FACULTAD DE POSTGRADO

TESIS DE POSTGRADO:
RECUPERACIÓN DE DESASTRES DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA NUBE EN EL RUBRO DE ASEGURADORAS MEDIADAS DE TEGUCIGALPA

SUSTENTADO POR:

CARLOS DANILO BONILLA RODAS

LEONIDAS GABRIEL REYES ESPINAL

PREVIA INVESTIDURA AL TÍTULO DE MÁSTER EN GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

TEGUCIGALPA, F.M. **HONDURAS, C.A.**

OCTUBRE, 2017

UNIVERSIDAD TECNOLÓGICA CENTROAMERICANA

UNITEC

FACULTAD DE POSTGRADO

AUTORIDADES UNIVERSITARIAS

RECTOR

LUIS ORLANDO ZELAYA MEDRANO

SECRETARIO GENERAL

ROGER MARTÍNEZ MIRALDA

DECANO DE LA FACULTAD DE POSTGRADO

JOSÉ ARNOLDO SERMEÑO LIMA

RECUPERACIÓN DE DESASTRES DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA NUBE EN LA MEDIANA EMPRESA DE TEGUCIGALPA

TRABAJO PRESENTADO EN CUMPLIMIENTO DE LOS REQUISITOS EXIGIDOS PARA OPTAR AL TÍTULO DE MÁSTER EN
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN

ASESOR
CARLOS ROBERTO ARIAS
JORGE RAUL MARADIAGA CHIRINOS

FACULTAD DE POSTGRADO

RECUPERACIÓN DE DESASTRES DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA NUBE EN LA MEDIANA EMPRESA DE TEGUCIGALPA

AUTORES:

CARLOS DANILO BONILLA RODAS Y LEONIDAS GABRIEL REYES ESPINAL

RESUMEN EJECUTIVO

El propósito del presente trabajo de investigación es conocer la situación actual de las compañías de seguros en la categoría de mediana empresa de la ciudad de Tegucigalpa, con respecto la aceptación e incorporación de un DRP en la nube, esto debido a que son entidades reguladas quien les exige tener un plan de recuperación de desastres en caso de ocurrir un incidente que pueda afectar los servicio críticos de la organización. Esto se ha logrado mediante instrumentos tales como entrevistas y encuestas dirigidas al personal que se encarga de dirigir, administrar las áreas de tecnología en las aseguradoras de la categoría de la mediana empresa y expertos en el tema de la implementación de soluciones de contingencia. Se concluyó que la mediana empresa en el rubro de las aseguradoras no implementa su plan de recuperación de desastres en la nube debido a que estas instituciones poseen el recurso económico suficiente para comprar la infraestructura e implementar su DRP tradicionalmente.

Palabras clave: DRP en la nube, DRP Tradicional, Ente regulador, Mediana Empresa, Servicios Críticos

GRADUATE SCHOOL

DISASTER RECOVERY OF INFORMATION TECHNOLOGIES IN THE CLOUD IN MEDIUM COMPANIES IN TEGUCIGALPA

AUTHORS:

CARLOS DANILO BONILLA RODAS Y LEONIDAS GABRIEL REYES ESPINAL

ABSTRACT

The purpose of this research is to know the current situation of insurance companies in the medium-sized category of the city of Tegucigalpa, regarding the acceptance and incorporation of a DRP in the cloud, this being because they are regulated entities who requires them to have a disaster recovery plan in the event of an incident that may affect the critical services of the organization. This has been achieved through tools such as interviews and surveys aimed at staff managing, managing technology areas in medium-sized category insurers, and experts in implementing contingency solutions. It was concluded that the median company in the insurance sector does not implement its cloud disaster recovery plan because these institutions have the sufficient economic resources to buy the infrastructure and implement its DRP traditionally.

Keywords: DRP in the cloud, Traditional DRP, Regulatory Entity, Medium Enterprise, Critical Services

DEDICATORIA

En primer lugar a Dios que es el ser supremo y soberano que nos brinda sabiduría para poder culminar nuestras metas.

A mis Padres Carlos Danilo Bonilla Flores que está en el cielo y sé que el estará celebrando este triunfo junto a nosotros, mi madre Maria Consuelo Rodas Zavala que es y ha sido un ejemplo, guía y fortaleza para emprender y lograr todas las metas que me he puesto en mi vida, a mi pequeña familia que son el motivo fundamental e impulso para seguir adelante Sagrario Ordoñez y Matteo Bonilla, a mis hermanas, sobrinos que son un pilar fundamental en la unión de nuestra familia.

Carlos Danilo Bonilla Rodas

Dedico este trabajo primero a Dios, por darme la sabiduría y el entendimiento para poder culminar esta importante meta.

A mis padres Leonidas Reyes Reyes y Xiomara Emperatriz Espinal Guevara que gracias a sus consejos, motivación y amor incondicional me han apoyado en todo este proceso, a mis hermanos y amigos que con su apoyo han sido un importante pilar para culminar con éxito esta etapa de mi vida.

Leonidas Gabriel Reyes Espinal

AGRADECIMIENTO

A Dios ya que nos ha proveído de salud y los recursos necesarios para culminar con éxito esta importante etapa profesional en nuestras vidas.

Al personal docente de UNITEC por todo su apoyo, por su tiempo y los conocimientos que transmitieron en las diferentes asignaturas que cursamos a lo largo de este tiempo y que serán de gran utilidad en nuestra vida profesional.

A nuestros compañeros de clase, que a través de estos años forjamos una gran amistad, nos apoyamos para poder dar lo mejor como grupo, compartiendo nuestras vivencias profesionales que enriqueció en alguna medida nuestras vidas.

A los Gerentes de Tecnología y Seguridad Informática de las aseguradoras de la mediana empresa por tomarse el tiempo de contestar nuestras preguntas y entrevistas, a los catedráticas Egdares Futch, Carlos Arias y Jorge Maradiaga que con su guía, experiencia y consejo hemos podido culminar con éxito este trabajo de tesis.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

Capítulo I. Planteamiento de la Investigación

1.1 Introducción

Actualmente tanto grandes empresas como PYMES (pequeñas y medianas empresas) generan grandes cantidades de información que son críticas para sus operaciones, esta información se vuelve un activo importante en las empresas que debe ser protegido. La continuidad es un requisito vital para la mayoría de las empresas ya que, una interrupción del servicio puede costar pérdidas significativas e incluso tener dificultades para sobrevivir (Alhazmi & Malaiya, 2013).

En consecuencia, las organizaciones deben tener un plan de recuperación de desastres (DRP) que se pueda ejecutar, probar, escalar y mantener. Este plan debe cumplir con los tiempos de recuperación (RTO) y con los puntos de recuperación (RPO), las organizaciones deben identificar los eventos probables que pueden causar desastres y evaluar su impacto, necesitan establecer objetivos y evaluar planes viables de recuperación (Alhazmi & Malaiya, 2013). Tradicionalmente este proceso de recuperación de desastres tecnológicos se ha llevado a cabo dentro de las mismas instalaciones de la empresa o en un entorno externo, pero hoy en día la computación en la nube proporciona una alternativa para pequeñas y medianas empresas debido a costos más bajos, mejor rendimiento, escalabilidad, incremento en movilidad, y uso de entornos virtualizados en comparación con los mecanismos tradicionales (Sungana & Suhasini, 2014).

En su mayoría, la mediana empresa en Tegucigalpa no está preparada para una recuperación de desastres tecnológicos es por eso que el objetivo principal de este trabajo es la evaluación de la esta situación que ayude a identificar las causas del por qué la mediana empresa no realiza planes de recuperación de desastres tecnológicos en la nube.

1.2 Antecedentes

El rubro de las aseguradoras medianas en Honduras data del año 1954 Aseguradora Hondureña S,A (Ahora Seguros Mapfre) en donde en un principio incursionó en los ramos de daños de incendios y automóviles expandiéndose por todo el todo el territorio nacional, ya para la década de los 90’s surgió Seguros Crefisa y posteriormente Seguros del País y Seguros Lafise, estas 4

aseguradoras forman parte de los principales grupos de aseguradoras del país con altos estándares de productos y servicios para su cartera de clientes.

En el año de 1995 la Comisión Nacional de Bancos y Seguros, emitió dos importantes leyes para el Sistema Financiero Nacional: la Ley de la Comisión Nacional de Bancos y Seguros y la Ley de Instituciones del Sistema Financiero, posteriormente en el año 2004 se deroga la última con la aprobación y vigencia de la Ley del Sistema Financiero que tiene como objetivo regular la organización, autorización, constitución, funcionamiento, fusión, conversión, modificación, liquidación y supervisión de las instituciones del sistema financiero y grupos financieros.

Con el objetivo de promover la adopción de buenas prácticas en la administración de los riesgos inherentes a las actividades que realizan las instituciones supervisadas, la Comisión Nacional de Bancos y Seguros (CNBS) en la resolución No.1301 emitida el 22 de noviembre de 2005 hace mención sobre los planes de contingencia y recuperación ante desastres, es entonces hasta esa fecha que el sistema financiero de Honduras empieza a madurar sobre los riesgos de no salvaguardar en base a mejores prácticas la información. Desafortunadamente en la actualidad la mayoría de empresas medianas en el país no son reguladas por la CNBS y no adoptan planes de contingencia ni recuperación de desastres tecnológicos.

1.3 Definición del problema

Después de establecer el antecedente, la problemática que se encuentra en la mediana empresa es la poca adopción que hay de un plan de recuperación de desastres de tecnologías de la información en la nube en Tegucigalpa, para esto se formula la siguiente pregunta.

Con el fin de dar respuesta al problema se planteó la siguiente pregunta:

- ¿Por qué la mediana empresa de Tegucigalpa en el rubro de aseguradoras no tiene implementado un plan de recuperación de desastres de Tecnologías de la Información en la nube?

1.4 Objetivos del Proyecto

1.4.1 Objetivo General

Evaluar la situación actual de las compañías aseguradoras medianas en Tegucigalpa frente a un plan de recuperación de desastres de tecnologías de la información en la nube.

1.4.2 Objetivos Específicos

- Fundamentar teóricamente el uso de la computación en la nube como mecanismo de recuperación antes desastres tecnológicos.

- Investigar por qué son pocas las aseguradoras medianas que optan a realizar un plan de recuperación de desastres de tecnologías de la información en la nube.

- Identificar el nivel de aceptación de un plan de recuperación de desastres de tecnologías de la información en la nube en las aseguradoras medianas de Tegucigalpa.

- Analizar la situación actual de las aseguradoras medianas de Tegucigalpa frente a un plan de recuperación en la nube.

1.5 Justificación

La presente investigación pretende ser de gran importancia para el sector de las aseguradoras medianas en Tegucigalpa, ya que se podrá entender lo relevante que es la adopción de un plan de recuperación de desastres tecnológicos en la nube principalmente a las empresas que cuentan con pocos recursos tanto económicos como humanos para adoptar un plan de recuperación de desastres local y como el costo de no estar preparados ante cualquier eventualidad que pueda poner en riesgo la información de la empresa puede ser alto.

En Honduras muchas empresas no tienen la madurez sobre la importancia que tienen las tecnologías de la información, se centran más en el negocio y miran al área de TI como un gasto

financiero, se piensa que un plan de recuperación de desastres únicamente el área de TI es el responsable cuando en realidad es responsabilidad de toda la empresa, este estudio no solo pretende dar a conocer el grado de importancia de la computación en la nube, sino que también se trace el camino a seguir para la prestación de nuevos servicios y/o mejorar los actuales por parte de los proveedores de servicios en la nube, así como la creación de nuevas empresas de tecnología que puedan suplir las necesidades de la mediana empresa.

Capítulo II. Marco Teórico

2.1 Análisis de la situación actual

La mediana empresa según la Real Academia Española la define como: Empresa mercantil, industrial, etc., compuesta por un número reducido de trabajadores, y con un moderado volumen de facturación. Actualmente en Honduras, las empresas medianas disponen de mayor inversión en activos fijos, en relación a las anteriores (Micro y pequeñas empresas). Así mismo, presentan una adecuada relación en cuanto a su capital de trabajo, una clara división interna del trabajo y formalidad en sus registros contables y administrativos, emplean un número de cincuenta y uno (51) empleados y un máximo de ciento cincuenta (150) empleados remunerados (Gaceta, 2009).

En Tegucigalpa la mediana empresa es muy importante ya que es una fuente generadora de empleo, permite que se produzcan, ofrezcan o demanden bienes y/o servicios que son decisivos en la generación de riqueza en el país. Según la Cámara de Comercio e Industrias de Tegucigalpa actualmente hay registradas 185 medianas empresas en la capital.

Actualmente muchas empresas en la capital dicen tener un plan de recuperación de desastres de tecnologías de la información, pero este carece de formalidad ya que son procedimientos que no son del conocimiento de la alta administración ni de los empleados que pertenecen a otras áreas distintas a la de tecnología, nunca se han realizado pruebas, no se tiene la infraestructura correcta, ni están establecidos controles de prevención, detección y corrección en caso de ocurrir alguna incidencia.

Un concepto clave de un plan de recuperación de desastres es la separación física del centro de datos primario del secundario, una fracción significativa de los desastres son causados por interrupciones geográficas. Como se puede ver en la tabla 1 unas de las mayores causas de desastres se debe a las actualizaciones de los sistemas y fallas de la energía eléctrica, actividades que en nuestro país son muy recurrentes debido a la mala planificación de muchas empresas y a la alta incidencia de cortes de energía eléctrica que a diario se dan en la capital.

Tabla 1: Desastres enfrentados en un período de cinco años

Causa	**Organización**
Actualizaciones de los sistemas	72%
Fallas de la energía eléctrica	70%
Fuego	69%
Cambios de configuración	64%
Ciberataques	63%
Empleados mal intencionados	63%
Pérdida de información	63%
Inundaciones	48%
Huracanes	47%
Terremotos	46%
Tornado	46%
Terrorismo	45%
Tsunami	44%
Erupción volcánica	42%
Guerras	42%
Otros	1%

Fuente: (Sungana & Suhasini, 2014)

2.2 Computación en la nube

La computación en la nube es un modelo que permite el acceso a la red de forma ubicua y conveniente a un conjunto de recursos informáticos configurables tal como se muestra en la figura 1. (Ejemplo: redes, servidores, almacenamiento, aplicaciones y servicios) estos recursos pueden rápidamente ser provistos y liberados con un esfuerzo administrativo o provisión de administración de servicio mínimo (National Institute of Standards and Technology, 2011).

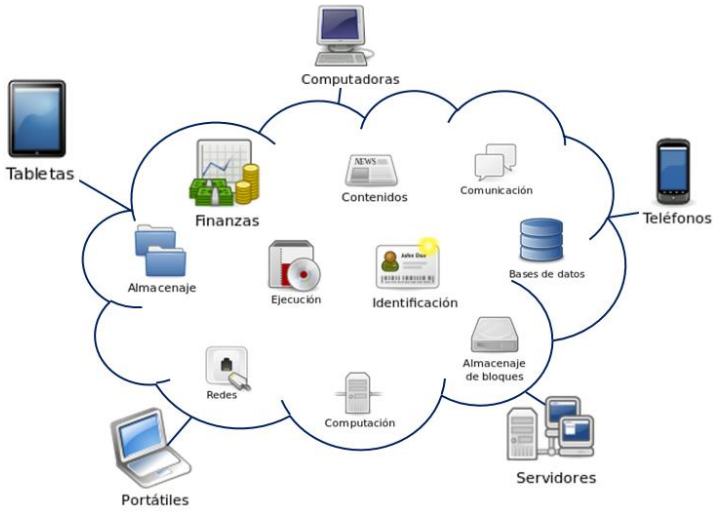

Figura 1: Diagrama de computación en la nube

Fuente: (Elaboración propia).

2.2.1 Características

No es necesario disponer de un equipo potente, tan solo de un aparato con conexión a internet; ya que el dispositivo sin necesidad de procesos complejos guardará los archivos en la nube. Los servidores en donde se hallan los programas que se utilicen son los encargados de las tareas complicadas que antes se realizaban localmente.

Con la facilidad que ofrece la computación en la nube no es necesario que los usuarios conozcan todos los procesos y la infraestructura que hay detrás de esta ya que pasa a ser una abstracción donde los aplicativos y servicios ofrecidos por las empresas fácilmente pueden funcionar más rápido, crecer y con el mínimo de fallas. Este tipo de servicio puede pagar alguna métrica de consumo, no por el equipo usado en sí, sino por unos de CPU/hora como ser el caso de Amazon EC2 (Ávila Mejía, 2011).

Entre otras características se menciona:

- Auto reparable: Esto indica que en caso de surgir alguna incidencia los respaldos de la aplicación son convertidos en una copia primaria para que en base a estos se reestablezcan los datos perdidos y que la continuidad del negocio no se vea afectada.

- Es escalable: conforme a la demanda de las operaciones en la empresa así será la infraestructura, si las operaciones funcionan en un servidor y al aumentar estas en un 100% se puede establecer un nivel de servicios para crear nuevas instancias y que las mismas pueden ser manejadas en 2 servidores haciendo que el sistema y toda su arquitectura sea predecible y eficiente.

- Virtualización: Independientemente de los aplicativos que corran en el hardware estos pueden funcionar en el mismo computador ya que se crea una representación del software en forma virtual en lugar de una física.

- Niveles de seguridad: Este es alto ya que el sistema es creado para permitir que los clientes de diferentes empresas puedan compartir la infraestructura sin necesidad que se vea comprometida la seguridad la información ya que la empresa que provee estos servicios es la encargada de cifrar los datos.

- Disponibilidad de la información: Ya que la información es almacenada en internet no hay necesidad que esta se almacene de forma local en la computadora o en medios de almacenamiento externo, esto permite que el usuario tenga acceso a su información desde cualquier dispositivo que tenga acceso a internet.

2.2.2 Arquitectura de la nube

Un servicio debe de cumplir con las siguientes características esenciales para ser considerado como servicio en la nube (National Institute of Standards and Technology, 2011).

- Auto-servicio por demanda:
  Un consumidor puede aprovisionar capacidades de cómputo como ser: tiempo de servidor, almacenamiento de red en la medida que los vaya necesitando sin la intervención humana por parte del proveedor del servicio.
- Acceso amplio desde la red:

El acceso a la infraestructura en la nube debe de estar disponible desde dispositivos clientes de cualquier tipo como una computadora, tableta o teléfono móvil que tenga un navegador a internet

- Conjunto de recursos:
  La infraestructura en la nube permite compartir infraestructura virtual y física con múltiples consumidores de acuerdo a sus necesidades, el consumidor no conoce la ubicación de sus recursos dentro del centro de datos.

- Rápida elasticidad:
  Las necesidades de procesamiento y demás pueden ser rápidamente aprovisionadas para el consumidor, usualmente estas características son ilimitadas y pueden ser adquiridas en cualquier momento, inclusive servicios que no necesitan estar activos pueden ser dados de baja para disminuir su consumo.

- Servicio medido:
  Automáticamente los servicios en la nube que se están ejecutando son optimizados mediante un nivel de abstracción adecuado al tipo de servicio.

Con la separación entre los aplicativos y el hardware la computación en la nube tiene una arquitectura con las siguientes capas:

- Software como Servicio (SaaS): Se encuentra en la capa más alta, es un modelo de entrega de aplicaciones de software, donde un proveedor de software despliega y aloja aplicaciones de software en sus servidores para que sus clientes operen la aplicación a través de Internet como servicios (Liu, Guo, Zhi, & Chou, 2010). Los proveedores de SaaS son responsables de la disponibilidad y funcionalidad de sus servicios no dejando de lado las necesidades de los clientes que finalmente son los que usarán el software.

- Plataforma como Servicio (PaaS): esta es la siguiente capa, básicamente su objetivo se centra en un modelo en el que se proporciona un servicio de plataforma con todo lo necesario para dar soporte al ciclo de planteamiento, desarrollo y puesta en marcha de aplicaciones y servicios web a través de la misma. El proveedor es el encargado de escalar los recursos en caso de que la aplicación lo requiera, de que la plataforma tenga un rendimiento óptimo, de la seguridad de acceso, etc. Para desarrollar software se necesitan bases de datos, herramientas de desarrollo y en ocasiones servidores y redes. Con PaaS el cliente únicamente se enfoca en desarrollar, depurar y probar ya que la herramienta necesaria para el desarrollo de software es ofrecida a través de Internet, lo que teóricamente permite aumentar la productividad de los equipos de desarrollo (Ávila Mejía, 2011).

- Infraestructura como Servicio (IaaS): Corresponde a la capa más baja. Es un modelo de servicio en el que una organización subcontrata el equipo utilizado para las operaciones de la empresa, este incluye almacenamiento, hardware, servidores y componentes de red. El proveedor de servicios es responsable del lugar, el funcionamiento y mantenimiento de los equipos (Chavan, Patil, & Kulkarni, 2013).

  Para hacer una distinción respecto a las plataformas como servicio, las IaaS se presentan como una propuesta con mucho más flexibilidad para el uso que el usuario desee, pero también requieren mucho más del cliente en lo que a instalación, configuración y mantenimiento del software se refiere. Para proyectos que no se adapten en ninguna PaaS o en los que se quiera contar con libertad al momento de hacerlos evolucionar, existe la opción (y es preferible) de una Infraestructura como servicio. Las IaaS permiten desplazar al proveedor la mayor parte de los factores relacionados con la gestión de las máquinas con el ahorro de costos al pagar sólo por lo consumido y olvidarse de tratar con máquinas y su mantenimiento. Por otro lado, IaaS puede permitir una escalabilidad automática o semiautomática, de forma que se puedan contratar más recursos según los se requieran (Ávila Mejía, 2011).

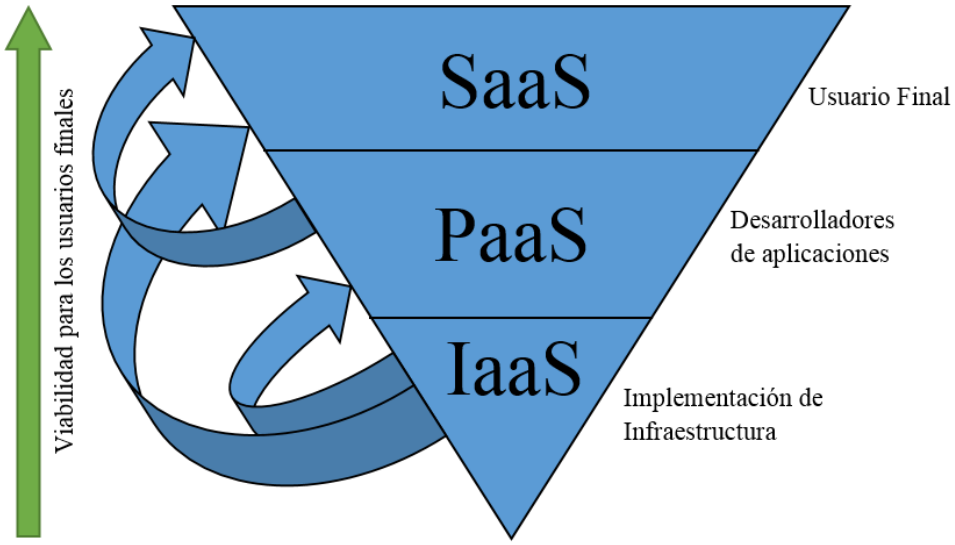

Figura 2: Capas de la nube

Fuente: (Ávila Mejía, 2011).

2.2.3 Riesgos y beneficios de la nube

Beneficios

Tal como se muestra en la figura 3, la computación en la nube ofrece ahorros significativos en cuanto a los costos, esto incluye la implementación, mantenimiento, menos compra de hardware y soporte, la eliminación de los costos de energía, refrigeración, espacio físico y almacenamiento ya que todos y cada uno de estos factores son trasladados al proveedor de servicios incluyendo una reducción en los costos operativos ya que únicamente se paga por lo que se usa. La computación en la nube permite a las organizaciones ser más competitivas debido a que proporciona escalabilidad y recursos de alto rendimiento, aplicaciones y datos altamente confiables y disponibles. Mediante la computación en la nube el departamento de tecnologías de la información ahorra en el desarrollo de aplicaciones, implementaciones, seguridad y tiempos de mantenimiento, estos ahorros son un punto de enfoque clave para toda la empresa, estos beneficios hacen a las empresas más sostenibles con lo cual pueden asignar recursos a tareas más estratégicas y las vuelve ambientalmente responsables (Kotze, Carroll, & Van der Merwe, 2011).

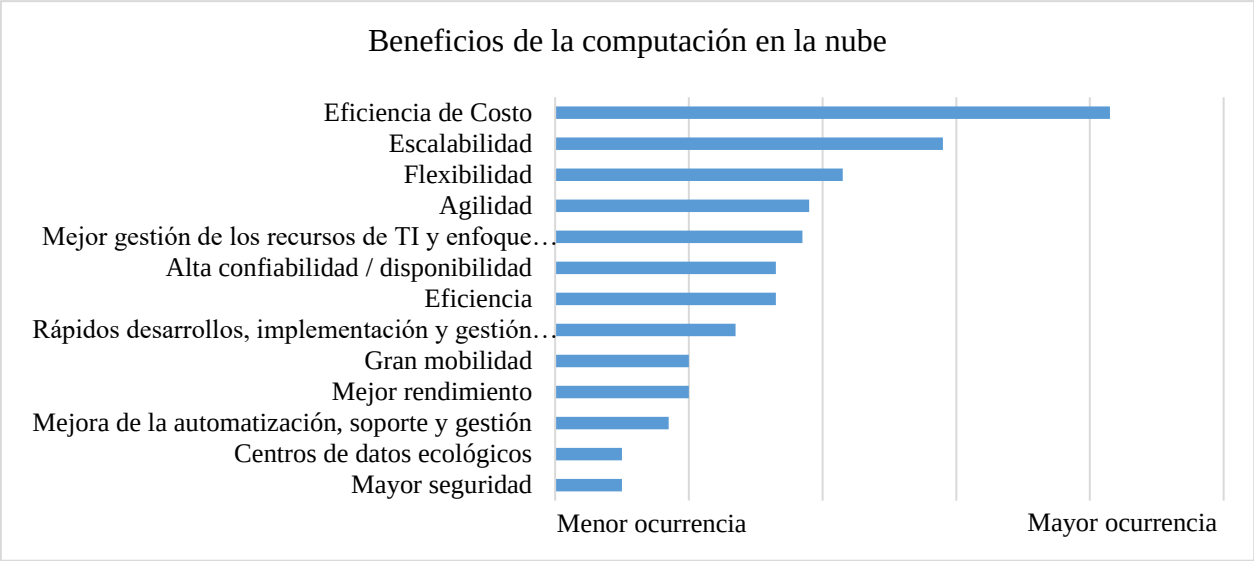

Gráfico 1: Beneficios de la computación en la nube

Fuente: (Kotze, Carroll, & Van der Merwe, 2011).

Riesgos

La computación en la nube no es completamente segura y Honduras no está exenta de dichos riesgos, la mitigación de los mismos representan un importante paso frente a la protección de estos ambientes para así aprovechar los beneficios.

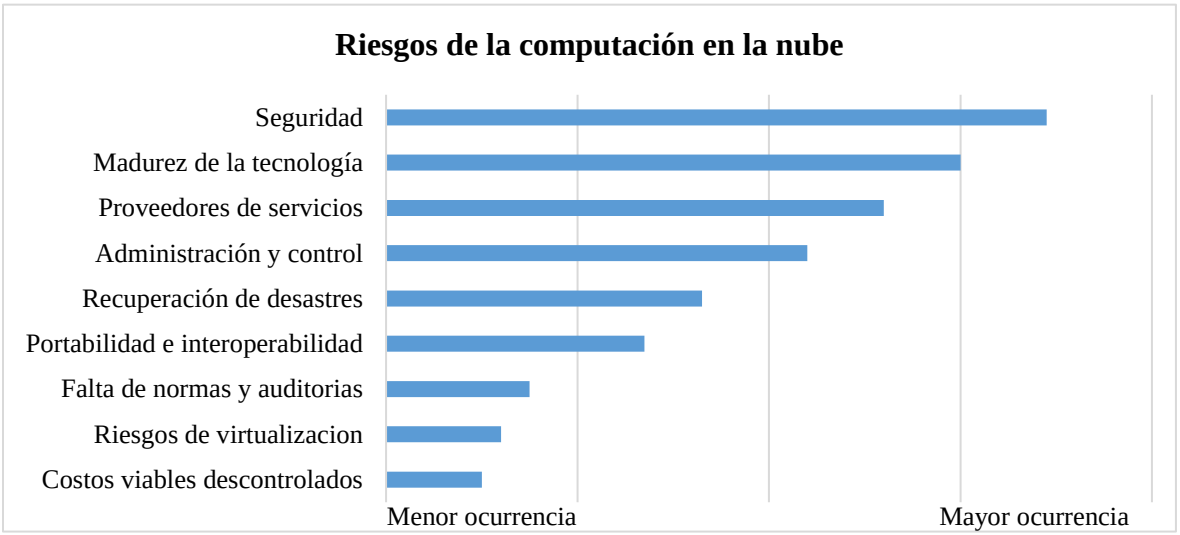

Gráfico 2: Riesgos de la computación en la nube

Fuente: (Elaboración propia).

Tal como se muestra en la figura 4, el mayor riesgo de la computación en la nube es la seguridad, esto debido a que las aplicaciones y los datos están siendo alojados por el proveedor de servicios y la información no está siendo administrada por la propia empresa, el alojamiento de aplicaciones e información en infraestructuras compartidas aumenta el potencial de accesos no autorizados así como preocupaciones en cuando a la privacidad, gestión de incidentes, autenticación, cumplimiento, confidencialidad, integridad, disponibilidad de datos, cifrado, seguridad de red y seguridad física. Aparte de los riesgos en la seguridad también hay otras preocupaciones que incluyen los acuerdos de nivel de servicio (SLA), la gestión de terceros, la calidad del servicio, viabilidad de proveedores, gestión, control de datos y aplicaciones, gestión de carga de trabajo entre otros.

2.2.4 Tipos de nubes

- Nubes públicas: Estas se administran externamente por terceros, los contenidos de distintos clientes pueden encontrarse ubicados en los mismos servidores y sistemas de almacenamiento, los usuarios finales usan la infraestructura de la nube en todas sus capas y no conocen que sistemas de otros clientes pueden estar corriendo en el mismo servidor o red.

- Nubes privadas: En este caso el proveedor es propietario de la infraestructura y pueden decidir qué usuarios están autorizados a utilizar la misma. Las nubes privadas están en una infraestructura manejada por un solo administrador que controla que aplicaciones debe correr y dónde. Son una buena opción para las compañías que necesitan alta protección de datos y manipulaciones a nivel de servicio.

- Nubes híbridas: Esta es una combinación de nubes públicas y privadas. El cliente está en posesión de una parte y comparte otra, esto además puede ser de manera controlada. Las nubes híbridas ofrecen la ventaja del escalado proporcionado bajo demanda, se añade la posibilidad de determinar cómo distribuir las aplicaciones a través de los diferentes ambientes.

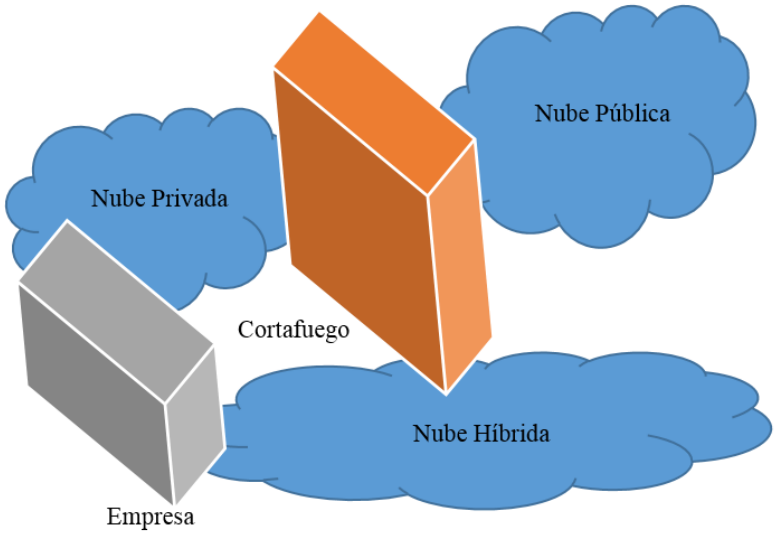

Figura 3: Tipos de nube

Fuente: (Elaboración propia).

2.3 Recuperación de desastres (DR)

2.3.1 Clasificación

Las empresas siempre están expuestas a riesgos, existe la probabilidad de que un evento no deseado impida el desarrollo normal de las actividades y que provoque pérdidas económicas y hasta pérdidas de clientes. Un plan de recuperación de desastres es un elemento de un sistema de control interno establecido para gestionar la disponibilidad y restaurar procesos críticos de TI en caso de interrupción (ISACA, Manual de Preparación al Examen CISA 2012, 2012).

Sin duda alguna un evento que hizo recordar la importancia de los planes de Recuperación de Desastres a nivel mundial, fue el ataque terrorista suscitado el 11 de septiembre de 2001 en las torres gemelas. Como se puede observar en la figura 6 posterior al año 2001 hay un punto de inflexión en la utilización de palabras clave como “Disaster Recovery Plan” en publicaciones realizadas en ese periodo de tiempo.

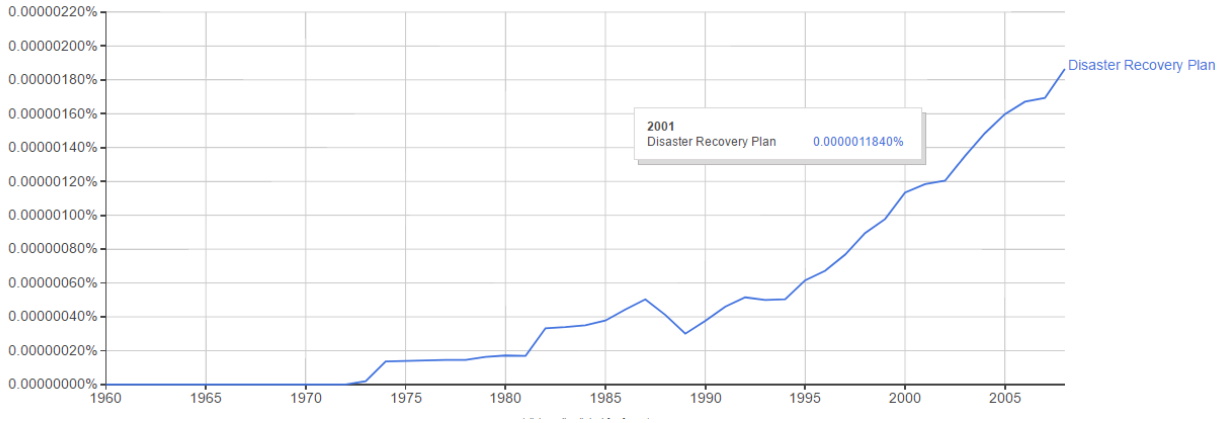

Gráfico 3: Tendencia de publicaciones DRP

Fuente: (Google Ngram Viewer, 2017).

2.3.2 Clasificación de los servicios

En el proceso de recuperación de desastres es vital importancia identificar aquellos procesos de negocio relacionados con las tecnologías de la información, dentro de los cuales se pueden clasificar como servicios de misión crítica y servicios que no son de misión crítica. Se les denomina servicios de misión crítica debido a que son servicios que no se pueden reemplazar de forma manual y estos deben de ser restaurados en un plazo máximo de 36 horas.

En caso contrario se tienen los servicios que no son de misión crítica, estos pueden ser restaurados hasta que se reestablezca el sitio dañado o hasta que se instale el nuevo reemplazo del equipo, mientras esto no ocurre este proceso puede ser realizado manualmente (Veeam Software, 2014).

2.3.3 Costos financieros

El plan de recuperación de desastres tiene como objetivo restaurar la operatividad de los sistemas de información lo más pronto posible, toda organización debería de tener un plan de este tipo; el no tenerlo puede representar altos costos financieros.

En la tabla 2 según el Veeam Availability Report se presenta una muestra de incidentes en las organizaciones de 10 países:

Tabla 2: Incidentes en organizaciones

País	Número de Incidentes
Italia	17
Brasil	16
Francia	15
Reino Unido	14
Suiza	13
Singapur	12
Estados Unidos	12
Alemania	11
Alemania	11
Australia	10
Holanda	9

Fuente: (Veeam Software, 2014)

El promedio de incidentes que se muestran en la tabla 2 es de 13, el promedio de horas de inactividad por aplicaciones clasificadas como misión crítica es de 1.33 horas y 3.97 horas para aplicaciones de no misión crítica, el promedio de costo por horas para aplicaciones de misión crítica es de $82,864 y para aplicaciones de no misión crítica es de $43,886; con lo cual se puede concluir que el costo de no tener un plan de recuperación de desastres representa pérdidas financieras representativas en las organizaciones a nivel mundial.

2.3.4 Implementación de un DRP

Para implementar un DRP se debe definir la estructura basado en los siguientes pasos:

- Elaboración de las políticas para implementar un plan de recuperación de desastres.
- Realizar un análisis de impacto de los negocios con respecto a los sistemas críticos de tecnología (BIA).
- Identificar los controles preventivos.
- Desarrollar estrategias de recuperación.
- Desarrollo de un plan de contingencia.
- Prueba formación y ejecución del plan.

- Mantenimiento del plan

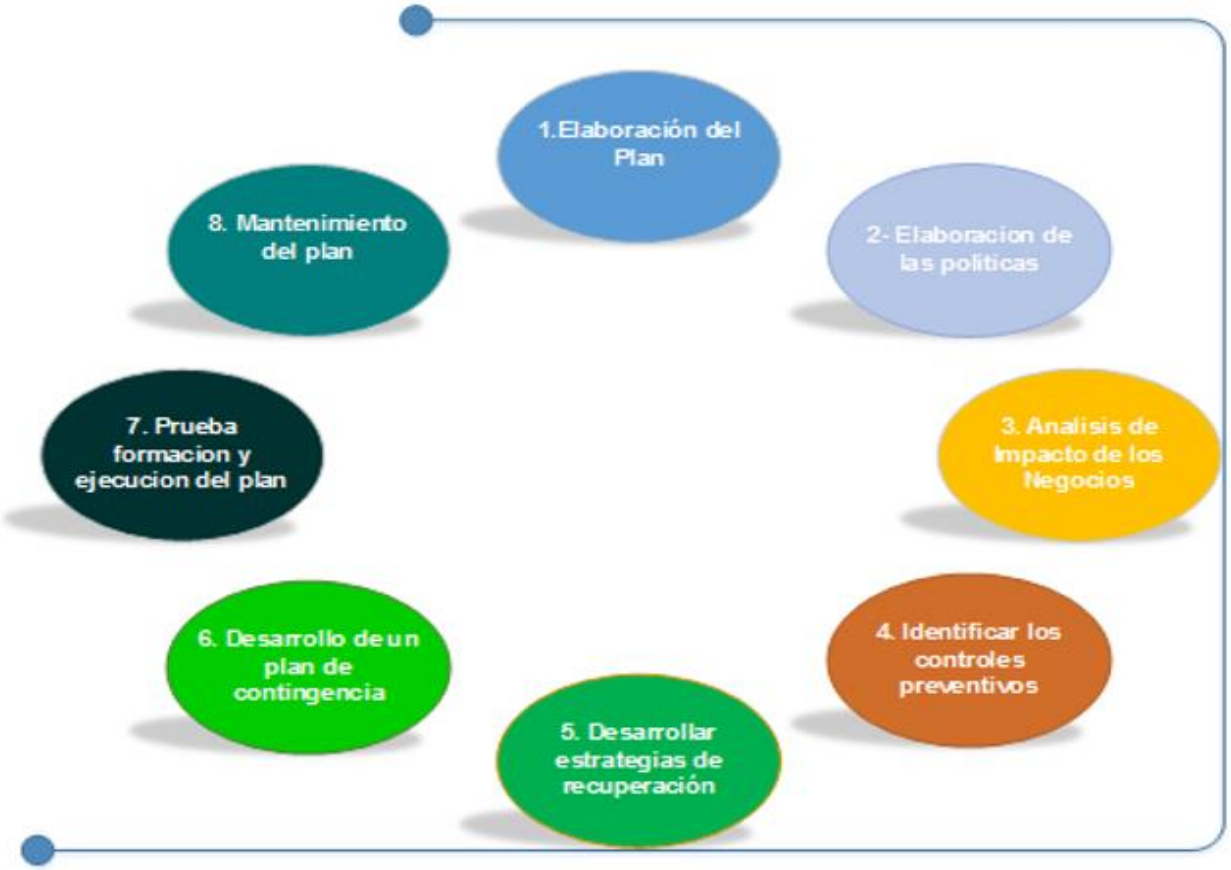

Figura 4: Pasos para implementar un DRP

Fuente: (National Institute of Standards and Technology, 2011)

2.3.5 Objetivo de punto de recuperación (RTO) y tiempo objetivo de recuperación (RPO)

A partir del análisis de impacto de los negocios con respecto a los sistemas críticos de tecnología (BIA) surgen dos elementos que permiten a las empresas hacer frente a la interrupción de los servicios o la perdida de información. El tiempo objetivo de recuperación (Recovery time object, RTO) y punto objetivo de recuperación (Recovery point object, RPO).

El RPO es el punto del tiempo en el cual la organización puede recuperarse a partir de la última copia de seguridad, por ejemplo, si ocurre un incidente que detenga el normal funcionamiento de los servicios y el último respaldo que se realizó en el momento que ocurrió un desastre fue de dos horas entonces el punto de restauración no deberá ser mayor a dos horas. El

RTO es el número de horas o días objetivo para la reanudación del normal funcionamiento del servicio después de ocurrido el desastre (Veeam Software, 2014).

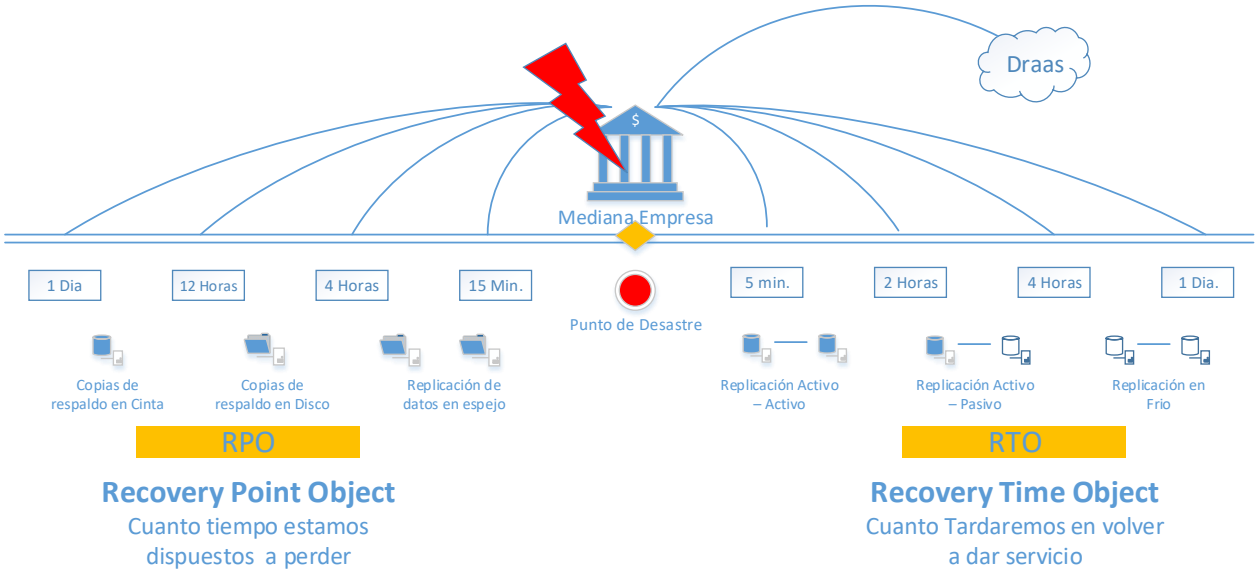

Figura 5: Relación entre RTO y RPO

Fuente: (Elaboración propia)

Los RTO y RPO están relacionados con las estrategias de respaldos con que cuente la organización, las estrategias de respaldo y copias de seguridad pueden provenir de tres fuentes diferentes:

- Empresas especializadas en proporcionar servicios de recuperación ante desastres.
- Otras oficinas de la organización.
- Un acuerdo mutuo con otra organización para compartir las instalaciones del centro de datos en caso de un desastre.

Cuando la organización ya cuenta con un sito de contingencia o recuperación que es el lugar donde la estrategia de recuperación tendrá efecto, dependiendo del presupuesto o del nivel de madurez que tengan sus directivos es posible establecer una estrategia de recuperación como las siguientes:

- Sitio de copia de seguridad fresco: Es el menos costoso de operar. No toma ninguna copia de seguridad de los datos, no incluye hardware, puede arrancar con un costo mínimo pero requiere más tiempo. Es necesario adquirir el hardware y todo lo necesario para restaurar los servicios. (Mr.Akshay A. Gharat, 2015)

- Sitio de copia de seguridad cálida: Cuenta con una configuración de hardware previa, para ponerlo a andar es necesario llevar una copia de seguridad de los datos y comenzar el proceso de restauración (Mr.Akshay A. Gharat, 2015).

- Sitio de copia de seguridad en caliente: El sitio de contingencia en caliente es muy costoso, este tipo de sitio es seleccionado en las organizaciones que replican su centro de datos en tiempo real. La pérdida de datos es mínima, ya que se pueden reubicar los datos y continuar con el trabajo que se está realizando, en muy poco tiempo este centro de datos permite operar como si se estuviera en el sitio principal. (Mr.Akshay A. Gharat, 2015)

Como se muestra en la figura 8, dependiendo de la estrategia de respaldo que la organización utilice así será el costo en el que debe incurrir, si la estrategia de recuperación es en un sitio de copia de seguridad frío los RTO Y RPO son menos recurrentes y sus costos son menores, caso contrario con la estrategia de recuperación en caliente que requiere de un sitio activo-activo lo cual implica mayor inversión ya que se cuenta con un centro de datos espejo con similares características a las del sitio principal.

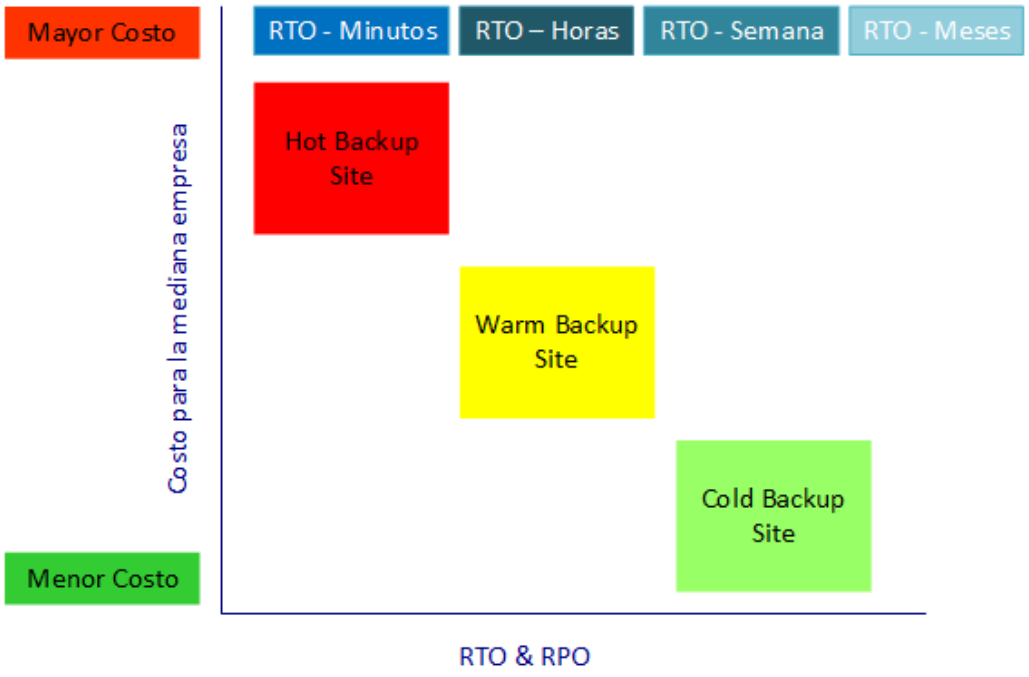

Figura 6: Relación entre Estrategia de Respaldos - Costo

Fuente: (Elaboración propia)

Para entender el establecimiento de métricas RTO/RPO en la mediana empresa se plantea el siguiente ejemplo:

El caso de una empresa mediana como una administradora de fondos de pensiones local, esta empresa forma parte de un grupo bancario con mucho prestigio en el país, todos sus ingresos que este caso son aportes de los afiliados son canalizados mediante un banco, dicho banco es parte del grupo de empresas, el banco como tal, sus RTO y RPO son casi nulas o muy bajas más o menos 5 minutos ya que cuentan con un redundancia a nivel de almacenamiento, servidores, etc. Aparte de la redundancia en sus dispositivos también cuentan con un sitio de contingencia activo-activo, lo cual les permite responder proactivamente a cualquier contingencia.

La empresa administradora de fondos de pensiones también cuenta con redundancia en sus aplicativos, sin embargo sus RPO son de 15 minutos que es el tiempo en el que sus sistemas e infraestructura más críticas están siendo replicadas en su sitio de contingencia, sus RTO son de 5 minutos que es el tiempo en que se demoran en reanudar los servicios críticos.

Recordemos que en el mejor de los casos estos tiempos de respuesta pueden ser los establecidos, sin embargo los incidentes no siempre son por desastres naturales, existen casos de un mal dimensionamiento de un UPS, una mala configuración de un conmutador que pueda causar un loop en la red que a su vez ocasione una pérdida en las conexiones, una actualización mal aplicada a los sistemas críticos de la empresa (Futch, 2015).

Los RTO y RPO deben ser asociados con los sistemas de información que previamente se ha clasificado como sistemas de misión crítica, una vez que ha ocurrido un desastre la organización debe de considerar la prioridad que debe tener para recuperar los componentes de hardware y software, con el objetivo de asegurar el cumplimiento de los plazos del RTO Y RPO. Todos los componentes red, hardware, software, personal involucrado etc. deben de ser identificados previamente. Para asegurar el funcionamiento posterior a un desastre es necesario asegurarse que la infraestructura de contingencia se encuentre en un sitio alejado del sitio principal o en un almacenamiento externo como cintas magnéticas que permitan resguardar la información. (Bahan, Chad, 2013)

2.3.6 Personal involucrado

Los sistemas de misión crítica dependen en la mayoría de los casos de personal con habilidades y conocimientos únicos, identificar a este personal que tiene conocimientos para recuperar la infraestructura es clave para el buen funcionamiento de un plan de recuperación de desastres.

El conocimiento debe de estar disperso geográficamente en la organización esto garantiza que la organización cuente con suficiente personal capacitado para la ejecución de un plan de recuperación de desastres. Todos estos procesos y conocimientos deben de ser documentados y actualizados constantemente. Se debe conformar equipos con personal de todas las áreas de la organización que deben de ser los encargados de conformar, desarrollar y actualizar el plan de recuperación de desastres debido a que son ellos los expertos conocedores del funcionamiento de los procesos de la institución. (Bahan, Chad, 2013)

Para asegurarse que el plan de recuperación de desastres tenga éxito es necesario realizar pruebas periódicas que permitan comprobar el buen funcionamiento de nuestro DRP en base a nuestros RTO Y RPO establecidos, es ahí donde se dará cuenta si se debe de hacer algún ajuste a nuestro plan, no realizar pruebas al plan de recuperación de desastres es equivalente a no tener un plan de recuperación de desastres (Bahan, Chad, 2013).

2.3.7 Evaluación de los esquemas DRP

El rango disponible de opciones de recuperación de datos a menudo es descrito en términos de niveles, la tabla 3 describe estos niveles, en donde pueden redefinirse a medida la tecnología avance, los niveles 1 y 2 representan el estado de reposo en frío y del 5 al 7 el estado de reposo en caliente.

Tabla 3. Niveles de recuperación

Niveles	**Descripción**	**RTO**	**RPO**
1	Copia de seguridad en tiempo real	2 - 7 días	2 - 24 horas
2	Copia de seguridad en cinta en sitio remoto	1 - 3 días	2 - 24 horas
3	Punto de disco en copia de tiempo	2 - 24 horas	2 - 24 horas
4	Registro remoto	12 - 24 horas	5 - 30 minutos
5	Concurrente ReEx	1 - 12 horas	5 - 10 minutos
6	Datos espejo	1 - 4 horas	0 - 5 minutos
7	Datos espejo con error	0 - 60 minutos	0 - 5 minutos

Fuente: (Alhazmi & Malaiya, 2013)

Históricamente el valor máximo de restauración ha sido de 24 horas para el RPO, si la copia de seguridad es un sistema de replicación síncrono este es de 0.

El tiempo objetivo de recuperación (RTO) y el punto objetivo de recuperación (RPO) son los principales objetivos que deben satisfacerse cuando se evalúa la solución óptima con un coste global determinado.

Aquí se examinan los factores que deben de considerarse para evaluar el costo del sistema asumiendo que los costos se calculan anualmente. El costo total anual del sistema se presenta como

C_T que es igual a la suma del costo inicial C_i (amortizado anualmente) más el costo en curso C_o más el costo anual esperado de desastres potenciales C_d

$$C_T = C_i + C_o + C_d$$

(1)

El costo en curso C_o es la suma de los costos de almacenamiento en curso C_{os} más el costo de la transferencia de datos C_{ot} mas el costo de procesamiento C_{op}

$$C_o = C_{os} + C_{ot} + C_{op}$$

(2)

El costo anual de desastres es el costo total esperado de las recuperaciones de desastres C_{ri} más el costo de los desastres irrecuperables C_{ui}. Para un tipo de desastres i la probabilidad de ocurrencia sería p_i

$$C_d = \sum_i p_i(C_{ri} + C_{ui})$$

(3)

Tenga en cuenta que el costo de recuperación incluye el costo de uso de la copia de respaldo después del error y el costo de las transacciones perdidas. El costo de las transacciones perdidas es proporcional a la duración del RTO. La pérdida de reputación también debe de ser considerada.

El RTO determina el tiempo que la empresa se tarda en reanudar las operaciones, esto dependerá de los factores que afectan al nivel en el plan de recuperación de desastres, en donde:

- Nivel 1: Configuración del equipo y tiempo de inicialización
- Nivel 2: Tiempo de arranque del sistema operativo
- Nivel 3: Tiempo de inicialización de las aplicaciones
- Nivel 4: Tiempo de restauración de los datos / procesos
- Nivel 5: Tiempo de preparación, verificación y conmutación IP.

El RTO dependerá principalmente del sitio alterno, como mínimo sería en el nivel 5, para un sitio que comienza completamente en frío se requerirán todos los niveles.

$$RTO = Fracción\ de\ RPO + \sum_{j\ min}^{5} T_j \quad (4)$$

Donde j min depende de la disponibilidad del servicio y la fracción de RPO representa la información perdida desde el último respaldo. En la tabla 4 se muestran algunas pérdidas de ingresos por tipo de industria en donde se observa que la industria energética y la de telecomunicaciones es la más afectada (Alhazmi & Malaiya, 2013).

Tabla 4. Pérdidas en industrias específicas

Industria	**Ingreso $ /Hora**	**Ingreso $/Empleado - Hora**
Energía	2,817,846	569.2
Telecomunicaciones	2,066,245	186.98
Manufactura	1,610,654	134.24
Instituciones Financieras	1,495,134	1079.89
Tecnologías de la Información	1,344,461	184.03
Aseguradoras	1,202,444	370.92
Ventas al por menor	1,107,274	244.47
Farmacéuticas	1,082,252	167.53
Bancos	996,802	130.52
Procesadoras de alimentos y bebidas	804,192	153.1
Productos de consumo	785,719	127.98
Químicos	704,101	194.53

Industria	Ingreso $ /Hora	Ingreso $/Empleado - Hora
Transporte	668,586	107.78
Utilidades	643,250	380.94
Salud	636,030	142.58
Fuentes naturales	580,588	153.11
Servicios profesionales de TI	532,510	99.59
Electrónica	477,366	74.48
Constructoras	389,601	216.18
Multimedia	340,432	119.74
Viajes	330,654	38.62

Fuente: (Alhazmi & Malaiya, 2013)

2.4 Recuperación de desastres en la nube (DRAAS)

Como se ha observado, la computación en la nube provee servicios que se ajustan a la realidad de las empresas como ser costos, ahorro de tiempo, menos dependencia de personal de tecnología, mejora de rendimientos etc. En esta sección se analiza la situación de la computación en la nube como mecanismo de recuperación de desastres de TI.

Recuperación de desastres como servicio es una nueva nomenclatura de computación en la nube, es una alternativa a muy bajo costo comparado con la tradicional recuperación de desastres, permite realizar una flexible recuperación de datos físicos o virtuales, cuenta con alternativas pre-construidas para ambientes virtuales de recuperación, incluyendo seguridad perimetral, conectividad en la red y conmutación por error cuando continuamente se está replicando entre servidores, cuando ocurre un desastre la organización puede operar y ejecutar sus aplicaciones hasta que se reanude la operación en el sitio principal. La recuperación de datos como servicio es gratis o de pago, cuando se producen cambios e incompatibilidades se puede producir una desconexión del servicio en la nube (Mr.Akshay A. Gharat, 2015).

La arquitectura de la recuperación de desastres en la nube se puede clasificar por tres modelos:

- Desde la nube: es cuando el sitio principal se encuentra en la nube y el sitio alterno se encuentra en un centro de datos privado.

- En la nube: cuando el sitio primario y el sitio secundario se encuentran en la nube.

- Hacia la nube: cuando la aplicación se encuentra en un centro de datos particular y el sitio alterno se encuentra en la nube.

Estas soluciones son servicios pre-empaquetados que proveen un estándar de recuperación a fallas que se pueden comprar o pagar por uso basado en los RTO Y RPO.

2.4.1 Ventajas y desventajas

- Ventajas

    - Reduce los costos de infraestructura tecnológica altamente costosa
    - Ejecución de respaldos de información fuera de la empresa
    - Tiempo de recuperación mínimo después de ocurrir algún desastre
    - El plan de recuperación de desastres se puede adoptar a una mezcla local y fuera de la empresa.

- Desventajas

    - Hay una gran dependencia con el proveedor de los servicios en la nube ya que es probable que haya muy poca penetración en los procedimientos de contingencia, los recursos financieros dependen de otra compañía así como problemas de calidad por parte del proveedor.
    - Se desconoce el almacenamiento de la información de la empresa lo que puede generar problemas de seguridad y un riesgo de pérdida de información confidencial.
    - Personalización de los servicios ofrecidos no siempre es posible.

- La incorporación de equipos externos es complicada ya que la información puede estar en diferentes centros de datos.
- La implementación de una solución es la nube puede ser problemática si no se cuenta con un ancho de banda apropiado.
- Las empresas miran las nubes públicas como inseguras por lo que evitan proveedores que den un servicio de este tipo.

2.4.2 Comparación entre DRP tradicionales y DRP en la nube

La computación en la nube ha sido sugerida como una nueva solución en la recuperación de desastres de TI, gracias a su costo de implementación bajo, escalabilidad y con un modelo que pagas por lo que usas claramente es una opción viable. Asimismo el control y la seguridad basada en la nube puede ser una preocupación si los datos críticos se almacenan fuera de la jurisdicción de una empresa. Los sistemas de respaldo pueden estar localmente o implementados usando servicios en la nube como Amazon Web Services.

Los planes de recuperación de desastres tradicionales son los más comunes en las empresas hoy en día, sin embargo este método contiene ciertas falencias que pueden ser compensadas con la incorporación de la computación en la nube. A continuación se presenta una comparación entre ambas soluciones:

- Protección casi continua de la información: En los DRP tradicionales los tiempos de recuperación de respaldos de información son más largos (horas e incluso días) teniendo en cuenta que los respaldos completos se realizan con cierta frecuencia y los incrementales diariamente, esto no es suficiente en muchas ocasiones para recuperarse de un desastre tecnológico. En cambio los DRP en la nube con la virtualización existen mecanismos que ayudan a determinar el cambio en el almacenamiento del disco duro para así respaldar esa información de forma programada que ayude a una protección continua de los datos.

- Mejora en los RTO y RPO: Considerable mejora en el objetivo de punto de recuperación (RPO) ya que la información está con protección casi continua a través

de soluciones de respaldo virtual, lo cual es contrastado con los métodos de recuperación tradicionales, para el caso del tiempo objetivo de recuperación (RTO) en caso de fallas de hardware se realizan recuperaciones del servidor virtual de forma inmediata.

- Instalación y uso: En los DRP tradicionales es necesario el uso de software y hardware especializado para la ejecución de los respaldos de información así como personal altamente capacitado para la ejecución del puesto ya que un respaldo mal ejecutado puede convertirse en pérdidas considerables para la empresa en caso de surgir algún desastre. Los DRP en la nube con la virtualización la facilidad de uso se vuelve una ventaja ya que se realizan respaldos completos de todo un servidor con una restauración muy rápida en caso de darse la necesidad si cuentan con un la infraestructura adecuada.

- Verificación y seguridad de los respaldos: El respaldo tradicional podría asegurar que se realizó con éxito pero no garantiza la utilidad al momento de realizar una restauración en caso de un desastre esto sin olvidar que los aplicativos que ofrecen mecanismos de encriptación generalmente son costosos. En la nube la verificación de los respaldos se realiza automáticamente independientemente del ambiente en que se ejecute, todo esto con un estándar de encriptación avanzada.

- Almacenamiento eficiente y flexible de la información: El uso eficiente del espacio en disco duro es crucial, la deduplicación ha demostrado ser una solución bastante estable en las soluciones tradicionales de respaldos de información a diferencia de las copias de seguridad con base en la nube que son una opción para tener flexibilidad en el almacenamiento de la información, tradicionalmente en caso de desastres estas copias deben almacenarse lejos de la infraestructura, esto indica llevar los respaldos en cintas fuera del lugar, esto es más propenso a riesgos debido a causas como errores humanos, pérdida o robo de información es por eso que la nube es una solución más confiable y rentable para obtener copias de seguridad en lugar de llevarlas fuera del sitio. (Manella Lemos, 2012).

2.4.3 Recomendaciones para un plan de recuperación de desastres en la mediana empresa

En la actualidad se piensa que una interrupción en las operaciones tiene un impacto económico de las grandes empresas, sin embargo la realidad es que el impacto es igual tanto para grandes, medianas o pequeñas empresas. A continuación se muestran ciertas recomendaciones que se deberían de adoptar en las medianas empresas ante la prevención de un desastre (Ávila Mejía, 2011):

- Cifrado de la información: En caso de ocurrir algún desastre y es necesaria la conexión remota se recomiendan conexiones seguras con un estándar de encripción avanzado.
- Redundancia: mantener múltiples copias de seguridad y de respaldos de los aplicativos críticos de la empresa al menos a una distancia de 250 kilómetros para que en caso de ocurrir alguna eventualidad poder reanudar las operaciones a la brevedad posible.
- Monitoreo: realizar revisiones continuas con el proveedor de los servicios en la nube al plan de recuperación de desastres y realizar pruebas trimestrales.
- Prevención de caídas de los sistemas: Con la adopción de un plan de recuperación de desastres en la nube se pueden crear réplicas de los ambientes de producción lo que permite a las organizaciones realizar pruebas de actualización de los sistemas antes de implementarlas en el ambiente de producción.

Capítulo III. Metodología

El objetivo de este capítulo es dar a conocer cómo se llevará a cabo el trabajo de investigación, se darán a conocer las metodologías para el desarrollo de la misma, los instrumentos a utilizar y la selección de las herramientas que servirán de base para contestar la pregunta de investigación.

3 Tipo y enfoque de la investigación

El enfoque para esta investigación es mixto con un alcance explicativo/exploratorio, es exploratorio porque la recuperación de desastres es la nube en la mediana empresa de Tegucigalpa es un tema poco estudiado, del cual se tienen muchas dudas y es explicativo ya que busca exponer por qué ocurre dicho fenómeno.

Las investigaciones cuantitativas buscan recolectar los datos con el objetivo principal de establecer un comportamiento y probar teorías a diferencia de las investigaciones cualitativas que buscan la comprensión de los fenómenos (Sampieri, 2014).

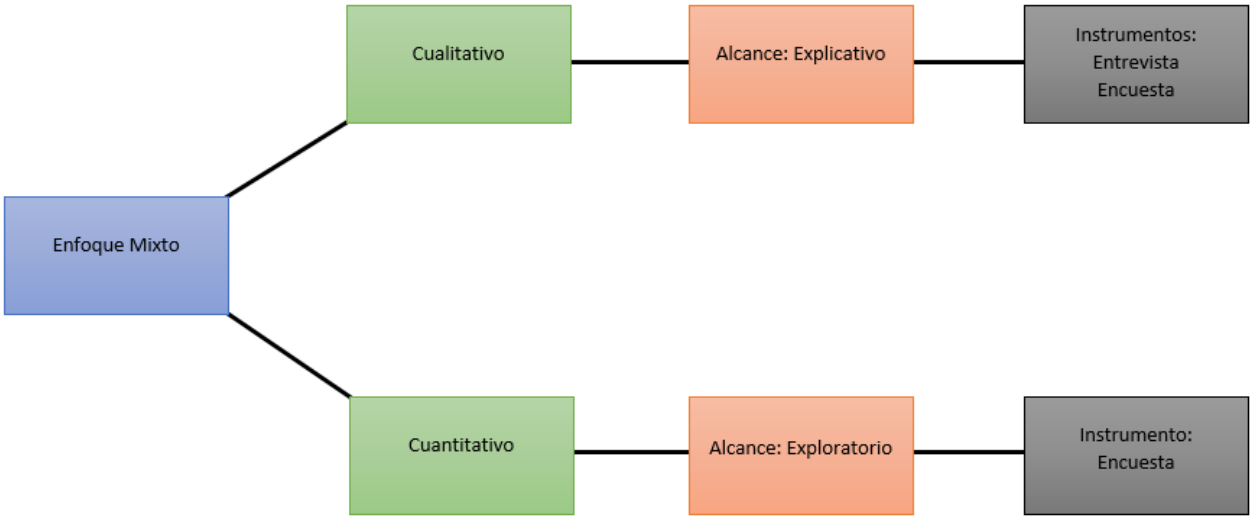

Figura 7: Diseño del enfoque y métodos

Fuente: (Elaboración propia)

3.1 Diseño de la investigación

En esta sección se muestra el diseño de la investigación así como los instrumentos a utilizar para la recolección de la información y el análisis de los resultados.

3.2 Esquema de la investigación

En la siguiente figura se muestran los pasos a seguir para el desarrollo de la investigación

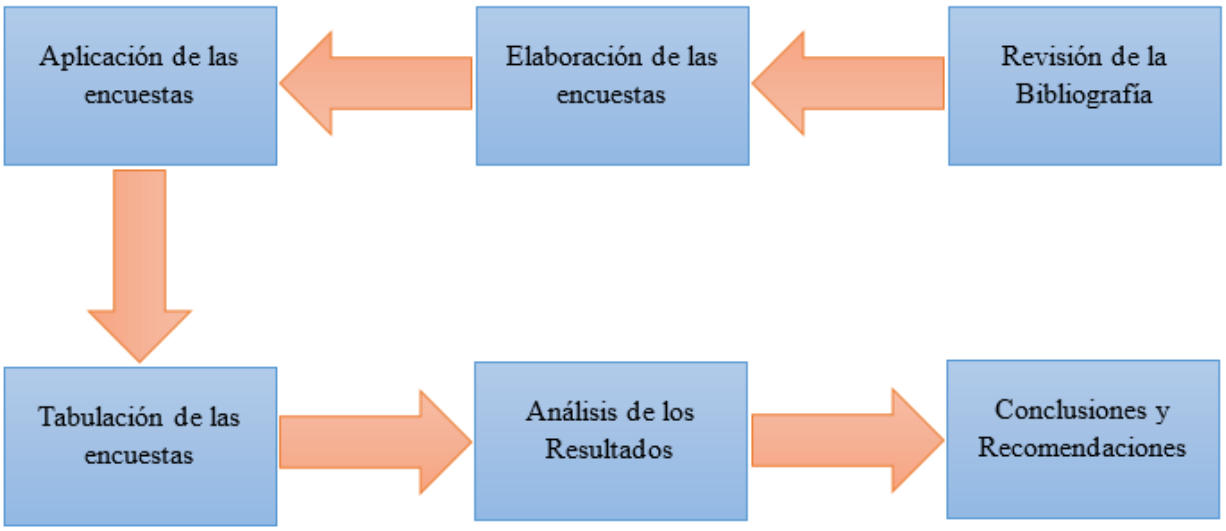

Figura 8: Desarrollo de la investigación

Fuente: (Elaboración propia)

3.2.1 Población

Esta investigación está dirigida para las compañías de seguros medianas en la capital de Tegucigalpa, según la Cámara de Comercio e Industria se registran 4 aseguradoras medianas con un rango de empleados de 51-150.

Tabla 5: Aseguradoras Medianas en Tegucigalpa

Nombre de la aseguradora
Seguros Crefisa S,A
Seguros del País S,A
Mapfre Seguros Honduras

Nombre de la aseguradora
Seguros Lafise S,A

Fuente: (Elaboración Propia)

3.2.2 Muestra

En base a la información obtenida la muestra consiste en tomar el total de la población de aseguradoras medianas en Tegucigalpa debido a que la población es finita y pequeña. El número total de aseguradoras medianas que integra la población es un total de 4.

3.2.3 Instrumentos a utilizar

Para poder desarrollar esta investigación como fuentes primarias se recurrirá al uso de herramientas que ayuden a la recolección de los datos, se detallan a continuación:

- Encuesta: es una técnica que recoge los datos por medio de la aplicación del cuestionario a la muestra seleccionada, por medio de las encuentras se pueden conocer las opiniones y comportamientos de la población, en el anexo 1 se podrá observar la encuesta que se aplicará a las empresas medianas en Tegucigalpa.

    - Objetivos: La definición del objetivo principal de la encuesta de investigación es primordial ya que ayudará a entender el cómo y por qué de la encuesta.

    - Diseño del cuestionario: Aquí se elaboran las preguntas que se realizarán a los encuestados de la muestra, las preguntas serán cerradas y deben ser realizadas con el objetivo de conseguir información planteada en los objetivos.

    - Recopilación de los datos: Aquí es aplicada la encuesta a la población seleccionada.

    - Análisis e interpretación de la información: Aquí se analiza la información obtenida de los encuestados y se interpretan los resultados obtenidos.

- Documentación de los hallazgos: Aquí se emitirán las conclusiones luego de aplicar la metodología y técnicas descritas anteriormente que responderán a la pregunta de investigación.

- La Entrevista: Esta es una técnica en donde la persona (entrevistador) aplica un cuestionario a los participantes; el entrevistador realiza un conjunto de preguntas y anota las respuestas (Sampieri, 2014). En el anexo 2 se encuentra el cuestionario que se aplicará a los conocedores del tema.

Capítulo IV. Resultados y Análisis

Este capítulo comprende la interpretación de la información recolectada mediante los instrumentos designados para la investigación. La encuesta realizada, así como las entrevistas dieron un panorama de cómo está la situación actual de las aseguradoras medianas en Tegucigalpa.

4 Antecedentes del rubro de las aseguradoras

Para obtener el número de aseguradoras medianas en Tegucigalpa se contactó a la Lic. Karla Ruiz quien tiene el cargo de Gerente General de la Cámara de Comercio e Industrias de Tegucigalpa en donde formalmente se le hizo el requerimiento de información en donde se puede observar en el anexo 3. Se identificó que actualmente en Tegucigalpa hay 195 empresas registradas de las cuales 4 son destinadas al rubro de las aseguradoras.

4.1 Resultados y Análisis de las encuestas

Se aplicó una encuesta por aseguradora siendo el gerente de tecnologías de la información o al oficial de seguridad de la información ya que estos son los principales encargados de velar por la continuidad del negocio en caso de ocurrir un desastre.

Se muestran a continuación el análisis de cada una de las preguntas formuladas en la encuesta que se aplicó dentro de las aseguradoras medianas de Tegucigalpa.

1. ¿Cuál es el porcentaje anual de presupuesto que la empresa asigna a la seguridad de la información?

Según los resultados obtenidos, las aseguradoras encuestadas 3 de ellas que representan un 75% de la población destinan entre un 6% y 10% de su presupuesto anual para la seguridad de la información y la otra que representa el 25% destina un 16% o más del presupuesto anual, esto indica que las compañías de este rubro tienen conciencia y conocen de la importancia que tiene la seguridad de la información, también representa un alto nivel de madurez en las diferentes áreas de la empresa ya que hoy en día la concesión de recursos para la protección de los datos suele generar conflictos entre las diferentes áreas de una empresa, a diferencia de inversiones en instalaciones o

maquinaria, el beneficio es más difícil de percibir ya que las herramientas de seguridad no buscan aumentar las ganancias, si no disminuir posibles pérdidas.

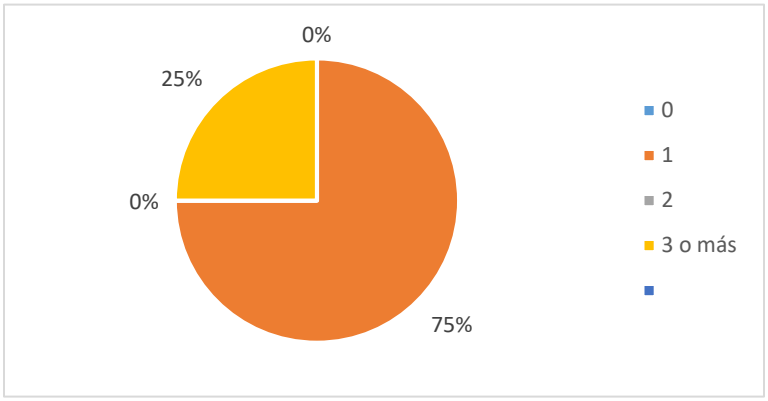

Gráfico 4: Porcentaje anual de presupuesto asignado a la Seguridad de la Información

Fuente: (Elaboración propia)

2. Para la administración de las tecnologías de la información, ¿La empresa cuenta con personal propio o es un tercero?

De manera unánime, observamos que las aseguradoras medianas en Tegucigalpa cuentan por personal propio que administra las tecnologías de la información, lo cual indica que las mismas presentan un grado de desconfianza hacia empresas terceras ya que la información que manejan es confidencial y una fuga de la misma puede afectar de forma negativa a la compañía.

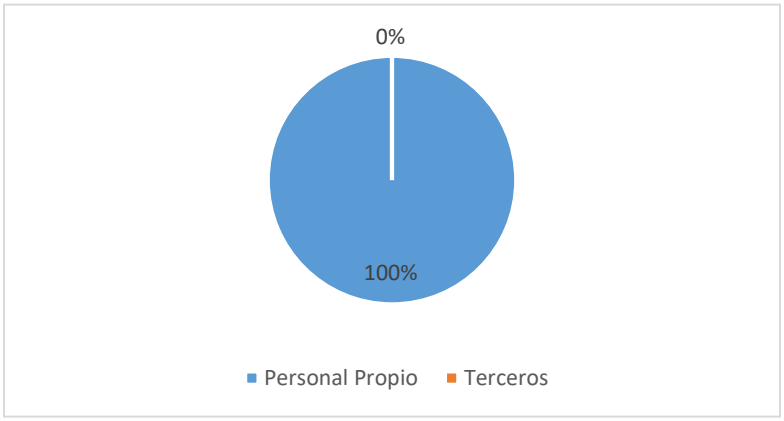

Gráfico 5: Administración de las Tecnologías de la Información

Fuente: (Elaboración propia)

3. ¿La empresa tiene implementado un plan de recuperación de desastres de TI?

El 100% de las aseguradoras cuenta con un plan de recuperación de desastres por lo que están preparadas ante alguna eventualidad que pueda ocurrir en su centro de datos.

Se puede concluir que las aseguradoras del rango de la mediana empresa en Tegucigalpa se encuentran preparadas en caso de ocurrir un desastre que pueda poner el riego los servicios principales.

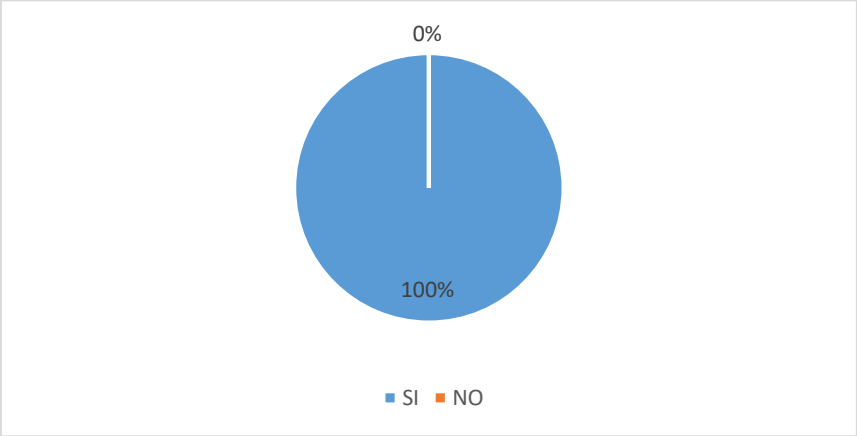

Gráfico 6: Implementación de un plan de recuperación de desastres

Fuente: (Elaboración propia)

4. ¿El plan de recuperación de desastres de TI implementado en la empresa es tradicional o en la nube?

Según las aseguradoras encuestadas afirman en un 100% que su plan de recuperación de desastres de tecnologías de la información es tradicional, esto indica que hay un grado de rechazo a un plan de recuperación de desastres en la nube, sabiendo que los planes de recuperación de desastres tradicionales son mucho más costosos ya que se necesita tener dos sitios idénticos (uno primario y otro secundario) situados a cierta distancia de separación.

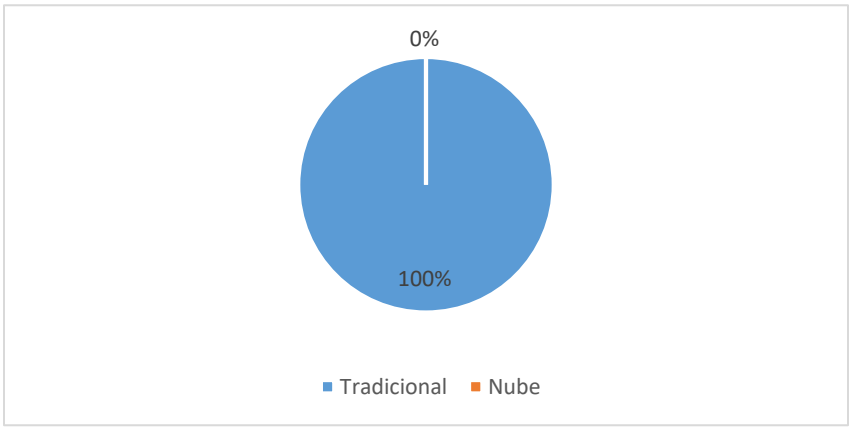

Gráfico 7: Tipo de plan de recuperación de desastres

Fuente: (Elaboración propia)

5. En los últimos 12 meses, ¿A ocurrido algún incidente en el que tenga que ejecutar su plan de recuperación de desastres?

De manera unánime, se observa que las aseguradoras encuestadas no han reportado incidentes en un año en el que se tenga que activar el plan de recuperación de desastres, esto indica que las mismas tienen implementados los controles necesarios para así poder mitigar posibles riesgos que en caso de suceder puedan ocasionar un desastre para la empresa.

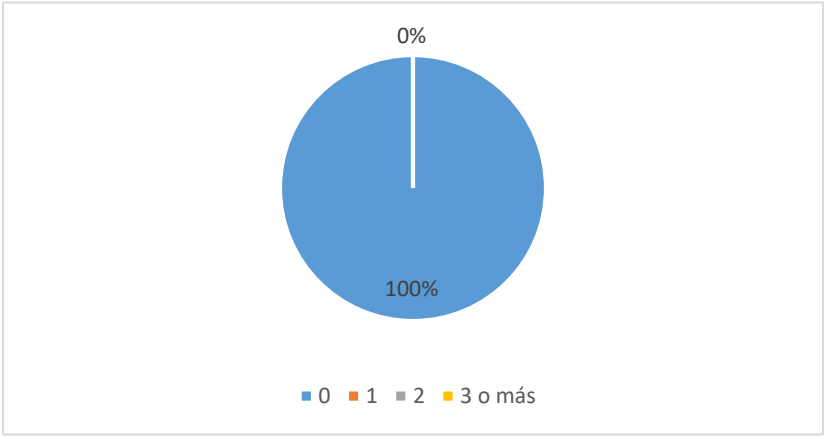

Gráfico 8: Incidencias en los últimos 12 meses

Fuente: (Elaboración propia)

6. En los últimos 12 meses ¿Cuantas veces ha realizado pruebas a su plan de recuperación de desastres?

El 75% por ciento de las aseguradoras encuestadas al menos una vez ha ejecutado pruebas de su plan de recuperación de desastres y un 25% ha realizado dichas pruebas al menos dos veces en los últimos 12 meses. Realizar pruebas al plan de recuperación de desastres debe de realizarse mínimo 2 veces al año esto debido a que los cambios en la infraestructura son constantes y hay cambios que puedan afectar los servicios al momento de ejecutar dicho plan.

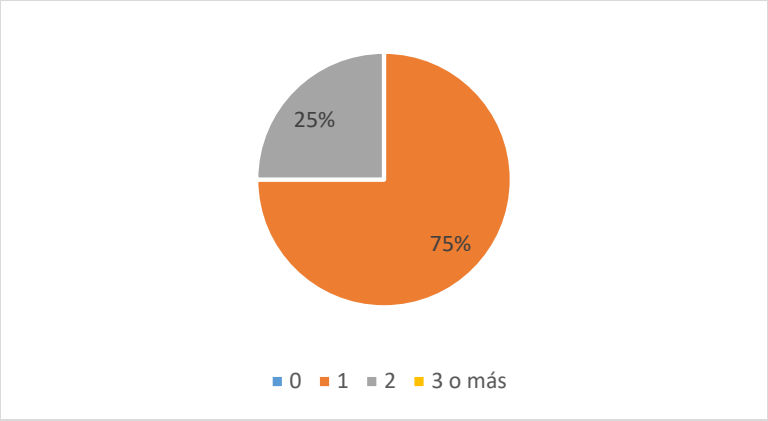

Gráfico 9: Pruebas al plan de recuperación de desastres

Fuente: (Elaboración propia)

7. En caso de ocurrir algún desastre, ¿Conoce el tiempo que le costará reanudar las operaciones (RTO) a la empresa y cuál es la capacidad de recuperar la información en el punto anterior (RPO)?

El 100% de las aseguradoras conocen el tiempo en que tardaran en reanudar los servicios críticos (RTO) y también han realizado un análisis de cuánto tiempo están dispuestos a tolerar para reanudad los servicios (RPO). Esto indica que las organizaciones han cuantificado sus tiempos y documentado sus procesos de respuesta en caso de ocurrir algún desastre

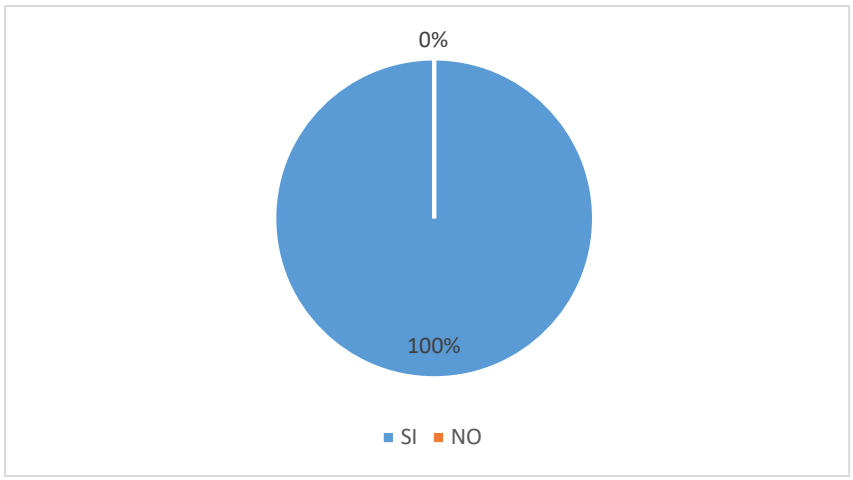

Gráfico 10: Reanudación de operaciones y capacidad de recuperar la información

Fuente: (Elaboración propia)

8. ¿La empresa está incursionando en algún nuevo proyecto de computación en la nube?

El 50% de las aseguradoras encuestadas están incursionando en al menos un proyecto que involucre la organización con respecto a servicios en la nube, esto es positivo ya que poco a poco las organizaciones están adaptándose a utilizar uno o más servicios en la nube y no de manera tradicional.

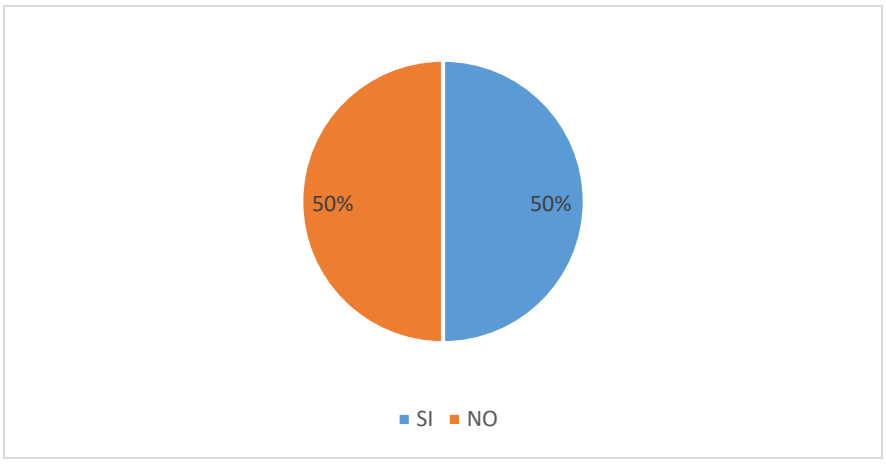

Gráfico 11: Incursión de la computación en la nube

Fuente: (Elaboración propia)

9. ¿La empresa tiene implementadas herramientas de colaboración en la nube?

El 75% por ciento de la población ya tiene implementadas herramientas de colaboración en la nube y el 25% de la población aun manejan herramientas de colaboración tradicional, se puede observar que existe aceptación por parte de la población en cuanto a herramientas de colaboración en la nube.

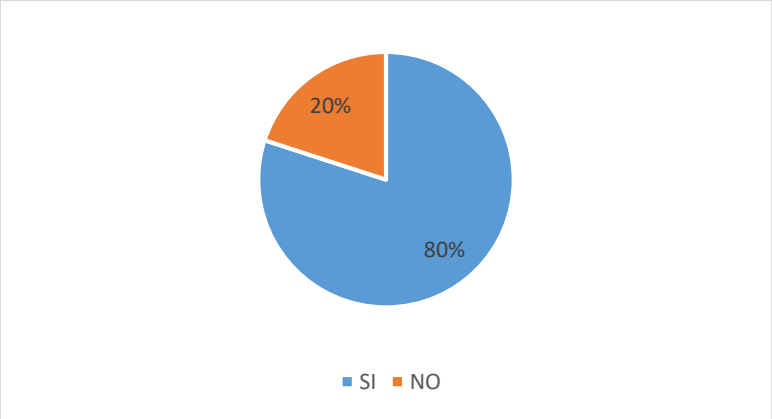

Gráfico 12: Herramientas de colaboración en la nube

Fuente: (Elaboración propia).

10. ¿Contrataría a un proveedor de servicios en la nube para que esté a cargo de su plan de recuperación de desastres?

El 100% de las aseguradoras NO implementarían su plan de recuperación de desastres en la nube, existe poca aceptación en cuanto a implementar una solución de este tipo en las aseguradoras que están en la categoría de mediana empresa de Tegucigalpa.

En la mayoría de los casos nos expresaron que la política interna no les permite sacar las bases de datos de sus clientes debido al riesgo de que esta base de datos pueda ser violentada exponiendo la información de sus clientes esto puede desencadenar en un riesgo reputacional que les impacte directamente y les pueda generar el retiro masivo de sus asegurados y esto pueda ser traducido en perdida monetarias e inclusive el cierre de la organización.

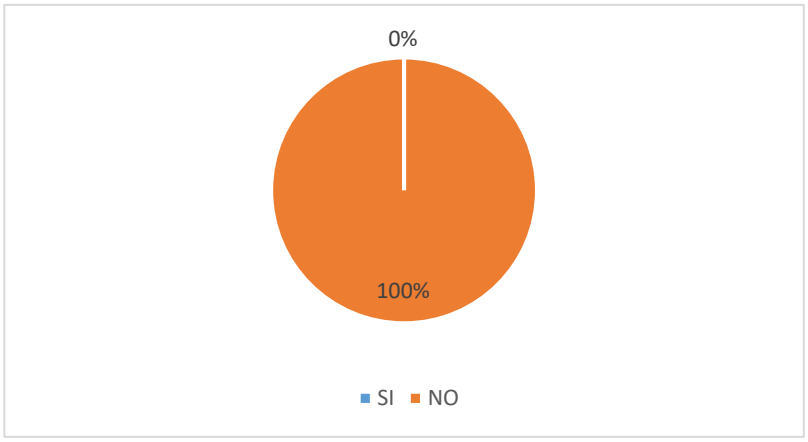

Gráfico 13: Proveedor a cargo de un plan de recuperación de desastres

Fuente: (Elaboración propia)

11. ¿Si usted implementara un plan de recuperación de desastres de tecnología en la nube preferiría que el proveedor de dichos servicios fuese local o internacional?

El 100% de la población contrataría un proveedor de servicios en la nube de origen internacional y ninguno contrataría proveedores de origen local. Esto ayudaría a mitigar algunos riesgos y consideraciones como por ejemplo la posición geográfica que debe de existir entre sitio principal y sitio alterno.

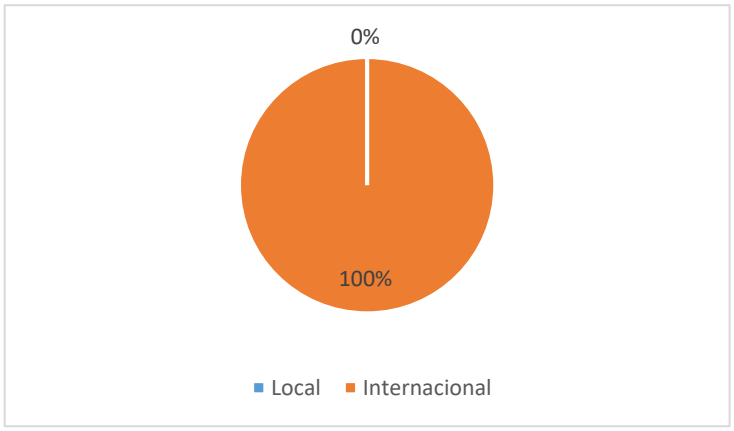

Gráfico 14: Proveedor local o internacional

Fuente: (Elaboración propia)

12. ¿Conoce alguna empresa local que provea servicios de recuperación de desastres en la nube?

El 75% de las aseguradoras tienen conocimiento de proveedores locales que les permitan implementar un plan de recuperación de desastres en la nube, se puede observar que la mayor parte de la población esta consiente de la existencia de esta alternativa de solución en cuanto a recuperación de desastres. Las empresas más conocidas que ofrecen servicios en la nube son Cable & Wireless y GBM.

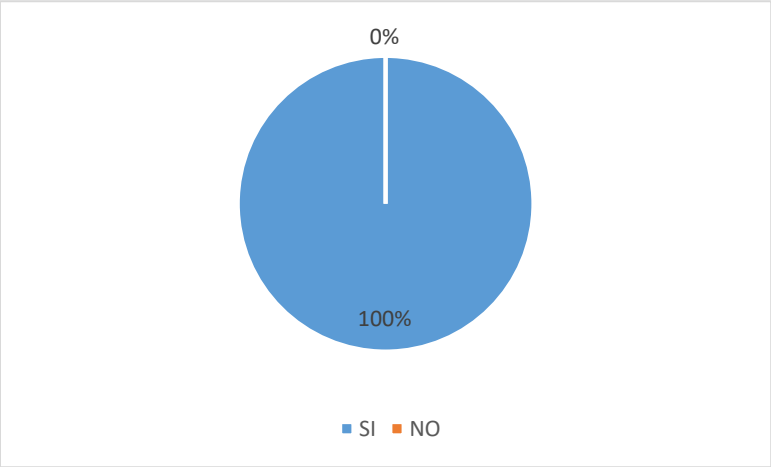

Gráfico 15: Empresas hondureñas que provean planes de recuperación de desastres en la nube

Fuente: (Elaboración propia)

13. Según su criterio ¿Cuáles son las causas de que las empresas no realicen sus planes de recuperación de desastres en la nube?

Según los resultados de las encuestas un 14.85% para problemas de seguridad y un 14.85% para políticas internas de la empresa son las mayores causas por las que las aseguradoras no realizan sus planes de recuperación de desastres en la nube. Este tipo de empresas maneja información confidencial de todos sus clientes y que un proveedor externo que no tenga los controles adecuados para resguardar esta información la pierda puede tener resultados catastróficos para la institución si cae en las manos incorrectas, es por eso que las empresas establecen políticas internas que evitan este tipo de soluciones como una alternativa en caso de un desastre.

La causa más baja es la renuencia al cambio con un 8.9% esto es positivo ya que indica que los altos ejecutivos de estas empresas saben la importancia del uso de las tecnologías de la información como una solución viable.

Los problemas en la red son una causa muy común ya que la información que se respalda en la nube generalmente son archivos muy grandes y se necesita de un proveedor que cumpla con el ancho de banda adecuado para poder hacer una carga y descarga correcta de los archivos en el tiempo oportuno.

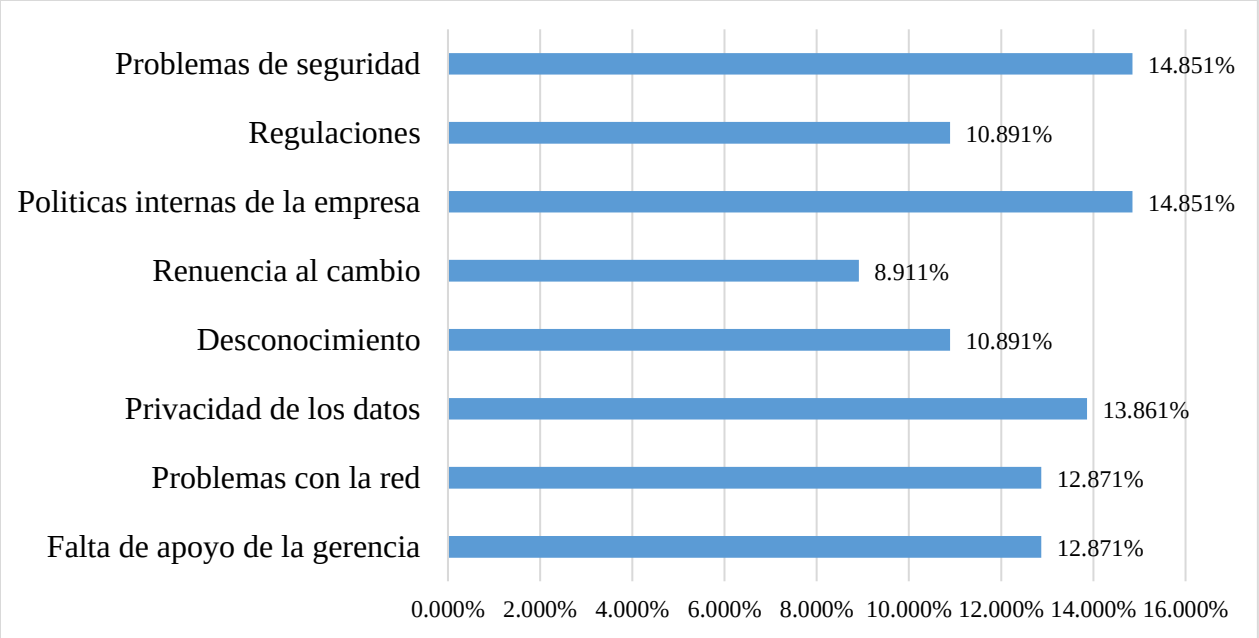

Gráfico 16: Causas de las empresas de no realizar DRP en la nube

Fuente: (Elaboración propia)

14. Para la implementación de un plan de recuperación de desastres en la nube el proveedor de dichos servicios es un factor clave, el proveedor debe asegurar:

Según los encuestados un 21.17% para la disponibilidad y un 21.17% para la seguridad son los atributos que más relevancia tienen que tener los proveedores que den este tipo de soluciones

ya que es importante contar con la información en el tiempo oportuno, así como la integridad y confidencialidad de los datos.

Con un 9.41% la fácil migración no es un factor tan clave para las aseguradoras ya que la responsabilidad recae directamente en el proveedor y es el mismo el que tiene que velar por la migración de la solución ya que si no se cumple con los tiempos establecidos en un principio en el contrato se pueden incurrir en penalizaciones.

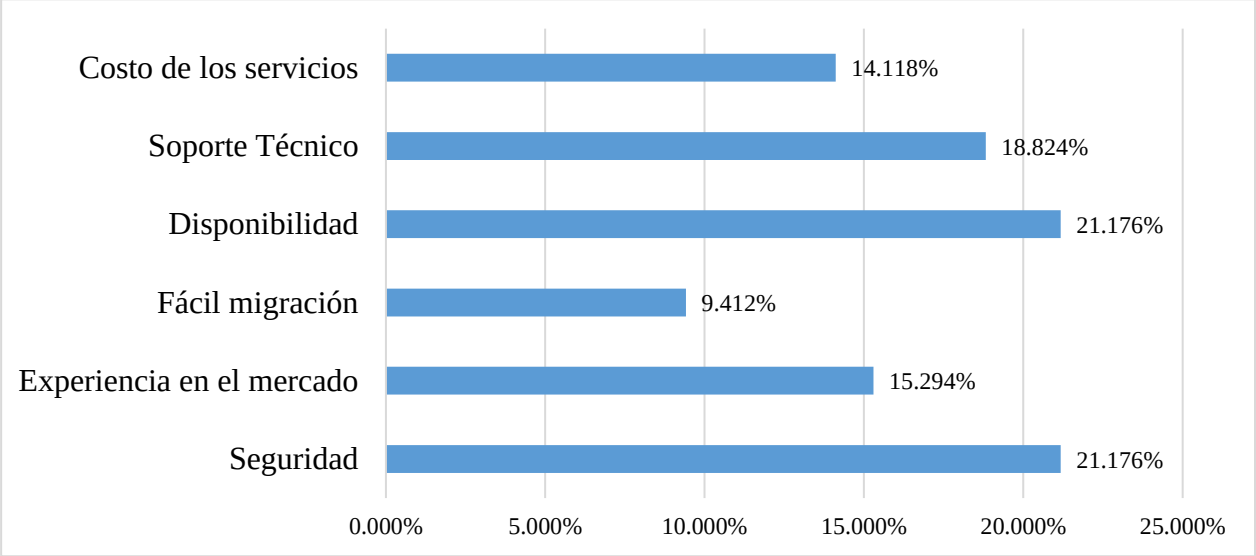

Gráfico 17: Factores a considerar por parte del proveedor al momento de incurcionar en una solución en la nube

Fuente: (Elaboración propia)

15. En caso de ocurrir algún desastre, ¿cuáles serían las consecuencias para la empresa y las partes interesadas (Accionistas, empleados, proveedores, entre otros)?

Según los datos obtenidos el 22.5% de los encuestados opina que la pérdida de confianza de los clientes es el factor que más consecuencias le traería a empresa por debajo de pérdidas financieras y retrasos con clientes y proveedores con un 21.25% para ambos.

Los despidos de personal 8.75% y cierre de la empresa 7.5% son factores muy poco probables esto debido a que las aseguradoras pertenecen a un grupo financiero en la que están respaldadas

por una o más empresas, esto indica que en caso de un desastre las consecuencias en este caso son mínimas ya que la empresa puede cubrir pérdidas con los ingresos de otras empresas que forman parte del mismo grupo financiero.

Un 13.75% piensa que se pierden oportunidades de negocio ya que al ser aseguradoras medianas pueden perder parte de su cartera de clientes y la generación de nuevos servicios que tienen las aseguradoras más grandes en el país.

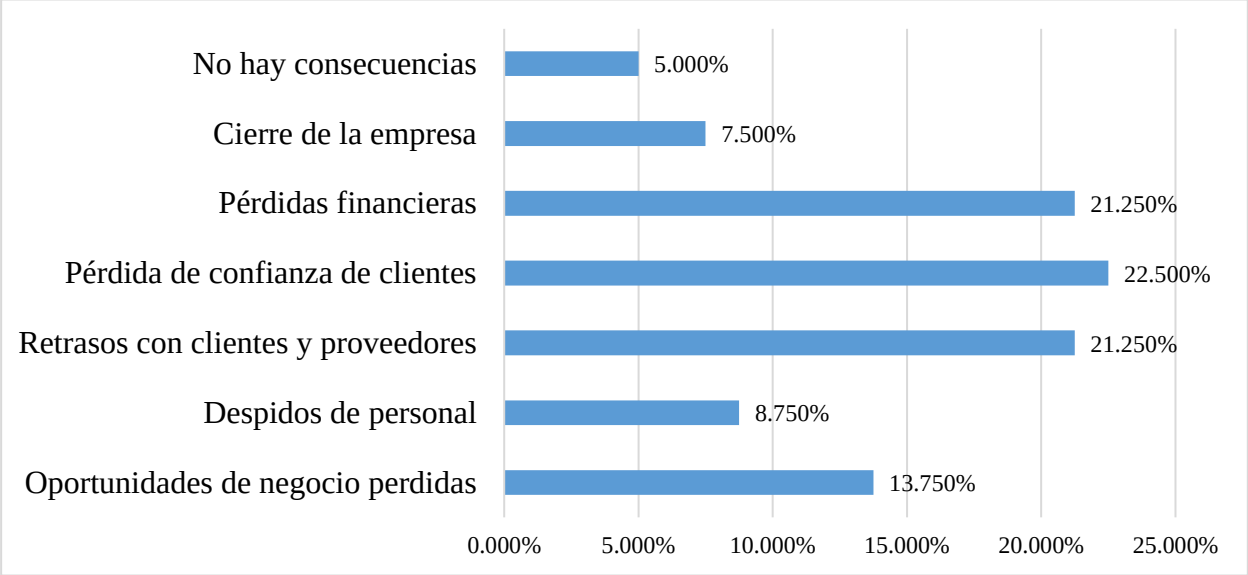

Gráfico 18: Consecuencias en caso de un desastre

Fuente: (Elaboración propia)

4.2 Resultados y análisis de las entrevistas

Como parte de la investigación se procedió a la aplicación del instrumento de la entrevista a expertos del sector de las tecnologías de la información en donde las empresas para las que trabajan ofrecen soluciones tecnológicas incluyendo servicios en la nube.

La entrevista que a continuación se detalla es la misma que se aplicó a los 2 expertos por lo que se condensó en una sola todas las respuestas obtenidas, tomando en cuenta la relación de la respuesta con la pregunta, así como los factores que más destacaron durante la misma.

Participantes:

- Ing. José Manuel Torres Banegas, Jetstereo

- Ing. Egdares Futch, Cable & Wireless

1) ¿Qué es un plan de recuperación de desastres en la nube?

Consiste en aprovechar un conjunto de recursos de procesamiento, memoria, almacenamiento, seguridad y comunicaciones con las que se puede construir cualquier configuración para recuperación de Desastres de aplicaciones y servicios tecnológicos en un Datacenter de terceros.

2) ¿Ha revisado y/o implementado planes de recuperación de desastres en la nube en Honduras?

Sí, he implementado varias soluciones de recuperación de desastres en la nube privada, tanto para grandes, medianas y pequeñas empresas en el país.

3) ¿En nuestro país cómo ve la adopción de un plan de recuperación de desastres en la nube en la mediana empresa?

La mediana empresa está deseosa de mejorar sus costos, y tener mayor agilidad y seguridad en su plataforma tecnológica, por lo que están analizando fuertemente el tema de la nube, esto es muy factible ya que están involucrados fuertes proveedores de estos servicios como ser canales de datos dedicados y diferentes alternativas de solución en plataformas de virtualización On Premise (Nube Privada).

4) ¿Qué es más viable para el rubro de aseguradoras medianas en nuestro país: Un plan de recuperación de desastres tradicional o un plan de recuperación de desastres en la nube?

Para cualquier empresa es más viable el DRP en la nube, sin embargo hay factores regulatorios que lo impiden, para el caso de las nubes públicas esto dependerá de presupuestos y lo que se pretenda proteger como parte de un plan de recuperación.

5) ¿Considera usted que el rubro de las aseguradoras en Tegucigalpa tiene un nivel de madurez alto en cuanto a la adopción de un DRP en la nube?

No conozco de ninguna aseguradora que implemente su DRP en la nube, esto es un tema relacionado a procesos ya que estos ofrecen los mecanismos necesarios para proporcionar continuidad a un negocio o servicio.

6) ¿Cuáles considera usted que son las mayores causas de que ocurra un desastre en una empresa Hondureña?

Los mayores problemas están relacionados a causas humanas más que una causa natural, pero ciertamente después del huracán Mitch es un evento que podría repetirse y se sabe que lamentablemente nuestro país es vulnerable en ese sentido, más allá de estos factores también hay causas como ser: Fallas en el servicio eléctrico, antigüedad de la infraestructura, mala aplicación de parches y malware.

7) ¿Considera usted que es una opción viable para las aseguradoras medianas en Tegucigalpa la adopción de un DRP en la nube?

Sí, siempre y cuando se entienda perfectamente el concepto, se definan y se delimiten responsabilidades y las personas que estarán a cargo de ejecutar un plan de recuperación, está solución en prácticamente viable para todo tipo de empresas.

8) ¿Conoce de casos de éxito de adopción de un plan de recuperación de desastres en la nube en la mediana empresa en Tegucigalpa?

Sí en nubes privadas, la divulgación de estos casos es confidencial por lo que no es posible publicarlos.

9) Las empresas hondureñas prefieren planes de recuperación de desastres en la nube local o internacional? ¿Por qué?

Generalmente no hay preferencia, sin embargo tenerla fuera del país agrega un componente de minoración de riesgo geográfico que permite continuar operaciones en caso de un desastre que afecte al país.

10) **En nuestro país, ¿Qué riesgos hay de que las empresas implementen un plan de recuperación de desastres de TI en la nube?**

Que lo implementen con empresas que no son dueñas de la infraestructura, y que solamente estén rentando o revendiendo servicios de terceros sin notificar a la empresa afectada.

4.3 Análisis de situación actual

El propósito de esta sección es mostrar cual es la situación actual de las aseguradoras medianas en Tegucigalpa.

Se sabe que actualmente las aseguradoras en el país son empresas sumamente rentables y que debido a problemas de seguridad, privacidad de los datos y de red entre otras no optan a una solución en la nube como mecanismo de recuperación de desastres ya que prefieren gastar en infraestructura propia, los riesgos siempre están latentes y por mucha rentabilidad que tengan las empresas al final todo va depender del apetito de riesgos que las mismas tengan para mitigar, reducir o transferir dichos riesgos.

A continuación se muestra y un comparativo entre los costos de implementar un plan de recuperación de desastres tradicional y uno en la nube con la infraestructura adecuada para las operaciones de una aseguradora mediana:

Con este comparativo de los dos esquemas se ha realizado con algunas asunciones como ser la aseguradora ya cuenta con una infraestructura virtual en su sitio principal, cuenta con una estrategia de respaldo en sitio mediante un software automatizado, para el caso de la infraestructura tradicional ya cuenta con un sitio de contingencia medianamente equipado ubicado en una oficina regional en otro departamento del territorio nacional.

Se realizó las respectivas cotizaciones en dos instituciones líderes en el mercado nacional, una oferta en infraestructura tradicional y otra oferta de recuperación de desastres como servicio de acuerdo al siguiente escenario:

Tabla 6: Escenario hipotético de infraestructura en sitio alterno

Cantidad de Máquinas Virtuales	Cuatro (4) Máquinas Virtuales
Memoria RAM por cada Máquina Virtual	16GB por cada máquina virtual
Cantidad de CPU'S	Cuatro (4) Virtual CPU'S
Espacio en Disco Duro	200GB De Disco Duro
Enlace de Datos	10MB

Fuente: (Elaboración Propia)

Tabla 7: Oferta para implementación de DRP tradicional para aseguradoras medianas

Item	**Descripción**	**Precio Unitario**	**Precio Total**
Hardware Software y Servicios			
1	Servidor para Virtualización	$. 9,052.41	$. 9,052.41
2	Switches para Virtualización	$. 4,863.32	$. 4,863.32
3	Licencias de Sistema operativo	$. 1,017.65	$. 1,017.65
4	Licencias de Software de Virtualización	$. 829.18	$. 829.18
5	Licencias de Software de Backup y Replicación	$. 2,117.65	$. 2,117.65
6	Servicios de Instalación y Configuración	$. 4000	$. 4000
Sub-Total			$. 21,880.21
Impuesto Sobre Ventas			$. 3,282.03
Total			$. 25,162.22

Fuente: (Elaboración Propia)

El costo de la inversión de una infraestructura tradicional es de $25,162.00 este equipo tiene garantía a tres (3) Años, posterior a estos tres años la aseguradora puede optar a una extensión de sus garantía tanto en software como hardware.

Tabla 8: Oferta de infraestructura tradicional en modalidad de leasing financiero

Precio del bien	Cuatro (4) Máquinas Virtuales
Plazo	36 Meses
Renta inicial	$. 0.00 más ISV
Renta mensual	$. 965.70 más ISV
Seguro mensual	$. 80.75 más ISV
Pago Mensual	$.1,046.45 más ISV
Total a pagar mensual + ISV	**$. 1,203.35**

Fuente: (Elaboración Propia)

El valor de la propuesta de la infraestructura tradicional en leasing financiero es de $.1203.35

Tabla 9: Oferta para la implementación de recuperación de desastres como servicio

Item	**Descripción**	**Precio Unitario**	**Precio Total**
SERVICIOS			
1	Cloud Connectivity (MPLS, VPN).	$ 500.00	$ 500.00
2	Conectividad de red (WAN, LAN).	$ 250.00	$ 250.00
3	Datacenters (Sitio Principal, Sitio Alteno de recuperación).	$ 700.00	$ 700.00
4	Infraestructura de almacenamiento (SAN)	$ 300.00	$ 300.00
5	Licenciamiento de Herramienta de Replicación	$ 200.00	$ 200.00
6	Servicios de administración, operación y monitoreo	$ 350.00	$ 350.00
7	Licenciamiento de Sistemas Operativos	$ 200.00	$ 200.00
Sub-Total			$ 2,500.00
Impuesto Sobre Ventas			$ 375.00
Total			$ 2,875.00

Fuente: (Elaboración Propia)

Al comparar los valores de las dos soluciones ambas diseñadas a tres años en modalidad de pago mensual, podemos observar que el costo de la infraestructura de recuperación de desastres como servicios es más cara con un valor de $. 2,875.00 comparada contra $. 1,203.00 que costaría la infraestructura tradicional en figura de leasing financiero, notablemente existiría un ahorro mensual de $. 1,672.00 si adquirieran en la solución de infraestructura tradicional.

Claramente podemos observar que tener un plan de recuperación de desastres en la nube es más caro en nuestro país que tener el plan de recuperación de desastres tradicional. El contratar estos servicios en estos momentos no es viable para las aseguradoras medianas de Tegucigalpa ya que debido a que no hay muchas empresas que proveen este tipo de servicios las que lo hacen se observa que sus costos son demasiado altos.

Desafortunadamente las aseguradoras medianas en el País no consideran la viabilidad de esta solución debido a que también las políticas internas no se lo permiten y la Comisión Nacional de Bancos y Seguros en la circular No.023/2012 exige tener una réplica de la base de datos en línea dentro del país independientemente del lugar en donde se lleve a cabo el procesamiento de la información. En donde queda establecido que en cualquier momento la CNBS pueda acceder de forma irrestricta desde el territorio nacional, a la información contenida tanto en la plataforma de procesamiento de información como en la réplica.

Capítulo V. Conclusiones y Recomendaciones

5. Conclusiones

- En base a los resultados obtenidos se concluye que la mediana empresa en el rubro de las aseguradoras no implementa su plan de recuperación de desastres en la nube debido a que estas instituciones poseen el recurso económico suficiente para comprar la infraestructura e implementar su plan de recuperación de desastres tradicionalmente que a la vez está respaldado por políticas internas de la empresa.

- Adicionalmente se puede concluir que en base al levantamiento inicial de información llevado en la fase previa permitió conocer la situación de la mediana empresa a nivel mundial, nacional y local respecto a los mecanismos utilizados para proteger su información ante desastres tecnológicos, y la implementación de planes de recuperación ante estos desastres utilizando la computación en la nube.

- El costo de implementar un plan de recuperación de desastres en la nube es muy alto, es por ello que obtener estos servicios en el mercado nacional con proveedores locales aun no es una opcion viable. Es mas economico y rentable implementar un plan de recuperación de desastres tradicional en la figura de leasing financiero.

- Las aseguradoras no están acostumbradas a tercerizar este tipo de servicios, se sienten más cómodas administrando su información desde su centro de datos local, esto debido a la desconfianza que hay con los proveedores que brindan estos servicios ya que hay factores como ser la seguridad de la información y la privacidad de los datos que generan desconfianza en las empresas, así como una total dependencia hacia las mismas.

- Las organizaciones consideran de muy alto riesgo tener una base de datos en la nube al ser considerada expuesta, esto debido a que la información de los afiliados podría ser vulnerada y generar riesgos reputacionales hacia la institucion, desembocando en un retiro masivo de sus afiliados traducido en pérdidas financieros a la organización.

- En caso de ocurrir un desastre las empresas analizadas consideran que las consecuencias más importantes son los retrasos de los clientes y proveedores en temas de servicio, pérdida de confianza y credibilidad con los clientes y consecuentemente las pérdidas financieras.

5.1 Recomendaciones

- Debido a que el rubro de las aseguradoras son instituciones reguladas por la Comisión Nacional de Bancos y Seguros deberían de exigir a este ente regulador actualizar su resolución No.1301 emitida el 22 de noviembre de 2005 ya que la tecnología ha avanzado a pasos agigantados hasta el día de hoy y se pueden estar dejando a un lado mecanismos y controles para disminuir el riesgo.

- En caso de no contar con un centro de datos alterno, geográficamente disperso, es factble considerar la implementación de un plan de recuperación de desastres en la nube como una estrategia secundaria de respaldos y contribuir como estrategia de continuidad del negocio en caso de ocurrir un incidente.

- Se deberían realizar pruebas a los planes de recuperación de desastres al menos 2 veces al año ya que según los datos de las encuestas únicamente lo realizan una vez al año, el hacer pruebas a los planes de recuperación frecuentemente facilitaría la recuperación de la informacion y validacion de los RTO y RPO en caso de ocurrir un desastre.

- La computación en la nube puede ser implementada en las empresas usando esquemas de nubes privadas, públicas o híbridas, pero para las aseguradoras se recomendaría utilizar nubes privadas debido al tipo de información que se maneja, ya que usualmente las aseguradores de la categoria mediana empresa son parte de un grupo financiero solido en el mercado nacional.

- Actualmente implementar una estrategia de recuperación de desastre en la nube se percibe un tanto distante para el rubro de las aseguradoras en la mediana empresa, sin embargo incorporar la nube como repositorio de datos en apoyo a la estrategia de continuidad del negocio es una estrategia factible y muy fácil de incorporar al negocio.

- A los proveedores de servicios en la nube recomendamos hacer un estudio de mercado en cuanto a la aceptación de este producto considerando que las organizaciones que son reguladas por la comisión nacional de banca y seguros no se les permite sacar la data de su centro de datos ya sea por lineamientos internos o por regulaciones no tan claras y contundentes por parte del regulador con respecto a los servicios en la nube.

5.2 Líneas futuras

Si bien particularmente en el rubro de las aseguradoras medianas un plan de recuperación de desastres en la nube se vuelve un tanto difícil poder ser concretado ya que existen muchos factores que impiden su implementación los cuales han sido mencionados a lo largo de la investigación, es muy probable que para otras rubros de la mediana empresa si es factible incorporar una estrategia de este tipo, desde el punto de vista que las demás rubros son dueños de la información y son de alguna manera autónomos a la hora de decidir en qué lugar físico depositar sus datos, además no son entidades sujetas a auditorias extensiva provenientes del ente regulador del país.

Las tendencias de tecnología en cuanto a infraestructura que hoy en día están surgiendo cada vez son diseñadas y listas para hacer despliegues en la nube "Cloud Ready" tal es el caso de soluciones de hiperconvergencia en donde el software tiene un papel importante ya que es el encargado de administrar servidores, redes y almacenamiento dando como resultado un dispositivo único administrado por software, la marca Dell adquirió recientemente EMC convirtiéndose hoy en día en la empresa de tecnología más grande a nivel mundial en donde uno de sus verticales más importante es el hardware administrado por software mediante las soluciones de hiperconvergencia.

Con las tecnologías en la nube es posible tener una nube hibrida en donde la empresas optaran por implementar su operación en cualquier lugar del mundo y el otro centro de datos de manera local esta combinación de sitios le permitirá al usuario poder tener control de la información en al menos un centro de datos.

Bibliografía

Alhazmi, O. H., & Malaiya, Y. K. (28 de Enero de 2013). Evaluating Disaster Recovery Plans Using the Cloud. (IEEE, Ed.) doi:10.1109/RAMS.2013.6517700

Ávila Mejía, Ó. (19 de Mayo de 2011). Computación en la nube.

Bahan, Chad. (Junio de 2013). *SANS INSTITUTE*. Obtenido de SANS INSTITUTE: https://www.sans.org

Chavan, P., Patil, P., & Kulkarni, G. (23 de Octubre de 2013). IaaS Cloud Security. (IEEE, Ed.) doi:10.1109/ICMIRA.2013.115

Futch, E. (31 de Julio de 2015). *Planificación de la Continuidad de Negocios*. Obtenido de Linkedin: https://www.linkedin.com/pulse/planificaci%C3%B3n-de-la-continuidad-negocios-egdares-futch-h-

Gaceta, L. (14 de Enero de 2009). Ley para el fomento y desarrollo de la competitividad de la micro, pequeña y mediana empresa. *La Gaceta*.

Google Ngram Viewer. (2017). *Google Ngram Viewer*. Obtenido de https://books.google.com/ngrams

Harris, S. (2013). *All in One CISSP* (Sexta Edición ed.). (S. Harris, Ed.) United States: McGraw Hill Companies.

ISACA. (2007). COBIT Control Practices. En ISACA.

ISACA. (2012). *Manual de Preparación al Examen CISA 2012.* ISACA.

ISO. (2013). *ISO/IEC 27001* (Segunda ed.).

Kotze, P., Carroll, M., & Van der Merwe, A. (17 de Agosto de 2011). Secure Cloud Computing: Benefits, Risks and Controls. (IEEE, Ed.) doi:10.1109/ISSA.2011.6027519

Lagos Mondragon, C. A., & Rivera Perdomo, D. I. (2014). *Servicios en la nube para mejorar la productividad en las PYMES de planta externa de Tegucigalpa.* Tegucigalpa.

Liu, F., Guo, W., Zhi, Q. Z., & Chou, W. (10 de Julio de 2010). SaaS Integration for Software Cloud. (IEEE, Ed.) doi:10.1109/CLOUD.2010.67

Manella Lemos, D. J. (2012). Diseño de guía para la implementación del uso de computación en la nube.

Mr.Akshay A. Gharat, M. D. (05 de Mayo de 2015). Disaster Recovery in Cloud Computing. (IEEE, Ed.) *ASM INSTITUTE OF MANAGEMENT & COMPUTER STUDIES (IMCOST), THANE, MUMBAI*.

National Institute of Standards and Technology. (Septiembre de 2011). The NIST Definition of Cloud Computing.

Sampieri, R. (2014). *Metodología de la Investigación* (Sexta ed.). México: Mc Graw Hill.

Sungana, S., & Suhasini, A. (27 de Febrero de 2014). Overview of Data backup and Disaster. doi:10.1109/ICICES.2014.7033804

Veeam Software. (2014). The Challenge of The - Always On Business. *Veeam Data Center Availability Report*.

Anexos

Anexo 1

FACULTAD DE POSTGRADO

ENCUESTA DIRIGIDA AL RUBRO DE LAS ASEGURADORAS MEDIANAS EN TEGUCIGALPA

Objetivo

La presente encuesta tiene como finalidad conocer el nivel de aceptación de un plan de recuperación de desastres en la nube en las aseguradoras medianas de Tegucigalpa.

Nombre del empleado: _____

Cargo: _____

1. ¿Cuál es el porcentaje anual de presupuesto que la empresa asigna a la seguridad de la información?
    a. ☐ 1 – 5%
    b. ☐ 6 – 10%
    c. ☐ 11 – 15%
    d. ☐ 16% o más
    e. ☐ No hay presupuesto específico

2. Para la administración de las tecnologías de la información, ¿La empresa cuenta con personal propio o es un tercero?
    a. ☐ Personal Propio
    b. ☐ Terceros

3. ¿La empresa tiene implementado un plan de recuperación de desastres de TI?
    a. ☐ SI

b. ☐ NO (Fin de la encuesta)

4. ¿El plan de recuperación de desastres de TI implementado en la empresa es tradicional o en la nube?
    a. ☐ Tradicional
    b. ☐ Nube

5. En los últimos 12 meses, ¿A ocurrido algún incidente en el que tenga que ejecutar su plan de recuperación de desastres?
    a. ☐ 0
    b. ☐ 1
    c. ☐ 2
    d. ☐ 3 o más

6. En los últimos 12 meses ¿Cuantas veces ha realizado pruebas a su plan de recuperación de desastres?
    a. ☐ 0
    b. ☐ 1
    c. ☐ 2
    d. ☐ 3 o más

7. En caso de ocurrir algún desastre, ¿Conoce el tiempo que le costará reanudar las operaciones (RTO) a la empresa y cuál es la capacidad de recuperar la información en el punto anterior (RPO)?
    a. ☐ SI
    b. ☐ NO

8. ¿La empresa está incursionando en algún proyecto de computación en la nube?
    a. ☐ SI
    b. ☐ NO

9. ¿La empresa tiene implementadas herramientas de colaboración en la nube?
    a. ☐ SI
    b. ☐ NO

10. ¿Contrataría a un proveedor de servicios en la nube para que esté a cargo de su plan de recuperación de desastres?
    a. ☐ SI
    b. ☐ NO ¿Por qué? _____

11. ¿Si usted implementara un plan de recuperación de desastres de tecnología en la nube preferiría que el proveedor de dichos servicios fuese local o internacional?
    a. ☐ Local ¿Por qué? _____
    b. ☐ Internacional ¿Por qué?_____

12. ¿Conoce alguna empresa **local** que provea servicios de recuperación de desastres en la nube? (Si su respuesta es afirmativa, favor indicar el nombre de la empresa)
    a. ☐ SI: _____
    b. ☐ NO

13. Según su criterio ¿Cuáles son las causas de que las empresas no realicen sus planes de recuperación de desastres en la nube? Valore en la escala del 1 al 5 siendo 1 la causa menor y 5 causa mayor.

Criterio	**1**	**2**	**3**	**4**	**5**
Problemas en la seguridad	☐	☐	☐	☐	☐
Regulaciones	☐	☐	☐	☐	☐
Políticas internas de la empresa	☐	☐	☐	☐	☐
Renuencia al cambio	☐	☐	☐	☐	☐
Desconocimiento	☐	☐	☐	☐	☐
Privacidad de los datos	☐	☐	☐	☐	☐
Problemas con la red	☐	☐	☐	☐	☐
Falta de apoyo de la gerencia	☐	☐	☐	☐	☐
Otros:_____	☐	☐	☐	☐	☐

14. Para la implementación de un plan de recuperación de desastres en la nube el proveedor de dichos servicios es un factor clave, valore en la escala del 1 al 5 siendo 1 lo menos importante y 5 lo más importante la importancia de los siguientes aspectos que el proveedor de los servicios debe asegurar:

Criterio	**1**	**2**	**3**	**4**	**5**
Costo de los servicios	☐	☐	☐	☐	☐
Soporte Técnico	☐	☐	☐	☐	☐
Disponibilidad	☐	☐	☐	☐	☐
Fácil migración	☐	☐	☐	☐	☐
Experiencia en el mercado	☐	☐	☐	☐	☐
Seguridad	☐	☐	☐	☐	☐
Otros:_____	☐	☐	☐	☐	☐

15. En caso de ocurrir algún desastre, ¿cuáles serían las consecuencias para la empresa y las partes interesadas (Accionistas, empleados, proveedores, entre otros)? Valore en la escala del 1 al 5 siendo 1 lo menos probable y 5 lo más probable.

Criterio	**1**	**2**	**3**	**4**	**5**
No hay consecuencias	☐	☐	☐	☐	☐
Cierre temporal de la empresa	☐	☐	☐	☐	☐
Pérdidas financieras	☐	☐	☐	☐	☐
Pérdida de confianza con clientes	☐	☐	☐	☐	☐
Retrasos con clientes y proveedores	☐	☐	☐	☐	☐
Despidos de personal	☐	☐	☐	☐	☐
Oportunidades de negocio perdidas	☐	☐	☐	☐	☐
Otros:_____	☐	☐	☐	☐	☐

¡Muchas por su colaboración!

Anexo 2

FACULTAD DE POSTGRADO

ENTREVISTA DIRIGIDA A LOS CONOCEDORES DEL TEMA

Objetivo

La presente encuesta tiene como finalidad conocer el nivel de aceptación de un plan de recuperación de desastres en la nube en base a su experiencia en el rubro de las tecnologías de la información.

Nombre: _____

Empresa donde trabaja: _____

Cargo actual: _____

Años de experiencia en el área: _____

1. ¿Qué es un plan de recuperación de desastres en la nube?

2. ¿Ha revisado y/o implementados planes de recuperación de desastres en la nube en Honduras?

3. ¿En nuestro país cómo ve la adopción de un plan de recuperación de desastres en la nube en la mediana empresa?

4. ¿Qué es más viable para el rubro de aseguradoras medianas en nuestro país: ¿Un plan de recuperación de desastres tradicional o un plan de recuperación de desastres en la nube?

5. ¿Considera usted que el rubro de las aseguradoras en Tegucigalpa tiene un nivel de madurez alto en cuanto a la adopción de un DRP en la nube?

6. ¿Cuáles considera usted que son las mayores causas de que ocurra un desastre en una empresa Hondureña?

7. ¿Considera usted que es una opción viable para las aseguradoras medianas en Tegucigalpa la adopción de un DRP en la nube?

8. ¿Conoce de casos de éxito de adopción de un plan de recuperación de desastres en la nube en la mediana empresa en Tegucigalpa?

9. ¿Las empresas hondureñas prefieren planes de recuperación de desastres en la nube local o internacional? ¿Por qué?

10. En nuestro país, ¿Qué riesgos hay de que las empresas implementen un plan de recuperación de desastres de TI en la nube?

¡Muchas por su colaboración!

Anexo 3

Tegucigalpa, 27 de julio de 2017

Lic. Karla Ruiz

Gerente General de Cámara de Comercio e Industrias de Tegucigalpa

Presente

Me dirijo a Ud., muy cordialmente con el objetivo de solicitarle información requerida en base a el proyecto de Tesis que están desarrollando los maestrantes Carlos Danilo Bonilla Rodas con número de cuenta 11313136 y Leonidas Gabriel Reyes Espinal con número de cuenta 11523025, maestrantes de la carrera de Gestión de Tecnologías de la Información de la Universidad Tecnológica Centroamericana UNITEC, actualmente cursando la clase de Tesis II con el cual están desarrollando el tema "Implementación de un Plan de Recuperación de Desastre en la Mediana Empresa de Tegucigalpa".

Con respecto al tema a desarrollar los maestrantes se encuentran en el proceso de aplicar trabajo de campo y para realizarlo es fundamental que ellos obtengan el listado de las medianas empresas registradas en la institución únicamente para la ciudad de Tegucigalpa para aplicar instrumentos de investigación como entrevistas y encuestas y poder culminar con éxito su trabajo de tesis.

Sin más a que hacer referencia.

Atentamente,

Msc. Jorge Maradiaga

Catedrático

CAMPUS TEGUCIGALPA
Bulevar Kennedy, zona Jacaleapa, frente a Residencial Honduras.
Tel: (504) 2268-1000

CAMPUS SAN PEDRO SULA
Bulevar del Norte, desvío a Armenta, contiguo a Altia Business Park
Tel: (504) 2564-5600

SISTEMA CEUTEC
Tegucigalpa: Sede Próceres: Tel: (504) 2202-4800
Sede Prado: Tels: (504) 2202-4400
Sede Centroamérica Tel: (504) 2202-4420
San Pedro Sula: Tel: (504) 2564-7400
La Ceiba: Sede Plaza Premiere Tel: (504) 2405-0007

La universidad global de Honduras | www.unitec.edu