cuadro 1.3*:* Definición de Análisis de Riesgo

Referencias.	**Concepto**
Francischetti, C. E., Bertassi, A. L., Camargo, L. S. G., Padoveze, C. L., & Calil, J. F. (2014).	El análisis de riesgos es la herramienta a través de la cual se obtiene una visión clara y priorizada de los riesgos a los que se enfrenta una entidad: tiene como propósito identificar los principales riesgos a los que una entidad está expuesta, ya sean desastres naturales, fallos en infraestructura o riesgos introducidos por el propio personal.
Torres, Cesar. (2017)	El análisis de riesgo (también conocido como evaluación de riesgo o PHA por sus siglas en inglés: Process Hazards Analysis) es el estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir.
De Leon, J. G. M. P. (2007)	El Análisis de Riesgos significa examinar la magnitud y la índole de los posibles efectos negativos de la introducción propuesta, así como la 125 probabilidad de que éstos se produzcan. Deberá identificar medios eficaces para reducir los riesgos y contemplar alternativas a la introducción propuesta.

Fuente: elaboración propia

El análisis de riesgo se define como la identificación de las posibles amenazas que puede tener una organización y así determinar cuáles serán los impactos de estos riesgos y las medidas de reducción que se implementa en una propuesta de reducción de riesgos.

1.4 Desastres informáticos

Con respecto a la información que se tiene de lo que es un desastre informático, se interpreta los siguientes tres conceptos:

Cuadro 1.4: Definición de Desastre

Referencias.	**Concepto**
Santán, L., & Delti, R. (2010).	Se define un desastre como un evento no planificado que inhabilita el centro de datos de la organización, a prestar los servicios necesarios para seguir su trabajo de forma normal. Condiciones que podrían ser declaradas desastres incluyen eventos de la naturaleza como huracanes, inundaciones, terremotos, incendios y otros. O eventos causados por el hombre como sabotaje, fraude, terrorismo y ataques maliciosos, entre otros, que al final causen daños a la infraestructura de cómputo.
Celsia. (2014).	Desastre o contingencia es la interrupción de la capacidad de acceso a información y procesamiento de esta a través de computadoras necesarias para la operación normal de un negocio. Tiene su origen en las fuerzas de la naturaleza y no solo afectan a la información contenida en los sistemas, sino también representan una amenaza a la integridad de todo el sistema (infraestructura, instalación, componentes, equipos).
Huidobro, J. (2007).	Interrupción de la capacidad de acceso a información y procesamiento de esta a través de computadoras necesarias para la operación normal de un negocio.

Fuente: elaboración propia

Un desastre informático se define como la interrupción total o parcial de la información y la incapacidad de procesamiento de datos durante un determinado lapso el cual afecta a la infraestructura y/o equipos de una organización la perdida de continuidad del negocio.

1.5 Desastres antrópicos

Con respecto a la información que se tiene de lo que son los desastres antrópicos, se interpreta los siguientes tres conceptos:

Cuadro 1.5*:* Definición de Desastres Antrópicos

Referencias.	**Concepto**
Narváez Morocho, N. E. (2012).	Se trata de las amenazas directamente atribuibles a la acción humana sobre los elementos de la naturaleza (aire, agua y tierra) y sobre la población, que ponen en grave peligro la integridad física y la calidad de vida de las comunidades.
Morales-Soto, N., & Alfaro-Basso, D. (2008).	Es la peligrosidad, a nivel catastrófico, que las acciones del hombre pueden alcanzar, tal como ocurre en las guerras o los daños por desastres tecnológicos en el transporte o la industria. Las luchas por la conquista del territorio o la subyugación del adversario conllevan hechos de violencia que ocasionan víctimas y destrucción.
Andres Coles. (2017)	Se tratan aquellas amenazas cuyo origen se refiere a las acciones que la humanidad impulsa para, aprovechar la transformación de la naturaleza ya sea por contaminación y/o a procesos tecnológicos.

Fuente: elaboración propia

Un desastre antrópico de puede definir, como aquellas amenazas producidas por el ser humano ya sea sobre la naturaleza o sobre una población en específico, se pone en riesgo la integridad de esta, el cual ocasiona problemas en el transporte, campo tecnológico o la industria.

1.6 Sabotaje informático.

Con respecto a la información que se tiene de lo que es un sabotaje informático, se interpreta los siguientes tres conceptos:

Cuadro 1.6: Definición de Sabotaje informático

Referencias.	**Concepto**
	El término sabotaje informático comprende todas aquellas conductas dirigidas a eliminar o modificar funciones o datos en una computadora

Contreras Clunes, A. (2003).	sin autorización, para obstaculizar su correcto funcionamiento, es decir, causar daños en el hardware o en el software de un sistema. Los métodos utilizados para causar destrozos en los sistemas informáticos son de índole muy variada.
Acurio Del Pino, S. (2016).	El sabotaje informático doctrinariamente, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.
Chaves, M. A. (2006)	El fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas.

Fuente: elaboración propia

Un sabotaje informático se define como una acción en la cual se modifica, se elimina la información sin autorización con el fin de suspender, destruir e inutilizar cualquier sistema informático, software y hardware con el fin de causar daño e interrumpir el funcionamiento normal de un determinado sistema.

1.7 Tipos de planes Asociados.

1.7.1 Planes de Respuesta.

Con respecto a la información que se tiene de lo que son los planes de respuesta, se interpreta los siguientes tres conceptos:

Cuadro 1.7*:* Definición de Planes de Respuesta

Referencias.	**Concepto**
	Los planes de respuesta a incidentes ayudan a evaluar la naturaleza del caso, identificar posibles implicaciones del caso si éste aumenta (o disminuye) en gravedad, establece líneas de comunicación con respecto al caso, ayuda a montar y poner en marcha el o los equipo(s) de

Paul Kirvan. (2013)	respuesta capacitado(s) para manejar el evento y fungir como un punto de decisión para el lanzamiento de los planes de recuperación de desastres, planes de continuidad de negocio, planes de evacuación, planes de emergencia contra incendios y otras actividades de respuesta a emergencias.
Bautista, M. (2014).	La planificación de la respuesta a desastres implica determinar, aumentar y organizar recursos y capacidades a fin de alcanzar un grado de preparación que permita responder oportuna y eficazmente a un desastre potencial.
Martínez, M. (2013).	El Plan de Respuesta es el documento escrito que recoge el conjunto de medidas de prevención y protección previstas e implantadas, así como la secuencia de actuaciones a realizar ante la aparición de un siniestro.

Fuente: elaboración propia

Un plan de respuesta se define como aquel permite recoger información sobre los posibles incidentes que puedan afectar a una determinada empresa, organización en el cual se realiza una planificación de cómo se responde a esta adversidad ya sea con planes de continuidad de negocio, planes de emergencia, planes de recuperación ante desastres.

1.7.2 Planes de contingencia

Con respecto a la información que se tiene de lo que es un plan de contingencia, se interpreta los siguientes tres conceptos:

Cuadro 1.8: Definición de Planes de Contingencia

Referencias.	**Concepto**
Shirly Marcela Ardila. (2016).	Es una estrategia que se compone de una serie de procedimientos que facilitan una solución alternativa que permite restituir rápidamente el funcionamiento de los servicios críticos de la

	Fundación ante la eventualidad que lo afecte de forma parcial o total.
Ladines Garcés, K. S. (2017).	Son procedimientos que definen como una entidad continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
Ramírez Ponce, J. A. (2014).	Un plan de contingencia es una salida del proceso de planeación de contingencias en donde se definen los procedimientos, recursos y sistemas necesarios para mantener o reestablecer las operaciones empresariales luego de una interrupción del negocio resultado de fallos de sistema o desastres. Además, proporciona información clave para la recuperación del sistema como procedimientos de recuperación, funciones y responsabilidades, procedimientos de evaluación, etc.

Fuente: elaboración propia.

Un plan de contingencia se define como un proceso que proporciona diferentes procedimientos para poder permitir la recuperación rápida y eficaz de un Sistema de Tecnologías de la Información, después de que se produzca una falla en el mismo, una interrupción que puede ser causada por desastres naturales o antrópicos que involucren la paralización de los servicios.

1.7.3 Planes de emergencia

Con respecto a la información que se tiene de lo que es un plan de emergencia, se interpreta los siguientes tres conceptos:

Cuadro 1.9: Definición de Planes de Emergencia

Referencias.	**Concepto**
Linaza, L. M. A. (2005).	Un plan de emergencia tiene el fin de establecer procedimientos que guíen a las personas a saber cómo actuar en caso de riesgo.
	Elaborar un plan de emergencia enmarca en la identificación del peligro y evaluación de riesgo en las diferentes áreas de instalación en la cual

Pazmiño Linzán, M. A. (2017).	permite determinar medidas de prevención y control en los sitios que se origine el riesgo.
Soto, N. E. M. (2013).	Un plan de emergencia es una estrategia de preparación que contribuirán a la reducción de impactos en el desarrollo, en términos de vidas humanas y pérdidas económicas por interrupción de las actividades productivas o de los servicios.

Fuente: elaboración propia

Un plan de emergencia se define como una serie de procesos y/o estrategias que permitan a las personas, empresas a identificar los riesgos y vulnerabilidades dentro de una empresa, y saber minimizar e implementar acciones para la reducción de estos para así tener acciones y tiempos previstos ante una emergencia.

1.7.4 Plan de Continuidad del Negocio

Con respecto la información que se tiene de lo que es un sabotaje plan de continuidad del negocio.

Cuadro 1.10: Definición de Plan de continuidad de negocio

Referencias.	**Concepto**
Mora Yomayuza David Felipe. (2016).	El plan de continuidad del negocio o BCP como también se le conoce como sus siglas (*Bussines Continuity Plan*), constituye básicamente un plan de emergencia con el objetivo de mantener la funcionalidad de la organización a un nivel mínimo durante una contingencia, además el BCP debe centrarse en las medidas preventivas y de recuperación el cual influye en una contingencia que afecte al negocio.
Gaspar, J., & Martínez, J. G. (2004).	El plan de continuidad de negocios busca amortiguar en lo posible el riesgo mediante un plan global, se obtiene la pronta recuperación de la operación y de la información, en caso de presentarse algún tipo de evento que afecte el

	flujo normal de las actividades de una organización.
Martínez, J. G. (2010).	El plan de continuidad de negocios está orientado a asegurar la continuidad del negocio, la satisfacción del cliente y la productividad a pesar de eventos inesperados. Se ejecuta permanentemente como parte de la administración de riesgos. Un plan de continuidad debe contener procedimientos que se ajusten a la realidad del negocio de cada institución.

Fuente: elaboración propia

Un plan de continuidad de negocio se define como la capacidad que tienen las organizaciones de planificar acciones preventivas y circunstanciales al momento de un siniestro, para así garantizar que la organización puede continuar con sus operaciones de manera aceptable, en base a la identificación de riesgos reales y potenciales que podrían interrumpir de manera breve o definida, las actividades regulares de una empresa debido a afectaciones causadas por entes naturales, humanos o tecnológicos.

Gráfico 1.1: Plan de Continuidad de negocios

Fuente: Miguel Ángel Mendoza. (2014)

1.8 Computación en la nube (*cloud computing)*

Es un tipo de computación donde las capacidades de la tecnología de la información son entregadas mediante el internet, esto se refiere al conjunto de programas y servicios alojados dentro de un servidor en red accesibles desde cualquier equipo con conexión a internet Gartner. (2016).

Según Peter Mell & Tomohy Grance (2011), la computación en la nube es un modelo para habilitar a un conjunto compartido de recursos configurables, por ejemplo: redes, aplicaciones y servicios los cuales tienen una alta disponibilidad los cuales pueden ser liberados y aprovisionados con un esfuerzo mínimo y baja interacción con el proveedor de servicios.

Los servicios *Cloud* son considerados como un componente esencial para el éxito y avance de las empresas pues, al facilitar el acceso de los usuarios a las aplicaciones, servicios, y almacenamiento de información, convierte a los servicios en la nube en un aliado del negocio, asume como característica esencial el aumentar la eficiencia de las operaciones.

1.9 Tipos de Servicios

1.9.1 Plataforma como servicio (PaaS)

Este modelo, el proveedor del servicio entrega al cliente una solución en la que se le permite albergar sus aplicaciones el cual utiliza el sistema operativo provisto por el proveedor de acuerdo a las necesidades del cliente, en este modelo el proveedor del servicio ofrece el uso de una plataforma tecnológica el cual el usuario tiene el control sobre las aplicaciones mas no sobre la plataforma, el usuario no sobredimensiona inicialmente las capacidades de almacenamiento frente a necesidades futuras, si no que expande el tamaño de su almacenamiento contratado según las necesidades existentes. (Devicro, 2016)

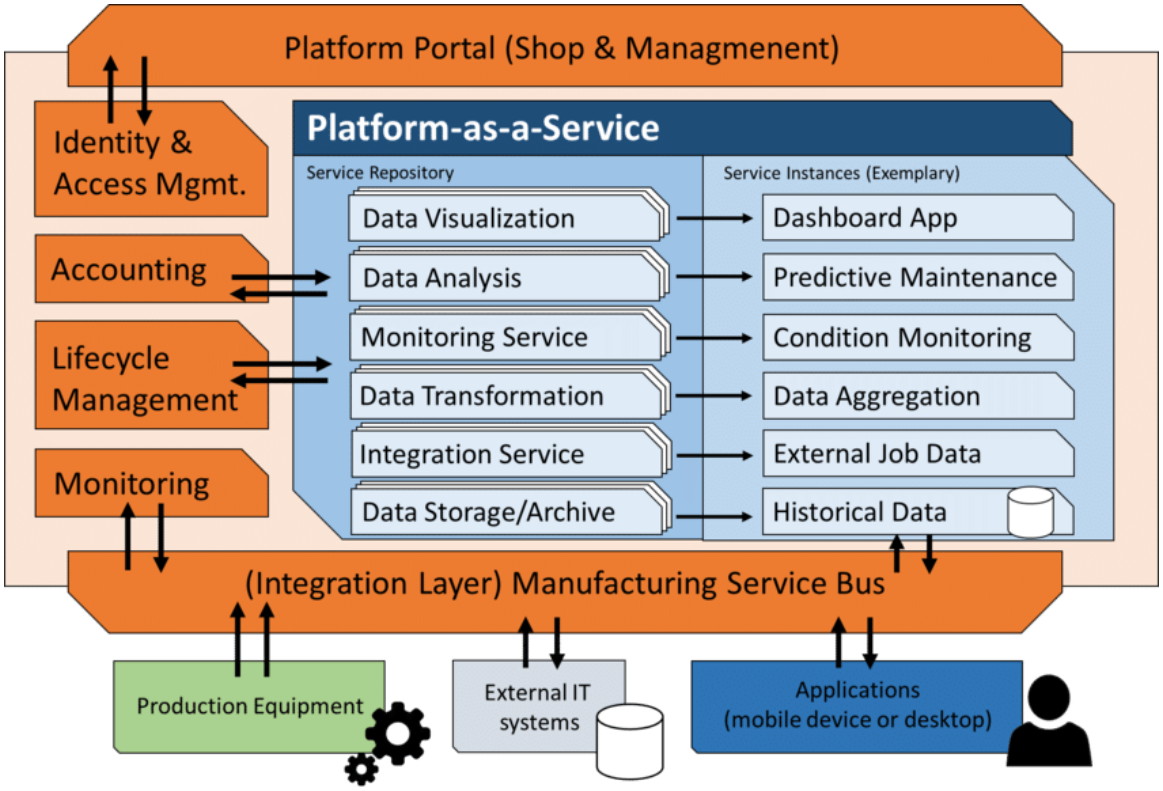


Gráfico 1.2: Plataforma de arquitectura de PaaS

Fuente: Dennis Bauer IT Manufacturing. (2018)

1.9.2 Infraestructura como servicio (IaaS)

En el presente modelo, el cliente renta la infraestructura como servicio, en el cual los clientes no usan sus propios equipos físicos, si no que usan equipos virtualizados los cuales son proporcionados por el proveedor del servicio *Cloud* , en este caso el cliente no gestiona la infraestructura (*routers*, *switch*, servidores, etc), pero si es responsable de la instalación mantenimiento y ejecución de sus propias aplicaciones, el costo de la infraestructura depende de los recursos compartidos (Interoute, 2016).

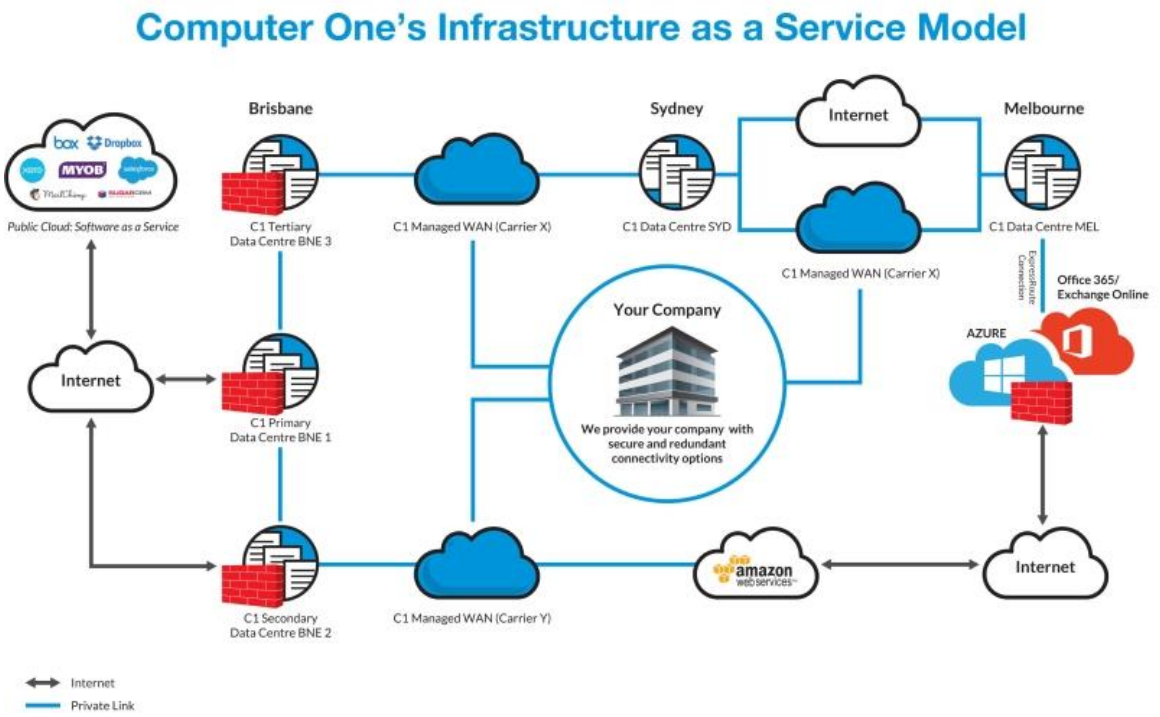


Gráfico 1.3: Plataforma de arquitectura de IaaS

Fuente: *Computer One*. (2018)

1.9.3 Software como servicio (SaaS)

En el modelo SaaS, el cliente tiene acceso de manera remota, desde cualquier lugar, mediante conexión a internet a diferentes aplicativos entregados por el proveedor del servicio, el proveedor es el encargado de mantener la operatividad, realizar el mantenimiento y actualizaciones de acuerdo con las necesidades del cliente, en este modelo los usuarios generalmente se suscriben por periodos mensuales.

Las aplicaciones y servicios funcionan en los servidores de los proveedores del servicio, uno de los ejemplos más claros es *Dropbox* en el cual se entrega un almacenamiento respectivo a los clientes los cuales ingresan mediante conexión remota a sus cuentas para poder guardar o descargar archivos desde cualquier equipo con acceso a internet. Gartner (2012).

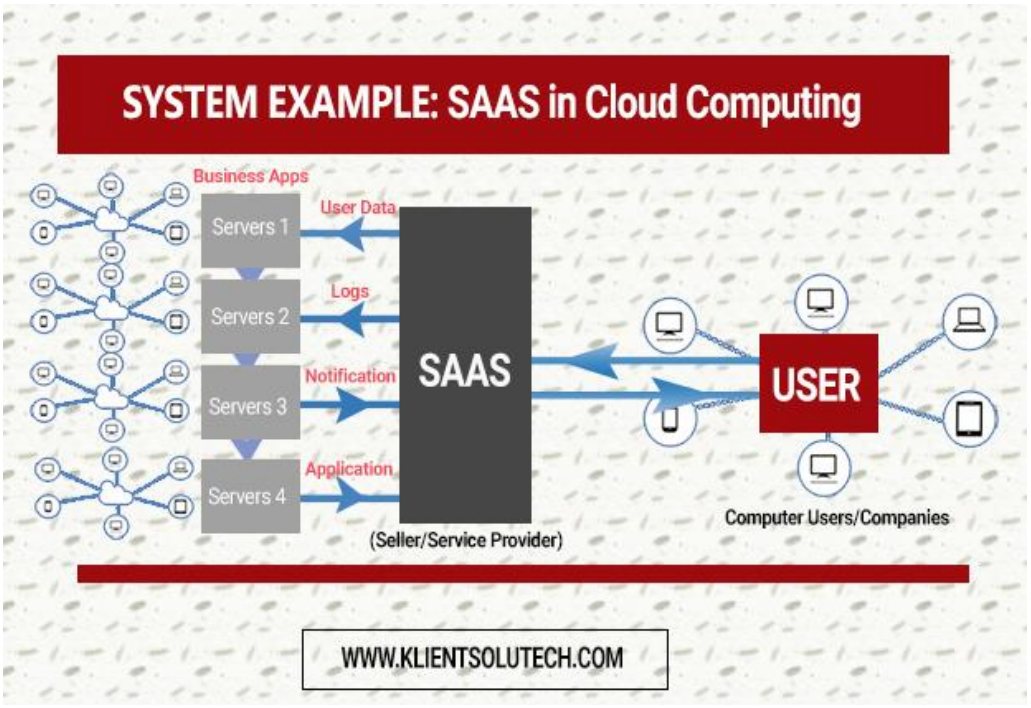


Gráfico 1.4: Plataforma de arquitectura de SaaS

Fuente: Klient Solutech. (2018)

1.9.4 Backend como servicio (BaaS)

La arquitectura BaaS es una de las más recientes arquitecturas *Cloud* que han repuntado en los últimos años, la cual consiste en omitir por completo del concepto de servidores y aplicaciones, pues BaaS ofrece una nueva forma de crear todo el *BackEnd* de nuestras aplicaciones basadas en *Cloud Functions* (funciones en la nube) las cuales son por lo general funciones programadas y que luego BaaS las expone como servicios, de tal forma que en lugar de tener una aplicación con cientos de objetos y procedimientos, tenemos una serie de *Cloud functions*, las cuales viven exclusivamente en la nube.

Lo que nos ofrece este modelo es todo un conjunto de utilerías ya implementadas en la nube, en la cual solo se desarrolla las funciones de negocio o servicios que necesitaran las aplicaciones para funcionar, de tal forma que, en lugar de desplegar aplicaciones, se desplieguen funciones que posteriormente será expuestas como servicios para ser consumidas por la red Oscar Blancarte (2018).

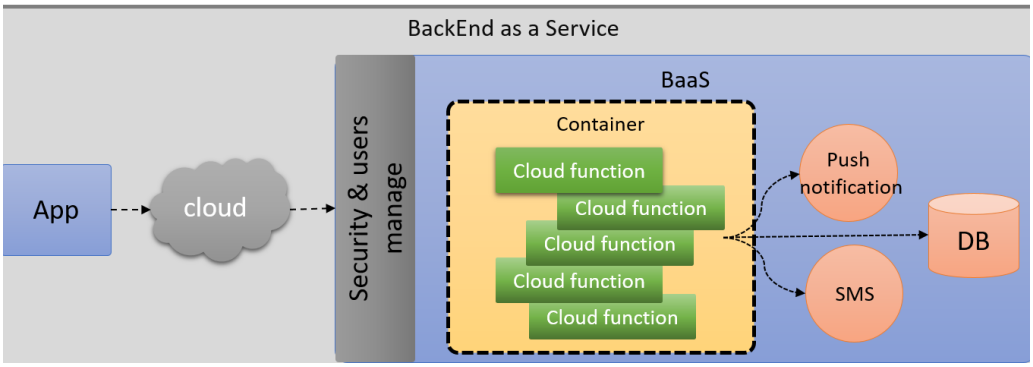


Gráfico 1.5: Plataforma de arquitectura de BaaS

Fuente: Oscar Blancarte. (2018)

1.9.5 Recuperación de desastres como servicio (DRaaS)

La recuperación de desastres como servicio DRaaS (Recuperación de desastres como servicio), se basa en la replicación, mediante el alojamiento de datos de una organización, en servidores físicos o virtuales pertenecientes a un tercero.

Es un elemento de seguridad TI (Tecnología de la información) y su objetivo primordial consiste en garantizar la continuidad de las operaciones de la empresa contratante del servicio, después de la interrupción de los procesos del negocio ocasionada por desastres naturales o por el hombre.

El servicio de recuperación de desastres no es una copia de seguridad que tiene la empresa, es una réplica del servidor corporativo, en la cual se incluyen aplicaciones, bases de datos e información.

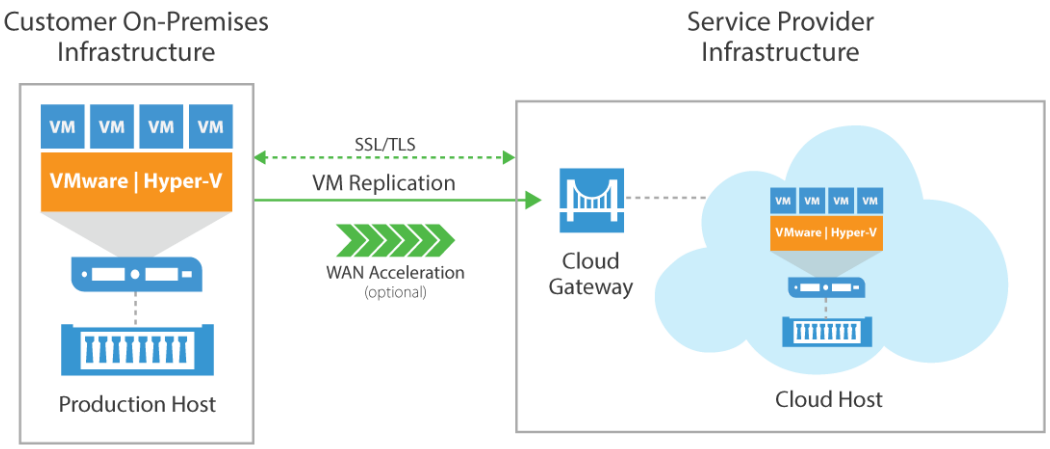


Gráfico 1.6: Plataforma de arquitectura de DRaaS

Fuente: Mercuriana. (2011)

Ante la ocurrencia de un evento adverso, la empresa se pone en contacto con la organización contratada y se establecen los niveles críticos y las prioridades de los servicios contratados, de esta manera se da inicio al plan que asegura la continuidad del negocio. Apser (2018).

CAPITULO II: DISEÑO METODOLÓGICO

2.1. Metodología de Investigación

Según Kerlinger (1993), la investigación científica es una investigación crítica, controlada y empírica de fenómenos naturales, guiada por la teoría y la hipótesis acerca de las supuestas relaciones entre dichos fenómenos.

"La investigación puede ser definida como una serie de métodos para resolver problemas cuyas soluciones necesitan ser obtenidas a través de una serie de operaciones lógicas, se toma en cuenta como punto de partida datos objetivos."(Arias G. (1974)).

La metodología de la investigación permitirá determinar y analizar los datos obtenidos de manera sistemáticamente sigue un conjunto de pasos, cuyos resultados se abarcarán a lo largo del desarrollo del presente proyecto.

2.1.1. Método General

Para el desarrollo de la presente investigación se ha considerado aplicar el método analítico sintético el cual según Ramon Ruiz (2007), argumenta que se encarga de analizar los elementos constituyentes. Se dice que va de lo abstracto a lo concreto significa que los elementos aislados se reúnen y se obtiene un todo concreto real.

El uso de este método permite la búsqueda de soluciones para un determinado problema, otorga una mejor recolección de datos para el presente desarrollo investigativo.

2.1.3 Técnicas e instrumentos de recolección de datos

Según Bavaresco (2006), la investigación no tiene significado sin las técnicas de recolección de datos, estas técnicas conducen a la verificación del problema planteado. Cada tipo de investigación determina las técnicas a utilizar y cada técnica establece sus herramientas, o instrumentos o medios que serán empleados. Los instrumentos que se construyeron llevaron a la obtención de los datos de la realidad y una vez recogidos podrán pasarse a la siguiente fase del procesamiento de los resultados obtenidos como información.

El presente proyecto se apoyará con dos técnicas que son:

- Entrevistas
- Observación
- Encuestas

2.1.4 Entrevista

Bravo, García, & Varela (2013) argumentan que la entrevista se define como una conversación con un determinado objetivo. Es un instrumento técnico de gran utilidad en la investigación cualitativa, para recabar datos. Para determinar los requerimientos y características que obtendrá el plan de continuidad de negocio se planteó una serie de preguntas a la gerencia del departamento de Tecnologías de la Información de la Pontificia Universidad Ambato y al departamento financiero. (ver Anexo 1 y Anexo 2)

2.1.5 Encuestas

Según Naresh K. Malhotra (2004), las encuestas son entrevistas con un determinado número de, personas con la aplicación un cuestionario estructurado que se da a los encuestados y que está diseñado para obtener información específica. Para determinar las preferencias y los posibles problemas dentro de la organización y así poder aplicar de mejor manera el plan de continuidad de negocio se desarrolló una encuesta dirigida al departamento de Tecnologías de la Información de la Pontificia Universidad Ambato. (Ver anexo 3)

2.1.6 Población

Para la realización del estudio se determinó como población al departamento de tecnologías de la Información, el cual se detalla a continuación:

Cuadro 2.1: Personal del Departamento de Tecnología de la Información

N°	Estructura del Departamento de Tecnologías de la Información	Número de Personas
1	Director del Departamento de Tecnología de la Información	1
2	Técnico multimedia del Departamento de Tecnología de la Información	1
3	Especialista en Aplicaciones y Desarrollo del Departamento de Tecnología de la Información	1
4	Técnico en Desarrollo del Departamento de Tecnología de la Información	2
5	Especialista de Comunicación e infraestructura del Departamento de Tecnología de la Información	1
6	Técnico en Infraestructura del Departamento de Tecnología de la Información	2

Fuente: elaboración propia.

Se consideró que para el departamento de tecnologías de la información se realizara una o varias encuestas, entrevistas y observaciones al Centro de Datos y los equipos además de la información que se procesa diariamente, como semestralmente para poder determinar los servicios dentro del funcionamiento transaccional de la universidad.

Cabe resaltar que la población elegida a participar en el presente proyecto es reducida, por lo cual los datos obtenidos representan el 100% y no se necesitaran una muestra de estos.

2.2 Metodología de Desarrollo

Para el desarrollo del presente proyecto se aplicó las mejores prácticas ITIL para un plan de continuidad del negocio, para Deavila Ferrero Fernando (2013), menciona que dentro del desarrollo de un plan de Continuidad del Negocio “La metodología de ITIL desarrolla una estrategia completa que permite la continuidad del negocio”.

El objetivo principal de la gestión de la continuidad es asegurar la prolongación de los sistemas de TI, ante cualquier eventualidad la metodología de ITIL desarrolla una estrategia completa que permite la continuidad del negocio, ofrece un planteamiento de continuidad de negocio el cual aporta de manera directa al desarrollo del BCP, desde realizar el análisis de impacto en el negocio, hasta implantar el entorno de contingencia.

Las etapas que propine ITIL para la gestión de continuidad son las que se muestran a continuación.

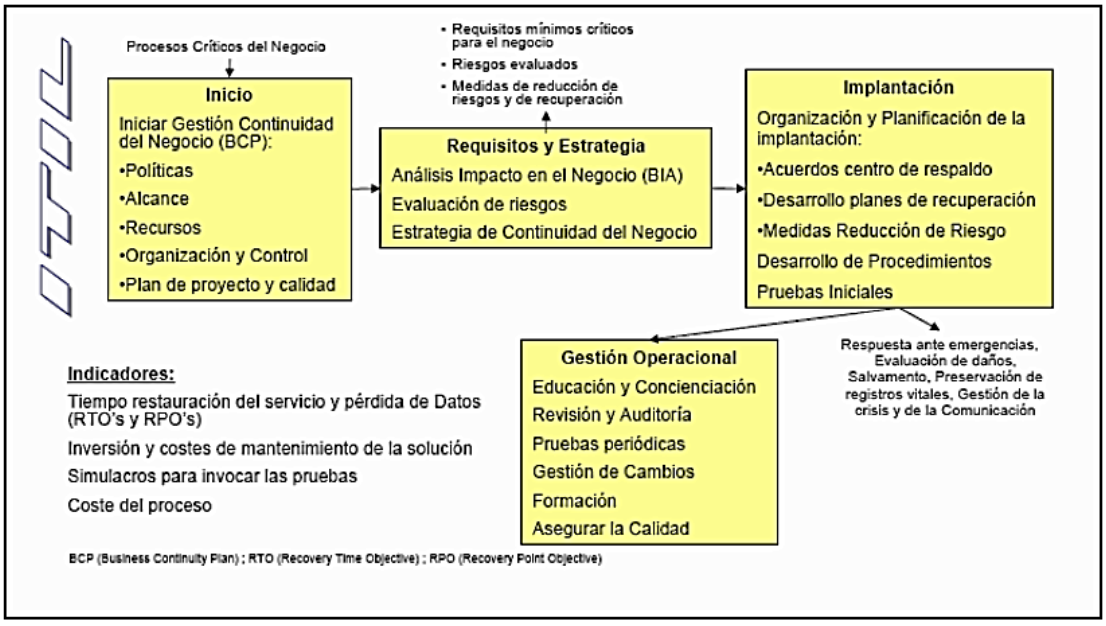


Gráfico 2.1: Esquema del Plan de continuidad del negocio propuesto por ITIL

Fuente: (Business Continuity Planning Methology, 2004)

Sin embargo, de acuerdo con las necesidades de la empresa, el esquema anteriormente mencionado se lo adapto de la siguiente manera con el fin de que sea aplicable al Departamento de Tecnologías de la información de la PUCE – A para su práctica implementación y mantenimiento, a continuación, se fundamenta el análisis de los aspectos a considerarse dentro de la metodología planteada.

2.2.1 Fase 1

2.2.1.1 Etapa de iniciación

Esta etapa comprenderá de 2 aspectos, donde:

El alcance: es necesario pues se definen temas a tomar en cuenta en el plan de continuidad.

Recursos: donde se asignan los recursos financieros, tecnológicos y humanos para así lograr el diseño del plan de continuidad del negocio para la PUCE – A

Organización y control: no son necesarias, puesto que los roles y responsabilidad están bien definidos dentro del departamento de tecnología de la información

Las políticas: no son necesarios los acuerdos entre la compañía y las personas que diseñan el plan, en este caso se trabaja directamente con la gerencia del departamento de tecnología de la información de la PUCE – A.

de la PUCE – A

Plan de proyecto y calidad: no es necesario pues los roles, recursos y están detallados en los puntos anteriormente mencionados además de que se complementa con el Impacto en el negocio el cual abarcará en su totalidad un plan de proyecto y calidad.

2.2.2 Fase 2: Requisitos y Estrategia

En esta etapa se ha desglosado el análisis impacto en el negocio (BIA) debido a que al tratarse de un plan de continuidad el cual utiliza servicios en la nube es necesario definir objetivos y alcances, además de la identificación y priorización de

servicios la cual permitirán tener una mejor evaluación de riesgos mediante la estimación del impacto financiero y operacional.

La estrategia de continuidad del negocio que plantea inicialmente ITIL como se muestra en el gráfico 2.1 se ha decido pasarlo a la fase 3 debido a que en esta sección se definirá la estrategia de recuperación.

2.2.2.1 Realizar un análisis del impacto en el Negocio (AIM o BIA)

Según Gaspar Martínez (2004) un análisis de impacto de negocio es una metodología diseñada para realizar una evaluación de las funciones del negocio y flujo de trabajo de una organización para desarrollar una comprensión de los servicios, además de los objetivos de tiempo de recuperación y de las necesidades de recursos, además de estimar el impacto financiero y operacional de una interrupción y el marco de tiempo de recuperación necesario para los servicios del negocio.

2.2.2.2 Objetivos y alcance del análisis del impacto en el negocio.

Aquí se definirán los objetivos que tendrá el presente plan de continuidad de negocios, además de delimitar el enfoque final y para quien va dirigido en su totalidad.

2.2.2.3 Identificación y priorización de servicios.

Esta etapa consiste en identificar los servicios críticos de la Pontificia Universidad Católica del Ecuador- Ambato (PUCE-A), además de priorizarlos en base al impacto operacional identificado.

2.2.2.4 Evaluar impacto financiero y operacional.

En esta etapa se evaluará el impacto financiero y operacional en caso de existir un desastre. La parte financiera del plan de continuidad del negocio será evaluada de manera cualitativa, debido a que las cifras reales son confidenciales.

2.2.2.5 Tiempo Objetivo de Recuperación:

RTO:

Recovery Time Objetive

Según *The Business Continuity Institute*, el tiempo objetivo de recuperación es el período en el cual los procesos críticos y/o sus dependencias deben ser recuperados en una organización.

RPO:

Recovery Point Operations

El RPO es el punto en el cual la información debe ser habilitada para activar una actividad en el proceso.

2.2.2.6 Evaluación de riesgos.

En esta etapa se realizará un análisis de riesgos que pueden afectar a la PUCE – A, para la identificación de amenazas y consecuencias, para así poder establecer un levantamiento de servicios oportuno.

2.2.3 Fase 3: Organización y planificación de la implementación

Como se mencionó anteriormente en la fase 2, en esta etapa se realizará la estrategia de recuperación la cual abarca los puntos 3 puntos (acuerdos de centro de respaldo, desarrollo de planes de recuperación, desarrollo de procedimientos) que plantea inicialmente ITIL debido a que al tratarse de un plan de recuperación en la nube es necesario detallar proveedores de servicio DRaaS y sus requisitos para la contratación, no se tomara en cuenta las medidas reducción de riesgo debido a que en el presente proyecto de investigación no se tomara en cuenta la infraestructura al momento de existir algún desastre.

2.2.3.1 Seleccionar la estrategia de recuperación: Forma y Modalidad

Según la norma ISO 22301 La determinación y selección de la estrategia se basarán en los resultados del análisis de impacto en el negocio y evaluación de riesgos.

La empresa debe determinar una estrategia de continuidad de negocio apropiado.

2.2.3.2 Requisitos del plan.

En esta etapa se detallarán aspectos pertinentes al Departamento de tecnología de la información de la PUCE – A para determinar los requerimientos necesarios para el correcto funcionamiento del Plan de continuidad del negocio.

2.2.3.4 Análisis de los proveedores de *DRaaS*.

Para el siguiente análisis se utilizará como referencia el cuadrante mágico de Gartner, para la recuperación ante desastres actualizado julio 2018 donde se detallan los principales proveedores de este servicio.

2.2.3.5 Requisitos para la contratación de proveedores.

Los requisitos para la contratación son definidos definidos por las políticas del departamento de tecnología de la información de la PUCE – Ambato en los cuales se definen los servicios previamente identificados, sus características, y los tiempos de restauración.

2.2.3.6 Comparativa entre proveedores.

En esta etapa se realiza la comparativa entre proveedores, en base a los parámetros de evaluación para así poder elegir un proveedor de servicio adecuado.

2.2.3.7 Evaluación general.

La evaluación general permitirá tomar una decisión en base a las comparativas realizadas a los proveedores, se toma en cuenta sus propuestas e información obtenida.

2.2.4 Fase 4: Gestión operacional.

En esta etapa los puntos inicialmente propuestos por ITIL (educación, concientización, revisión, auditoria, pruebas periódicas, gestión de cambios, formación y aseguramiento de la calidad), son agrupados dentro del desarrollo del plan de continuidad del negocio, debido a que al tratarse de un procedimiento de recuperación en la nube los puntos anteriormente mencionados se consideran de manera más general.

2.2.4.1 Equipo de la continuidad del negocio.

Según Ramon Serrano Bejar, resulta vital para todas las organizaciones implementar un Plan de Continuidad de Negocios para amortiguar y minimizar los efectos de la contingencia críticos, operativos y financieros, se reduce el tiempo en la recuperación de la información, el cual restaura los procesos operacionales clave de sus recursos y servicios de TI, ocasionadas por fallas, desastres naturales, siniestros, e incluso epidemias.

En esta etapa se realiza la asignación de personal al plan de continuidad de negocio los cuales permitirán una mejor gestión luego del desastre, dentro de la fase 4 se realizarán las siguientes actividades:

- Asignación de roles.
- Asignación del personal al plan de continuidad de negocios.
- Actividades para la ejecución del plan de continuidad del negocio.
- Escenario del plan de continuidad.

Una vez aclarado los aspectos el esquema planteado es el siguiente:

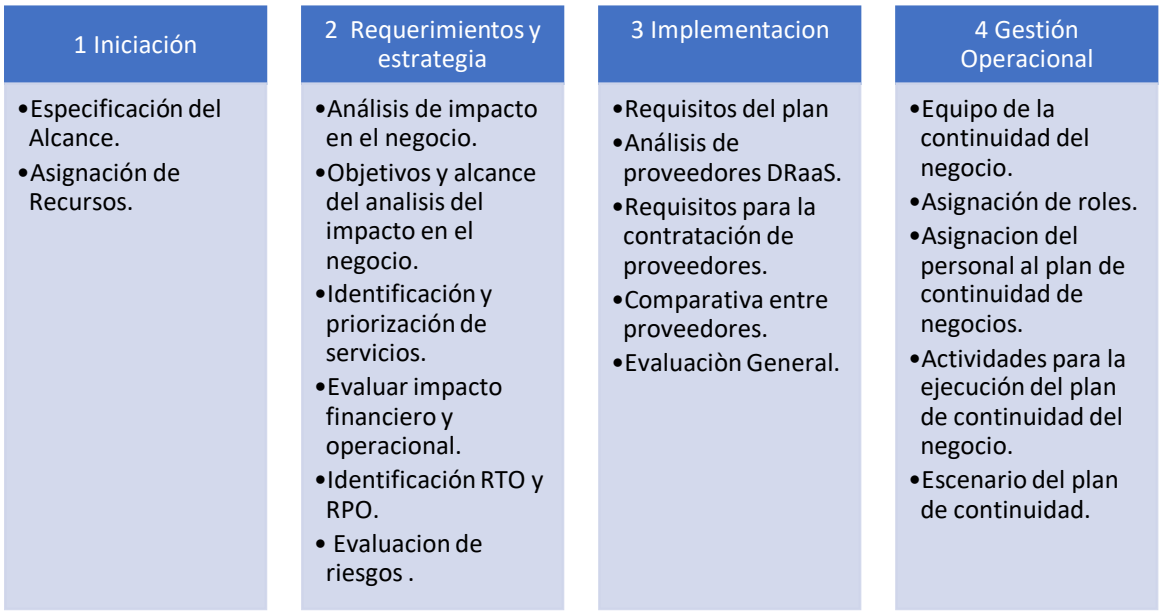


Gráfico 1.2: Esquema adaptado del Plan de continuidad del negocio propuesto por ITIL

Fuente: elaboración propia

CAPÍTULO III: Resultados

En el presente capítulo se presenta los resultados de las fases, los cuales fueron acoplados de la información obtenida del departamento de tecnologías de la información de la Pontificia Universidad Católica del Ecuador, detallados según la metodología anteriormente mencionada.

3.1 Fase 1

3.1.1 Especificación del Alcance

El plan de comunidad del negocio para la PUCE – A pretende establecer los lineamientos generales que se sigue para continuar en operación a pesar de que la interrupción ocasionado por algún tipo de desastre, se cubre el ciclo de vida del plan de continuidad del negocio que propone ITIL con sus cuatro etapas, se toma en cuenta los servicios críticos del Departamento de tecnología de la información de la PUCE – A.

3.1.2 Asignación de Recursos

La asignación de recursos permite identificar los recursos disponibles en el Departamento de tecnología de la información de la PUCE – A los cuales permiten dimensionamiento y alcance el plan de continuidad del negocio, así como la definición de una política adecuada para la ejecución de este.

Los recursos con los que cuenta el Departamento de tecnología de la información de la PUCE – A son:

Recursos financieros: Existe un presupuesto anual que se asigna al departamento de tecnología de la información de la PUCE- A.

Recursos humanos: Al momento existen 8 personas en el departamento de TI, quienes se encargan de la gestión del departamento, así como de la correcta administración de los servicios que se proporcionan a la comunidad universitaria.

Recursos tecnológicos: Una de las ventajas que tiene el departamento de tecnología de la información de la PUCE- A es que puede disponer de todos los recursos que requiera, así como su mantenimiento y soporte, cabe mencionar que hay un fácil acceso para la gestión de los recursos susceptibles a beneficiarse del plan de continuidad.

3.2 Fase 2

3.2.1 Realizar un análisis del impacto en el Negocio

El análisis del impacto en el negocio tiene como objeto analizar los impactos que la organización puede enfrentarse a la discontinuidad de sus operaciones, determinar los requerimientos necesarios una vez ocurrido el desastre.

Para determinar el verdadero impacto del negocio se ha considerado las respuestas obtenidas en las encuestas y entrevista realizadas al Departamento de Tecnología de la Información (TI), Departamento Financiero, el formato de estas se encuentra en el Anexo 1, Anexo 2, Anexo 3 respectivamente, debido a que al ser un número reducido de personas encuestadas y entrevistadas se realizó las siguientes conclusiones en base a sus respuestas.

Las conclusiones fueron las siguientes:

- Existe comunicación directa con las diferentes áreas académicas, dirección administrativa, recursos humanos y sistema financiero, esta comunicación se la da por correo electrónico institucional, llamadas telefónicas, tickets y de manera presencial.
- La cantidad de gigabytes de información que se almacena por semestre es de 1024 gigabytes, proviene de las diferentes Unidades Académicas, el mayor porcentaje de información proviene de los registros de notas y cargas horarias de los docentes.
- El tiempo estimado de atención a la resolución de incidencias dentro de las diferentes Unidades Académicas, Dirección Administrativa, Recursos Humanos y Sistema Financiero, depende del tipo de requerimiento, prioridad y la importancia del usuario, las personas encargadas de la categorización de incidencias son la gerencia del departamento de tecnología de la información y el especialista en infraestructura.
- Toda información que proviene de las distintas Unidades Académicas, Dirección Administrativa, Recursos Humanos y Sistema Financiero es crítica en todas sus instancias y todas sus unidades.
- Actualmente el Departamento de Tecnologías de la Información no cuenta con un plan de continuidad de negocios por lo cual es necesaria su implementación puesto que permitirá a la institución recuperarse ante un desastre total de perdida de información, la recuperación de los servicios de manera rápida y oportuna, se toma en cuenta aspectos importantes como son la criticidad de los servicios, la alta disponibilidad que el plan debe atender y la velocidad de reacción ante una catástrofe.
- Para el presente proyecto de investigación no existe impacto económico una vez transcurrido un desastre tecnológico en la institución, pues los procesos de matriculación, el cual es el único proceso que provee un ingreso económico a la universidad se encuentra ya disponible en una plataforma virtual en la nube, existiría un impacto económico si se considerara la infraestructura y los procesos que tomaría adquirir nuevos servidores físicos que fueron afectados por algún tipo de desastre.

- Las funciones críticas que realiza el personal del departamento de tecnologías de la información las cuales se verían afectadas por una interrupción en su continuidad son aquellas que involucran el manejo de base de datos, de igual manera el control de los distintos servicios que se ofrecen a la comunidad universitaria: internet, registro y verificación de notas, procesos de matriculación, etc.
- El personal del Departamento de Tecnología de la Información maneja diferentes tipos de procedimientos ya sea con el reemplazo la infraestructura y realizar respaldos de la base de datos como, por ejemplo: discos duros de los servidores que se vean afectados por fallas, realizar respaldos de la información de los servidores y aplicaciones que se desarrollen.
- El mayor periodo de tramitación de información es en matriculas, cierre de periodos académicos, pase de notas, evaluación docente, procesos en los cuales se involucren la participación de la comunidad universitaria, se mantiene protocolos de emergencia en caso de pérdida de conectividad de internet mediante un enlace alterno a otro proveedor y políticas de respaldo de información RTO y RPO.

3.2.2 Objetivos y Alcance del análisis del impacto en el Negocio

Objetivos

- Identificar el impacto de una interrupción en el negocio
- Usar los resultados del análisis del impacto en el negocio para estimaciones del BCP

3.2.2.1 Alcance

El análisis del impacto en el negocio que se desarrolla, se enfoca exclusivamente para el Departamento de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador- Ambato. Se realizó el análisis de impacto en el negocio que provoca un desastre y las medidas que se tomaran para poder recuperar los servicios tales como:

- Repositorio Digital Institucional.
- Servidores de Nombre de Dominio.
- Academics.
- Catálogo en línea.
- Laboratorios.
- Impresión web.
- Registro biométrico.
- Eduroam.
- *Spiceworks*.
- Sincronización de credenciales (correo electrónico, dominio, moodle).
- Consultorio jurídico.

3.2.3 Identificar Servicios

Esta etapa consiste en la identificación de los servicios críticos de la Pontificia Universidad Católica del Ecuador- Ambato (PUCE-A) donde:

Servicios: Son los servicios tecnológicos que la institución brinda a la comunidad.

Departamento: Unidades pertenecientes a la Pontificia Universidad Católica del Ecuador.

Los departamentos que intervienen dentro del Plan de Continuidad del Negocio son:

- Tecnología de la Información.

Se ha considerado este departamento debido a que los servicios mencionados son administrados por el Departamento de Tecnología de la Información, excluye los demás departamentos que pertenecen a la PUCE- A como, por ejemplo: Departamento de investigación, Dirección Administrativa, etc.

Los servicios anteriormente mencionados en el alcance se incluyen dentro del Plan de Continuidad del Negocio, pues estos se encuentran en funcionamiento dentro de un servicio de almacenamiento virtual dentro de la universidad, el cual no cuenta con un plan de continuidad.

Los servicios que se excluyen son:

- Moodle.
- Saci (Sistema Administrativo para la Facturación Digital).
- SquarNet (Gestión digital de nómina).

Los servicios anteriormente mencionados se excluyen dentro del Plan de Continuidad del Negocio, pues se encuentran en funcionamiento dentro de un servicio de almacenamiento en la nube alterno a la universidad.

Los departamentos que intervienen en el Plan de Continuidad del Negocio son:

- Tecnologías de la Información.

Cuadro 3.1: Servicios críticos de la Pontificia Universidad Católica del Ecuador- Ambato

Departamento: Tecnología de la Información PUCE - A

Servicio	**Definición**
Repositorio digital Institucional	El repositorio digital institucional es aquel en la cual se almacenan recursos digitales tales como: • Tesis de Pregrado • Tesis de Postgrado • Ponencias de congresos • Investigación de la Sede • Publicaciones de la Sede. Estos recursos digitales están disponibles para la comunidad universitaria, y personas fuera a la misma.
Servidores de Nombres de Dominio	El servidor de dominio es aquel que permite la administración de los usuarios, en este caso la administración y privilegios de los docentes dentro de la red. • Acceso a los equipos personales.

Academics	Servicios integrados a través de un portal web, en el cual el estudiante y el docente tienen acceso a: • Seguimiento de Syllabus. • Tutorías. • Notas Parciales y Finales del estudiante. • Aprobación de hojas de aranceles. • Proceso de Matriculación. • Evaluación Docente.
Catalogo en línea	El servicio en el cual la comunidad universitaria tiene acceso al repositorio de libros disponibles de manera digital.
Laboratorios	El Servicio en el cual la comunidad universitaria puede realizar una reserva para el uso de los laboratorios.
Impresión web	Servicio de impresión el cual se provee a los docentes.
Eduroam	Servicio de red inalámbrica el cual permite el acceso a internet de personas ajenas a la institución mediante sus credenciales. Este servicio solo está disponible para instituciones que sean miembros de cedia.
Spiceworks	Este servicio permite a los docentes, administrativos realizar solicitudes de soporte y mantenimiento tanto en software como en hardware.
Registro biométrico	Servicio el cual permite el control de ingreso y salida de personal.
Servicio de sincronización de credenciales	Servicio el cual permite a los usuarios cambiar su contraseña en el electrónico correo institucional del correo y este automáticamente se actualiza con el dominio y el Moodle.
Consultorio jurídico	Servicio disponible para la escuela de jurisprudencia en el cual se realiza el ingreso de casos.

Fuente: elaboración propia

3.2.4 Evaluar el Impacto Financiero y Operacional

En esta etapa se evalúa el impacto financiero y operacional en caso de existir un desastre. La parte financiera del plan de continuidad del negocio será evaluada de manera cuantitativa, adicional no se podrá poner cifras reales puesto que son confidenciales.

3.2.4.1 Evaluación del Impacto Financiero

Para poder realizar una correcta evaluación del impacto financiero se realiza la siguiente interrogante:

¿Cuál sería la magnitud del impacto de la perdida financiera en caso de pérdida total de servicios ocasionado por un desastre?

El impacto financiero se evalúa en el momento más crítico de cada servicio, en este caso los valores se especifican de manera cualitativa dado por el grado de confidencialidad, a continuación, se detallan los valores utilizados en pérdidas se definen los siguientes rangos:

Estos datos fueron tomados en base a la información otorgada por ITIL para el Plan de continuidad del Negocio.

Cuadro 3.2: Rangos del impacto financiero / rangos otorgados por ITIL para el Plan de continuidad del Negocio.

Impactos	**Días**
Impacto 0: no hay perdidas	0 días
Impacto 1: bajo	1 – 10 días
Impacto 2: medio	5 – 20 días
Impacto 3: alto	Mas de 20 días

Fuente: elaboración Propia

Cuadro 3.3: Valores de Impacto financiero

Departamento	Servicio	Impacto financiero
Tecnología de la Información	Repositorio digital Institucional	0
Tecnología de la Información	Servidores de Nombres de Dominio	0
Tecnología de la Información	Academics	0
Tecnología de la Información	Catalogo en línea	0
Tecnología de la Información	Laboratorios	0
Tecnología de la Información	Impresión web	0
Tecnología de la Información	Eduroam	0
Tecnología de la Información	Spiceworks	0
Tecnología de la Información	Registro biométrico	0
Tecnología de la Información	Servicio de sincronización	0
Tecnología de la Información	Consultorio jurídico	0

Fuente: elaboración propia

Los servicios anteriormente mencionados reciben un valor de 0 dentro del impacto financiero, dada la información obtenida en la entrevista realizada al Departamento financiero en el cual se informó que no existe pérdida económica de ningún tipo por discontinuidad de servicios tecnológicos puesto que dichos servicios no generan ningún tipo de ingreso en efectivo además de encontrarse fuera de la institución como es el caso de SAP y Banner, el impacto que se produce es a nivel operacional el cual se detalla en el siguiente punto del análisis del impacto en el negocio.

3.2.4.2 Evaluación del Impacto Operacional

El impacto operacional se da por la variación de los factores tales como: suficiencia del servicio prestado, imagen que proyecta la institución, dinero circulante de la institución, etc.; puede ser medido con los siguientes valores:

Cuadro 3.4: Valores de Impacto Operacional

Valor	Impacto
0	No produce impacto
1	Bajo impacto
2	Impacto medio
3	Alto impacto

Fuente: elaboración propia (Estos datos fueron tomados en base a la información otorgada por ITIL.)

Impacto Operacional:

Cuadro 3.5: Evaluación de impacto operacional en los Repositorios Digitales

Departamento	Servicio	Impacto operacional
Tecnología de la información	Repositorio Digital	1

Fuente: elaboración propia

El impacto operacional en el repositorio digital fue asignado el valor de bajo impacto (1) por el departamento de tecnología de la información el cual se argumenta que no tiene mayor incidencia la caída de este servicio por una catástrofe tecnológica pues se interrumpe la catalogación y consulta de trabajos de titulación, investigaciones y publicaciones de la sede.

Cuadro 3.6: Evaluación de impacto operacional en los Servidores de nombre de dominio

Departamento	Servicio	Impacto operacional
Tecnología de la información	Servidores de nombre de dominio	2

Fuente: elaboración propia

El impacto operacional en los servidores de nombre de dominio fue asignado el valor de impacto medio (2) por el Departamento de Tecnología de La Información el cual argumenta que existe un impacto la operatividad de los servicios de dominio

ya al haber una catástrofe tecnológica, los docentes, administrativos no podrán ingresar a sus equipos personales hasta restaurar este servicio, se vería dificultado el acceso los computadores personales asignados

Cuadro 3.7: Evaluación de impacto operacional en los Academics

Departamento	Servicio	Impacto operacional
Tecnología de la información	Academics	3

Fuente: elaboración propia

El impacto operacional en el Academics fue asignado el valor de alto impacto (3) por el departamento de tecnología de la información el cual argumenta que existe varios procesos vitales que se verían afectados en el caso de ocurrir una catástrofe tecnológica el cual afecta directamente a este servicio, dichos procesos son, matriculación, cierre de ciclos semestrales, consultas de notas, aprobación de hojas de aranceles, seguimiento de syllabus, etc., se interrumpe su disponibilidad a la comunidad universitaria.

Cuadro 3.8: Evaluación de impacto operacional en el Catálogo en línea

Departamento	Servicio	Impacto operacional
Tecnología de la información	Catalogo en línea	1

Fuente: elaboración propia

El impacto operacional en el Catálogo en Línea fue asignado el valor de bajo impacto (1) por el Departamento de Tecnología de la Información el cual argumenta que no tiene mayor incidencia la caída de este servicio por una catástrofe tecnológica puesto que solamente se realizan consultas libros disponibles de manera digital.

Cuadro 3.9: Evaluación de impacto operacional en los Laboratorios

Departamento	Servicio	Impacto operacional
Tecnología de la información	Laboratorios	1

Fuente: elaboración propia

El impacto operacional en el servicio de Laboratorio fue asignado el valor de bajo impacto (1) por el Departamento de Tecnología de la Información el cual argumenta que no tiene mayor incidencia la caída de este servicio por una catástrofe tecnológica puesto que a través de este servicio se realiza la reserva de los laboratorios para la comunidad universitaria.

Cuadro 3.10: Evaluación de impacto operacional en los servicios de impresión web

Departamento	Servicio	Impacto operacional
Tecnología de la información	Impresión web	1

Fuente: elaboración propia

El impacto operacional en el servicio de Impresión Web fue asignado el valor de bajo impacto (1) por el Departamento de Tecnología de la Información el cual argumenta que no tiene mayor incidencia la caída de este servicio por una catástrofe tecnológica puesto que a través de este servicio se brinda a todos los docentes una asistencia de impresión.

Cuadro 3.11**:** Evaluación de impacto operacional en el servicio Eduram

Departamento	Servicio	Impacto operacional
Tecnología de la información	Eduroam	1

Fuente: elaboración propia

El impacto operacional en el servicio de Eduroam fue asignado el valor de bajo impacto (1) por el Departamento de Tecnología de la Información el cual argumenta que no tiene mayor incidencia la caída de este servicio por una catástrofe tecnológica pues a través de este servicio brinda internet a personas ajenas a la Universidad y a aquellas que no se encuentran dentro del perímetro de alcance de la red local

Cuadro 3.12: Evaluación de impacto operacional en el servicio de spiceworks

Departamento	Servicio	Impacto operacional
Tecnología de la información	Spiceworks	3

Fuente: elaboración propia

El impacto operacional en el servicio de *Spiceworks* fue asignado el valor de alto impacto (3) por el Departamento de Tecnología de la Información el cual argumenta que tiene un gran impacto la perdida de este servicio por una catástrofe tecnológica el cual inhabilita la respuesta a incidencias como: requerimientos y soporte de la comunidad universitaria ante posibles problemas de hardware y software.

Cuadro 3.13: Evaluación de impacto operacional en el registro biométrico

Departamento	Servicio	Impacto operacional
Tecnología de la información	Registro biométrico	3

Fuente: elaboración propia

El impacto operacional en el servicio de registro biométrico fue asignado el valor de alto impacto (3) por el Departamento de Tecnología de la Información el cual argumenta que el impacto que tiene la perdida de este servicio ocasionado por una catástrofe tecnológica, se ocasionan problemas en el ingreso a la universidad tanto a personal administrado, profesores, alumnos y de servicio el cual ocasiona la discontinuidad en los registros de ingreso y salida de la comunidad universitaria.

Cuadro 3.14: Evaluación de impacto operacional en el servicio de sincronización

Departamento	Servicio	Impacto operacional
Tecnología de la información	Servicio de sincronización de credenciales	2

Fuente: elaboración propia

El impacto operacional en el servicio de sincronización fue asignado el valor de medio impacto (2) por el Departamento de Tecnología de la Información el cual argumenta que tiene un gran impacto la perdida de este servicio por una catástrofe tecnológica el cual inhabilita sincronización real entre contraseñas de los servicios de Moodle, correo institucional y dominio de la comunidad universitaria, ocasionado el impedimento al ingreso de sus cuentas personales

Cuadro 3.15: Evaluación de impacto operacional en el consultorio jurídico

Departamento	Servicio	Impacto operacional
Tecnología de la información	Consultorio Jurídico	1

Fuente: elaboración propia

El impacto operacional en el servicio de consultorio jurídico fue asignado el valor de bajo impacto (1) por el Departamento de Tecnología de la Información el cual argumenta que tiene un bajo impacto la perdida de este servicio por una catástrofe tecnológica puesto que únicamente es una asistencia que está disponible para la escuela de jurisprudencia y la cual funciona únicamente en horarios específicos.

3.2.4.3 Identificar Servicios Críticos

Para definir los servicios que son críticos dentro del negocio se toman los siguientes aspectos.

Un servicio se considera critico si:

- El impacto financiero se tiene un valor de medio impacto (2) o alto impacto (3)

O a su vez:

- Si en el impacto operacional se asigna al menos un valor entre medio impacto (2) o alto impacto (3)
- La estructura para la elaboración de la siguiente Cuadro fue tomada de: Syed, Akhytar; *Business Continuity Planning Methology*. (2004).

Servicio	Impacto financiero	Impacto operacional
Repositorio digital Institucional	0	1
Servidores de Nombres de Dominio	0	2
Academics	0	3
Catalogo en línea	0	1
Laboratorios	0	1
Impresión web	0	1
Eduroam	0	1
Spiceworks	0	3
Registro biométrico	0	3
Servicio de sincronización	0	3
Consultorio jurídico	0	1

Cuadro 3.16: Evaluación de impacto de operaciones

Fuente: elaboración propia

3.2.4.4 Priorización de Servicios Críticos

Se conoce el impacto operacional, la priorización de servicios críticos los cuales deben tener prioridad de levantamiento luego de una catástrofe tecnología se asignará de la siguiente forma.

Cuadro 3.17: Valores de Impacto Operacional

Valor	Impacto
0	No produce impacto
1	Bajo impacto
2	Impacto medio
3	Alto impacto

Fuente: elaboración propia

Si a los servicios se le asigna un valor de alto impacto (3) la prioridad de levantamiento de servicios será inmediata, si al servicio se le asigna un valor de impacto medio (2) la prioridad de levantamiento se realizará una vez que los servicios de alto impacto estén operativos y así consecutivamente, cabe mencionar que pueden existir uno o más servicios con la misma asignación de valores.

Departamento: Tecnología de la información

Cuadro 3.18: Impacto operacional

Servicio	**Impacto operacional**
Repositorio digital Institucional	1
Servidores de Nombres de Dominio	2
Academics	3
Catalogo en línea	1
Laboratorios	1
Impresión web	1
Eduroam	1
Spiceworks	3
Registro biométrico	3
Servicio de sincronización	3
Consultorio jurídico	1

Fuente: elaboración propia

En base al cuadro anterior se argumenta que el orden de recuperación de los servicios está asignado por el impacto operacional. El orden de recuperación de servicios se muestra a continuación en el siguiente cuadro, ordenados los servicios de mayor impacto a menor impacto.

Departamento: Tecnología de la información

Cuadro 3.19: Prioridad de recuperación de servicios

Servicio	Impacto operacional
Academics	3
Spiceworks	3
Registro biométrico	3
Servicio de sincronización	3
Servidores de Nombres de Dominio	2
Catalogo en línea	1
Laboratorios	1
Impresión web	1
Eduroam	1
Repositorio digital Institucional	1
Consultorio jurídico	1

Fuente: elaboración propia

3.2.4.5 Identificar MTD's

Los servicios críticos del negocio definen el *Maximun Tolerable Downtimes* (MTD), el cual indica el tiempo máximo que un proceso puede estar fuera de servicio. La estimación del MTD está basada en los valores del RTO institucional otorgado por el Departamento de Tecnología de la Información.

Se realiza la equivalencia, con la elaboración de una regla de proporción simple en base al impacto operacional. Si el valor de impacto operacional es de bajo impacto (1) se le asigna un valor de 6 (horas) máximo de recuperación dicho valor concuerda con el **RTO** institucional **(*Recovery Time Objetive)*** (anexo5).

Cuadro 3.20: Equivalencias MTD

Asignación del impacto operacional	Horas
1 (bajo impacto)	6 horas
2 (impacto medio)	3 horas
3 (alto impacto)	1 hora

Fuente: elaboración propia

La estructura para la elaboración del siguiente cuadro fue tomada de: Syed, Akhytar, *Business Continuity Planning Methology*; (2004), se realiza la asignación de *Maximun Tolerable Downtimes* (MTD) en base a la equivalencia mencionada en el cuadro anterior.

Departamento: Tecnología de la información PUCE-A

Cuadro 3.21: Identificación del MTD

Servicio	Impacto financiero	Impacto operacional	MTD
Repositorio digital Institucional	0	1	6 horas
Servidores de Nombres de Dominio	0	2	3 horas
Academics	0	3	1 hora
Catalogo en línea	0	1	6 horas
Laboratorios	0	1	6 horas
Impresión web	0	1	6 horas
Eduroam	0	1	6 horas
Spiceworks	0	3	1 hora
Registro biométrico	0	3	1 hora
Servicio de sincronización	0	3	1 hora
Consultorio jurídico	0	1	6 horas

Fuente: elaboración propia

En base al cuadro de equivalencia de *Maximun Tolerable Downtimes* (MTD) se menciona por ejemplo que el Academics que tiene un valor total de 3 puntos, el máximo tiempo que puede estar dado de baja este servicio es de una hora.

3.2.4.6 Análisis del daño que causa la interrupción de un proceso

Es importante determinar las consecuencias de la interrupción de un servicio soportado por el Departamento de tecnología de la información de la PUCE – A con el fin de tener idea del impacto que se produce en la institución si hay una catástrofe tecnológica y perdida de servicios.

A continuación, se da una descripción de las consecuencias de la detención de servicios soportado por el Departamento de Tecnología de la Información de la PUCE-A y el lugar donde se encuentra localizado dicho servicio.

La estructura para la elaboración de la siguiente Cuadro fue tomada de: Syed, Akhytar, *Business Continuity Planning Methology*; 2004

Departamento: Tecnología de la información PUCE-A

Cuadro 3.22: Consecuencia de la interrupción de los servicios.

Servicio	**Consecuencia**	**Ubicación**
Repositorio digital Institucional	Inaccesibilidad a los recursos digitales tales como: • Tesis de Pregrado • Tesis de Postgrado • Ponencias de congresos • Investigación de la Sede • Publicaciones de la Sede. Estos recursos digitales están disponibles para la comunidad universitaria, y personas fuera a la misma.	Local
Servidores de Nombres de Dominio	Inaccesibilidad a los servidores de dominio el cual permite la administración de los usuarios, en este caso la administración y privilegios de los docentes dentro de la red. • Acceso a los equipos personales	Local
Academics	Inaccesibilidad a los Servicios integrados a través de un portal web, en el cual el estudiante y el docente tienen acceso a: • Seguimiento de Syllabus	Local

	• Tutorías • Notas Parciales y Finales del estudiante • Proceso de Matriculación • Evaluación Docente	
Catalogo en línea	Inaccesibilidad a la comunidad universitaria a los libros disponible sen línea	Local
Laboratorios	Inaccesibilidad a las reservas de los laboratorios	Local
Impresión web	Inaccesibilidad a los servicios de impresión web que afectara a los docentes de medio tiempo	Local
Eduroam	Inaccesibilidad al Servicio de red inalámbrica el cual permite el acceso a internet de personas ajenas a la institución mediante sus credenciales Este servicio solo está disponible para instituciones que sean miembros de cedia	Local
Spiceworks	Inaccesibilidad al servicio permite la monitorización integral de la red.	Local
Registro biométrico	Interrupción del Servicio el cual permite el control de ingreso y salida de personal.	Local
Servicio de sincronización de credenciales	Interrupción del Servicio el cual permite a los usuarios cambiar su contraseña en el correo electrónico institucional y este automáticamente se actualiza con el dominio y el Moodle.	Local
Consultorio jurídico	Interrupción del Servicio disponible para la escuela de jurisprudencia en el cual se realiza el ingreso de casos.	Local

Fuente: elaboración propia

3.2.4.7 RTO Y RPO

Retención /RPO (*Recovery Point Objetive)*

24 horas

Restauración /RTO (*Recovery Time Objetive)*

Seis horas recuperación objetivo, estos datos **RPO y RTO** se obtuvieron de la política de respaldo e información del Departamento de Tecnología de la Información PUCE-A (Anexo 7)

3.2.5 Evaluación de riesgos

Para el plan de continuidad es necesario realizar un análisis de riesgos que pueden afectar la PUCE – A en el cual se identifica las amenazas y consecuencias, para así poder establecer un levantamiento de servicios oportuno.

En la evaluación de riesgos se desarrollarán los siguientes puntos.

- Identificación de riesgos.
- Identificar las consecuencias de la amenaza.

3.2.5.1 Identificación de riesgos

Se toma en cuenta los componentes ilustrados en la siguiente imagen

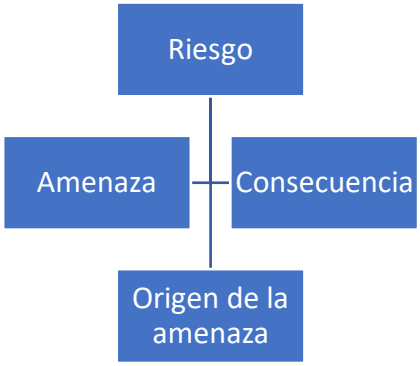


Gráfico 2.1: Componentes del Riesgo

Fuente: elaboración propia

Imagen adaptada de: Syed, Akhytar, Business Continuity Planning Methology; 2004

3.2.5.2 Identificar el origen de la amenaza

En esta etapa se identifica la fuente que origina la amenaza para el Centro de Base de Datos de la PUCE - A, las amenazas pueden ser de tipo técnico, natural, antrópico

A continuación, se enlistan las posibles amenazas para el centro de base de datos de la PUCE- A, dichas amenazas fueron revisadas por la Gerencia del Departamento de Tecnología de la Información de la PUCE - A

La estructura para la elaboración del siguiente cuadro fue tomada de: Syed, Akhytar, *Business Continuity Planning Methology*; 2004

Cuadro 3.23: Identificación de amenazas

Amenazas técnicas	Amenazas antrópicas	Amenazas naturales
Incendio	Caída de un avión	Terremoto
Interrupción de energía eléctrica	Problemas de seguridad	Erupción volcánica
Fallas en los servidores	Terrorismo	

Fuente: elaboración propia

3.2.5.3 Identificar las consecuencias de la amenaza

En esta etapa se identifica las consecuencias de las amenazas identificadas en el cuadro anterior.

La estructura para la elaboración del siguiente cuadro fue tomada de: Syed, Akhytar, *Business Continuity Planning Methology*; 2004

Cuadro 3.24: Identificación de consecuencias de amenazas

Amenazas	Recursos	Consecuencias
Incendio	Centro de base de datos	• Equipos fuera de funcionamiento • Inaccesibilidad al edificio • Equipos dañados en tu totalidad
Interrupción de energía eléctrica	Centro de base de datos	• Equipos fuera de funcionamiento
Fallas en los servidores	Centro de base de datos	• Equipos fuera de funcionamiento • Equipos dañados en su totalidad
Caída de un avión	Centro de base de datos	• Equipos fuera de funcionamiento • Equipos dañados en su totalidad • Inaccesibilidad al edificio

Problemas de seguridad	Centro de base de datos	• Equipos fuera de funcionamiento • Equipos dañados en su totalidad
Terrorismo	Centro de base de datos	• Equipos fuera de funcionamiento • Equipos dañados en su totalidad • Inaccesibilidad al edificio
Erupción volcánica	Centro de base de datos	• Equipos fuera de funcionamiento • Inaccesibilidad al edificio

Fuente: elaboración propia

Cabe mencionar que las consecuencias de las amenazas son de manera catastrófica, es decir que el centro de datos quedara totalmente inhabilitado para su funcionamiento.

3.3 Fase 3

3.3.1 Etapa de implementación

Para el presente proyecto la fase de implementación y el modo de recuperación se ha considerado el servicio en la nube DRaaS (*Disaster Recovery as a Service),* el cual se menciona en el capítulo anterior pues permite a las instituciones disponer de una réplica exacta de sus sistemas y aplicaciones en un Centro de datos alojado en una nube pública o privada, este Centro de datos actúa de como una plataforma remota de contingencia en caso de ocurrir algún desastre tecnológico el cual ocasione el pare total de los servicios, es posible tener una réplica exacta de estos servicios.

DRaaS (*Disaster Recovery as a Service)* lleva el concepto de recuperación más allá, puesto que no se trata solo de la recuperación de datos o servicios críticos sino de recuperarla continuidad del negocio en el menor tiempo posible; DRaaS (*Disaster Recovery as a Service)* es una estrategia que incluye poder de computo en la nube, seguridad, almacenamiento y servicios de conectividad (Revista MyM, 2015).

3.3.2 Fase de requisitos para la implementación del plan

Se detallará a continuación los aspectos pertinentes al Departamento de tecnología de la información de la PUCE – A para determinar los requerimientos necesarios para el correcto funcionamiento del Plan de continuidad del negocio.

3.3.3 Gestión de Red LAN

La gestión de la infraestructura de red LAN la realiza el departamento de tecnología de la información de la PUCE -A, ha definido que la red LAN debe mantenerse operativa 24 horas durante los 7 días de la semana, con monitoreo en sitio de 7:00 am a 7:00 pm y monitoreo presencial adicional un monitoreo remoto las 24 horas, este monitoreo está presente dentro de las políticas del departamento de tecnología de la información de la PUCE – A (Anexo 7)

3.3.4 Internet

Los proveedores de internet son: CEDIA y TELCONET como respaldo.

3.3.5 Infraestructura

La infraestructura de red de la Institución se encuentra ubicada en un centro de datos, ubicado en el cuarto piso del bloque 1, en este centro de datos se encuentran los dispositivos de conectividad, servidores, cajas de almacenamiento de la institución.

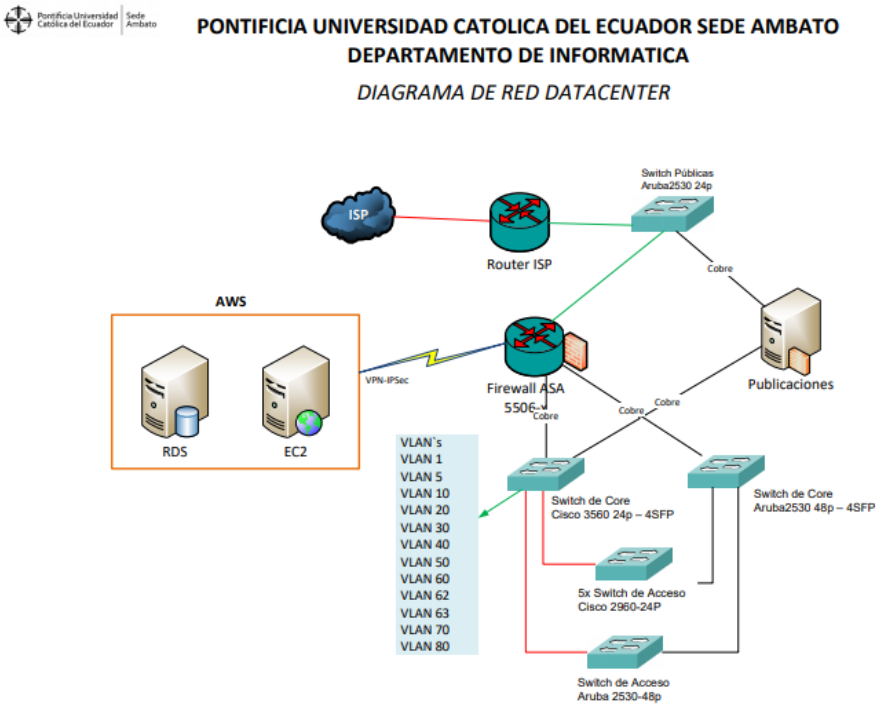


Gráfico 3.2: Diagrama de Red Data Center PUCE – A

Fuente: Departamento de Tecnología de la Información PUCE-A

Características.

- Se tiene dos proveedores de internet Telconet y Cedia cada uno tiene su propio router el cual provee internet, estos dos routers están bajo un protocolo de redundancia (*Virtual Router Redundancy Protocol VRRP*), esto permite continuar con el servicio de internet en caso de que uno de los dos proveedores falle.
- El *Data Center* cuenta con un switch de IP públicas, a través de este equipo se conecta: Firewall ASA (Firewall perimetral) y el servidor de publicaciones (permite acceder a los servicios identificados en la fase número dos).
- El *Firewall* ASA, además de ser un firewall perimetral también es un servidor proxy, lo que permite tener acceso a internet a la comunidad universitaria además de tener un control de contenido de navegación.
- También se cuenta con los *Switch* de Core los cuales están bajo un protocolo de redundancia (*Virtual Router Redundancy Protocol VRRP*), lo que permite continuar con los servicios en caso de que un *Switch* de Core llegue a fallar.

- Los *Switch* de acceso llegan los enlaces de los *Swtich* de Core los cuales permiten la disponibilidad de servicio, si un cliente entra a los *Switch* de acceso y uno de los *Switch* de Core falla el cliente puede tener acceso a internet por el otro enlace disponible.
- Los servidores se conectan a los *Switch* de Core.
- Las Vlan’s (Red de área local virtual) están segmentadas por escuelas y departamentos.

3.3.6 Inventario de servidores

Se detalla a continuación las especificaciones técnicas de los servidores principales, donde se encuentran alojadas las aplicaciones mencionadas en la fase dos (Análisis d impacto en el negocio).

Cuadro 3.25: Inventario de Servidores

Tipo	Nombre	Disco	HDD GB	Memoria MB	Procesador	Sistema Operativo	Servicio	Respaldos
Virtual	BIOSECAMB01	Hard disk 1	184.320	4.096	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows 10 (64-bit)	ADMINISTRACION SISTEMA DE INGRESO	24 horas
Virtual	DCAMB01	Hard disk 1	102.400	4.096	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2012 (64-bit)	CONTROLADOR DE DOMINIO	24 horas
Virtual	DSPACEPUCESA	Hard disk 1	204.800	5.120	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	CentOS 4/5 or later (64-bit)	REPOSITORIO DIGITAL	24 horas
Virtual	EDUROAM01	Hard disk 1	20.480	2.048	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	CentOS 4/5 or later (64-bit)	EDUROAM CEDIA	Cada 7 días
Virtual	FILEAMB01	Hard disk 1	81.920	4.096	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2008 R2 (64-bit)	SERVIDOR DE IMPRESIÓN	24 horas
Virtual	helpdesk02	Hard disk 1	412.034	10.176	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2008 R2 (64-bit)	SERVIDOR DE MESA DE AYUDA	24 horas
Virtual	MBRAMB01	Hard disk 1	81.920	4.096	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2012 (64-bit)	SERVICIO DE RESERVA DE LABORATORIOS	24 horas
Virtual	PRDAMB01	Hard disk 2	307.200	8.192	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2008 R2 (64-bit)	SERVICIO ACADEMICS PRODUCCION	24 horas
		Hard disk 1	81.920					
Virtual	SIABUCAMB01	Hard disk 1	102.400	4.096	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2008 R2 (64-bit)	SERVICIO BILBIOTECA SIABUC	24 horas
		Hard disk 2	307.200					
Virtual	SYNCAMB01	Hard disk 1	153.600	8.192	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows Server 2012 (64-bit)	SERVICIO SINCRONIZACION DIRECTORIO ACTIVO CON O365	Cada 7dìas
Virtual	WEBPRINT01	Hard disk 1	81.920	2.048	Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz	Microsoft Windows 7 (32-bit)	SERVICIO IMPRESIÓN WEB	Cada 7 días

Fuente: Departamento de Tecnología de la Información PUCE - A

En base a los datos obtenidos en el cuadro anterior con respecto a los tiempos de respaldo como los servicios que tienen un respaldo semanal (7 días), los servicios que tienen un respaldo diario (24 horas), estas asignaciones son políticas del departamento de tecnología de la información de la PUCE– A

3.3.7 Análisis de los proveedores de DRaaS

Para el siguiente análisis se utilizó como referencia el cuadrante mágico de Gartner para la recuperación ante desastres actualizado julio 2018 donde se detallan los principales proveedores de este servicio.

Gráfico 3.3: Gartner – Proveedores de DRaaS

Fuente: (Gartner,2018)

Para el presente proyecto se toma en cuenta el proveedor de DRaaS *(Disaster Recovery as a Service)*, provenientes del diagrama de Gartner los cuales son:

1. Microsoft (Azure)

Además, por petición de la gerencia se analizaron costos de proveedores locales por la confianza que se tiene con la empresa, además que Cedia trabaja con las universidades locales como proveedor de internet.

1. Adistec
2. Cedia

Al momento de contactarse con Adistec, manifestaron que ellos trabajan a manera de *partners* con Virtual- IT, se proporciona el alojamiento en la nube, solicitaron que se contacte directamente con Virtual – IT.

Los proveedores que se analizan luego de esta aclaración son los siguientes:

1. Cedia
2. Virtual - IT
3. Microsoft

3.3.8 Requisitos para la contratación

Los requisitos para la contratación están definidos por las políticas del departamento de tecnología de la información de la PUCE – A en los cuales se definen los servicios previamente identificados, sus características, y los tiempos de restauración. (anexo 7)

3.3.9 Parámetros de evaluación a proveedores.

Los siguientes parámetros de evaluación a proveedores se basó en las mejores prácticas en términos de contratación de Servicios de Computación en la Nube de ENISA (2014).

1. **Continuidad del servicio.**

Los proveedores del servicio DRaaS *(Disaster Recovey as a Service),* deben garantizar la continuidad de los servicios, pues la institución debe garantizar a la comunidad universitaria el acceso a la información de cada miembro de la universidad, así como los servicios que permiten la continuidad del negocio con alta disponibilidad 24/7 una vez ocurrido el desastre.

2. **Confidencialidad de la información.**

Los datos subidos a la nube deben tener un estricto grado de confidencialidad de la información y datos, se prioriza la importancia a los datos personales y sensibles, información secreta y privada. Se exige a los proveedores del servicio cláusulas de confidencialidad sobre los datos almacenados, se prohíbe que esta información sea puesta en conocimiento d terceros no autorizados.

3. **Borrado de datos.**

El borrador de información es un punto importante que tratar pues en el caso de no continuar con al servicio de DRaaS (*Disaster Recovey as a Service)*, el proveedor debe asegurar toda la eliminación de la información existente de la institución, por ello es importante que se mencione en el convenio de confidencialidad una vez culminado el contrato se elimine la información por completo, además de considerar los respaldos de información que el proveedor posea.

4. **Seguridad de la información:**

Para verificar la seguridad de la información, se ha tomado en consideración los siguientes puntos.

- El proveedor del servicio debe tener o implementar medidas administrativas que garantice que la información almacenada no se pierda, dañe o se modifique.
- La información que se almacene no sebera ser utilizado por terceras personas.
- La información que se almacena no será utilizada para fines distintos a los que establece el contrato.

- La comunicación de datos, entre el proveedor y la institución debe ser de manera segura adicional garantizar que las comunicaciones y acceso remoto entre el proveedor y la institución tenga la seguridad adecuada para no ser interceptada por terceros.

5. **Facilidad de uso.**

La institución requiere de una solución de fácil manejo para así disminuir las cargas de trabajo a la gestión del departamento de Tecnología de la Información, por lo que se requiere que el proveedor del servicio brinde una solución amigable para los usuarios.

6. **Calidad de soporte.**

Se requiere que el proveedor entregue un soporte inmediato a los requerimientos y problemas que se presenten durante y después de la implementación del servicio de recuperación ante desastres.

7. **Costo**

Para la implementación de una solución que ayude al plan de continuidad de negocios se analiza las proformas del servicio enviadas por los proveedores anteriormente mencionados.

3.3.10 Comparativa entre Proveedores

Una vez descrito los parámetros de evaluación a proveedores, es necesario realizar una priorización, se asigna un factor de importancia de 1 a 3 puntos, donde 3 es el valor de mayor importancia.

Se asignó estos valores en base a la escala nominal la cual me permite clasificar unidades de estudio en base a una o más características como se muestra a continuación.

Para valorar a los proveedores se asignó una calificación en base a las mejores prácticas en términos de contratación de Servicios de Computación en la Nube de ENISA (2014) donde:

- 0 = no cumple
- 1 = cumple levemente.
- 2 = en proceso de mejora.
- 3 = cumple en su totalidad.

Se procedió a la asignación de puntos a los parámetros de evaluación de proveedores con el departamento de tecnología de la información, dichos parámetros de evaluación se asignaron en base a las mejores prácticas en términos de contratación de Servicios de Computación en la Nube de ENISA (2014).

Cuadro 3.26: Asignación de parámetros evaluación de proveedores.

Parámetros	Importancia
Continuidad del servicio	3
Confidencialidad de la información	3
Borrado de información	3
Seguridad de la información	3
Facilidad de uso	3
Calidad de soporte	3
Costo	3

Fuente: elaboración propia

Para valorar a los proveedores se asignó una calificación en base a las mejores prácticas en términos de contratación de Servicios de Computación en la Nube de ENISA (2014) donde:

- 0 = no cumple
- 1 = cumple levemente.
- 2 = en proceso de mejora.
- 3 = cumple en su totalidad.

Para la elaboración de la siguiente Cuadro se analizó las proformas entregadas por los proveedores (ver Anexo 4, Anexo 5, Anexo 6), además de la información

obtenida de la página web de cada uno de ellos, adicional dichos valores se revisaron con la gerencia del departamento de tecnologías de la información de la PUCE – A, los cuales fueron aprobados para su respectiva comparativa.

El total de cada uno de los parámetros se obtiene de la suma de la importancia (imp)+ calificación (cal).

Cuadro 3.27 Comparativa de proveedores.

	Windows Azure			**Virtual - IT**			**Cedia**		
Parámetros	**Imp**	**Cal**	**Total**	**Imp**	**Cal**	**Total**	**Imp**	**Cal**	**Total**
Continuidad del servicio	3	3	6	3	3	6	3	3	6
Confidencialidad de la información	3	3	6	3	3	6	3	3	6
Borrado de la información	3	2	6	3	3	6	3	3	6
Seguridad de la información	3	3	6	3	3	6	3	3	6
Facilidad de uso	2	2	4	3	3	6	3	2	5
Calidad de soporte	2	2	4	3	3	6	3	3	6
Costo	3	2	5	3	3	6	3	2	5
Total			**37**	**Total**		**42**	**Total**		**40**

Fuente: elaboración propia

Tanto Microsoft, Virtual - IT, Cedia cumplen con los requerimientos necesarios para convertirse en proveedores del servicio de recuperación para desastre, se concluye que Virtual IT es el que alcanza la mayor puntación.

3.3.11 Análisis operativo *On Premise vs Cloud.*

Es necesario valorar la solución *On Premise vs Cloud*, para ello se realizaron las siguientes preguntas las cuales se realizaron en colaboración del departamento de tecnología de la información y un asesor de Veeam.

Se realizó la comparativa con Veeam debido a que el departamento de tecnología de la información trabaja con Veeam con versión ESXi 6,5.

Cuadro 3.28: Solución *on premise vs cloud*

Pregunta	**Solución *On Premise***	**Solución en la nube**
¿Cuántos mantenimientos preventivos al centro de datos se realizan al año?	Mantenimiento de nivel de hardware dos veces al año de manera semestral, y mantenimiento a nivel de software trimestral.	No requiere mantenimiento por parte del cliente puesto que no se traslada al personal para que revise la infraestructura que se contrató, el mantenimiento lo realiza la empresa la cual oferta el servicio ya sea con actualizaciones de software o de hardware.
¿Cuánto tiempo les toma recuperar el servicio viéndose afectado los servidores principales?	Actualmente se toma un máximo de 6 horas recuperar los servidores.	El DRaaS permite disminuir el RTO *(recovery time objetive)* de manera significativa de 10 minutos a 30 minutos.
¿Cuenta con una solución de respaldo?	En este caso se trabaja con Veeam *Backup* el cual permite realizar respaldos de los servidores cada cierto tiempo.	En caso de requerir la base de datos se realiza una replicación incremental, además de realizar una replicación de la imagen de la máquina virtual.
¿Realiza el monitoreo de los servidores con herramientas?	Si actualmente se realiza un monitoreo presencial como remoto de los servidores.	Veeam cuenta con herramientas de monitoreo continuo las 24 horas, además de ofrecer una herramienta adicional la cual se instala en la máquina del personal de infraestructura la cual permite un mejor monitoreo de los servidores dado el desastre, además de contar con la instalación de JOBS para monitoreo.

Fuente: elaboración propia

3.3.12 Análisis de costos entre proveedores.

Se realizó un análisis de costo entre proveedores, basado en las proformas entregadas por los mismos, esto permitirá tomar una mejor decisión al momento de realizar el contrato de un proveedor que se adapte al presupuesto y a las necesidades del departamento de tecnología de la información.

3.3.12.1 Análisis proveedor Virtual IT

Cuadro 3.29: Análisis proveedor Virtual IT

Concepto	**Costo único**	**Costo mensual**	**Costo anual**
Implementación de los servidores incluido licenciamiento de los servidores y configuración de *Veeam Backup and Replication.*	5.512,37$	**-**	**-**
Servicio DRaaS		912,48$	

Fuente: elaboración propia

El proveedor de este servicio realiza la contratación mínima de un año, así al primer y único de USD 5.512,37 y luego un pago mensual de 912,48, esto quiere decir que sin importar el número de servidores que se lleguen a levantar al momento del desastre, el pago será el mismo, esto valores se tomaron del anexo

3.3.12.2 Análisis proveedor Cedia.

El proveedor de este servicio incluye el soporte, el *storage* dentro del valor total de la propuesta que se muestra a continuación, estos valores de tomaron del anexo 5.

Cuadro 3.30: Costos Cedia

Concepto	**Costo único**	**Costo mensual**	**Costo anual**
Implementación de los servidores	880,00$	**-**	**-**

Licenciamiento de los servidores	-	-	1.980,00$
Servicio DRaaS		1.677,00$	

Fuente: elaboración propia

El costo anual del servicio de DRaaS es de USD 20.124,00, de igual manera se paga una mensualidad sin importar el número de servidores que se lleguen a levantar al momento del desastre, el pago será el mismo.

Estos valores se tomaron del anexo 5.

3.3.12.3 Análisis proveedor Microsoft.

El proveedor de este servicio, el *storage* dentro del valor total de la propuesta que se muestra a continuación, estos valores de tomaron del anexo 6.

Cuadro 3.31: Costos Microsoft

Concepto	Costo único	Costo mensual	Costo anual
Implementación de los servidores incluido licenciamiento.	6.010,00$	-	-
Servicio DRaaS (Infraestructura en AZURE)		2.300,00$	

Fuente: elaboración propia

El costo anual del servicio de DRaaS es de USD 6.010,00$ adicionalmente Microsoft utiliza el pago por uso, es decir, los USD 6.010,00$ es para mantener el servicio DRaaS activo, y el costo mensual por mantener los servicios activos es de 2.300,00$

3.3.13 Análisis RTO (*Recovery Time Objective*) entre los proveedores.

El *Recovery Time Objective* es un factor decisivo al momento de elegir un proveedor pues la institución no puede permanecer inoperativa más de seis horas, se considera que los servicios previamente identificados los cuales están con un

RTO máximo de una hora deben estar operativos en menor tiempo, para ello se realizó el siguiente cuadro comparativo del factor entre los proveedores.

Cuadro 3.32: Cuadro RTO proveedores.

Proveedores	RTO
Cedia	15 minutos
Azure	20 minutos
Virtual IT	10 minutos

Fuente: elaboración propia

En relación al cuadro anterior se argumenta que Virtual IT ofrece el menor tiempo de recuperación de los servidores, esto quiere decir que una vez suscitado el desastre los servidores estarán operativos en un máximo de 10 minutos.

3.3.14 Evaluación General.

Los análisis realizados determinan que el proveedor de servicios de Virtual IT tiene un mejor puntaje dentro del cuadro de valoración de proveedores, además de ofrecer mejores precios anuales en comparativa a los demás, cabe recalcar que una de las principales ventajas de este proveedor es que el centro de datos y sus servidores trabajan con Veeam por lo cual el tiempo de implementación del servicio una vez realizado el contrato será de un máximo de 30 días, se sugiere que la migración de los servidores sea de manera paulatina, aunque estas policitas son definidas por el proveedor, en este caso Adistec trabaja conjuntamente con Virtual IT quienes son los que proporcionaron la proforma de Veeam.

3.4 Fase 4

3.4.1 Equipo de la continuidad del Negocio.

Una vez ocurrido un desastre la persona encargada de liderar la recuperación ante desastres es el Gerente del Departamento de Tecnología de la Información, quien luego del desastre convoca inicialmente a los miembros del departamento de Tecnología de la Información para realizar la evaluación del sitio afectado.

3.4.2 Centro de reuniones alternativo en caso de desastre.

Una vez realizada la evaluación del sitio afectado y en dependencia del tipo de desastre se tiene las siguientes prioridades de puntos de encuentro para la reunión de los miembros del departamento de Tecnología de la Información.

1. **Si el bloque 1 luego del desastre es accesible:**

Punto de reunión

- PUCE – Ambato / Bloque 1 – 4to piso

Sala de reuniones localizada en el 4to piso

2. **Si el bloque 1 luego del desastre es inaccesible:**

Punto de reunión

- PUCE – Ambato / Cualquier localización dentro de la universidad con acceso a internet

3. **Si la Sede luego del desastre es inaccesible:**

Punto de reunión.

- Sala virtual de reuniones del personal de TI

4. **Si el desastre afecto a la ciudad:**

Canales de comunicación.

- Sala virtual de reuniones del personal de TI.

3.4.3 Equipo para la Continuidad del Negocio.

Para la implementación del Plan de Continuidad del negocio para la PUCE – Ambato se define el equipo el cual se encargará de la recuperación y levantamiento de servicios los cuales ofrece el Departamento de Tecnología de la Información.

Para el Departamento de Tecnología de la Información de la PUCE – Ambato los miembros del equipo serán de 8 personas que conforman el Departamento de TI.

La estructura que el equipo del Plan de Continuidad del Negocio se muestra a continuación.

La estructura para la elaboración de la siguiente figura fue tomada de: Syed, Akhytar, *Business Continuity Planning Methology*; 2004

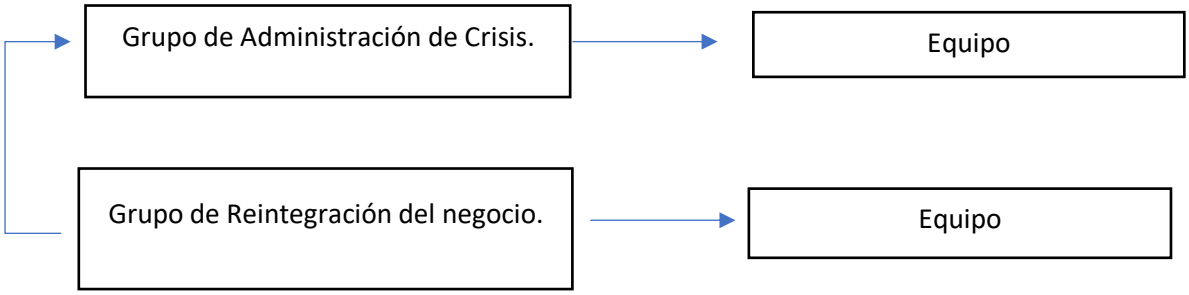


Gráfico *3*.3: Estructura del equipo del Plan de Continuidad del Negocio

Fuente: elaboración propia

Imagen adaptada de: Syed, Akhytar, Business Continuity Planning Methology; 2004

3.4.4 Grupo de Administración de la Crisis

3.4.4.1 Equipo de Administración de la Crisis (CTM- Crisis Managment Team):

Roles:

Este equipo se encarga de la administración y control del Plan de Continuad del Negocio, una vez ocurrido el desastre el CTM se traslada al centro de administración del desastre, dado el caso al sitio alternativo designado, el CTM es el que está autorizado de solicitar el Plan de Continuidad del Negocio en caso de ser necesario.

3.4.4.2 Coordinador del Plan de Continuidad del Negocio

Es el encargado de supervisar la respuesta inicial y notificación del desastre, evaluación de daños, escalamiento, recuperación y levantamiento de servicios afectados.

3.4.4.3 Equipo de Evaluación de Daños (DAT- Damage Assessment Team)

Es el equipo el cual se encarga de realizar la evaluación de daños una vez ocurrido el desastre para si determinar el tiempo que tomara la recuperación física del centro de datos.

3.4.4.4 Equipo de Comunicación de la Crisis (*CCT – Crisis Comunication Team)*

Es el equipo responsable de proveer la información a todo el personal sobre el evento ocurrido, esta información debe ser oportuna y exacta

3.4.4.5 Equipo de Administración de Usuarios (UMT- User Management Team)

Es el equipo encargado de mediar e interactuar con los usuarios luego de ocurrido el desastre, para solventar dudas, inquietudes sobre los servicios que puedan estar caídos.

3.4.5 Grupo de reintegración del negocio:

3.4.5.1 Equipo de Unidades del Negocio (BUT- Business Unit Team)

Es un equipo conformado por una persona clave de cada área del departamento de Tecnología de la Información, los cuales evalúan las necesidades de su área una vez suscitado el desastre e informan al coordinador del plan de continuidad del negocio.

3.4.5.2 Asignación del Personal

Para el presente Plan de continuidad del negocio se ha tomado en consideración a las 8 personas que conforman el departamento de Tecnología de la Información, en la cual cada miembro debe cumplir una o varias tareas:

Departamento Tecnologías de la Información Puce - A	Gerente del departamento	Técnico multimedia	Especialista en aplicaciones y desarrollo	Técnico en desarrollo	Especialista de comunicación	Técnico en infraestructura
Equipo de Administración de Crisis	x	x	x			
Coordinador de la continuidad del negocio	x					
Equipo de evaluación de daños	x	x	x	x	x	x
Equipo de comunicación de la crisis	x	x	x	x	x	x
Equipo de administración de usuarios.	x	x	x	x	x	x
Equipo de unidades del negocio		x	x	x	x	x

Cuadro 3.32: Matriz de responsabilidades

Fuente: elaboración propia

Imagen adaptada de: Responsibility assignment matrix (RACI)

- **Gerente del Departamento de TI.**
  a) Equipo de Administración de la Crisis.
  b) Coordinador de la Continuidad del negocio.
  c) Equipo de evaluación de daños.
  d) Equipo de Comunicación de la Crisis.
  e) Equipo de administración de usuarios.
- **Técnico multimedia del Departamento de Tecnología de la Información.**
  a) Equipo de Administración de la Crisis.
  b) Equipo de evaluación de daños.
  c) Equipo de Comunicación de la Crisis.
  d) Equipo de administración de usuarios.

e) Equipo de unidades de negocio.

- **Especialista en Aplicaciones y Desarrollo del Departamento de Tecnología de la Información.**
    a) Equipo de Administración de la Crisis.
    b) Equipo de evaluación de daños.
    c) Equipo de Comunicación de la Crisis.
    d) Equipo de administración de usuarios.
    e) Equipos de unidades de negocio.
- **Técnico en Desarrollo del Departamento de Tecnología de la Información.**
    a) Equipo de evaluación de daños.
    b) Equipo de Comunicación de la Crisis.
    c) Equipo de administración de usuarios.
    d) Equipos de unidades de negocio.
- **Especialista de Comunicación e infraestructura del Departamento de Tecnología de la Información.**
    a) Equipo de evaluación de daños.
    b) Equipo de Comunicación de la Crisis.
    c) Equipo de administración de usuarios.
    d) Equipos de unidades de negocio.
    e) Equipo de administración de la Crisis.
- **Técnico en Infraestructura.**
    a) Equipo de evaluación de daños.
    b) Equipo de Comunicación de la Crisis.
    c) Equipo de administración de usuarios.
    d) Equipos de unidades de negocio.

3.4.6 Actividades para la ejecución del Plan de Continuidad del Negocio

Para una correcta implementación del Plan de continuidad del negocio se sigue una serie de pasos que ayuden a mejorar de forma óptima la administración de un desastre, se minimiza el tiempo de recuperación y retorno a las actividades normales de la institución, para restablecer lo más antes posible las comunicaciones, servicios, que se brinda a los usuarios, para esta recuperación

cabe recalcar que se utilizarán los servicios de la nube : DRaaS *(Disaster Recovery as a Service)* el cual permite una rápida recuperación de la continuidad del negocio.

Las actividades que se detallan a continuación están tomadas como referencia del libro Syed, Akhar; Syed, Afsar; Business Continuity Planning Methodology: 2004 y adaptadas a las necesidades y recursos del Departamento de Tecnología de la Información.

3.4.6.1 Respuesta inicial y notificación.

En esta etapa una vez sucedida el desastre, se evalúa el impacto de daños, todos los miembros del plan de continuidad son notificados y el plan es activado, se ha definido un conjunto de actividades:

- Definir el lugar de reunión del equipo de la continuidad del negocio
- Cada miembro del departamento de tecnología de la información recibe la notificación del desastre por parte del equipo de comunicación de la crisis, el cual previamente ya se definió.
- El Coordinador del plan de continuidad del negocio o a su vez el equipo de administración de la crisis se encargará de informar a los proveedores de DRaaS *(Disaster Recovery as a Service)* sobre el desastre ocurrido.
- Determinar si el edificio es accesible.
- Si el desastre ocurre en horas no laborables, trasladarse a la institución de manera inmediata.
- Evaluación de daños al centro de datos.
- Evaluación del impacto del desastre al centro de datos.
- Preparar un informe del desastre y los daños que este ocasiono al centro de datos, este informe deberá ser elaborado por el equipo encargado de la crisis y el equipo de evaluación de daños y presentado al Coordinador del plan de continuidad.

El informe permitirá conocer la idea global del problema para alimentar el plan de continuidad, se detalla el impacto y los daños causados por el desastre.

3.4.6.2 Evaluación del problema y escalamiento.

En esta etapa se determinará la magnitud del desastre basado en el informe anteriormente presentado. Las actividades que seguir son las siguientes.

- Recepción del informe por parte del Coordinador del Plan de Continuidad.
- Revisión de la magnitud del impacto de los daños en el informe presentado.
- Inspeccionar el sitio del desastre para así evaluar el impacto causado por la interrupción.
- Evaluar la interrupción de servicios y el daño en el centro de datos.
- Identificar los servicios que fueron afectados y fuera de funcionamiento, en el caso de no ocurrir daños a los servicios, ni a los servidores del centro de datos, Se realiza un monitoreo de situación, caso contrario seguir con la siguiente fase.
- Se realiza un informe por parte del equipo de Administración de Crisis, Equipo de evaluación de daños e informar al Coordinador del Plan de continuidad del negocio.

Para la elaboración del problema y escalamiento basarse en el anexo 9.

3.4.6.3 Declaración del Desastre.

La decisión de declarar el desastre está a cargo del Coordinador del Plan de continuidad del negocio, esta decisión se basará en el informe entregado por parte del equipo de Administración de Crisis. Las actividades que seguir son las siguientes:

1. Revisar el informe detallado del problema, se analiza la magnitud del desastre y los impactos que este causo al centro de datos.
2. Una vez declarado el desastre el Coordinador del plan de continuidad del negocio o a su vez el equipo de administración de la crisis inmediatamente deberá contactarse con el proveedor de servicio DRaaS *(Disaster Recovery as a Service)* el cual deberá inmediatamente responder con el levantamiento

de los servicios afectados, para así evitar pérdidas de continuidad de negocio de la institución.

3.4.6.4 Plan de implementación de logística

En esta etapa se realiza un monitoreo de los servidores levantados por el proveedor de DRaaS *(Disaster Revovery as a Service)*, este monitoreo estará a cargo del equipo de Administración de la crisis para evaluar el desempeño de los servicios que están levantados en la nube.

Los equipos de Administración de usuarios deberán atender los requerimientos de los clientes, como a su vez solucionar cualquier soporte que se presente post - desastre para evitar problemas de operatividad dentro de la institución.

Se toma en cuenta que el punto de restauración objetivo de los servicios es 1 hora, esto quiere decir que luego de declararse el desastre, los servicios que estén inoperativos estarán en funcionamiento en un máximo de una hora.

3.4.6.7 Recuperación.

En esta etapa una vez pasado las 24 horas de ocurrido el desastre, el Coordinador del plan de continuidad, deberá preparar un informe detallado de los servicios que están levantados en la nube, además de informar a los demás miembros del departamento de tecnología de la información que los servicios que estaban afectados ahora se encuentran totalmente operativos y funcionales.

3.4.6.8 Simulacro

El presente simulacro de desastre el cual se considerará la caída del bloque 1, a causa de un terremoto el cual origina la destrucción total del centro de datos de la Pontificia Universidad Católica del Ecuador - Ambato. Los servidores en los cuales se encontraban almacenados los 9 servicios previamente identificados están totalmente inoperativos, se asume que el desastre ocurrió un martes en la mañana en el periodo semestral febrero- junio.

Este desastre causo la perdida de continuidad operativa de los 9 servicios previamente identificados el cual causas inconvenientes a la comunidad universitaria.

A continuación, se describen las acciones a tomarse para el levantamiento de los servicios afectados, que permiten la continuidad del negocio.

3.4.7 Escenario del plan de continuidad.

3.4.7.1 Etapa 1: Respuesta Inicial y Notificación.

Se registra la siguiente información.

1. **Registrar las personas que notaron el desastre**
   Identificar a la persona que se dio cuenta de la ocurrencia del desastre, fecha y hora.
   En este escenario la persona que se dio cuenta fue el Técnico de infraestructura a las 7:00 AM del martes el cual notifico al Gerente del Departamento de Tecnología de la Información.

2. **Definir el lugar de reunión del equipo de continuidad.**
   Debido a que el desastre afecto a todo el bloque 1, lo cual ocasiona la destrucción total del centro de datos, se define el lugar de reunión del equipo de continuidad dentro de la universidad pues el sitio si es accesible.
   El Departamento de Tecnología de la Información hace un breve análisis del desastre, y definen las características del desastre:
   - El data center ubicado en el último piso del bloque 1 está totalmente destruido.
   - Los servidores están inoperativos.
   - Se ha determinado que el grado de severidad del impacto es alto, se toma en cuenta en cuenta los valores predefinidos en la evaluación del impacto operacional que se encuentra en el BIA (Impacto en el negocio) se cataloga como alto impacto en función de los servicios inoperativos que se encontraban dentro de los servidores que se encuentran fuera de servicio.

3. **Cada miembro del equipo recibe la alerta del desastre.**

   En esta etapa es necesario definir si se necesita la presencia de todo el Departamento de Tecnología de la información para poner en marcha el plan de continuidad. En este escenario es necesario convocar a todo el Departamento de Tecnología de la Información para poner en marcha el Plan de Continuidad del Negocio, el cual en este escenario estará conformado por:

   - Gerente del Departamento de TI.
   - Técnico Especialista del Departamento de Tecnología de la Información
   - Especialista en Aplicaciones y Desarrollo del Departamento de Tecnología de la Información
   - Técnico en Desarrollo del Departamento de Tecnología de la Información
   - Especialista de Comunicación e infraestructura del Departamento de Tecnología de la Información
   - Técnico en Infraestructura

4. **Convocar a proveedores.**

   De acuerdo con el desastre ocurrido y los daños que tiene el centro de datos, se realiza la llamada a los proveedores, el Coordinador del plan de continuidad del negocio o a su vez el equipo de administración de la crisis inmediatamente deberá contactarse con el proveedor de servicio DRaaS *(Disaster Recovery as a Service)* el cual deberá inmediatamente responder con el levantamiento de los servicios afectados, para así evitar pérdidas de continuidad de negocio de la institución.

5. **Determinar la hora y condiciones del siniestro.**

   Si el desastre llegara a ocurrir en horarios no laborables, se tiene que trasladar al establecimiento de manera inmediata. En este caso el desastre ocurrió en horas de la mañana en la jornada laboral.

6. **Preparar un informe sobre el desastre.**

   Se realiza un informe sobre el desastre y las consecuencias que este tuvo dentro del centro de datos, se completa así la primera etapa de implementación del plan de continuidad del negocio.

- Respuesta inicial.
- Notificación del desastre.

3.4.7.2 Etapa 2: Evaluación del problema y escalamiento

En esta etapa se realiza la recepción del informe por parte del Coordinador del Plan de Continuidad, en el cual se detalla que existe la destrucción total del centro de datos, además la inoperatividad de los servidores los cuales contenían los servicios que se identificaron previamente.

1. **Evaluar la interrupción de los servicios y el daño ocasionado.**
   Determinar cuáles de los nueve servicios fueron afectados, los equipos y recursos en general.
2. **Estimar el impacto del desastre como alto, medio, bajo.**
   De acuerdo con el análisis realizado en el informe entregado al Coordinador de Plan de Continuidad se cataloga el desastre como alto debido a la inoperatividad de los servidores y la destrucción total del centro de datos.
3. **Determinar si se continua con la siguiente fase.**
   Si el desastre no causa la inoperatividad de los servidores, ni de la inaccesibilidad al centro de datos se realiza un monitoreo continuo de la situación, caso contrario continuar a la siguiente fase.

   La elaboración del informe de situación y escalamiento se presenta de la siguiente manera:

Informe de situación y escalamiento No.	#001

Nombre de la emergencia:
Terremoto ciudad de Ambato

Fecha y hora de elaboración del informe:	
Fecha : 29/10/2019	Hora: 08:00 am
Rol que desempeña dentro del Departamento de Tecnología de la Información	
ROL:	Técnico de infraestructura

Area de afectación : Por favor , marque el area afectada del bloque 1 , si la insfraestructura no se encuentra afectada por el siniestro, por favor pase directamente a la descripción del problema.

Preparado por: (Nombre y cargo)

Técnico de infraestructura del Departamento de Tecnología de la Información.

Fuente de información: (Organismos e instituciones de primera respuesta , personal de la Institución)

- Técnico de infraestructura del Departamento de Tecnología de la Información.
- Ecu-911 sala de monitoreo Ambato

1. Descripción de la emergencia
(Resuma de manera descriptiva el evento. Gravedad estimada de los daños. Zonas afectadas)

- El data center ubicado en el último piso del bloque 1 está totalmente destruido.
- Los servidores están inoperativos.
- Se ha determinado que el grado de severidad del impacto es alto, se toma en cuenta los valores predefinidos en la evaluación del impacto operacional que se encuentra en el BIA (Impacto en el negocio), se cataloga como alto impacto en función de los servicios inoperativos que se encontraban dentro de los servidores que se encuentran fuera de servicio.

2. Servicios afectados por el siniestro.
Marque con una X los servicios que están inoperativos.

Servicio	
Repositorio digital Institucional	x
Servidores de Nombres de Dominio	x
Academics	x
Catalogo en línea	x
Laboratorios	x
Impresión web	x
Eduroam	x
Spiceworks	x
Registro biométrico	x
Servicio de sincronización	x
Consultorio jurídico	x

Firma y nombre de responsables del informe Nombre y cargo (o función) de:

Elaborado por:	..... Técnico de infraestructura del Departamento de Tecnología de la Información.

Registro Fotográfico (Adjuntar las fotos de la infraestructura afectada)

3.4.7.3 Etapa 3: Declaración del Desastre.

La decisión de declarar un desastre será declarada en base al informe presentado al Coordinador de plan de continuidad.

1. **Opción de recuperación para la situación actual.**
   Para el presente plan de continuidad del negocio, se ha tomado en cuenta la recuperación mediante servicios *cloud¸* el cual consta del servicio de DRaaS (*Disaster Recovery as a Service),* el mismo que permite la replicación de los servidores, y ponerlos en funcionamiento en un tiempo menor a 1 una hora dada la declaración del desastre.
2. **Preparar la declaración del desastre.**
   - Anuncio del desastre.
   - Fecha y hora del desastre.
   - Categorizar el desastre en nivel: bajo, medio o alto.
   - Seleccionar la opción de recuperación.
   - Informe de la situación de recuperación.
   - Estimación del tiempo de recuperación.
   - Nombre de la autoridad que declara el desastre.
   - Notificar y declarar el desastre a toda la institución.

3.4.7.4 Etapa 4: Plan de implementación de logística

En esta etapa se realiza un monitoreo de los servidores levantados por el proveedor de DRaaS *(Disaster Revovery as a Service)*, este monitoreo estará a cargo del equipo de Administración de la crisis para evaluar el desempeño de los servicios que están levantados en la nube.

Los equipos de Administración de usuarios deberán atender los requerimientos de los clientes, como a su vez solucionar cualquier soporte que se presente post - desastre para evitar problemas de operatividad dentro de la institución.

3.4.7.5 Etapa 5: Recuperación.

Actividades que seguir:

- Asegurar el correcto funcionamiento de los servidores que están el cual funciona en la nube.
- Hay que asegurar que el equipo de administración de usuarios, atiende de manera correcta en temas de soporte.
- Inspeccionar que los servicios que se encuentran dentro de los servidores montados en la nube estén accesibles y con todos los datos correspondientes a los respaldos obtenidos un día anterior.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Se concluye que la fundamentación teórica y metodológica de un plan de continuidad de negocios para un departamento de Tecnología de la Información, permite recuperar de manera oportuna los servicios que estos posean a la disponibilidad de los clientes y usuarios luego de haber ocurrido un desastre.
- Se concluye que el punto de partida fundamental, para la correcta elaboración de un plan de continuidad de negocios es realizar un correcto análisis de impacto en el negocio (BIA), identificando los servicios que permiten responder a las necesidades de la institución.
- Se concluye que el uso de la solución DRaaS para la implementación dentro del plan de continuidad de negocios para la PUCE- Ambato es factible operativamente pues facilitará la respuesta ante desastres que afecten totalmente al centro de datos, además de poder recuperar los servicios que sean afectados.

Recomendaciones.

- Se recomienda que una vez realizado el contrato con el proveedor de servicio DRaaS, es importante tomar en consideración realizar un salto progresivo a la nube, se toma en cuenta en cuenta primero las aplicaciones más críticas a las menos críticas para así tener un mejor control y monitoreo de estas, esto ayudara a mejorar el éxito del plan de continuidad.
- Se recomienda que se realice una difusión del plan de continuidad de negocios al departamento de tecnología de la información, como a las autoridades de la PUCE – A, el cual realiza un énfasis sobre la importancia para la institución invertir en un plan que asegure la continuidad de negocios el cual permita continuar con sus operaciones internas sin irrupciones luego de haber ocurrido un desastre.
- Se recomienda realizar pruebas y mantenimientos al plan de continuidad de negocios, se realiza una retroalimentación sobre los servicios y

procedimientos cada 6 meses para poder tener un plan actualizado y así lograr una respuesta más eficaz ante desastres.

- Se argumenta que el proveedor de servicios de Veeam tiene un mejor puntaje dentro del cuadro de valoración de proveedores , además de ofrecer mejores precios anuales en comparativa a los demás, cabe recalcar que una de las principales ventajas de este proveedor es que el centro de datos y sus servidores trabajan con Veeam por lo cual el tiempo de implementación del servicio una vez realizado el contrato será de un máximo de 30 días, se sugiere que la migración de los servidores sea de manera paulatina, aunque estas policitas son definidas por el proveedor, en este caso Adistec trabaja conjuntamente con Virtual IT quienes son los que proporcionaron la proforma de Veeam.

BIBLIOGRAFÍA

Albarracín Lazo, C. A. (2011). Estudio de la Seguridad Informática y sus aplicaciones para prevenir la infiltración de los Hackers en las empresas (Bachelor's thesis, Quito: Universidad Israel, 2011).

Andres Coles. (2017). Amenazas de Origen antrópico. Recuperado de https://sites.google.com/site/lagestionderiesgosdedesastres/amenazas-y-su-clasificacion/amenazasdeorigenantropico.

Acurio Del Pino, S. (2016). Delitos informáticos: generalidades.

Bautista, M. (2014). Marco de Referencia para la Formulación de un Plan de Continuidad de Negocio para TI, un caso de estudio. Revista Técnica Energía.

Contreras Clunes, A. (2003). Delitos informáticos: un importante precedente. Ius et Praxis, 9(1), 515-521.

Chaves, M. A. (2006). Panorama general de la InformátIca forense y de los delItos InformátIcos en costa rIca. InterSedes: Revista de las sedes regionales, 7(12), 141-154.

Celsia. (2014). Política de Seguridad de la información. Recuperado de https://www.celsia.com/Portals/0/contenidos-celsia/nuestra-empresa/politicas-y-adhesiones/politicas/politica-seguridad-de-la-informacion.pdf

De Leon, J. G. M. P. (2007). Introducción al análisis de riesgos. Editorial Limusa.

Francischetti, C. E., Bertassi, A. L., Camargo, L. S. G., Padoveze, C. L., & Calil, J. F. (2014). El análisis de riesgos como herramienta para la toma de decisiones relativas a inversiones. Invenio, 17(33), 73-85.

Gaona Vásquez, K. D. R. (2013). Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala (Bachelor's thesis).

Gaspar, J., & Martínez, J. G. (2004). Planes de contingencia la continuidad del negocio en las organizaciones. Ediciones Díaz de Santos.

Huidobro, J. (2007). Tecnologías de información y comunicación. Universidad Politécnica de Madrid, 2.

Lara, L. (2006). Vulnerabilidades en ausencia de Seguridad. En L. Lara, Vulnerabilidades en ausencia de Seguridad. Quito: Macrew

Ladines Garcés, K. S. (2017). Plan, informático de contingencia para la seguridad de la información del departamento de TIC de la PUCESE (Doctoral dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación).

Linaza, L. M. A. (2005). Elaboración de un Plan de Emergencia en la Empresa. FC Editorial.

Morales-Soto, N., & Alfaro-Basso, D. (2008). Génesis de las contingencias catastróficas: etiopatogenia del desastre. Revista Peruana de Medicina Experimental y Salud Pública, 25(1), 101-108.

Martínez, M. (2013). Integración de la prevención en las empresas.

Mora Yomayuza David Felipe. (2016). Plan de Continuidad de Negocio Como Base del Éxito Organizacional. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4635/00004908.pdf?sequence=1&isAllowed=y.

Martínez, J. G. (2010). El plan de continuidad de negocio: Una guía práctica para su elaboración. Ediciones Díaz de Santos.

Narváez Morocho, N. E. (2012). Elaboración de un plan de emergencia escolar con niños y niñas de la escuela Víctor Manuel Rendón. Cantón Balzar. PU Santa Lucía. 2012 (Bachelor's thesis, Escuela Superior Politécnica de Chimborazo).

Paul Kirvan. (2013). Cómo construir un Plan de Respuesta a Incidentes. Recuperado de: https://searchdatacenter.techtarget.com/es/consejo/Como-construir-un-Plan-de-Respuesta-a-Incidentes

Pazmiño Linzán, M. A. (2017). Implementación de un plan de emergencia en la estación de servicio Petrocomercial Ponceano (Master's thesis, Quito, 2017.).

Pulido, S. C. H., Guerrero, E. J., Chavarro, K. P. V., & Soto, N. E. M. (2013). Formulación del plan de emergencias y contingencias para la Facultad Tecnológica de la Universidad Distrital Francisco José de Caldas. Tekhnê, 10(1), 49-62.

Pinto, M. G. H., & Sánchez, B. A. N. (2016). Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial. Obtenido de Escuela Superior Politécnica del Litoral: https://www. dspace. espol. edu. ec/retrieve/94448/D-71165. pdf.

Rodríguez Carrillo, A. M. (2014). Análisis y diagnóstico de la Seguridad Informática de Indeportes Boyacá.

Ramírez Ponce, J. A. (2014). Elaboración de un plan de emergencia y desarrollo e implementación del plan de contingencia, ante el riesgo de un incendio en el

Palacio del Muy Ilustre Municipio de Guayaquil (Master's thesis, Universidad de Guayaquil. Facultad de Ingeniería Industrial. Maestría en Gestión de Riesgos y Desastres.).

Santán, L., & Delti, R. (2010). Plan de contingencia informático para el conjunto de bodegas Parkenor (Bachelor's thesis, SANGOLQUÍ/ESPE/2010).

Shirly Marcela Ardila. (2016). Planes de Contingencia. Recuperado de: http://www.uninavarra.edu.co/wp-content/uploads/2016/12/GT-PL-02-PLAN-DE-CONTIGENCIA-INFORMATICO-1-1.pdf

Tarazona, T., & Cesar, H. (2007). Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología, 28, 137.

Torres, Cesar. (2017) LA IMPORTANCIA DE REALIZAR UN ANÁLISIS DE RIESGO EN LAS EMPRESAS. Recuperado de http://polux.unipiloto.edu.co:8080/00003266.pdf.

Vmware, 2016. Soluciones Virtuales. Recuperado el 20 de septiembre de 2016, de https://www.vmware.com/cl/products/vsphere/features/virtual-volumes

Weller A., 2013. Tipos de Computación en la Nube. Recuperado el 24 de septiembre de 2016, de https://www.crucial.com.au/blog/2013/05/27/types-of-Cloud-Computing/

ANEXO 1.

Entrevistas y Encuestas

Pontificia Universidad Católica del Ecuador | Sede Ambato

Objetivo:

La presente entrevista tiene como objetivo determinar los requerimientos y características del plan de continuidad de negocios para la Pontificia Universidad Católica del Ecuador – Ambato

Por favor sírvase contestar de la manera más detallada las siguientes preguntas.

Entrevista

1. ¿Describa la arquitectura de comunicación entre el departamento de TI y las distintas unidades académicas, recursos humanos y sistema financiero?
2. ¿Qué cantidad promedio de Gigas de información se tramitan y se almacenan durante el semestre?
3. ¿Cuál es el tiempo estimado en la resolución adecuada de incidencias provenientes de las diferentes unidades académicas, recursos humanos y sistema financiero?
4. ¿Qué información proveniente de las diferentes unidades académicas, recursos humanos y sistema financiero se almacena de manera digital?

5. ¿Cuáles es la información más crítica y/o importante que se maneja dentro del Departamento de Tecnologías de la Información?
6. ¿Conoce usted que función cumple un Plan de Continuidad de Negocios?

7. ¿Cree usted factible que el Departamento de Tecnologías de la información cuente con un sistema de respaldo de la información los mismos que en caso de alguna vulnerabilidad se pongan en marcha mediante servicios CLOUD como es el DRass (*Disaster Recovery as a Service*)? Si su respuesta es SI describa las ventajas que obtendría, si su respuesta es NO porque lo considera así.
8. ¿Considera usted que un Plan de Continuidad de Negocios ayudará a una rápida recuperación de los servicios que el en caso de algún desastre o vulnerabilidad de la información proveniente de las diferentes unidades académicas, recursos humanos y sistema financiero?
9. ¿Qué aspectos considera importante que deben estar inmersos en el Plan de Continuidad de Negocios para poder recuperar de manera rápida y eficiente los servicios provenientes de las diferentes unidades académicas, recursos humanos y sistema financiero?

Anexo 2.

Pontificia Universidad Católica del Ecuador | Sede Ambato

Objetivo:

La presente entrevista tiene como objetivo determinar el impacto financiero que ocasionaría la interrupción de los servicios que brinda el departamento de tecnologías de la información hacia la comunidad universitaria.

Por favor sírvase contestar de la manera más detallada las siguientes preguntas.

Entrevista

1. Cree usted que exista perdida financiera al momento de ocurrir una catástrofe ya sea natural o causada por el hombre, dentro de la universidad la cual ocasionaría la interrupción de los siguientes servicios:
    - Academics
    - Registro Biométrico

Anexo 3

Encuesta

Pontificia Universidad Católica del Ecuador | Sede Ambato

Objetivo:

La presente encuesta tiene como objetivo determinar los requerimientos y características del plan de continuidad de negocios.

Por favor sírvase a contestar de la manera más detallada las siguientes preguntas.

1) ¿Ha escuchado hablar sobre un plan de continuidad del negocio?

_____ SI

_____ No (pase a la pregunta número 3)

2) ¿Qué significa para usted un plan de continuidad del negocio?

3) ¿En el departamento de TI hay implementado un plan de continuidad del negocio?

   _____ SI (explique qué características tiene el plan de continuidad de negocios)

   _____ NO

4) ¿Existe un plan de contingencia En el caso de que sus procedimientos normales fallen?

   _____ SI (mencione cual es el plan de contingencia)

   _____ NO

5) Dentro de sus funciones cuales son las actividades más críticas que usted realiza.
6) ¿La interrupción en el funcionamiento normal de su departamento generaría alguna implicación legal en caso de que se interrumpa dicha actividad?
7) Identifique el período de mayor trabajo del año. ¿Hay alguna precaución en el caso de que se presente una emergencia en ese lapso?
8) ¿Con cuáles herramientas (software, entre otros) necesita para desarrollar sus funciones?
9) ¿Cuáles son los servicios que brinda su departamento?
10) Normalmente, ¿cuentan con procedimientos para reemplazar el equipo vital de la planta/edificio y suministros para prevenir en caso de que se presente un desastre? (justifique su respuesta)

    _____ SI

    _____ NO

Anexo 4

Cotización Virtual IT

VIRTUALIT

Virtual IT S.A.
Gaspar de Escalona N38-39
y Villalengua - Quito
RUC: 1792018080001
593-23-815952

COTIZACIÓN

Nro.:	VITQ7358
Fecha	May 28, 2019
Vendedor:	Carlos Arauz

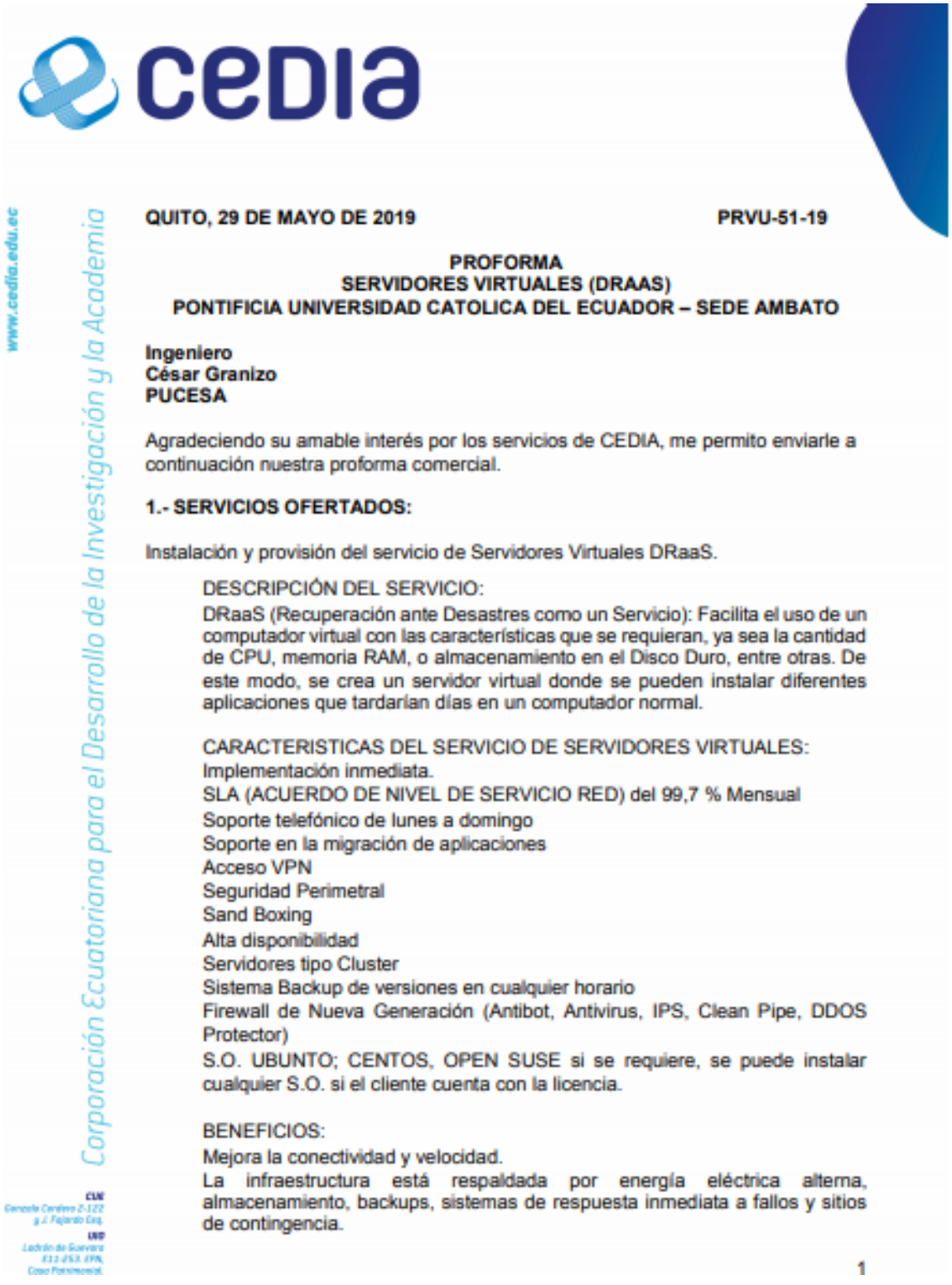
Cotización Para:	Enviar a:
Pontificia Universidad Católica del Cesar Andrés Granizo Medina	Pontificia Universidad Católica del Cesar Andrés Granizo Medina

Validez de la Oferta:	30 días
Forma de Pago:	80% a la orden de compra y 20% a la entrega del los servicios contratados
Tiempo de Entrega	30 días una vez recibido el anticipo

Cant.	Descripción	Precio Unitario	Precio Extendido
	BACKUP AS A SERVICE BAAS		
1	Veeam Cloud Connect Storage - 1TB Monthly, 5MBps IBW, 1 IP, 8x5 Support PN: ACP-VCC-STORAGE-1TB-1M	$69,52	$69,52
11	Veeam Cloud Connect Backup (SP) - Server - (Lic by Agent) - Monthly PN: ACP-H-CCEBCK-0R-R0000-19	$9,99	$109,89
11	Veeam Agent Server (On-Premise) - by Server - Monthly PN: ACP-H-VAG000-0R-R0000-19	$13,31	$146,41
	DISASTER RECOVERY AS A SERVICE DRAAS		
1	DR 20% - M - Monthly - vCPU 10GHz, vRAM 48GB , Std 1TB, 5 Mbps IBW, 1 IP, 8x5 Support PN: ACP-DR20-C10-R48-S1T-N05-M-1M	$197,47	$197,47
1	1 x Public IP Address, Monthly PN: ACP-NET-IP-ADD-1-1M	$27,73	$27,73
1	Veeam Cloud Connect Storage - 1TB Monthly, 5MBps IBW, 1 IP, 8x5 Support PN: ACP-VCC-STORAGE-1TB-1M	$69,52	$69,52
11	Veeam Cloud Connect Replica (SP) - (Lic. by VM) - Monthly PN: ACP-H-CCEREP-0V-R0MNC-17	$15,16	$166,76
11	Veeam Backup & Replication Ent. for VMware - (Lic. by VM) - Monthly PN: ACP-H-VBRENT-VV-R0MNC-17	$11,37	$125,07
1	Implementación Solución Disaster Recovery As a Service DRAAS. Tareas: Instalación de Consola Veeam Backup and Replication Instalación de Veeam Enterprise Manager Configuración de servidores ESXi a respaldar y máquinas a replicar Configuración de Veeam Proxi Configuración de Veeam Repository Configuración de Jobs de Backup y Réplica Pruebas funcionales Memoria Técnica	$2.600,00	$2.600,00
20	Horas de soporte Post Implementación	$60,00	$1.200,00
1	Capacitación de Respaldos y Replicación con VEEAM BACKUP AND REPLICATION	$800,00	$800,00
	Notas:	**Subtotal:**	**$5.512,37**

Anexo 5

Cotización Cedia



www.cedia.edu.ec

Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia

CUE
Gonzalo Cordova E-122
y J. Tejada Esq.

UIO
Ladrón de Guevara
E11-253. EPN,
Casa Patrimonial.

QUITO, 29 DE MAYO DE 2019 **PRVU-51-19**

PROFORMA
SERVIDORES VIRTUALES (DRAAS)
PONTIFICIA UNIVERSIDAD CATOLICA DEL ECUADOR – SEDE AMBATO

Ingeniero
César Granizo
PUCESA

Agradeciendo su amable interés por los servicios de CEDIA, me permito enviarle a continuación nuestra proforma comercial.

1.- SERVICIOS OFERTADOS:

Instalación y provisión del servicio de Servidores Virtuales DRaaS.

DESCRIPCIÓN DEL SERVICIO:
DRaaS (Recuperación ante Desastres como un Servicio): Facilita el uso de un computador virtual con las características que se requieran, ya sea la cantidad de CPU, memoria RAM, o almacenamiento en el Disco Duro, entre otras. De este modo, se crea un servidor virtual donde se pueden instalar diferentes aplicaciones que tardarían días en un computador normal.

CARACTERISTICAS DEL SERVICIO DE SERVIDORES VIRTUALES:
Implementación inmediata.
SLA (ACUERDO DE NIVEL DE SERVICIO RED) del 99,7 % Mensual
Soporte telefónico de lunes a domingo
Soporte en la migración de aplicaciones
Acceso VPN
Seguridad Perimetral
Sand Boxing
Alta disponibilidad
Servidores tipo Cluster
Sistema Backup de versiones en cualquier horario
Firewall de Nueva Generación (Antibot, Antivirus, IPS, Clean Pipe, DDOS Protector)
S.O. UBUNTO; CENTOS, OPEN SUSE si se requiere, se puede instalar cualquier S.O. si el cliente cuenta con la licencia.

BENEFICIOS:
Mejora la conectividad y velocidad.
La infraestructura está respaldada por energía eléctrica alterna, almacenamiento, backups, sistemas de respuesta inmediata a fallos y sitios de contingencia.

1

2.- COSTOS DE LA PROPUESTA

Instalación

ITEM	DESCRIPCION	CANT	PRECIO	SUB TOTAL
1	Instalación Servidores Virtuales	11	$ 80,00	$ 880,00
TOTAL INSTALACIÓN USD				**$ 880,00**

Licenciamiento Anual

ITEM	DESCRIPCION	CANT (AÑOS)	PRECIO	SUB TOTAL
1	Licenciamiento Veeam (para 11 instancias)	3	$1.980	$ 5.940
TOTAL LICENCIAMIENTO USD (3 AÑOS)				$ 5.940

Servicios Mensuales

ITEM	DESCRIPCION	CANT	PRECIO	SUB TOTAL
1	• Servidor 1 o 8 vCPU o 4 GB RAM o 185 GB HDD	1	$ 134,12	$ 134,12
2	• Servidor 2 o 8 vCPU o 4 GB RAM o 105 GB HDD	1	$ 130,92	$ 130,92
3	• Servidor 3 o 8 vCPU o 5 GB RAM o 205 GB HDD	1	$ 137,86	$ 137,86
4	• Servidor 4 o 8 vCPU o 2 GB RAM o 25 GB HDD	1	$ 121,84	$ 121,84
5	• Servidor 5 o 8 vCPU o 4 GB RAM o 85 GB HDD	1	$ 130,12	$ 130,12
6	• Servidor 6 o 8 vCPU o 10 GB RAM	1	$ 160,96	$ 160,96

	○ 415 GB HDD			
7	• Servidor 7 ○ 8 vCPU ○ 4 GB RAM ○ 85 GB HDD	1	$ 130,12	$ 130,12
8	• Servidor 8 ○ 8 vCPU ○ 8 GB RAM ○ 390 GB HDD	1	$ 154,08	$ 154,08
9	• Servidor 9 ○ 8 vCPU ○ 4 GB RAM ○ 410 GB HDD	1	$ 143,12	$ 143,12
10	• Servidor 10 ○ 8 vCPU ○ 8 GB RAM ○ 155 GB HDD	1	$ 144,68	$ 144,68
11	• Servidor 11 ○ 8 vCPU ○ 2 GB RAM ○ 85 GB HDD	1	$ 124,24	$ 124,24
TOTAL SERVICIOS MENSUALES USD				**$ 1.512,06**

VALOR TOTAL DE LA PROPUESTA

ITEM	DESCRIPCION	SUB TOTAL
1	Instalación Servidores Virtuales	$ 880,00
2	Licenciamiento (3 años)	$ 5.940,00
3	Servicios mensuales (36 meses)	$ 54.434,16
VALOR TOTAL DEL CONTRATO (36 MESES)		**$ 61.254,16**

3.- FORMA DE PAGO

- Instalación: 100% a la presentación de la primera factura
- Licenciamiento anual: Valor por un año de licencia junto con las primeras facturas de los años 1, 2 y 3
- Servidores Virtuales: Mensualmente contra presentación de factura

4.- DETALLES DE LA PROFORMA

Validez: 60 días.

Impuestos: Los costos de la presente no contemplan impuestos de ley.

Anexo 6

Cotización Binaria IT

binaria INNOVATION

binaria IT SERVICES

Propuesta Económica

La propuesta referencial incurre en los siguientes valores:

La propuesta económica es la siguiente:

Inversión requerida en base a asignación de recursos	
Descripción	**INVERSION**
Servicios profesionales. (un solo pago)	$ 6,010,00
Espacio de almacenamiento (mensual)	$ 450,00
Infraestructura virtual en Azure (mensual)	$ 2.300,00

- Costos no incluyen impuestos de ley.
- Validez de la oferta 15 días
- Forma de pago: Contado
- Tiempo de entrega: por coordinar referencial de 10 a 15 días.
- Servicio a desarrollarse en la ciudad de Ambato

Anexo 7

Política de Respaldo

Católica del Ecuador | Ambato	respaldar	**Fecha Aprobación:** 27/09/2017 **Fecha Modificación:** 27/09/2017 **Revisión:** 01
Elaborado por: Ing. Eduardo Remache, Ing, Gabriel Altamirano, Mg. Mónica Mena	**Revisado por:** Ing. Gabriel Altamirano	**Aprobado por:** Ing. Gabriel Altamirano

POLÍTICA DE RESPALDO DE INFORMACIÓN DE LA PUCE SEDE AMBATO

Propósito

La presente política tiene como objetivos proteger los datos, aplicaciones y servicios informáticos contra todo tipo de fallas o desastres tecnológicos, y establecer directrices que posibiliten la recuperación de la información en el menor tiempo posible.

Alcance

La aplicación de esta política se extiende a toda la información alojada en servidores físicos y virtuales, equipos de comunicación y estaciones de trabajo que contengan datos, aplicaciones y configuraciones de la PUCE Sede Ambato. Así también, rige para todos los usuarios con cargos administrativos y de docencia que presten servicios a la institución.

La PUCE Sede Ambato a través de su Prorrectorado garantizará y facilitará la adquisición de ambientes físicos y virtuales, como también licencias para la correcta ejecución de la presente política.

Fuentes de Información a Respaldar

La información susceptible de respaldo se encuentra categorizada de la siguiente forma:

- Servidores físicos y virtuales (Ver Anexo 2, Anexo 3, Anexo 4):
  - Bases de datos
  - Código fuente
  - Archivos de configuración
  - Aplicaciones
  - Instaladores
- Equipos de comunicación (Ver Anexo 5):
  - Archivos de configuración
- Equipos de personal administrativo y docente:
  - Documentación institucional individual y colaborativa.

Tipos de Respaldo

- Servidores virtuales: completo e incremental.
- Bases de datos en servidores físicos: completo.
- Equipos de comunicación: completo, luego de cada cambio realizado.
- Equipos del personal administrativo y docente: libre elección del usuario propietario de la información, quien será el responsable absoluto sobre la gestión de la misma.

Regla de Respaldo

La PUCE Sede Ambato aplicará la regla 3-2-1, para el respaldo de la información alojada en su Centro de Datos:

- Por lo menos 3 copias:
  - La primera, en el servidor de producción.

- La segunda, direccionada al sistema de almacenamiento del Centro de Datos de la Universidad (storage).
- La tercera, direccionada al sitio de almacenamiento local alterno (que no sea el storage), del Centro de Datos de la Universidad.

- En 2 medios diferentes:
  - El primero, en el sistema de almacenamiento del Centro de Datos de la Universidad (storage)
  - El segundo, en un sitio de almacenamiento local alterno (que no sea el storage), del Centro de Datos de la Universidad.
- 1 Copia física en otro lugar
  - Una copia de información se localizará en la nube (semanalmente).

La PUCE Sede Ambato facilitará un espacio en la nube, para el respaldo de información institucional tanto individual y colaborativa alojada en equipos del personal administrativo y docente (ver Anexo 6 y Anexo 7).

Horarios de Generación de Respaldos

Los respaldos se realizarán en horarios que no saturen el tráfico de la red, en general entre las 19h00 y 03h00 del día siguiente.

Codificación de Respaldos

- Los nombres de los respaldos deberán tener la siguiente estructura:
  - [Nombre de la aplicación-Fecha de respaldo (aaaa-mm-dd)]
- Los directorios donde se almacenarán los respaldos serán estructurados, así:
  - [Nombre de la aplicación]/[Nombre del respaldo]

Herramientas de Respaldo

- Herramientas propias de las bases de datos instrumentadas automáticamente a través de tareas programadas en el sistema operativo de cada servidor.
- En el caso de servidores virtuales y físicos se usará una solución empresarial de respaldo y disponibilidad, que proporcione una recuperación rápida, flexible y confiable de aplicaciones y datos virtualizados. Se deberá considerar el uso de software especializado para respaldos y un agente para la copia del mismo hacia la nube (ver Anexo 1).
- En el caso de equipos locales, se usará un agente que permita la sincronización de información hacia la nube (ver Anexo 1 y Anexo 7).

Retención y Restauración

- **Retención / RPO (Recovery Point Objective):** 24 horas, como punto de recuperación objetivo.
- **Restauración / RTO (Recovery Time Objective):** 6 horas máximo, como tiempo de recuperación objetivo (Ver Anexo 8).

Pruebas de Restauración

Las herramientas adquiridas por la PUCE Ambato deben garantizar la integridad de la información en los respaldos generados.

Archivo

La información destinada al archivo será la correspondiente a la de cinco años atrás. Considerando la fecha más antigua, la de aprobación de la presente política.

Baja de Aplicaciones

El descarte de aplicaciones implicará, una solicitud por parte del propietario de la información y la autorización por parte de la Jefatura del Departamento de TI.

Responsabilidades

Departamento / Área	Responsabilidades					
	1	2	3	4	5	6
TI / Jefatura	X	X			X	X
TI / Plataformas	X	X	X	X		X
TI / Infraestructura	X	X	X	X		
TI / Desarrollo	X					
TI / Soporte	X					
Académica	X					
Administrativa	X					

1. Notificar nuevas fuentes de información a respaldar (Ver Anexo 6).
2. Mantener operativas las herramientas y medios de respaldo.
3. Planificar, ejecutar y monitorear respaldos.
4. Planificar, ejecutar y monitorear resturación de respaldos.
5. Autorizar solicitudes de respaldo y resturación de los mismos.
6. Mantener actualizada la política.

Anexos:

Anexo 1: Herramientas de Respaldo

Herramienta	Propósito de respaldo
Veeam Backup & Replication	Servidores virtuales.
Cobian Backup	Gestión de respaldos.
Microsoft Azure Backup	Agente para copia de respaldo hacia la nube.
Microsoft One Drive Empresarial	Agente para sincronización hacia la nube.
Microsoft SharePoint Online	Plataforma de colaboración empresarial.

Anexo 3: Servidores Virtuales a Respaldar

SERVIDOR	APLICACIÓN	RESPONSABLE	FRECUENCIA	HORA	TIPO RESPALDO	FORMA
DSPACEPUCESA	REPOSITORIO DIGITAL DSPACE	ASISTENTE DE PLATAFORMAS	DIARIO	1:30 AM	COMPLETO	AUTOMÁTICO
EDUROAM01	EDUROAM-CEDIA	ASISTENTE DE PLATAFORMAS	SEMANAL (DOMINGOS)	11:30 PM	COMPLETO	AUTOMÁTICO
FILEAMB01	PAPERCUT	ASISTENTE DE PLATAFORMAS	SEMANAL (DOMINGOS)	2:00 AM	COMPLETO	AUTOMÁTICO
FILEAMB02	INVENTARIO TALLER	ASISTENTE DE PLATAFORMAS	MENSUAL (PRIMER DOMINGO)	12:30 AM	COMPLETO	AUTOMÁTICO
	MANTENIMIENTOS PUCESA					
	TURNOS					
	INVENTARIO SUMINISTROS					
FireSigth Cisco ASA	FIREWALL	ASISTENTE DE PLATAFORMAS	SEMANAL (DOMINGOS)	12:00 AM	COMPLETO	AUTOMÁTICO
PRDAMB01	ACADEMICS	ASISTENTE DE PLATAFORMAS	DIARIO	1:00 AM	COMPLETO	AUTOMÁTICO
	CONTROL LABORATORIOS					
	CONTROL MEDICO					
	BOLSA DE EMPLEO PARA TRABAJADORES					
	CONSULTORIOS JURIDICOS GRATUITOS					
SIABUCAMB01	SIABUC - CATALOGO EN LINEA	ASISTENTE DE PLATAFORMAS	DIARIO	2:30 AM	COMPLETO	AUTOMÁTICO
TABLERO	TABLERO DE CONTROL	ASISTENTE DE PLATAFORMAS	DIARIO	3:00 AM	COMPLETO	AUTOMÁTICO

Anexo 8

Plan de continuidad del negocio.

Pontificia Universidad Católica del Ecuador | Sede Ambato	Plan de continuidad del negocio	**Fecha de revisión: 21/10/2017**
		Fecha de aprobación: 21/10/2017
		Revisión: 01
Elaborado por: César Andrés Granizo Medina	**Revisado por**: Ing. Gabriel Altamirano	**Aprobado por:** Ing. Gabriel Altamirano

Plan de Continuidad del negocio.

Una vez ocurrido un desastre la persona encargada de liderar la recuperación ante desastres es el Gerente del Departamento de Tecnología de la Información, quien luego del desastre convoca inicialmente a los miembros del departamento de Tecnología de la Información para realizar la evaluación del sitio afectado.

1. Centro de reuniones alternativo en caso de desastre.

Una vez realizada la evaluación del sitio afectado y acorde al tipo de desastre se tiene las siguientes prioridades de puntos de encuentro para la reunión de los miembros del departamento de Tecnología de la Información.

1) Si el bloque 1 luego del desastre es accesible:

Punto de reunión

- PUCE – Ambato / Bloque 1 – 4to piso

Sala de reuniones localizada en el 4to piso

2) Si el bloque 1 luego del desastre es inaccesible:

Punto de reunión

- PUCE – Ambato / Cualquier localización dentro de la universidad con acceso a internet

3) **Si la Sede luego del desastre es inaccesible:**

Punto de reunión.

- Sala virtual de reuniones del personal de TI

4) **Si el desastre afecto a la ciudad:**

Canales de comunicación.

- Sala virtual de reuniones del personal de TI.

5) **Equipo para la Continuidad del Negocio.**

Para la implementación del Plan de Continuidad del negocio para la PUCE – Ambato se define el equipo el cual se encargará de la recuperación y levantamiento de servicios los cuales ofrece el Departamento de Tecnología de la Información.

Para el Departamento de Tecnología de la Información de la PUCE – Ambato los miembros del equipo serán de 8 personas que conforman el Departamento de TI.

La estructura que el equipo del Plan de Continuidad del Negocio se muestra a continuación.

La estructura para la elaboración de la siguiente figura fue tomada de: Syed, Akhytar, *Business Continuity Planning Methology*; 2004

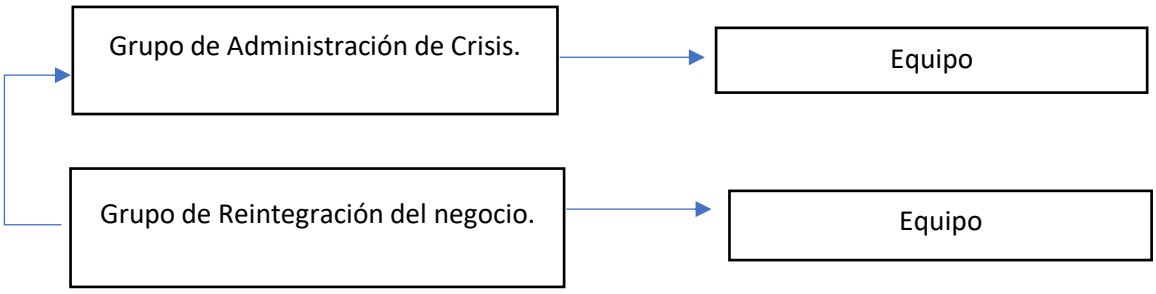


Gráfico 1.1: Estructura del equipo del Plan de Continuidad del Negocio

Fuente: elaboración propia

Imagen adaptada de: Syed, Akhytar, Business Continuity Planning Methology; 2004

2. Grupo de Administración de la Crisis

2.1 Equipo de Administración de la Crisis (CTM- Crisis Managment Team): Roles:

Este equipo se encarga de la administración y control del Plan de Continuad del Negocio, una vez ocurrido el desastre el CTM se traslada al centro de administración del desastre, dado el caso al sitio alternativo designado, el CTM es el que está autorizado de solicitar el Plan de Continuidad del Negocio en caso de ser necesario.

2.2 Coordinador del Plan de Continuidad del Negocio

Es el encargado de supervisar la respuesta inicial y notificación del desastre, evaluación de daños, escalamiento, recuperación y levantamiento de servicios afectados.

2.3 Equipo de Evaluación de Daños (DAT- Damage Assessment Team)

Es el equipo el cual se encarga de realizar la evaluación de daños una vez ocurrido el desastre para si determinar el tiempo que tomara la recuperación física del centro de datos.

2.4 Equipo de Comunicación de la Crisis (CCT – Crisis Comunication Team)

Es el equipo responsable de proveer la información a todo el personal sobre el evento ocurrido, esta información debe ser oportuna y exacta

2.5 Equipo de Administración de Usuarios (UMT- User Management Team)

Es el equipo encargado de mediar e interactuar con los usuarios luego de ocurrido el desastre, para solventar dudas, inquietudes sobre los servicios que puedan estar caídos.

2.6 Grupo de reintegración del negocio:

2.6.1 Equipo de Unidades del Negocio (BUT- Business Unit Team)

Es un equipo conformado por una persona clave de cada área del departamento de Tecnología de la Información, los cuales evalúan las necesidades de su área una vez suscitado el desastre e informan al coordinador del plan de continuidad del negocio.

2.6.2 Asignación del Personal

Para el presente Plan de continuidad del negocio se ha tomado en consideración a las 8 personas que conforman el departamento de Tecnología de la Información, en la cual cada miembro debe cumplir una o varias tareas:

Departamento Tecnologías de la Información Puce - A	Gerente del departamento	Técnico multimedia	Especialista en aplicaciones y desarrollo	Técnico en desarrollo	Especialista de comunicación	Técnico en infraestructura
Equipo de Administración de Crisis	x	x	x		x	
Coordinador de la continuidad del negocio	x					
Equipo de evaluación de daños	x	x	x	x	x	x
Equipo de comunicación de la crisis	x	x	x	x	x	x
Equipo de administración de usuarios.	x	x	x	x	x	x
Equipo de unidades del negocio		x	x	x	x	x

Cuadro 1.1: Matriz de responsabilidades

Fuente: elaboración propia

Imagen adaptada de: Responsibility assignment matrix (RACI)

Gerente del Departamento de TI.

f) Equipo de Administración de la Crisis.
g) Coordinador de la Continuidad del negocio.
h) Equipo de evaluación de daños.
i) Equipo de Comunicación de la Crisis.

j) Equipo de administración de usuarios.

Técnico multimedia del Departamento de Tecnología de la Información.

f) Equipo de Administración de la Crisis.
g) Equipo de evaluación de daños.
h) Equipo de Comunicación de la Crisis.
i) Equipo de administración de usuarios.
j) Equipo de unidades de negocio.

Especialista en Aplicaciones y Desarrollo del Departamento de Tecnología de la Información.

f) Equipo de Administración de la Crisis
g) Equipo de evaluación de daños
h) Equipo de Comunicación de la Crisis
i) Equipo de administración de usuarios
j) Equipos de unidades de negocio

Técnico en Desarrollo del Departamento de Tecnología de la Información.

e) Equipo de evaluación de daños.
f) Equipo de Comunicación de la Crisis.
g) Equipo de administración de usuarios.
h) Equipos de unidades de negocio.

Especialista de Comunicación e infraestructura del Departamento de Tecnología de la Información.

f) Equipo de evaluación de daños.
g) Equipo de Comunicación de la Crisis.
h) Equipo de administración de usuarios.
i) Equipos de unidades de negocio.
j) Equipo de administración de la Crisis.

Técnico en Infraestructura.

e) Equipo de evaluación de daños.
f) Equipo de Comunicación de la Crisis.
g) Equipo de administración de usuarios.
h) Equipos de unidades de negocio.

2.7 Actividades para la ejecución del Plan de Continuidad del Negocio

Para una correcta implementación del Plan de continuidad del negocio se sigue una serie de pasos que ayuden a mejorar de forma óptima la administración de un desastre, se minimiza el tiempo de recuperación y retorno a las actividades normales de la institución, para restablecer lo más antes posible las comunicaciones, servicios, que se brinda a los usuarios, para esta recuperación cabe recalcar que se utilizarán los servicios de la nube : DRaaS *(Disaster Recovery as a Service)* el cual permite una rápida recuperación de la continuidad del negocio.

Las actividades que se detallan a continuación están tomadas como referencia del libro Syed, Akhar; Syed, Afsar; Business Continuity Planning Methodology: 2004 y adaptadas a las necesidades y recursos del Departamento de Tecnología de la Información.

2.7.1 Respuesta inicial y notificación.

En esta etapa una vez sucedida el desastre, se evalúa el impacto de daños, todos los miembros del plan de continuidad son notificados y el plan es activado, se ha definido un conjunto de actividades:

- Definir el lugar de reunión del equipo de la continuidad del negocio
- Cada miembro del departamento de tecnología de la información recibe la notificación del desastre por parte del equipo de comunicación de la crisis, el cual previamente ya se definió.
- El Coordinador del plan de continuidad del negocio o a su vez el equipo de administración de la crisis se encargará de informar a los proveedores de DRaaS *(Disaster Recovery as a Service)* sobre el desastre ocurrido.
- Determinar si el edificio es accesible.
- Si el desastre ocurre en horas no laborables, trasladarse a la institución de manera inmediata.
- Evaluación de daños al centro de datos.
- Evaluación del impacto del desastre al centro de datos.
- Preparar un informe del desastre y los daños que este ocasiono al centro de datos, este informe deberá ser elaborado por el equipo encargado de la crisis

y el equipo de evaluación de daños y presentado al Coordinador del plan de continuidad.

El informe permitirá conocer la idea global del problema para alimentar el plan de continuidad, se detalla el impacto y los daños causados por el desastre.

2.7.2 Evaluación del problema y escalamiento.

En esta etapa se determinará la magnitud del desastre basado en el informe anteriormente presentado.

Las actividades que seguir son las siguientes.

- Recepción del informe por parte del Coordinador del Plan de Continuidad.
- Revisión de la magnitud del impacto de los daños en el informe presentado.
- Inspeccionar el sitio del desastre para así evaluar el impacto causado por la interrupción.
- Evaluar la interrupción de servicios y el daño en el centro de datos.
- Identificar los servicios que fueron afectados y fuera de funcionamiento, en el caso de no ocurrir daños a los servicios, ni a los servidores del centro de datos, se realiza un monitoreo de situación, caso contrario seguir con la siguiente fase.
- Se realiza un informe por parte del equipo de Administración de Crisis, Equipo de evaluación de daños e informar al Coordinador del Plan de continuidad del negocio.

2.7.3 Declaración del Desastre.

La decisión de declarar el desastre está a cargo del Coordinador del Plan de continuidad del negocio, esta decisión se basará en el informe entregado por parte del equipo de Administración de Crisis.

Las actividades que seguir son las siguientes:

1. Revisar el informe detallado del problema, se analiza la magnitud del desastre y los impactos que este causo al centro de datos.
2. Una vez declarado el desastre el Coordinador del plan de continuidad del negocio o a su vez el equipo de administración de la crisis inmediatamente deberá contactarse con el proveedor de servicio DRaaS *(Disaster Recovery as a Service)* el cual deberá inmediatamente responder con el levantamiento de los servicios afectados, para así evitar pérdidas de continuidad de negocio de la institución.

2.7.4 Plan de implementación de logística

En esta etapa se realiza un monitoreo de los servidores levantados por el proveedor de DRaaS *(Disaster Revovery as a Service)*, este monitoreo estará a cargo del equipo de Administración de la crisis para evaluar el desempeño de los servicios que están levantados en la nube.

Los equipos de Administración de usuarios deberán atender los requerimientos de los clientes, como a su vez solucionar cualquier soporte que se presente post - desastre para evitar problemas de operatividad dentro de la institución.

Se toma en cuenta que el punto de restauración objetivo de los servicios es 1 hora, esto quiere decir que luego de declararse el desastre, los servicios que estén inoperativos estarán en funcionamiento en un máximo de una hora.

2.7.5 Recuperación.

En esta etapa una vez pasado las 24 horas de ocurrido el desastre, el Coordinador del plan de continuidad, deberá preparar un informe detallado de los servicios que están levantados en la nube, además de informar a los demás miembros del departamento de tecnología de la información que los servicios que estaban afectados ahora se encuentran totalmente operativos y funcionales.

2.7.6 Simulacro

El presente simulacro de desastre el cual se considerará la caída del bloque 1, a causa de un terremoto el cual origina la destrucción total del centro de datos de la Pontificia Universidad Católica del Ecuador - Ambato. Los servidores en los cuales se encontraban almacenados los 9 servicios previamente identificados están totalmente inoperativos, se asume que el desastre ocurrió un martes en la mañana en el periodo semestral septiembre - diciembre.

Este desastre causo la perdida de continuidad operativa de los 9 servicios previamente identificados el cual causas inconvenientes a la comunidad universitaria.

A continuación, se describen las acciones a tomarse para el levantamiento de los servicios afectados, lo cual permite la continuidad del negocio.

2.7.7 Escenario del plan de continuidad.

2.7.7.1 Etapa 1: Respuesta Inicial y Notificación.

Se registra la siguiente información.

1. **Registrar las personas que notaron el desastre**
   Identificar a la persona que se dio cuenta de la ocurrencia del desastre, fecha y hora.
   En este escenario la persona que se dio cuenta fue el Técnico de infraestructura a las 7:00 AM del martes el cual notifico
2. **Definir el lugar de reunión del equipo de continuidad.**
   Debido a que el desastre afecto a todo el bloque 1 el cual ocasiona la destrucción total del centro de datos, se define el lugar de reunión del equipo de continuidad dentro de la universidad pues el sitio si es accesible.
   El Departamento de Tecnología de la Información hace un breve análisis del desastre.

Se definen las características del desastre:

1. El data center ubicado en el último piso del bloque 1 está totalmente destruido.
2. Los servidores están inoperativos.
3. Se ha determinado que el grado de severidad del impacto es alto, se toma en cuenta los valores predefinidos en la evaluación del impacto operacional que se encuentra en el BIA (Impacto en el negocio), se cataloga como alto impacto en función de los servicios inoperativos que se encontraban dentro de los servidores que se encuentran fuera de servicio.
4. **Cada miembro del equipo recibe la alerta del desastre.**

   En esta etapa es necesario definir si se necesita la presencia de todo el Departamento de Tecnología de la información para poner en marcha el plan de continuidad.

   En este escenario es necesario convocar a todo el Departamento de Tecnología de la Información para poner en marcha el Plan de Continuidad del Negocio, el cual en este escenario estará conformado por:

   - Gerente del Departamento de TI.
   - Técnico Especialista del Departamento de Tecnología de la Información
   - Especialista en Aplicaciones y Desarrollo del Departamento de Tecnología de la Información
   - Técnico en Desarrollo del Departamento de Tecnología de la Información
   - Especialista de Comunicación e infraestructura del Departamento de Tecnología de la Información
   - Técnico en Infraestructura
5. **Convocar a proveedores.**

   De acuerdo con el desastre ocurrido y los daños que tiene el centro de datos, se realiza la llamada a los proveedores, el Coordinador del plan de continuidad del negocio o a su vez el equipo de administración de la crisis inmediatamente deberá contactarse con el proveedor de servicio DRaaS *(Disaster Recovery as a Service)* el cual deberá inmediatamente responder

con el levantamiento de los servicios afectados, para así evitar pérdidas de continuidad de negocio de la institución.

6. **Determinar la hora y condiciones del siniestro.**

   Si el desastre llegara a ocurrir en horarios no laborables, se tiene que trasladar al establecimiento de manera inmediata.

   En este caso el desastre ocurrió en horas de la mañana en la jornada laboral.

7. **Preparar un informe sobre el desastre.**

   Se realiza un informe sobre el desastre y las consecuencias que este tuvo dentro del centro de datos, se completa así la primera etapa de implementación del plan de continuidad del negocio.

   - Respuesta inicial.
   - Notificación del desastre.

2.7.7.2 Etapa 2: Evaluación del problema y escalamiento

En esta etapa se realiza la recepción del informe por parte del Coordinador del Plan de Continuidad, en el cual se detalla que existe la destrucción total del centro de datos, además la inoperatividad de los servidores los cuales contenían los servicios que se identificaron previamente.

1. **Evaluar la interrupción de los servicios y el daño ocasionado.**

   Determinar cuáles de los 9 servicios fueron afectados, los equipos y recursos en general.

2. **Estimar el impacto del desastre como alto, medio, bajo.**

   De acuerdo con el análisis realizado en el informe entregado al Coordinador de Plan de Continuidad se cataloga el desastre como alto debido a la inoperatividad de los servidores y la destrucción total del centro de datos.

3. **Determinar si se continua con la siguiente fase.**

   Si el desastre no causa la inoperatividad de los servidores, ni de la inaccesibilidad al centro de datos se realiza un monitoreo continuo de la situación, caso contrario continuar a la siguiente fase

   La elaboración del informe de situación y escalamiento se presenta de la siguiente manera:

Informe de situación y escalamiento No.	#001

Nombre de la emergencia:
Terremoto ciudad de Ambato

Fecha y hora de elaboración del informe:	
Fecha : 29/10/2019	Hora: 08:00 am
Rol que desempeña dentro del Departamento de Tecnología de la Información	
ROL:	Técnico de infraestructura

Area de afectación : Por favor , marque el area afectada del bloque 1 , si la insfraestructura no se encuentra afectada por el siniestro, por favor pase directamente a la descripción del problema.

Preparado por: (Nombre y cargo)

Técnico de infraestructura del Departamento de Tecnología de la Información.

Fuente de información: (Organismos e instituciones de primera respuesta , personal de la Institución)

- Técnico de infraestructura del Departamento de Tecnología de la Información.
- Ecu-911 sala de monitoreo Ambato

1. Descripción de la emergencia
(Resuma de manera descriptiva el evento. Gravedad estimada de los daños. Zonas afectadas)

- El data center ubicado en el último piso del bloque 1 está totalmente destruido.
- Los servidores están inoperativos.
- Se ha determinado que el grado de severidad del impacto es alto, se toma en cuenta los valores predefinidos en la evaluación del impacto operacional que se encuentra en el BIA (Impacto en el negocio), se cataloga como alto impacto en función de los servicios inoperativos que se encontraban dentro de los servidores que se encuentran fuera de servicio.

2. Servicios afectados por el siniestro.
Marque con una X los servicios que están inoperativos.

Servicio	
Repositorio digital Institucional	x
Servidores de Nombres de Dominio	x
Academics	x
Catalogo en línea	x
Laboratorios	x
Impresión web	x
Eduroam	x
Spiceworks	x
Registro biométrico	x
Servicio de sincronización	x
Consultorio jurídico	x

Firma y nombre de responsables del informe Nombre y cargo (o función) de:

Elaborado por:	..... Técnico de infraestructura del Departamento de Tecnología de la Información.

Registro Fotográfico (Adjuntar las fotos de la infraestructura afectada)

2.7.7.3 Etapa 3: Declaración del Desastre.

La decisión de declarar un desastre será declarada en base al informe presentado al Coordinador de plan de continuidad.

1. **Opción de recuperación para la situación actual.**
   Para el presente plan de continuidad del negocio, se ha tomado en cuenta la recuperación mediante servicios *cloud¸* el cual consta del servicio de DRaaS (*Disaster Recovery as a Service),* el mismo que permite la replicación de los servidores, y ponerlos en funcionamiento en un tiempo menor a 1 una hora dada la declaración del desastre.
2. **Preparar la declaración del desastre.**
   - Anuncio del desastre.
   - Fecha y hora del desastre.
   - Categorizar el desastre en nivel: bajo, medio o alto.
   - Seleccionar la opción de recuperación.
   - Informe de la situación de recuperación.
   - Estimación del tiempo de recuperación.
   - Nombre de la autoridad que declara el desastre.
   - Notificar y declarar el desastre a toda la institución.

2.8 Etapa 4: Plan de implementación de logística

En esta etapa se realiza un monitoreo de los servidores levantados por el proveedor de DRaaS *(Disaster Revovery as a Service)*, este monitoreo estará a cargo del equipo de Administración de la crisis para evaluar el desempeño de los servicios que están levantados en la nube.

Los equipos de Administración de usuarios deberán atender los requerimientos de los clientes, como a su vez solucionar cualquier soporte que se presente post - desastre para evitar problemas de operatividad dentro de la institución.

2.9 Etapa 5: Recuperación.

Actividades que seguir:

- Asegurar el correcto funcionamiento de los servidores que están el cual funciona en la nube.
- Hay que asegurar que el equipo de administración de usuarios está, atiende de manera correcta en temas de soporte.
- Inspeccionar que los servicios que se encuentran dentro de los servidores montados en la nube estén accesibles y con todos los datos correspondientes a los respaldos obtenidos un día anterior.

Anexo 9

Formato para la elaboración del informe de situación y escalamiento.

Pontificia Universidad Católica del Ecuador | Sede Ambato

Informe de situación y escalamiento No.	

Nombre de la emergencia:

Fecha y hora de elaboración del informe:	
Fecha :	Hora:
Rol que desempeña dentro del Departamento de Tecnología de la Información	
ROL:	
Area de afectación : Por favor , marque el area afectada del bloque 1 , si la insfraestructura no se encuentra afectada por el siniestro, por favor pase directamente a la descripción del problema.	
	
Preparado por: (Nombre y cargo)	
Fuente de información: (Organismos e instituciones de primera respuesta , personal de la Institución)	

1. Descripción de la emergencia (Resuma de manera descriptiva el evento. Gravedad estimada de los daños. Zonas afectadas)

2. Servicios afectados por el siniestro. Marque con una X los servicios que están inoperativos.

Servicio	
Repositorio digital Institucional	
Servidores de Nombres de Dominio	
Academics	
Catalogo en línea	
Laboratorios	
Impresión web	
Eduroam	
Spiceworks	
Registro biométrico	
Servicio de sincronización	
Consultorio jurídico	

Firma y nombre de responsables del informe Nombre y cargo (o función) de:

Elaborado por:	……

Registro Fotográfico (Adjuntar las fotos de la infraestructura afectada)	