ESCUELA POLITÉCNICA DEL EJÉRCITO

VICERRECTORADO DE INVESTIGACIÓN Y VINCULACIÓN CON LA COLECTIVIDAD

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

MAESTRÍA EN GERENCIA DE SISTEMAS

DISEÑO DE UNA GUÍA PARA LA IMPLEMENTACIÓN DEL USO DE COMPUTACIÓN EN LA NUBE COMO MECANISMO DE RECUPERACIÓN ANTE DESASTRES TECNOLÓGICOS EN PYMES EN EL DMQ.

Tesis de Grado

Autor: Danilo José Mannella Lemos

Sangolquí, 2012

Certificación del Director

Certifico que el presente trabajo fue realizado en su totalidad por el Señor DANILO JOSÉ MANNELLA LEMOS como requerimiento parcial a la obtención del Título de MAGÍSTER EN GERENCIA DE SISTEMAS.

Sangolquí, 9 de noviembre de 2012

ING. FRANCIS SALAZAR

DIRECTOR

Declaración de Responsabilidad

El proyecto de tesis de grado denominado “DISEÑO DE UNA GUÍA PARA LA IMPLEMENTACIÓN DEL USO DE COMPUTACIÓN EN LA NUBE COMO MECANISMO DE RECUPERACIÓN ANTE DESASTRES TECNOLÓGICOS EN PYMES EN EL DMQ”, ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de tesis de grado en mención.

Sangolquí, 9 de noviembre de 2012

_____

Danilo José Mannella Lemos

Autorización

Yo, Danilo José Mannella Lemos, autorizo a la Escuela Politécnica del Ejército la publicación en la biblioteca virtual de la Institución el trabajo “DISEÑO DE UNA GUÍA PARA LA IMPLEMENTACIÓN DEL USO DE COMPUTACIÓN EN LA NUBE COMO MECANISMO DE RECUPERACIÓN ANTE DESASTRES TECNOLÓGICOS EN PYMES EN EL DMQ”, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, 9 de noviembre de 2012

_____

Danilo José Mannella Lemos

Agradecimiento

Deseo agradecer en primer lugar a Dios por acompañarme en este camino de la Maestría y de mi vida en general. De igual manera deseo agradecer al Ing. Francis Salazar, MBA, por su acertada dirección en todo este proyecto de tesis, y quien más allá de su trabajo supo guiarme como un amigo. Dentro del desarrollo de la tesis merecen mi agradecimiento todas aquellas empresas que participaron del estudio. No puedo dejar de expresar mi agradecimiento al Colegio Alemán de Quito, en la persona del Sr. Manfred Ziltz, quien también me apoyó para que adquiriera nuevos conocimientos con el desarrollo de esta Maestría.

Agradezco también a mis padres, por brindarme su amor y consejos incondicionales en todos los aspectos de mi vida, y de igual modo agradezco a mi esposa Jenny, y mis hijos, Gianluca y Samanta, a quienes les debo su paciencia por el tiempo que les he dejado de dedicar, pero que ahora rinde sus frutos.

Finalmente quisiera agradecer a todos mis familiares y amigos por todas sus muestras de apoyo en todo momento.

Dedicatoria

Dedico esta tesis a mi esposa Jenny, quien me ha sabido dar palabras de aliento en los momentos más difíciles en estos años dedicados a la Maestría, y a quien me ha sabido enseñar que la perseverancia es más importante que el talento o la inteligencia, y que “las cosas que más nos cuestan son las que más valen la pena”.

Esta tesis va dedicada también a mis hijos, Samanta y Gianluca, la razón primordial de tanto esfuerzo y a quienes les debo tanto cariño, y de quienes aprendo un poco cada día.

Índice de Contenidos

Índice de Cuadros

Índice de Ilustraciones

Introducción

La rápida evolución de la tecnología de la información y comunicaciones, juntamente con el continuo aprovechamiento del Internet ha provocado que las empresas a nivel mundial, nacional y local generen una gran cantidad de información que le son vitales, o críticas para las mismas, y esto no es exclusivo de las grandes empresas sino también de las pequeñas y medianas empresas (Pymes), siendo esta información crítica de suma importancia para ser protegida.

El almacenamiento y gestión de la información de las Pymes, como de cualquier otra empresa, debe considerar la posibilidad de que existan interrupciones en el servicio proporcionado al negocio, y estas interrupciones se pueden deber a errores humanos – sean éstos intencionados o no – o a factores externos de tipo climático, y todo esto se conoce como desastre tecnológico empresarial. Este tipo de desastres tecnológicos han sido por muchos años cubiertos por mecanismos tradicionales tales como el respaldo y recuperación de información en cintas de datos (CDs, DVDs o incluso recientemente en discos externos), duplicación de servidores, uso de imágenes, etc. pero cada vez más han demostrado ser ineficientes tanto en su desempeño como en su alto costo, y hoy en día existen nuevas posibilidades de llevar a cabo esta protección de datos a través del uso de la computación en la nube.

El presente documento, en el primer capítulo, destaca la importancia, justificación y objetivos de este trabajo. A continuación en el segundo capítulo se hace una fundamentación teórica en donde se lleva a cabo una revisión sobre el estado actual de las Pymes, su preparación ante una recuperación ante desastres, su conocimiento sobre la computación en la nube y los mecanismos de recuperación ante desastres en la nube. En el tercer capítulo se procede con un diagnóstico de la situación de las Pymes ante el uso de planes de recuperación ante desastres. Posteriormente en el cuarto capítulo se elabora una propuesta de guía para usar a la

computación en la nube como el mecanismo más idóneo para la recuperación ante desastres tecnológicos a través de la validación de la guía mediante el criterio de expertos en el tema. Finalmente se muestran las principales conclusiones y recomendaciones de este trabajo.

Resumen

Las pequeñas y medianas empresas (Pymes) deben cuidar hoy en día su activo más importante: la información que posee. Siendo así, no es de extrañar que se la deba proteger en caso de cualquier evento que pueda provocar una interrupción en su servicio, ya sea que se trate de errores humanos o de otros factores externos (tales como robo, desastres naturales o error de hardware), y consecuentemente se vea afectada la calidad del servicio y rentabilidad de la empresa. Si bien algunas Pymes cuentan con un Plan de Recuperación de Desastres sencillo, todavía se desconoce las prestaciones en respaldo y recuperación de información que ofrece la computación en la nube, y esa es la razón de este estudio.

Abstract

Small and medium enterprises (SMEs) should take care today of their most important asset: its information. Thus, it is not surprising that it has to be protected in any event that may cause an interruption in their service, whether in the case of human error or other external factors (such as theft, natural disaster or hardware failure), and consequently affecting the quality of service and profitability. While some small businesses have a simple Disaster Recovery Plan, the benefits in data backup and recovery offered by cloud computing are still unknown, and that is the reason for this research.

.

1 Capítulo I: Antecedentes

1.1 Introducción

1.1.1 Motivación y contexto

Las empresas de cualquier tamaño, y en particular las Pymes (pequeñas y medianas empresas) deben cuidar hoy en día el que se cree es su activo más importante, y aunque hay diferentes percepciones al respecto, existe un gran consenso en que este activo se trata de la información que posee. Siendo la información el activo más importante no es de extrañar que se la deba proteger en caso de cualquier evento que pueda provocar una interrupción en su servicio, ya sea que se trate de errores humanos o de otros factores externos, tales como robo, desastres naturales o error de hardware, y consecuentemente se vea afectada la calidad del servicio y rentabilidad de la empresa.

Muchas empresas a nivel mundial, dentro de sus departamentos de TI, cuentan con un mecanismo para afrontar estas interrupciones y que consiste en la elaboración de un **Plan de Recuperación de Desastres** (DRP, por sus siglas en inglés), que tiene como finalidad recuperar software, datos, y/o hardware necesarios para retomar sus operaciones normales en caso de verse afectados por un desastre tecnológico. Tradicionalmente este proceso de recuperación de desastres tecnológicos se lo ha llevado a cabo dentro de las mismas instalaciones de la empresa o en un entorno externo, sin embargo, hoy en día están teniendo su mejor aliado en la computación en la nube (mejor conocido como *Cloud Computing*) debido a costos más bajos, mejor rendimiento, escalabilidad, un desarrollo de aplicaciones rápido, incremento en movilidad, y uso de entornos virtualizados, en comparación con los mecanismos tradicionales mencionados anteriormente.

Ahora bien, si ésta parece ser la panacea a los problemas de recuperación ante desastres de las empresas, ¿pueden y/o deben las Pymes en el DMQ[1] también dar el salto a la computación en la nube?, ¿hoy en día es factible utilizar a la computación en la nube para llevar a cabo un plan de recuperación ante desastres tecnológicos?, ¿Qué tan grande es la penetración de las TICs en las Pymes de nuestra ciudad? Éstas y otras inquietudes serán analizadas en el presente trabajo de tesis.

1.1.2 Justificación e importancia

La presente tesis es de gran importancia para las Pymes de Servicios del DMQ por cuanto les permitirá, en primer lugar, comprender la relevancia que tiene la adopción de un DRP, y cómo el costo de no estar preparado puede ser alto.

Esta investigación es necesaria porque con frecuencia se considera que estos temas están relacionados únicamente con el área de TI (*Tecnología de la Información*) cuando en realidad es un aspecto que concierne a toda la empresa, empezando por sus ejecutivos. Hasta hace algunos años se consideraban los aspectos de TI como una responsabilidad o gasto financiero, pero hoy en día es un activo de la empresa, y a la empresa lo que le interesa es centrarse en su negocio, más que en la tecnología.

En nuestro medio no existe un estudio que determine cómo están utilizando las PYMES a la computación en la nube, o siquiera si tienen planes de hacerlo en el corto o mediano plazo, y este estudio puede significar una guía no solamente para conocer el grado de utilización de la computación en la nube, sino para establecer una ruta a seguir que puede incluir otros servicios y/o aplicaciones ofrecidos por el proveedor de servicios en la nube. Además permitirá develar un gran potencial para que empresas de tecnología puedan brindar soluciones no satisfechas ante la demanda de atención

[1] DMQ: Distrito Metropolitano de Quito

PYMES que anteriormente no consideraban prioritaria la protección de sus datos ante un desastre tecnológico.

1.2 Objetivos

1.2.1 Objetivo general

- Estructurar una guía que conduzca al uso adecuado de la computación en la nube como mecanismo de recuperación ante desastres tecnológicos para las Pymes de servicios en el DMQ.

1.2.2 Objetivos específicos

- Fundamentar teóricamente el uso de la computación en la nube como mecanismo de recuperación ante desastres tecnológicos en Pymes.
- Efectuar el diagnóstico sobre la situación actual de las Pymes frente a la implementación de un plan de recuperación ante desastres.
- Elaborar una guía de implementación de recuperación ante desastres a través del uso de la computación en la nube enfocada a las PYMES.
- Validar la guía implementada que resulte del estudio mediante el criterio de expertos.

1.3 Planteamiento del problema

1.3.1 Descripción del Problema

El problema a resolver consiste en que “Las Pymes no están preparadas para una recuperación ante desastres tecnológicos de cualquier índole, Esto se debe al bajo grado de importancia otorgado por parte de sus ejecutivos, y/o debido al desconocimiento de mecanismos de recuperación ante desastres tecnológicos, provocando incluso pérdidas económicas sustanciales y hasta de cartera de clientes”. A continuación se describe un poco más en detalle acerca de esta situación.

En ningún lugar del planeta se puede afirmar que las empresas no corren ningún riesgo, y de que un incidente, sea provocado por el hombre o por otros factores, vaya repercutir en una rápida recuperación de su información o que incluso pudiera provocarle grandes pérdidas económicas, e incluso el quiebre de la empresa.

Aun cuando las grandes empresas a nivel mundial y nacional pueden acceder a diferentes mecanismos para protegerse ante desastres tecnológicos, las PYMES no tienen los suficientes recursos tecnológicos, humanos y sobre todo económicos para poner en marcha un DRP[2]. Paradójicamente las Pymes son las candidatas más idóneas para aprovechar la coyuntura actual y prepararse con un DRP, mediante la utilización de la computación en la nube, ya que los costos de operación e inversión son relativamente bajos y se puede tener acceso a tecnología y aplicaciones que antes estaba destinada únicamente a las grandes empresas, pero se evidencia que hay un desconocimiento de cómo subirse a la nube y beneficiarse de las prestaciones de ella.

1.3.2 Preguntas de Investigación

Debido al tipo de investigación, que en este caso se es de tipo exploratoria, descriptiva y sobre todo explicativa, y con la finalidad de medir el objeto de estudio se han definido las siguientes preguntas de investigación, con una corta explicación acerca del por qué de cada una:

1. **¿Cuál es el grado de penetración de las TICs en las Pymes?** En todas las empresas es fundamental contar con información segura, íntegra y disponible, pero con frecuencia la realidad indica que la inversión en tecnología es escasa,

[2] DRP: Disaster Recovery Plan (Plan de recuperación ante desastres)

y es importante saber qué factores no permiten que las TICs[3] tengan un alto grado de penetración en las Pymes.

2. **¿Qué causas inciden en la poca implementación de un DRP en las PYMES?** Toda organización tiene una probabilidad, alta o baja, de que en algún momento ocurra algún incidente que pueda afectar sus negocios, sin embargo no se da la debida importancia a tener un DRP sino hasta que es demasiado tarde, y es importante conocer qué determina la implementación de un DRP en las PYMES.

3. **¿Cuáles son las razones para considerar a la computación en la nube como la opción más idónea como mecanismo de recuperación ante desastres tecnológicos para las PYMES de servicios en el DMQ?** Dentro de las diferentes opciones para la elaboración de un DRP es necesario hacer un balance entre la computación en la nube y otros tipos de mecanismos alternos que permitan justificar la incursión en un DRP, y se debe conocer por qué en otras empresas e industrias lo están aplicando, y verificar si esto es posible en el caso de las PYMES de Quito en el segmento de Servicios, utilizando a la computación en la nube como mecanismo para ello.

De todas las preguntas de investigación antes propuestas aquella que puede considerarse de mayor interés para el proceso investigativo es la tercera: **¿Cuáles son las razones para considerar a la computación en la nube como la opción más idónea como mecanismo de recuperación ante desastres tecnológicos para las PYMES de servicios en el DMQ?**

[3] TICs: Tecnologías de la Información y Comunicación

1.4 Hipótesis y operacionalización de variables

1.4.1 Hipótesis de investigación

Hipótesis nula (Ho): Las Pymes son afectadas considerablemente en el evento de un desastre tecnológico, pudiendo provocarle pérdidas económicas, disminución en cartera de clientes y hasta el cierre de la empresa.

Hipótesis alternativa (Ha): Las Pymes que formulen un DRP utilizando un modelo de computación en la nube tendrán un menor impacto en recuperación ante desastres que aquellas que utilizan un modelo tradicional, o que no lo tengan siquiera contemplado, con una inversión relativamente baja.

1.4.2 Operacionalización de variables

- Variable independiente: Uso de la computación en la nube para la recuperación ante desastres tecnológicos aplicado a las PYMES.
    - Indicadores: 1) Porcentaje de presupuesto que las Pymes invierten en tecnología; 2) Cantidad de Pymes que implementan un DRP; 3) Cantidad de Pymes que usan servicios en la nube; 4) RTO (Objetivo de Tiempo de recuperación); 5) RPO (Objetivo de Punto de Recuperación).
- Variable dependiente: estabilidad en el negocio de las PYMES.
    - Indicadores: 1) Cantidad de negocios completados gracias al uso de tecnología; 2) Porcentaje de quejas por parte de usuarios; 3) Porcentaje de clientes satisfechos; 4) Imagen de la empresa; 5) Porcentaje de retención de empleados.

1.5 Síntesis del Capítulo I

En este capítulo se ha expuesto la importancia de contar con un estudio que permita conocer el efecto que puede tener para las Pymes el contar con una guía que permita llevar a cabo un Plan de Recuperación ante desastres (DRP) que resulte

idóneo para este tipo de empresas, al utilizar a la computación en la nube como el mejor mecanismo para ello, permitiéndoles ahorros en costos e inversión ya que se puede contar con tecnología y aplicaciones antes reservada para las grandes empresas, y que ahora, están a su alcance.

En el siguiente capítulo se proporcionará el fundamento teórico que permitirá conocer en detalle lo que son las Pymes, los métodos usados para efectuar un DRP, y cómo la computación en la nube se va convirtiendo en un modelo de negocio capaz de proporcionar servicios de recuperación ante desastres tecnológicos apropiados para las Pymes.

2 Capítulo II: Fundamentación teórica

2.1 Pequeñas y medianas empresas (Pymes)

2.1.1 Definición de Pymes

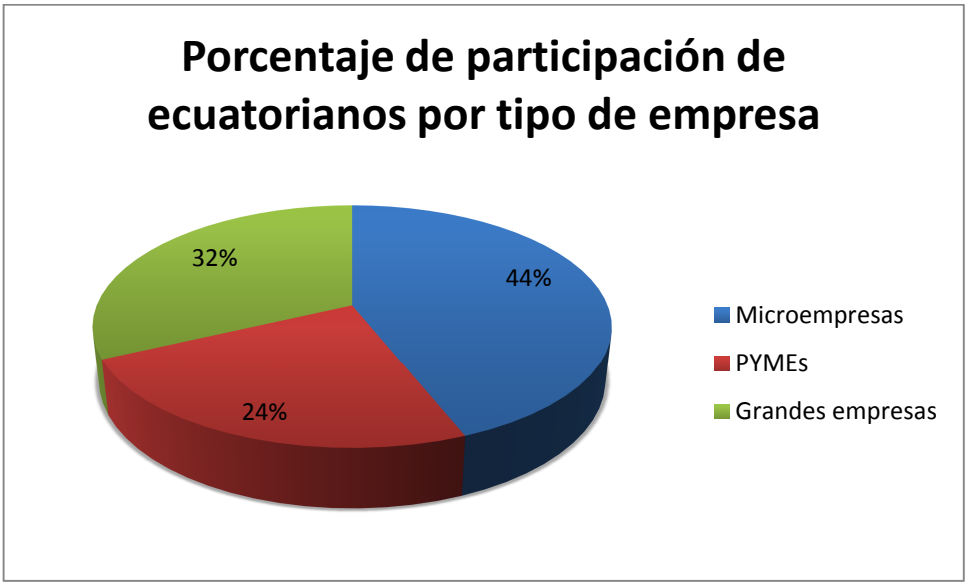
Dentro del mundo empresarial, se ha determinado que la PYME – que quiere decir Pequeña y Mediana Empresa – tiene una connotación que va cambiando de país en país, pero de manera general, se refiere a una empresa que tiene características propias que están determinadas por la cantidad limitada de empleados que laboran en la misma, y la cantidad de capital con el que operan, o también por la cantidad reducida de sus ingresos, en comparación con sus similares mayores, las grandes empresas.

La Real Academia de la Lengua Española define a una PYME como una "Empresa mercantil, industrial, etc., compuesta por un número reducido de trabajadores, y con un moderado volumen de facturación." (Real Academia Española). Por otro lado, dado que este estudio se enfoca en el Estado Ecuatoriano, resulta muy apropiado tomar la definición que tiene el Servicio de Rentas Internas del Ecuador (SRI) que define a las PYMES como "al conjunto de pequeñas y medianas empresas que de acuerdo a su volumen de ventas, capital social, cantidad de trabajadores, y su nivel de producción o activos presentan características propias de este tipo de entidades económicas" (SRI). Cabe destacar que en la Asamblea Nacional del Ecuador existe una propuesta de **Ley de Creación, Promoción y Fomento de Micro, Pequeñas y Medianas Empresas**, en la cual el legislador proponente, en el Art. 2.- Definiciones, menciona que "se entiende por micro, pequeña y mediana empresa, toda unidad de explotación económica, realizada por persona natural o jurídica, en actividades empresariales, agropecuarias, industriales, mineras, turísticas, comerciales o de servicios, rural o urbana" (Viteri Velasco, 2010).

2.1.2 Importancia de las Pymes

Las Pymes son importantes en un país porque permiten que su gente se desarrolle, y sea una fuente generadora de empleo, se mueva la economía y se produzcan, ofrezcan o demanden bienes y/o servicios que son decisivos en la generación de riqueza del país. En el caso del Ecuador las pequeñas empresas son las que más dan trabajo en el país, en donde 911,146 personas son parte de microempresas, 642,010 pertenecen a Pymes y el resto a grandes empresas, de un total de 2,053,422, de acuerdo al Censo Económico efectuado por el INEC en el año 2010 (Agencia Andes, 2011) . En el siguiente cuadro se ilustra en porcentaje la participación de personas en microempresas, Pymes y grandes empresas:

Cuadro 1. Participación de personas en microempresas, Pymes y grandes empresas en el Ecuador



Fuente: Censo Económico del Ecuador. INEC (2010)
Elaborado por: Danilo Mannella L.

Adicionalmente, las PYMES son importantes debido a su flexibilidad para adaptarse a los constantes cambios del mercado y a su facilidad por emprender proyectos que pueden ser innovadores.

Un punto a considerar en la importancia de las Pymes, es que “El fomentar este sector de la economía, significa cimentar las bases para que se desarrolle el sector productivo de nuestro país porque ayuda a crear fuentes de empleo, fomentar la competencia y competitividad, fundamentales para alcanzar un mejor nivel económico.” (Vargas Palacios, 2009).

No obstante la importancia mencionada en párrafos anteriores es de destacar que en muchos países en vías de desarrollo las Pymes reciben poco apoyo a través de políticas económicas por parte de sus gobiernos, siendo un gran motor en el desarrollo económico de sus países.

2.1.3 Características de las Pymes

Tal y como se indicó en el capítulo anterior, las Pymes tienen diversas características dependiendo del país en el cual se desarrollan, sin embargo poseen las siguientes características de manera general:

- Son empresas mayoritariamente familiares.
- La constitución de la empresa se efectúa con capital del dueño.
- La administración es independiente, es decir, por lo general, el dueño es también el gerente general.
- Tamaño de la empresa es relativamente pequeño en el sector en el que se desenvuelve (*ver siguiente capítulo*).
- Aunque existen Pymes estructuradas de una manera más formal en general su personal tiene poca formación y puede ser mal remunerado.
- En el caso de las Pymes industriales se manifiesta un escaso nivel tecnológico.

- De igual forma, en el caso de las Pymes industriales la mayoría de ellas cuenta con un nivel adecuado de control de calidad, aunque prevalecen los sistemas informales.
- Las Pymes carecen de créditos bancarios aceptables
- En muchos casos, sus limitaciones económicas no les permiten modernizarse, y consecuentemente no pueden crecer y competir en el mercado nacional e internacional.
- Existe una baja participación en los mercados internacionales, puesto que su producción se enfoca en el mercado interno.

En nuestro país las Pymes industriales tienen ciertas características particulares, según lo menciona (Barrera, 2001):

Desafíos

- Escaso nivel tecnológico
- Baja calidad de la producción, ausencia de normas y altos costos
- Falta de crédito, con altos costos y difícil acceso
- Mano de obra sin calificación
- Producción se orienta más al mercado interno
- Incipiente penetración de PYMES al mercado internacional
- Ausencia total de políticas y estrategias para el desarrollo del sector
- Son insuficientes los mecanismos de apoyo para el financiamiento, capacitación, y uso de tecnología
- El marco legal para el sector de la pequeña industria es obsoleto

Potencialidades

- Son factores claves para generar riqueza y empleo.
- Al dinamizar la economía, diluye los problemas y tensiones sociales, y mejorar la gobernabilidad.
- Requiere menores costos de inversión.
- Es el factor clave para dinamizar la economía de regiones y provincias deprimidas.
- Es el sector que mayormente utiliza insumos y materias primas nacionales.
- Tiene posibilidades de obtener nichos de exportación para bienes no tradicionales generados en el sector.
- El alto valor agregado de su producción contribuye al reparto más equitativo del ingreso.
- Mantiene alta capacidad para proveer bienes y servicios a la gran industria (subcontratación).
- Es flexible para asociarse y enfrentar exigencias del mercado.

2.1.4 Clasificación de las empresas por su tamaño

La definición de PYME, tal y como se ha mostrado en capítulos anteriores, depende mucho del país en el cual se desenvuelve, y su clasificación está atada a ello, con lo cual a continuación se muestra un cuadro con la clasificación de varios países en el mundo, y luego se analiza – por separado – la situación en el Ecuador. Hay que tomar en cuenta que en varios países se toma en consideración para la clasificación no solamente a las pequeñas y medianas empresas, sino también a las microempresas, y en los estudios se las conoce como miPymes[4].

[4] Mipyme: Micro, pequeñas y medianas empresas.

Es importante destacar que la clasificación de las micro, pequeñas, medianas y grandes empresas dependen de las necesidades propias de cada país o de los objetivos que persigan, de acuerdo a las necesidades singulares y los intereses generados en cada uno de ellos la clasificación va ligada a las políticas, estrategias y medidas económicas de estos países.

De acuerdo a la Comunidad Europea las Pymes se clasifican de acuerdo a su tamaño, en:

Cuadro 2. Clasificación de empresas conforme la C.E.

	Empleados	Ventas	Activo
Microempresa	Hasta 9	Hasta 2 millones de €	Hasta 2 millones de €
Pequeña	Hasta 49	Hasta 10 millones de €	Hasta 10 millones de €
Mediana	Hasta 249	Hasta 50 millones de €	Hasta 43 millones de €

Fuente: Comisión de las Comunidades Europeas. Recomendación 2003/361/CE, de 6 de mayo
Elaborado por: Danilo Mannella L.

Existen otros organismos que tienen una clasificación diferente, como se ve a continuación en el **Cuadro 3**:

Cuadro 3. Clasificación de Pymes conforme varios organismos internacionales

Institución	Tamaño de la empresa	Número de trabajadores
INSEE[5]	Pequeña	De 50 a 250
	Mediana	De 250 a 1000
SBA[6]	Pequeña	Hasta 250
	Mediana	De 250 a 500
CEPAL[7]	Pequeña	Entre 5 y 49
	Mediana	De 50 a 250

Fuente: Cada organismo mencionado en el cuadro.
Elaborado por: Danilo Mannella L.

Si bien en el ámbito mundial existen criterios bastante homogéneos determinados por asociaciones estadísticas o de agrupaciones de empresarios, para clasificar a las Pymes en el caso de América Latina, la clasificación es bastante

[5] Instituto Nacional de Estadística y Estudios Económicos (INSEE) en Francia, Ver: www.insee.fr
[6] Small Business Administration (SBA) de Estados Unidos, Ver: www.sba.gov
[7] Comisión Económica para América Latina (CEPAL). Ver www.cepal.org

heterogénea, pues aún al interior de cada país existen diversos criterios de clasificación. Los parámetros de clasificación más comunes tienen relación con empleos, ventas, activos y otros.

Un estudio llevado a cabo en la Universidad Autónoma del Estado de Hidalgo, México (Saavedra García & Hernández Callejas, 2006) muestra la clasificación de las Pymes de acuerdo principalmente a dos criterios: Empleo y Ventas.

Cuadro 4. Definición de las Pymes en Latinoamérica

Tamaño/ País	Argentina (Ventas) (1)	Bolivia (Empleo)	Brasil (Empleo)	Chile (Empleo)	Colombia (Empleo)	Costa Rica (Empleo)	El Salvador (Empleo)	Guatemala (Empleo)	México (Empleo)	Panamá (Ingresos brutos) (2)	Perú (Empleo)	Uruguay (Empleo)	Venezuela (Empleo)
Micro	Hasta 0.5	Hasta 10	Hasta 19	Hasta 4	Hasta 10	Hasta 10	Hasta 10	Hasta 10	Hasta 10	Hasta 150,000	Hasta 9	Hasta 4	Hasta 10
Pequeña	Hasta 3	Hasta 20	Hasta 99	Hasta 49	Hasta 50	Hasta 30	Hasta 49	Hasta 25	Hasta 50	Hasta 1,000,000	Hasta 20	Hasta 19	Hasta 50
Mediana	Hasta 24	Hasta 49	Hasta 199	Hasta 199	Hasta 200	Hasta 100	Hasta 100	Hasta 60	Hasta 250	Hasta 2,500,000	Hasta 100	Hasta 99	Hasta 100
Grande	Más de 24	Más de 49	Más de 199	Más de 199	Más de 200	Más de 100	Más de 100	Más de 60	Más de 250	Más de 2,500,000	Más de 100	Más de 99	Más de 100

Fuente: Extracto de la Caracterización de las MPYMES en Latinoamérica: Un estudio comparativo
Elaborado por: Danilo Mannella L.

(1) En millones de pesos argentinos. Dependiendo de la industria estos valores se modifican.

(2) En dólares o balboas. En Panamá el tipo de cambio es de 1 a 1 con el dólar norteamericano.

En diciembre de 2008 la CAN[8], a través de su Sistema Estadístico Comunitario, en su Resolución 1260 “establece que las PYMES comprenden a todas las empresas formales legalmente constituidas y/o registradas ante las autoridades competentes, que lleven registros contables y/o aporten a la seguridad social, comprendidas dentro de los umbrales establecidos en el artículo 3 de la Decisión 702 del 9 y 10 de diciembre del 2008”, y definen que los parámetros para segmentar a las Pymes se basen en diferentes rangos de personal ocupado y de valor bruto de las ventas anuales, de este modo se tienen los siguientes estratos:

Cuadro 5. Clasificación de las Pymes por estratos de acuerdo a Resolución 1260 de la CAN

Variables (**)	Estrato I	Estrato II	Estrato III	Estrato IV
Personal ocupado	1 – 9	10 – 49	50 – 99	100 – 199
Valor bruto de las ventas anuales (*)	< 100,000	100,001 – 1,000,000	1,000,001 – 2,000,000	2,000,001 – 5,000,000

Fuente: Boletín No. 12 de la Superintendencia de Compañías del Ecuador.
Elaborado por: Danilo Mannella L.

(*) Margen comercial para las empresas comerciales.

(**) Prevalecerá el valor bruto de las ventas anuales sobre el criterio de personal ocupado.

De acuerdo a esta Normativa, y conforme a la legislación interna vigente, el Ecuador en diciembre de 2010, a través de la Superintendencia de Compañías (Resolución No. SC.INPA.UA.G.10.005, publicada en el R.O. N°. 335), decide acogerse a la misma, y clasificar a las empresas de la siguiente manera:

[8] CAN: Comunidad Andina de Naciones

Cuadro 6. Clasificación de las Pymes en Ecuador

Variables	Microempresa	Pequeña empresa	Mediana empresa	Grandes empresas
Personal ocupado	1 – 9	10 – 49	50 – 199	> 200
Valor Bruto de las ventas anuales	< 100,000	100,001 – 1,000,000	1,000,001 – 5,000,000	> 5,000,000
Montos activos	Hasta US $100,000	De US $100,001 hasta US $750,000	De US $750,001 hasta US $3,999,999	> US $4,000,000

Fuente: Boletín No. 12 de la Superintendencia de Compañías del Ecuador.
Elaborado por: Danilo Mannella L.

Ahora bien, dado que en el ámbito tributario se ha aprobado la implementación de las NIIF[9] para todas las empresas en general (Superintendencia de Compañías del Ecuador, 2011), y desde luego para las Pymes en particular, existe desde el 1º de enero de 2012 la obligatoriedad de su implementación, habiendo tenido desde el 1º de enero de2011un año de transición, conforme la Resolución No. SC.Q.ICI.CPAIFRS.11.01 emitida por la Superintendencia de Compañías del Ecuador[10], y consecuentemente en el Artículo. Primero se resuelve que "Para efectos del registro y preparación de estados financieros, la Superintendencia de Compañías califica como PYMES a las personas jurídicas que cumplan con las siguientes condiciones:"

1. Activos totales inferiores a CUATRO MILLONES DE DÓLARES;
2. Registren un Valor Bruto de Ventas Anuales inferior a CINCO MILLONES DE DÓLARES, y;
3. Tengan menos de 200 trabajadores (Personal ocupado). Para este cálculo se tomará el promedio anual ponderado.

[9] NIIF: Normas Internacionales de Información Financiera
[10] Documentación detallada en el sitio web de la Superintendencia de Compañías. http://www.supercias.gov.ec/niaa.htm

En este estudio se tomará en cuenta a las Pymes en su conjunto de acuerdo ambas resoluciones de la Superintendencia de Compañías (SC.INPA.UA.G.10.005 y SC.Q.ICI.CPAIFRS.11.01), en tanto que son complementarias entre sí.

2.1.5 Clasificación de las Pymes por su giro de negocio

De acuerdo al (SRI), las principales actividades económicas en las cuales se desenvuelven las Pymes en el Ecuador son:

- Comercio al por mayor y al por menor.
- Agricultura, silvicultura y pesca.
- Industrias manufactureras.
- Construcción.
- Transporte, almacenamiento, y comunicaciones.
- Bienes inmuebles y servicios prestados a las empresas.
- Servicios comunales, sociales y personales.

Para el presente estudio se considerarán a las Pymes de servicios en general.

2.2 Recuperación ante desastres (DR)

2.2.1 Definición de Recuperación ante desastres

En cualquier actividad del ser humano existe la probabilidad de que un evento no deseado impida el desarrollo normal de sus actividades, y en el caso empresarial esto puede provocar pérdidas económicas y hasta pérdida de clientes. Una definición de **recuperación ante desastres** (DR, por sus siglas en inglés) puede decirse que “es el proceso que usa una organización para recuperar el acceso a su software, datos y/o hardware, necesario para retomar el rendimiento normal de funciones críticas de

negocios después de un evento producido por un desastre natural, o un desastre causado por el ser humano.”

2.2.2 Evolución de la Recuperación ante Desastres

Desde los inicios de la computación, alrededor de la década de los años 70, la importancia de mantener la información a salvo ha sido fundamental para las empresas en general, y para el usuario común en particular. En aquella época, en la cual se operaba con equipos grandes, conocidos como *mainframes*, y con una operación por lotes (o *batch*) si se producía algún tipo de desastre en el mantenimiento de la información podían pasar varios días antes de que se pudiera tener a la empresa operativa nuevamente. Conforme se hacía más palpable la recuperación ante desastres a finales de los 70’s, empieza a crecer toda una industria dedicada a proveer centros de datos de respaldos de información empresariales.

En la década de los 80’s y 90’s, la concienciación sobre recuperación de desastres de TI (Tecnologías de la Información) se incrementó, y uno de los factores para el crecimiento de esta industria de recuperación ante desastres tecnológicos fue el incremento de regulaciones gubernamentales que exigían planes de continuidad de negocios y de recuperación ante desastres en varios sectores económicos.

Con el rápido crecimiento del Internet en la década de los 90's y 2000s, las organizaciones de todos los tamaños se hicieron más dependientes de la disponibilidad continua de sus sistemas de TI, con muchas organizaciones teniendo como objetivo alcanzar el 99.999% de disponibilidad en sistemas críticos. Esta dependencia sobre los sistemas de TI, así como una creciente concienciación de desastres a gran escala como el 9/11 en EE.UU., contribuyeron a un crecimiento mayor de industrias relacionadas con la recuperación ante desastres desde soluciones de alta disponibilidad a instalaciones de hospedaje en caliente.

2.2.3 Recuperación ante desastres (DR) y Continuidad del Negocio (BC).

La **Continuidad del Negocio** es la actividad llevada a cabo por una organización para asegurarse que las funciones críticas del negocio estén disponibles continuamente para todos los involucrados (clientes, proveedores, entes reguladores y otras entidades), que deben tener acceso a dichas funciones. La Continuidad del Negocio no es algo que se implemente al momento de presentarse un desastre, y aquí se presenta la primera diferencia con la Recuperación ante Desastres (DR), sino que se trata de tareas ejecutadas a diario para mantener el servicio, la consistencia en la información y su recuperabilidad.

Con frecuencia se tiende a confundir al BC con DR, pero la diferencia consiste en que, “la DR es el proceso por el cual se retoman las actividades después de un evento perjudicial para la organización, la BC sugiere un enfoque integral para asegurarse de que se puede hacer dinero no solamente después de que ocurra una calamidad natural, sino también de otros desafíos tales como un corte de energía, o el cambio de empleados en la empresa, situaciones con las que se puede enfrentar la empresa cada día”. (Slater, 2012).

La Continuidad del Negocio es toda una “metodología” que se basa en toda una serie de estándares, políticas, procedimientos, guías y actividades que se llevan a cabo a través de una adecuada **Gestión de Continuidad del Negocio** (BCM, por sus siglas en inglés). Como se mencionó, el término Continuidad del Negocio consiste en una "metodología" para llevar a cabo los negocios día a día, pero esto se soporta en algo llamado **Planeación de Continuidad del Negocio** (BCP, por sus siglas en inglés), que en sí es la "actividad" de determinar qué es lo que esa metodología debería ser.

La BCM es un proceso de gestión continuo que las organizaciones emplean para identificar impactos potenciales y establecer los acuerdos necesarios y planes

para mantener la capacidad de su Continuidad del Negocio (BC). La BC, se asegura de que los siguientes puntos sean manejados de una forma permanente:

- Identificar los intereses de la organización y sus partes interesadas "stakeholders".
- Salvaguardar los intereses identificados al:
    - Identificar las funciones de negocios críticas que apoyan estos intereses
    - Identificar interrupciones potenciales para estas funciones de negocios críticas
    - Minimizar el número de interrupciones potenciales
    - Reducir el impacto de las interrupciones para estas funciones de negocios críticas
    - Asegurarse de que estas funciones de negocios críticas puedan continuar para mantener - si no apoyado en una base moderada - los intereses identificados

Dentro de la BCM debe tomarse en cuenta que el producto tangible que se obtiene del mismo es un **Plan de Continuidad de Negocios** (BCP) que si bien puede diferir entre empresas, y si bien es cierto que no se va a ahondar en los mismos en este estudio, rápidamente se ilustrará los pasos por los que debe incurrir, conforme la Guía práctica para PYMES acerca de cómo implantar un Plan de Continuidad de Negocio de INTECO[11]:

[11] El Instituto Nacional de Tecnologías de la Comunicación (INTECO), la sociedad estatal española adscrita al Ministerio de Industria, Turismo y Comercio a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, es una plataforma para el desarrollo de la Sociedad del Conocimiento a través de proyectos del ámbito de la innovación y la tecnología.

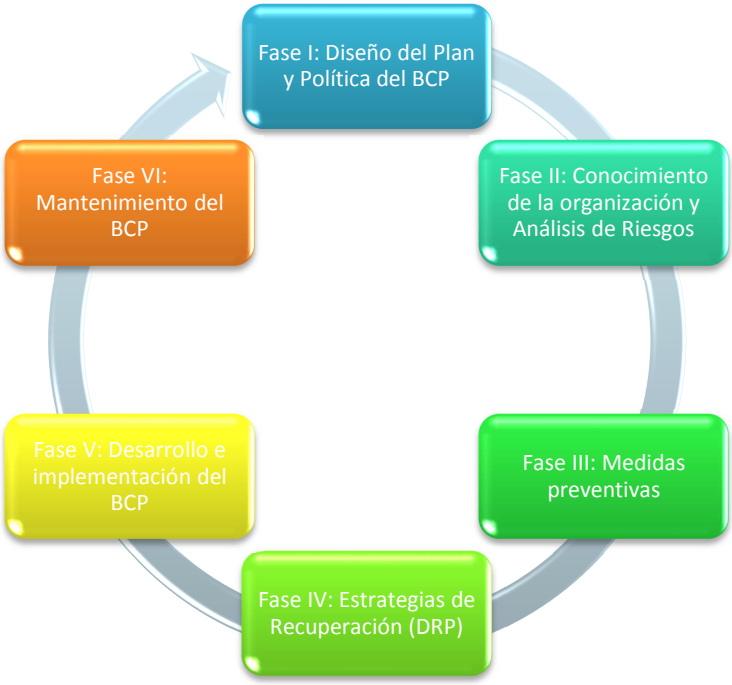


Ilustración 1. **Fases para la implementación de un BCP**

Fuente: Guía práctica para PYMES: Cómo implementar un plan de continuidad de negocios. (INTECO)
Elaborado por: Danilo Mannella L.

Tal y como se aprecia en la **Ilustración 1**, en la Fase IV se tienen las Estrategias de Recuperación como parte del BCP, y dentro de estas estrategias se encuentra la Recuperación ante Desastres, que se maneja a través de un **Plan de Recuperación ante Desastres** (DRP), que se analizará en detalle en el siguiente capítulo.

En resumen:

- La **Continuidad del Negocio** (BC) es el proceso para asegurar que las operaciones continuarán en el evento de que se produzca un desastre natural, o provocado por el hombre.

- La **Recuperación ante Desastres** (DR) se asegura de que la información perdida o destruida pueda ser restaurada dentro de un período de tiempo predefinido.

2.2.4 Los Planes de Recuperación ante Desastres o DRP

Como se ha mencionado anteriormente los desastres pueden ser básicamente de dos tipos: naturales y provocados por el hombre, y cualquiera de ellos puede tomar por sorpresa a las organizaciones, con poca o ninguna advertencia. La recuperación ante desastres puede ser una experiencia agotadora, cara, y tomar mucho tiempo, particularmente para aquellas organizaciones que no han tenido suficiente tiempo para prepararse para estos eventos. Sin embargo, cuando algún desastre se presenta, aquellas empresas que se han preparado y efectuado sus **Planes de Recuperación ante Desastres** (DRP) sobreviven con una interrupción de su productividad o pérdida mínima de datos.

Muchas organizaciones si bien están conscientes de la posibilidad de que ocurra algún desastre en la empresa existe un falso sentido de *seguridad* de que esto "no es probable que nos ocurra a nosotros". No obstante, si se ha efectuado una preparación adecuada la recuperación ante desastres no tiene por qué ser agotadora, y por el contrario, aquellas organizaciones que se toman el tiempo de implementar planes de recuperación ante desastres con tiempo salen delante de estas catástrofes con pérdidas mínimas, o aún sin pérdidas, de datos, hardware, software o ingresos en los negocios. El factor que marca la diferencia entre las organizaciones que han manejado exitosamente estas crisis, con un esfuerzo y costo mínimo y una alta velocidad, de aquellas que no se recuperaron, y que incluso tuvieron que cerrar su negocio, es la Planeación de Recuperación ante Desastres.

Los DRPs detallados pueden prevenir muchos dolores de cabeza que experimenta una organización en tiempos de un desastre. Los DRPs deberían ser practicados de manera tal que los actores claves estén familiarizados con las acciones específicas que deberán llevar a cabo en el caso de ocurrir un desastre. Los DRPs deben ser adaptables y actualizados rutinariamente, por ejemplo, si se incrementa nuevo personal, una nueva sucursal, o se incluye nuevo HW o SW, estos deberían ser inmediatamente incorporados en el DRP de la organización. Las empresas tienen que considerar todas estas facetas de su organización así como actualizar y practicar su plan si quieren maximizar su recuperación después de un desastre.

Hay un sinfín de opciones a las cuales pueden recurrir las empresas para empezar a implementar su DRP. Una de ellas es recurrir a alguien con experiencia al interior de la empresa para ayudar a crear el plan de recuperación ante desastres que se ajuste a la realidad de la organización. Aquellas organizaciones que no cuenten con este personal podrían recurrir a empresas externas especializadas o implementar software para el efecto.

Una de las prácticas más comunes, particularmente usada por empresas pequeñas o que no cuenten con personal especializado para la creación de un DRP, es la de utilizar plantillas. Si bien es cierto que las plantillas pudieran no cubrir todas las necesidades específicas de cada organización, es un buen lugar para empezar a crear su DRP. Las plantillas ayudan a que el proceso de implementación sea más simple y enfocado en la realidad de la empresa proveyendo de una guía que pudiera revelar aspectos que ordinariamente pasan desapercibidos, después de todo, un DRP sencillo es mejor que no tener ninguno.

Debemos recordar que la meta de un DRP es ayudar a que la organización mantenga la continuidad de su negocio, minimice los daños y prevenga pérdidas. Consecuentemente, y de acuerdo a lo mencionado en párrafos anteriores lo

importante de un DRP es estar seguro de que cuando se lo ponga en práctica funcione, y para ello hay que ejecutarlo regularmente.

Antes de implementar un DRP es necesario tomar en cuenta varios aspectos, y dependiendo del proveedor, se tienen distintos enfoques, pero de manera general se centrará esta parte en los componentes mostrados en la **Ilustración 2**:

Ilustración 2. **Componentes de un DRP**

Fuente: Sitio web Disaster Recovery
Elaborado por: Danilo Mannella L.

2.2.4.1 Conocimiento de las actividades de la organización

El primer paso en la planeación de recuperación ante desastres consiste en darse cuenta de que hay una necesidad para este tipo de preparación. Las organizaciones que valoran sus negocios necesitan establecer y mantener DRPs que sean efectivos. Cuando llegue el momento, estos planes pueden minimizar las interrupciones en la operación normal del negocio y limitará la extensión del daño e interrupción en la productividad del negocio.

La responsabilidad de establecer DRPs recae en la Mesa Directiva y ejecutivos de la organización. Ellos tienen que organizar y mantener un lineamiento claro de qué acciones quieren seguir, y cuáles empleados necesitan jugar un rol en el proceso de una recuperación ante desastres cuando ocurran eventos que no fueron previstos.

Los DRPs deben ser bien conocidos y bien repasados por todos aquellos que tendrán un rol en el proceso de recuperación. Toda la Administración y el personal deberían estar al tanto del DRP y lo que se requiere de ellos en el caso de que se produzca un desastre serio.

Para poder cumplir lo anterior es necesario que se conozca el negocio completamente, y con ello poder determinar las áreas que requerirán ser provistas de mayor prioridad al momento de llevar a cabo el DRP, en pocas palabras qué procesos son los más importantes para mantener a la empresa en funcionamiento. De acuerdo a un estudio efectuado por Vision Solutions “Una vez que haya identificado dichos procesos empresariales, trabaje con las unidades de negocio a fin de determinar sus requisitos de disponibilidad para cada proceso.” (Vision Solutions, 2008).

Dentro de esta etapa de conocimiento de las actividades de la organización, y cuando se esté listo para empezar a crear el DRP se deben seguir los siguientes pasos:

1. **Definición de metas para el DRP**.- La organización debe, por ejemplo, determinar qué debería lograr el plan, y en qué marco de tiempo.
2. **Levantamiento de información de personal**.- La organización debería crear una lista precisa y actualizada del personal por cada uno de sus departamentos.
3. **Levantamiento de información de aplicaciones de red**.- Esta parte del plan involucra hacer una lista de todas las aplicaciones de red, el personal que las ejecuta, y qué tan frecuentemente se debería respaldar la información.

4. **Lista de inventario de elementos físicos de la red**.- Esta tarea tiene relación con llevar a cabo un inventario de todos los elementos necesarios para que funciones la LAN (red de área local) y WAN (red de área extendida, usualmente conexión a Internet) de la organización.
5. **Levantamiento de procedimientos de respaldos**.- La organización necesita tomar nota de los procedimientos involucrados en los respaldos de sus servicios de información.
6. **Levantamiento de procedimientos para recuperación ante desastres**.- De ser posible se deberá contar con el plan actual para recuperación ante desastres de una manera detallada.

Los pasos anteriores pudieron haberse recogido en la preparación del BCP, y de lo contrario éste es un buen momento para hacerlo. Esta información y documentación puede incluir (The Disaster Recovery Guide, 2002):

1. Organigrama de la organización que muestre los nombres y posiciones
2. Plan existente (si lo hubiera)
3. Información de contacto de emergencia del personal
4. Lista de proveedores y números de contacto
5. Lista de servicios de emergencia y números de contacto
6. Direcciones de los locales y mapas
7. Procedimientos de evacuación existentes y regulaciones del cuerpo de bomberos
8. Procedimientos de Salud y Seguridad Física
9. Procedimientos Administrativos y de Operaciones
10. Lista de asesores profesionales e información de contacto de emergencia
11. Procedimientos administrativos de personal

12. Copias de planos de los pisos
13. Inventario de activos
14. Inventarios de activos de información
15. Inventarios de TI
16. Especificación de sistemas de TI
17. Especificación de sistemas de comunicaciones
18. Copias de acuerdos de mantenimiento / acuerdos de nivel de servicio
19. Procedimientos de almacenamiento fuera del sitio
20. Regulaciones y guías relevantes de la industria
21. Información del Seguro

2.2.4.2 Análisis de riesgos e impactos

Uno de los componentes claves dentro de la planeación de recuperación ante desastres está el **Análisis o evaluación de riesgos** (RA, por sus siglas en inglés). Este RA permite determinar qué posibles riesgos podrían ocurrir en la organización de manera tal que afecte sus operaciones. Para que los esfuerzos en esta etapa sean lo más provechosos la alta gerencia y ejecutivos de la organización deben considerar cada posible escenario cuando se analicen los riesgos que la organización pueda enfrentar. Este proceso de análisis le brinda a la organización la oportunidad de conocer de mejor manera lo que es importante para ella.

Como un complemento al RA se encuentra el **Análisis de Impacto del Negocio** (BIA, por sus siglas en inglés), en donde se determina el efecto que tendría cada tipo de amenaza potencial sobre la organización en caso de llegarse a producir el riesgo detectado en la evaluación de riesgos. Entre los tipos de criterios asociados a estos impactos que pueden ser evaluados están (Salazar Villalobos, 2008):

1. Servicios al cliente
2. Operaciones internas
3. Asuntos legales
4. Asuntos financieros

Para crear un DRP lo más efectivo posible, para enfrentar una calamidad que afecte adversamente a la empresa se debe considerar en la Evaluación de riesgos elementos tan grandes como la ocurrencia de terremotos, inundaciones o incluso (en algunos países) actos terroristas, como situaciones tan mundanas como cortes eléctricos, sobretensiones o ataques de malware. La idea es predeterminar la mayor cantidad posible de desastres con los que la organización se pueda encontrar, y luego determinar cómo la organización los enfrentará.

Dependiendo de la evaluación de impactos se determina la estrategia a utilizar para la recuperación ante desastres. Las siguientes preguntas pueden ayudar a determinar la prioridad de las acciones a incluir en el plan (Salazar Villalobos, 2008):

1. ¿Qué aplicaciones son críticas o vitales?
2. ¿Cuál es la configuración mínima de hardware aceptable?
3. ¿Cuántos usuarios deben acceder a las aplicaciones críticas?
4. ¿Cuáles son los requerimientos funcionales del negocio?

El BIA es de vital importancia para el desarrollo de los objetivos que persigue la creación del DRP, tomando en cuenta que muchas de sus actividades involucran entrevistas a usuarios finales y personal de Sistemas, y que esta información se recoge y documenta para esta siguiente etapa que es la creación del DRP.

En resumen, los objetivos del RA y el BIA son (Salazar Villalobos, 2008):

1. Identificar los activos de la organización y las funciones que son necesarias para la recuperación del negocio en caso de desastre y priorizarlas de acuerdo a su criticidad (BIA).
2. Identificar las amenazas más probables a los activos y funciones (RA).
3. Crear objetivos para el desarrollo de estrategias que eliminen los riesgos eliminables y minimicen el impacto de aquellos riesgos que no se pueden eliminar (RA).
4. Crear objetivos para el desarrollo de estrategias para el respaldo y/o recuperación de aquellas funciones que son críticas para el negocio y que podrían verse afectadas en un desastre.

2.2.4.3 Creación del DRP

El DRP es uno de los documentos más importantes que tiene la organización, pues a éste se recurrirá en caso de que ocurra alguna interrupción de servicios o desastres, y es el documento que permitirá guiar a la organización particularmente cuando ocurran eventos que pudieran afectar el normal desenvolvimiento de las actividades del negocio y que pudieran afectar la productividad del mismo. Este documento ayudará a la organización a recuperarse de una manera rápida e incluso evitar pérdidas de ingresos.

Aun cuando este documento es de vital importancia para la organización muchas de ellas, particularmente las Pymes sienten que la creación del mismo puede ser abrumadora y no llegan a efectuarla y por ello existen plantillas provistas por terceras empresas que pueden alivianar esta tarea.

Un DRP debe cubrir desde el impacto inicial que puede provocar una interrupción del servicio en el negocio hasta los pasos que se deben llevar a cabo para que el negocio vuelva a su operación normal.

Como se indicó en el capítulo anterior, el DRP debe considerar aspectos de inventario del hardware, software y comunicaciones que posee el negocio, así como del personal que lo opera e incluir, de acuerdo al BIA y RA efectuado previamente, las aplicaciones prioritarias y sistemas que deberán ser respaldados, y los sitios alternos en donde se deberá llevar a cabo estos respaldos, sea al interno de la organización o hacia afuera, en caso de problemas en el edificio en donde se opera. Por último, es importante establecer la cadena de mando en caso de que ocurra un desastre, y que cada uno sepa qué debe hacer si esta situación se presentara. Todo lo anterior permitirá que la organización regrese a operar rápidamente y de la manera más eficaz.

Un estudio efectuado por la empresa Vision Solutions, empresa mundial proveedora de soluciones de alta disponibilidad, software dedicado a la continuidad del negocio y recuperación ante desastres, sugiere considerar – adicionalmente a los criterios anterior – calcular el costo del tiempo de inactividad del negocio (Rennels, 2006): “Esto ayudará a colocar las prioridades respecto de qué áreas del negocio serán protegidas y en qué nivel. Nótese que mientras algunos sistemas no tienen un alto valor económico asociado en cuanto a estar fuera de servicio, pudiera haber ramificaciones legales que se deberían tomar en cuenta en caso de que no estuvieran disponibles o irrecuperables. El costo no se asocia solamente a ingresos perdidos, sino al impacto global que los datos de la empresa deben cumplir respecto de obligaciones financieras, legales, con empleados o clientes del negocio.”

Es importante recordar que no existe un DRP único que sea útil para todas las organizaciones, pues cada una de ellas posee sus propias características y necesidades. Cuando se recurre a una plantilla es necesario verificar que sea lo suficientemente flexible para aprovechar la experiencia de quienes se dedican a la

seguridad informática en esta industria, pero que permita integrar la visión del negocio y sus directivos.

2.2.4.4 Difusión del DRP como política empresarial

Si bien es cierto que un DRP simple es mejor que no tener ninguno, no es menos cierto que esto se logra a partir de la difusión de todo el proceso anterior al personal de la empresa. Por lo tanto, los miembros directivos y la Gerencia necesitan emitir declaraciones claras respecto de la concienciación del DRP como una política empresarial. Para que el DRP sea efectivo debe pasar del papel a la realidad.

El DRP debe ser probado, actualizado y mantenido regularmente por todo el personal de la empresa que está inmerso en la planeación del mismo, así como de aquellos que tienen alguna responsabilidad en la implementación de lo que ha sido planeado. El resto de miembros de la empresa debe ser capacitado e informado regularmente sobre cambios que existan en el DRP, y deberán conocer los procedimientos a seguir conforme su rol, en el proceso de recuperación, en el caso de que surja alguna emergencia.

La verificación del funcionamiento del DRP se puede efectuar a través de simulaciones en ambientes de prueba, de forma que se pueda determinar posibles falencias en caso de que se tuviera que implementar en ambientes reales. Una ventaja de llevar a cabo pruebas del DRP en ambientes reales es que el personal puede permanecer relativamente calmado en caso de que algún desastre suceda en una situación de emergencia real, y permita regresar a la operación normal del negocio de la manera más organizada y con la menor pérdida posible.

En resumen:

- Convertir al DRP en una política empresarial es un paso clave en el proceso de recuperación ante desastres, por cuanto se tiene el apoyo de la alta gerencia, y

la colaboración de toda la empresa en caso de que un desastre llegar a ocurrir en una situación real.

2.2.4.5 Mantenimiento del DRP

La implementación de un DRP que sea ampliamente exitoso y que se ejecute sin problemas depende en gran medida de las personas responsables de implementar el plan. Para que el resultado de este DRP sea exitoso las personas involucradas deben entender su rol en el proceso y lo que afecta su rendimiento en el resto del proceso, para esto es fundamental (Disaster Recovery):

1. Capacitar al personal involucrado en el proceso de la recuperación ante desastres.
2. Que el personal involucrado en el DRP revise regularmente (de manera trimestral o semestral) sus responsabilidades en las que participan.
3. Que se revise y actualice la lista del personal que debe estar involucrado en el proceso de recuperación ante desastres. Cambios en la nómina, tales como promociones, despidos y renuncias deben ser tomados en cuenta para una actualización y reemplazos en las responsabilidades asignadas en el DRP.
4. Recordar que tener una lista de empleados que son capacitados en sus roles en el DRP eleva la probabilidad de un mayor éxito en el proceso de recuperación ante desastres.
5. No olvidar que un personal adiestrado implementará de mejor manera un DRP y asegurará la continuidad del negocio cuando se presente algún desastre. Sin práctica, una emergencia inesperada puede sobrecoger al personal, y debilitar la habilidad para implementar correctamente un DRP, dando como resultado una pérdida de productividad e incluso de ingresos.

Finalmente, cuando existan cambios en la infraestructura de la empresa estos se deben incorporar inmediatamente en el DRP para conocer cómo reaccionar con las nuevas modificaciones.

2.2.5 Métodos tradicionales de recuperación ante desastres

Para evaluar la recuperación ante desastres se utilizan básicamente dos métricas:

- el **RTO** (Objetivo de tiempo de recuperación) que mide el tiempo que transcurre entre el momento en que se produce el desastre y el momento en que se reanudan las operaciones del negocio;
- y el **RPO** (Objetivo de Punto de recuperación) que consiste en el tiempo entre el último respaldo efectuado y el momento en que se produce el desastre, representando el punto histórico más cercano en el tiempo en el cual el sistema se puede recuperar, en pocas palabras, cuánta información se puede perder desde la última vez que se efectuó un respaldo de datos y el momento en que se vuelve operacional el negocio.

Ambas métricas se aprecian gráficamente a continuación en la **Ilustración 3**.

Ilustración 3. **Identificación de métricas RTO y RPO**

Fuente: Elaboración del autor.
Elaborado por: Danilo Mannella L.

Las soluciones tradicionales de recuperación ante desastres incluyen, respaldos en medios externos (como cintas. CDs, DVDs o discos externos), captura de imágenes y clustering, que resultan inadecuadas en términos de RTO y RPO dentro de restricciones razonables de presupuesto. A continuación se detalla cada una de estas opciones (Platespin, Microsoft y Dell, 2007):

1. **Respaldo en cinta**.- El respaldo en cinta es la alternativa prudente más económica y utilizada por muchos años, sin embargo puede ser difícil de administrar y frecuentemente la restauración de datos toma algunos días. NOTA: Si bien hoy en día existen respaldos en medios tales como CDs, DVDs o discos externos los respaldos en cinta son más utilizados o difundidos.
2. **Captura de imágenes**.- La captura de imágenes es una tecnología un poco más costosa y mantiene un adecuado RPO, pero el tiempo de recuperación

tiende a ser un poco adormecido y proclive a errores debido a la inflexibilidad de la tecnología de imágenes sobre la cual se apoya.

3. **Clustering**.- Finalmente, el *clustering*, que viene a ser algo así como un agrupamiento, logra cumplir completamente los objetivos del RTO y RPO, pero puede ser tremendamente costoso y complicado de implementar. Con excepción de los ambientes servidores de misión crítica no es una opción viable.

Para que una organización sea verdaderamente confiable en su estrategia, solución y procedimientos de recuperación de desastres, éstos deberían ser probados. Sin embargo, la mayoría de soluciones de recuperación de desastres son increíblemente complejas e invasivas en las operaciones de los negocios y por consiguiente no son factibles de probar regularmente. Cuando una organización más necesita que una solución de recuperación ante desastres funcione, puede ser la primera vez en que verdaderamente se la implemente en la realidad. Los métodos de recuperación ante desastres tradicionales presentan algunos inconvenientes que se los analizarán en detalle en la siguiente sección.

2.2.5.1 Inconvenientes de los métodos tradicionales de recuperación ante desastres

Mientras la necesidad de proteger los recursos de TI de los desastres es un imperativo del negocio, los administradores de TI se enfrentan con muchos obstáculos al momento de desarrollar un DRP, y esto incluye:

1. **La recuperación ante desastres tradicional es <u>cara</u>**
    a. Para asegurar que una recuperación ante desastres sea exitosa, con un esquema tradicional, se requiere configuraciones de hardware idénticas en

el sitio de recuperación, lo cual implica a menudo compras costosas de nuevos servidores.

b. Los sitios de recuperación de desastres permanecen con frecuencia inactivos o *adormecidos*, y sin embargo ocupan espacio fuera o dentro de la organización, requiere una administración periódica e incurre en costos de energía y sistemas de enfriamiento.

2. La recuperación ante desastres tradicional es <u>compleja y lenta</u>

a. Herramientas y procesos complejos, tales como herramientas de imágenes de sistemas, respaldos en cintas y procesos de restauración en otros servidores “desde cero”, recuperación de datos y aplicaciones requieren de habilidades especiales y recursos que son difíciles de adquirir y mantener.

b. Los datos de configuración, sistemas y aplicaciones necesitan ser guardados y *clonados* o replicados usando procesos únicos y complejos.

c. El aprovisionamiento de sistemas físicos para la recuperación ante desastres y la configuración de estos sistemas consume mucho tiempo (Ver **Ilustración 4**). Adicionalmente, la recuperación de datos y aplicaciones puede tomar desde varias horas a varios días por cada sistema, lo cual tiene un alto impacto en el RTO al que debería ajustarse el DRP. Este problema empeora aún más cuando se tienen diversos servidores que requieren una imagen separada.

Ilustración 4. **Proceso de recuperación física**

Fuente: Disaster Recovery Solutions from VMware
Elaborado por: Danilo Mannella L.

d. Los métodos tradicionales tales como los respaldos en cinta y captura de imágenes tienen una alta tasa de fallos, lo cual tiene un grave impacto en el RPO al que debería ajustarse el DRP.

3. La recuperación ante desastres tradicional no es confiable

a. Los métodos tradicionales representan todo un desafío cuando se efectúan pruebas, especialmente cuando se trata de aplicaciones multi-capa.
b. La utilización de procesos únicos y herramientas complejas para la recuperación de datos, aplicaciones y sistemas hace que las pruebas de recuperación sean tediosas, consuman mucho tiempo y conduzca a pruebas poco frecuentes o incompletas.
c. Finalmente, un DRP que no ha sido probado puede guiar a un falso sentido de seguridad y a menudo no se ejecutará correctamente, sobre todo cuando más se lo necesite. La dependencia estricta de hardware a menudo impide tener confianza en la recuperación.

2.2.5.2 La virtualización y la recuperación ante desastres

Conforme se les pide a los departamentos de TI hacer más y más con presupuestos estáticos o crecientemente reducidos, éstos se están dirigiendo

progresivamente a la virtualización como un medio para reducir gastos en hardware y reducir costos de energía, espacio y recursos humanos por servidor.

La virtualización hizo su aparición en escenarios de desarrollo y pruebas, lo que habilitaba a las organizaciones a que pudieran evaluar rápidamente software en diferentes ambientes operativos. Hace no mucho las organizaciones han puesto su mirada en la virtualización de servidores para consolidación de información para beneficiarse de la utilización de recursos de infraestructura incrementada y reducción de costos de hardware y mantenimiento así como de la instalación y configuración acelerada de servidor.

Una nueva aplicación de la virtualización de servidores emergió para el planeamiento y recuperación ante desastres. Las organizaciones ahora son capaces de apalancarse en los beneficios de la tecnología de la virtualización para proteger a los servidores en la red que comúnmente se los deja desprotegidos.

Las organizaciones tienden a compartir un conjunto esencial de necesidades de planeación y recuperación:

- El proceso de respaldo y recuperación tiene que ser rápido,
- tiene que tener un impacto mínimo en las operaciones de producción, y
- tiene que ser recuperable con un alto nivel de integridad de datos.

Estas necesidades orientadas al rendimiento son siempre balanceadas contra la necesidad económica de contar con una solución asequible. Más a menudo de lo que se piensa, la realidad muestra que las organizaciones acceden a una o más de estas necesidades debido al costo.

Una organización típica puede asignar hasta un 80% de su presupuesto para recuperación ante desastres en sus servidores de vitales solamente – frecuentemente

tan pocos como un 20% del total de servidores de la red. Estos son los servidores de misión crítica y de negocios críticos, tolerantes a fallos y con alta disponibilidad.

Un presupuesto de recuperación ante desastres que se alinee con estas políticas deja al 80% restante de servidores sin ser asegurados en caso de cualquier catástrofe. Mientras la pérdida de cualquiera de estos servidores no detenga las operaciones, su pérdida cuesta dinero. Si una carga de trabajo vale la pena que se esté ejecutando, vale la pena mantenerlo de esa manera. Claramente muchos planes de recuperación ante desastres a lo largo de las organizaciones son deficientes.

2.2.5.3 Estrategias de métodos tradicionales de DR

Todos los métodos anteriores de recuperación ante desastres tradicionales, incluyendo la virtualización, pueden ser aplicados dentro de la organización o fuera de ella, con los costos económicos, logísticos y humanos que conllevan. A continuación se detallan cada uno de ellos:

- ***Centro de recuperación in-house***

En tanto los administradores crean estrategias de recuperación de sus negocios para protegerlos de desastres naturales o provocados por el hombre, pudieran considerar la instalación de un centro de recuperación de datos en la propia empresa, o *in-house*, conocido también como centro *hot-site*. El beneficio de este enfoque es el completo control sobre el ambiente de recuperación, pero esta opción puede ser costosa y compleja de administrar.

El uso de un *hot-site* comercial puede proveer más flexibilidad y es una solución más efectiva en costo. Algunas empresas a menudo encuentran que les toma más tiempo y dinero construir este tipo de centro de datos de lo que se pudieran permitir. Adicionalmente a los costos obvios, tales como la compra de sistemas

redundantes para el uso de recuperación ante desastres, la operación de un *hot-site* ocasiona muchos costos en hardware, software, personal y soporte.

De todas las opciones de recuperación, la estrategia *in-house* es generalmente considerada la más costosa.

Ejemplos de potenciales costos escondidos son:

- Compra de hardware
- Mantenimiento de hardware
- Los costos de software, un componente importante dentro del presupuesto de recuperación del negocio, son a menudo subestimados por las empresas, al momento de considerar un hot-site interno.
- Espacio. El piso falso y los costos de espacio de oficinas generales varían considerablemente.
- Ambiente. Los generadores eléctricos son una necesidad, y es altamente recomendable un UPS (proveedor de energía ininterrumpida)
- Personal. Los hot-sites necesitan de personas que hagan el trabajo de recuperación de sistemas.
- Comunicaciones de datos. La recuperación de sistemas computacionales por sí mismos no tienen ningún efecto en la recuperación del negocio si los usuarios no pueden acceder a la información.

- ***Estrategia comercial -hot-site – Dedicada***

Esta estrategia provee un nivel alto en la capacidad de recuperación ante desastres con un tiempo de inactividad mínimo. Esto consiste en tener un equipamiento y sitio de recuperación de desastres dedicado, que puede ser activado bajo demanda en el evento de un desastre.

Esta estrategia habilitará la recuperación de funciones críticas o sistemas que tengan un RTO inferior a 24 horas.

Para proveer la justificación para este tipo de solución se recomienda que se lleve a cabo un BIA. Un BIA provee la información en los posibles impactos a causa de las interrupciones de las funciones de negocio críticas, y proveerán un RTO preciso para los sistemas y procesos de negocios críticos en cuestión.

- ***Estrategia comercial warm-site – Compartida***

Una instalación compartida, conocida como *warm-site*, se la considera generalmente como la manera más efectiva de proveer capacidades de recuperación ante desastres.

Un sitio de recuperación compartido es aquel que es utilizado por varias empresas en diversas ubicaciones geográficas, y por tanto los costos son distribuidos a través de la base de clientes. Los plazos de recuperación se incrementan en relación al sitio dedicado debido a la necesidad de reconfigurar la infraestructura compartida.

El establecimiento de este tipo de estrategia de recuperación requiere una planeación exhaustiva para determinar, en primer lugar cuál es el RTO requerido, y en segundo lugar qué configuración será requerida para lograr ese RTO.

- ***Estrategia cold-site***

La estrategia *cold-site* consiste en proporcionar un espacio de trabajo cerrado o una instalación de sala de computadores sin ningún equipo informático instalado, en el que la recuperación de los sistemas de tecnología se puede lograr.

La estrategia *cold-site* normalmente tiene toda la infraestructura necesaria en el lugar, tal como piso falso para los equipos de TI, controles ambientales, distribución de energía y las comunicaciones. Se acepta en general que puede tomar varias semanas

para activar una instalación de sitio frío dependiendo de los requerimientos. Luego, tomará varios días más para traer de vuelta todos los sistemas restaurados al estado deseado para su uso.

Por lo general, y como una buena práctica de seguridad informática, no es recomendable tener el sitio alterno para efectuar una recuperación ante desastres dentro de las mismas instalaciones de la empresa, con lo cual usualmente se contrata los servicios de una tercera empresa para utilizar los servicios e infraestructura de éstos, con la finalidad de que el DRP sea útil.

Obviamente las Pymes en su mayoría se decantan por un servicio de tipo compartido por sus costos, sin embargo las métricas de RTO y RPO no son las óptimas debido al *mejor esfuerzo* que ofrecen las empresas proveedoras de estos servicios, en contraste con una solución dedicada, aunque sus costos sean elevados.

2.2.5.4 Beneficios de la virtualización para las Pymes

Las Pymes, que con frecuencia tienen proporcionalmente más restricciones y demandas en cuanto a recursos en comparación a las grandes empresas, enfrentan desafíos significativos para implementar soluciones de recuperación ante desastres. Sin embargo, las Pymes cada vez más implementan tecnología más sofisticada como una parte central de sus operaciones, y aun así tienden a concentrar todos sus activos de TI en un grupo compacto de servidores. Con un escenario así, incluso un desastre tan pequeño como el fallo de un solo servidor puede conducir a interrupciones operacionales mayores o hasta el cierre del negocio.

La implementación de una solución de recuperación ante desastres a través de la virtualización permite que incluso las Pymes puedan cosechar los beneficios de una infraestructura lista para recuperarse ante desastres.

Estos beneficios incluyen:

1. **Rapidez**.- La virtualización provee una recuperación extremadamente rápida, ahorrando tiempo perdido y productividad al levantar de nuevo y ejecutar las operaciones del negocio.
2. **Precisión**.- El punto desde el cual se recupera la información es un punto conocido, ahorrando estimación de tiempo cuando se efectuaron los últimos respaldos y cómo recuperar los datos perdidos.
3. **Asequible**.- El bajo costo total de la solución la hace ideal para las Pymes.
4. **Fácil de usar**.- La solución es relativamente fácil de usar y administrar, permitiendo que Pymes con pocos o limitados recursos de TI le saquen provecho.
5. **Cobertura**.- Una solución de virtualización permite que se protejan no solamente los servidores de misión crítica, sino otros servidores que regularmente no son protegidos.

Las Pymes verán una mejora en su continuidad del negocio con una solución fuerte de recuperación ante desastres que sea asequible, y sin embargo, poderosa.

Las Pymes pueden aprovechar el contar con una solución de clase de un centro de datos por un precio que es factible de acceder para soluciones propias de Pymes.

2.2.6 Situación de la Recuperación ante Desastres de Pymes en el mundo

Cualquier empresa a nivel mundial reconoce la importancia de poder estar preparados ante un evento catastrófico en su centro de datos por cuanto esto podría provocarle pérdidas económicas de gran magnitud, e incluso pérdida de clientes, de hecho en el estudio efectuado por la firma Freeform Dynamics, por encargo de Quest Software, se recogen algunos datos respecto de la poca preparación que tienen las

Pymes en Europa, concretamente en Francia, el Reino Unido y Alemania. A continuación algunos datos proporcionados por este estudio (Lock, Bennett, & Vile, 2010):

- El término "recuperación de desastres" no es ampliamente usado en organizaciones de tipo PYMES. Un 39% admite que no conoce del tema, en tanto que un 44% admite tener una idea general de qué se trata.
- Pocas Pymes tienen planes formales de "recuperación de desastres", aunque manejan el riesgo de manera proactiva. Solamente un 23% tiene un DRP formal.
- Pocas Pymes usan una selección reducida de soluciones de DR disponibles, tradicionalmente respaldos basados en archivos.
- Las Pymes reconocen que su protección de datos y capacidades de DR puede ser mejor.

En la Encuesta 2011 sobre preparación ante Desastres en las PYMES (Symantec, 2011), se evaluó las actitudes y prácticas de las PYMES frente a la ocurrencia de un desastre, y la preparación que tenía para enfrentar dichos eventos, y se tuvieron los siguientes resultados.

- A pesar de advertencias las Pymes aún no están preparadas.- El 46% de las empresas encuestadas en Latinoamérica dijo no considerar prioritario la preparación ante desastres, y ese mismo porcentaje manifestó que en caso de un desastre perdería al menos un 40% de su información.
- Las Pymes no actúan hasta después de un desastre.- El 34% de los clientes de Pymes encuestados como parte del estudio para Latinoamérica

afirmó que sus proveedores Pymes habían suspendido sus servicios temporalmente a causa de un desastre. Esta interrupción le cuesta $3000 al día a los clientes.

- Planificación reactiva.- El 36% de las Pymes encuestadas manifestó que planea armar un plan de recuperación ante desastres.

Todo lo anterior se puede sintetizar en la infografía mostrada en la **Ilustración 5**:

Ilustración 5. **Infografía sobre la situación de las Pymes respecto de la recuperación ante desastres.**

Fuente: Symantec. Encuesta 2011 sobre Preparación ante Desastres en las Pymes. Hallazgos América Latina.
Elaborado por: Danilo Mannella L.

Conforme los datos antes citados, se aprecia la falta de preparación o desconocimiento por parte de las Pymes de lo que un buen DRP puede ayudar en sus

negocios. Los costos directos e indirectos de no contar con un DRP se puede apreciar en la siguiente tabla (Vision Solutions, 2008):

Cuadro 7.Costos directos e indirectos de las Pymes de no contar con un DRP

Costos tangibles / directos	Costos intangibles / indirectos
• Pérdida de ingresos por transacciones	• Pérdidas de oportunidades empresariales
• Pérdida de salarios	• Pérdida de empleados o desmoralización de los mismos
• Pérdida de inventario	• Disminución del valor de las acciones (si es que aplica)
• Costes laborales de saneamiento	• Pérdida de los fondos de comercio de los clientes y de los socios
• Costos de marketing	• Pérdida de negocio en favor de la competencia
• Tasas bancarias	• Mala publicidad y prensa
• Multas legales	

Fuente: *Whitepaper*: La guía fundamental para la recuperación de desastres. Vision Solutions (2008)
Elaborado por: Danilo Mannella L.

Sin embargo, de que la implementación tradicional de un DRP toma en cuenta situaciones extremas, principalmente a causa del clima (huracanes, terremotos, inundaciones, etc.), el mundo "siempre conectado" se ve afectado frecuentemente con interrupciones hasta cierto punto cotidianas como puede ser una falla eléctrica, fallas de hardware y brechas de seguridad, y esto en un esquema de DRP tradicional significa que la empresa deberá recurrir a un centro de datos externos que puede ser privado o mediante servicios de un tercero, de cualquier forma su costo puede ser elevado (IBM Global Technology Services, 2012).

2.3 Computación en la nube (Cloud Computing)

2.3.1 Definición de computación en la nube

Antes de definir lo que es la **computación en la nube**, o cloud computing (terminología en inglés) hay que destacar cada término por separado, de este modo:

- Cloud (Nube).- Tradicionalmente la nube se la ha asociado al Internet, como una manera de indicar, particularmente en diagramas, la compleja infraestructura que oculta esta red de redes.
- Computing (Computación).- Hace referencia a cualquier actividad de TI llevada a cabo cuando se hace uso de un computador personal o una red de computadoras, lo que implica el uso de recursos de TI que están bajo el exclusivo control del usuario, o también se refiere al almacenamiento, administración y procesamiento de datos, de tipo privado, en cuanto a que le pertenecen a un usuario en particular, aun cuando pueda ser accedido por terceros.

En la **Ilustración 6** se observa un bosquejo explicativo de la computación en la nube.

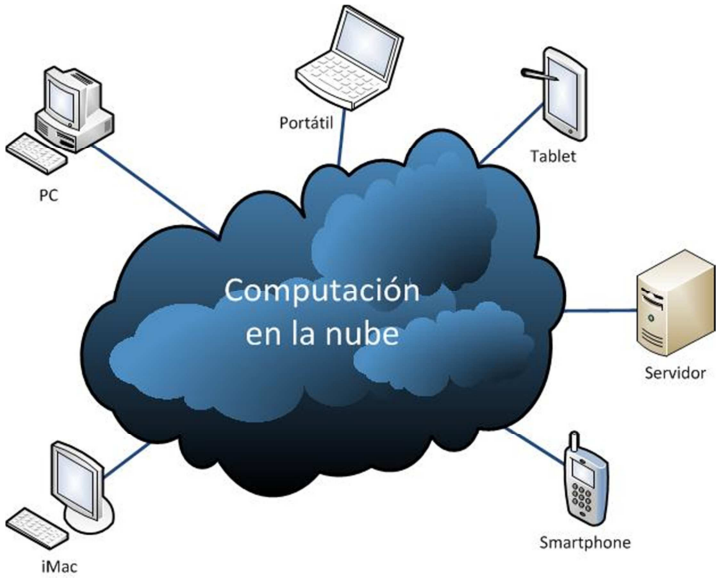


Ilustración 6. **Diagrama explicativo de computación en la nube**

Fuente: Elaborado por el autor

En su conjunto, sin embargo, una definición más formal la establece el Instituto Nacional de Estándares y Tecnología estadounidense (NIST) mencionando que “La computación en la nube es un modelo que permite el acceso ubicuo, conveniente, a demanda de una fuente compartida de recursos computacionales configurables (p. ej.

Redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y liberados con un esfuerzo administrativo o provisión de administración de servicio mínimo.” (NIST, 2011)

La IEEE Computer Society también define a la computación en la nube como una fuente de recursos computacionales que están al servicio de los usuarios y empresas, pero a través de esquemas de virtualización. Basados en este concepto de virtualización, la computación en la nube es un paradigma que permite que la carga de trabajo sea implementada y escalada rápidamente, a través del aprovisionamiento ágil de máquinas reales o virtuales.

El Vicepresidente de Investigación y Consultoría de América Latina de IDC, Ricardo Villate, señala que la computación en la nube “es un modelo de distribución de software conveniente para los clientes quienes lo bajan y lo utilizan según sus necesidades. Se estima que en cinco años el 80% de aplicaciones serán desarrolladas para la nube.” (Computerworld, 2011)

2.3.2 Componentes de la computación en la nube

Es importante destacar que la computación en la nube se trata de un modelo y no de una tecnología, algo que suele confundir con frecuencia a muchos, particularmente a empresarios. En este modelo, como se indicó anteriormente los centros de datos ofrecen a los usuarios ciertos recursos de cómputo como servicios, a través de una conexión a Internet, de manera tal que se pague un determinado valor por el tipo y cantidad de servicios requeridos.

La computación en la nube es la suma de la evolución de varias tecnologías (INTECO, 2011):

1. **Aumento de la capacidad de procesamiento**.- Desde el origen de la Informática, la capacidad de cómputo de los ordenadores personales se ha ido incrementando de forma vertiginosa.
2. **Conexión a Internet**.- La Red se ha convertido en una herramienta casi indispensable en la vida cotidiana de las personas. Su evolución implica aumento en la velocidad de conexión y en el número de conexiones en el hogar y en el trabajo.
3. **Dispositivos móviles**.- La miniaturización de los componentes informáticos ha permitido la aparición de dispositivos móviles que permiten la conexión permanentemente a Internet. Hoy en día, en un negocio es necesario poderse conectar con los recursos de la empresa, tanto desde ordenadores fijos como desde dispositivos portátiles, convirtiéndose la ubicuidad y movilidad en requisitos de gran importancia.

La implementación exitosa de una computación en la nube va más allá de los elementos antes citados, y esto no depende de una sola persona, sino de expertos en la industria que se han dedicado años para poder brindar a los usuarios finales, particularmente a las empresas, los beneficios del uso de la computación en la nube. Brevemente se detalla los componentes básicos de la computación en la nube en la **Ilustración 7** (Exforsys, 2009):

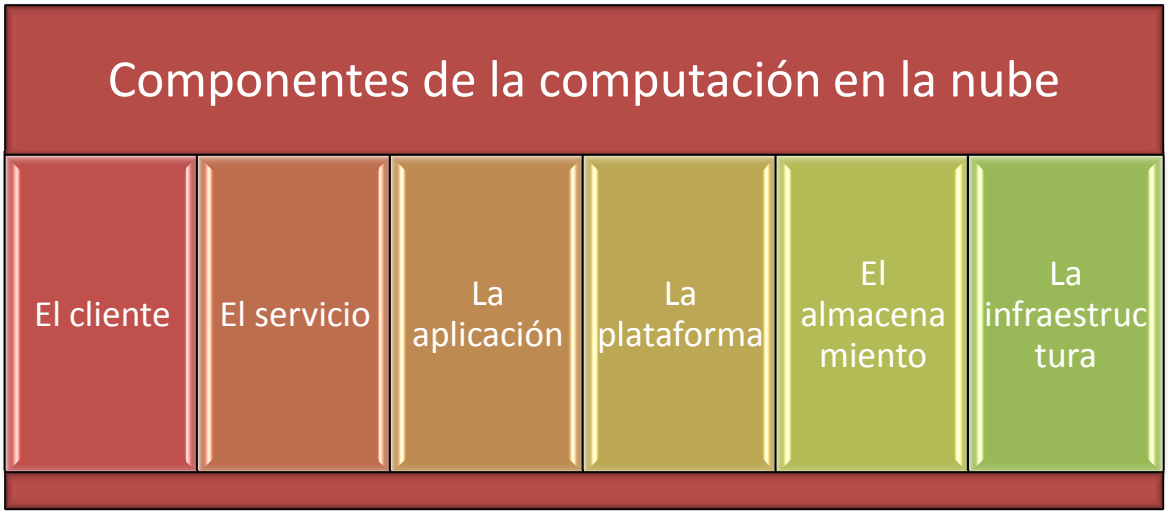


Ilustración 7. **Componentes de la computación en la nube**

Fuente: Recopilado por el autor. Exforsys (2009).

1. **El cliente – el usuario final**.- Se refiere al hardware y programas que se requerirá el usuario para poder acceder, a través del Internet, a los servicios que serán provistos por la empresa que brindará el soporte de computación en la nube. Es importante resaltar que esto se optimiza con la capacidad del hardware local y el software de seguridad del cliente.
2. **El servicio – las funciones de la computación en la nube**.- Una de las razones por las que la computación en la nube ha obtenido popularidad es debido a la adopción de negocios como la forma más fácil de implementar procesos de negocio. La optimización de los servicios se basa en dos cosas: el apropiado desarrollo de aplicaciones, y el usuario final.
3. **La aplicación – el eje fundamental del servicio**.- A menudo se confunde la aplicación con el servicio, sin embargo la aplicación es completamente diferente porque es a través de la aplicación que se brinda el servicio. La optimización de la aplicación se basa en la codificación de los desarrolladores, a través de pruebas extensivas en manejo de carga, seguridad y funcionalidad.

4. **La plataforma – la "infraestructura suave" de la aplicación**.- En aplicaciones o sitios web regulares que no tienen relación con la computación en la nube, la aplicación está directamente conectada con el servidor. En la computación en la nube, la aplicación todavía se activa a través de otra aplicación, llamada plataforma. La plataforma usualmente viene con lenguajes de programación tales como Ajax o Rubi. En este punto, se deberá considerar los lenguajes de programación requeridos por el proveedor para la plataforma de computación en la nube.
5. **El almacenamiento – el depósito de la computación en la nube**.- Todo lo que la aplicación conoce, y las funciones provistas por el servicio son posibles gracias al almacenamiento. El almacenamiento mantiene datos e información de las funciones acerca de cómo todo esto será implementado. La optimización del almacenamiento se basa en la protección de las instalaciones del almacenamiento de ataques, y la disponibilidad para la ejecución de respaldos, después de todo, la computación en la nube se trata siempre de consistencia y disponibilidad del servicio, lo cual se logra con un almacenamiento disponible todo el tiempo.
6. **La infraestructura – el eje fundamental de la computación en la nube**.- Cada servicio, función y disponibilidad de almacenamiento para proveer los datos necesarios es posible a través de una infraestructura optimizada. La infraestructura es una plataforma en donde se balancea la disponibilidad del almacenamiento en contra del número de peticiones. La infraestructura tiene la habilidad de hacer algunos cambios al balancear la carga e incluso la administración.

Más adelante, y de acuerdo al modelo en el cual querrán incursionar las empresas, se explicará en detalle a las aplicaciones, la plataforma y la infraestructura, como parte del servicio ofrecido por las empresas que ofrecen

2.3.3 Características de la computación en la nube

La computación en la nube presenta cinco características esenciales (NIST, 2011):

1. **Autoservicio por demanda**.- Un consumidor puede solicitar unilateralmente el aprovisionamiento de prestaciones de cómputo, tales como tiempo de servidor y almacenamiento de red, conforme se requiera, sin necesidad de requerir interacción humana con cada proveedor de servicio.
2. **Acceso de red ubicuo**.- Las prestaciones o servicios están disponibles en la red, y se acceden a través de mecanismos que promueven el uso mediante diferentes plataformas heterogéneas de dispositivos (teléfonos móviles, tabletas, portátiles y estaciones de trabajo).
3. **Fuente común de recursos**.- Los recursos de cómputo del proveedor se ofrecen de manera común a varios consumidores en un modelo *multi-tenant*[12], con diferentes recursos físicos y virtuales asignados dinámicamente y reasignados de acuerdo a la demanda del consumidor. Hay un sentido de independencia de la ubicación en donde el cliente no tiene control o conocimiento acerca de la ubicación exacta de los recursos provistos pero puede conocer la ubicación desde un nivel abstracto más alto (p. ej. país, estado, centro de datos, etc.). Como ejemplo de estos

[12] Se conoce como *multi-tenant*, o multi-inquilino a los diferentes consumidores (clientes) de servicios de la computación en la nube, que comparten la misma aplicación, sistema operativo y otros recursos de hardware del proveedor de servicios.

recursos se incluye el almacenamiento, procesamiento, memoria y ancho de banda.

4. **Rápida elasticidad**.- Las prestaciones pueden ser provistas y liberadas elásticamente, en algunos casos automáticamente, para escalar rápidamente hacia arriba o abajo proporcionalmente de acuerdo a la demanda. Para el consumidor las prestaciones disponibles para su aprovisionamiento a menudo parecen ser ilimitadas asignadas en cualquier momento y en cualquier cantidad.
5. **Servicio medido**.- Los sistemas en la nube automáticamente controlan y optimizan el uso de recursos al medir la prestación usada conforme determinado nivel de abstracción apropiado para el tipo de servicio (p. ej. Almacenamiento, procesamiento, ancho de banda y cuentas de usuario activas). El uso de los recursos puede ser monitoreado, controlado, y reportado, proveyendo de transparencia tanto para el consumidor como para el proveedor del servicio.

A pesar de que estas características esenciales, definidas por el NIST son la base de la computación en la nube, existen otras características comunes que se mencionan a continuación:

- Agilidad
- Computación resistente[13]
- Confiabilidad
- Empoderamiento a usuarios
- Escala masiva

[13] El término usado en inglés es *resilient*, y que se refiere al poder de recuperación o adaptación ante cualquier eventualidad.

- Homogéneo
- Mantenimiento
- Orientada al servicio
- Rendimiento
- Seguridad
- Software (o servicios en general) a bajo costo
- Virtualización

2.3.4 Modelos de servicio de la computación en la nube

La computación en la nube, como se indicó anteriormente, consiste en un modelo computacional, y se han definido 3 tipos de servicios, tal y como se muestra en la **Ilustración 8**:

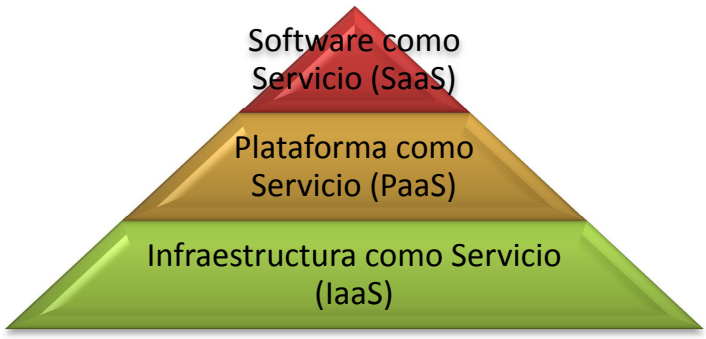


Ilustración 8. **Modelos de servicio de la computación en la nube**

Fuente: Elaborado por el autor
Elaborado por: Danilo Mannella L.

2.3.4.1 SaaS (Software como Servicio)

Este modelo de servicio es posiblemente la forma más ampliamente y conocida de computación en la nube. En el SaaS, o *Software como Servicio*, "los servicios

provistos al consumidor se los hace a través de aplicaciones del proveedor, que se ejecutan en una infraestructura de la nube. Las aplicaciones se acceden a través de diferentes dispositivos clientes, mediante una interface de cliente liviana, tal y como un navegador web o una interface de programa. El consumidor no administra o controla la infraestructura de red subyacente, incluyendo redes de datos, servidores, sistemas operativos, almacenamiento, o incluso servicios de aplicaciones individuales, con la posible excepción de limitadas configuración de usuario" (NIST, 2011).

En algunos casos los servicios son gratuitos, y el proveedor obtiene ingresos a partir de publicidad en el sitio web en donde aloja sus servicios. En otros casos los ingresos provienen de la actividad propia de rentar sus servicios.

En resumen, en el SaaS las aplicaciones se ejecutan en la nube y se brindan según demanda del usuario. Ejemplos de este tipo de servicio son:

Cuadro 8. Ejemplos de SaaS (Software como Servicio).

TIPO DE SERVICIO	EJEMPLO
Aplicacionescomo sitios Web	• Box.net (Box.net) • Microsoft Office Live (Microsoft) • Facebook (Facebook, Inc.) • LinkedIn (LinkedIn Corporation) • Twitter (Twitter, Inc.) • MySpace (MySpace.com) • Zillow (Zillow.com) • Google Maps (Google).
Colaboración y aplicacionesde oficina	• Cisco WebEx Weboffice (Cisco Systems, Inc.) • Google Docs (Google) • Google Talk (Google) • IBM BlueHouse (IBM, Corp.) • Microsoft Exchange Online (Microsoft) • RightNow (RightNow Technologies, Inc.) • Gmail (Google) • Microsoft Hotmail (Microsoft Hotmail) • Yahoo! Mail (Yahoo! Inc.).
Servicios de pago	• Amazon Flexible Payments Service (Amazon FPS) • (Amazon Web Services, LLC) • Amazon DevPay (Amazon Web Services, LLC).
Software basado en Web integrable a otras aplicaciones	• Flickr Application Programming Interface (API) (Flickr, LLC) • Google Calendar API (Google) • Saleforce.com´s AppExchange (Salesforce.com, Inc.) • Yahoo! Maps API (Yahoo! Inc.) • Zembly (Sun Microsystems, Inc.).

Fuente: Cloud Computing – Una perspectiva para Colombia.
Elaborado por: Danilo Mannella

2.3.4.2 PaaS (Plataforma como Servicio)

En el modelo de servicio PaaS, o *Plataforma como Servicio*, los servicios intentan brindar soporte a las aplicaciones. “El servicio que se entrega al consumidor es el de implementar en la infraestructura de la nube aplicaciones adquiridas o creadas para el consumidor usando lenguajes de programación, librerías, servicios y herramientas apoyadas por el proveedor. El consumidor no administra o controla la infraestructura de red subyacente, incluyendo redes de datos, servidores, sistemas

operativos, almacenamiento, pero tiene control sobre las aplicaciones implementadas y posiblemente sobre las configuraciones del ambiente de hospedaje de la aplicación." (NIST, 2011)

Las aplicaciones que residen en el proveedor de la nube se pueden ejecutar desde un tradicional centro de datos empresarial, o en la nube como tal. Los servicios de plataforma permiten que se ofrezca a los consumidores las aplicaciones que cumplirán sus necesidades, y se ajusta según su demanda. Ejemplos de este tipo de servicios son:

Cuadro 9. Ejemplos de PaaS (Plataforma como Servicio).

TIPO DE SERVICIO	EJEMPLO
Plataformasde desarrollo	• Amazon Simple Queue Service (Amazon SQS) (Amazon Web Services, Amazon Simple Queue Service (Amazon SQS)), Amazon Simple Storage Service (Amazon S3) (Amazon Web Services, LLC) • Google App Engine (Google) • GRIDS Lab Aneka (Vecchiol, Chu, & Buyya, 2009).
Bases de datos	• Amazon SimpleDB (Amazon Web Services, Amazon SimpleDB) • Big Table (Chang, y otros, noviembre de 2006) • Microsoft SQL Azure Database (Microsoft).
Cola de mensajes	• Amazon Simple Queue Service (Amazon SQS) (Amazon Web Services, Amazon Simple Queue Service (Amazon SQS)).
Servidores de aplicaciones	• NetSuite Business Operating System (NS-BOS) (NetSuite, Inc.)

Fuente: Cloud Computing – Una perspectiva para Colombia.
Elaborado por: Danilo Mannella

2.3.4.3 IaaS (Infraestructura como Servicio)

La IaaS, o *Infraestructura como Servicio*, proporciona al cliente una infraestructura de computación como un servicio, usando principalmente la virtualización. "El servicio que se presta al consumidor consiste en la provisión de procesamiento, almacenamiento, redes y otros recursos computacionales

fundamentales en donde el consumidor es capaz de implementar y ejecutar software arbitrario, que puede incluir sistemas operativos y aplicaciones. El consumidor no administra o controla la infraestructura de red subyacente pero tiene control sobre los sistemas operativos, almacenamiento y aplicaciones implementadas; y posiblemente un control limitado de componentes de red selectos, tales como *firewalls*[14]." (NIST, 2011)

Como se mencionó en el párrafo anterior el IaaS se trata de un conjunto de recursos físicos que se ofrecen como servicios, y en donde se emplean técnicas tales como la virtualización pudiendo alcanzar ahorros en costos porque se maximiza la utilización de: Energía, espacios, y equipos, entre otros. Ejemplos de este tipo de servicios son:

Cuadro 10. Ejemplos de IaaS (Infraestructura como Servicio)

TIPO DE SERVICIO	EJEMPLO
Procesamiento	• Amazon Elastic Compute Cloud (Amazon EC2) (Amazon Web Services, LLC) • Sun Network.com (Sun Grid) (SUN Microsystems, Inc.) • ElasticHost (ElasticHosts Ltd,) • Eucalyptus (Nurmi, y otros, 2009) • Nimbus (Alliance) • OpenNebula (Grupo de Arquitectura Distribuida), • Enomaly (Enomaly, Inc.).
Distribuciónde contenido a través de servidores virtuales	• Akamai (Technologies) • Amazon CloudFront Beta (Amazon Web Services,LLC).

[14] Un *firewall* es un dispositivo, o un programa de software que controla el tráfico de entrada y salida de una red.

Almacenamiento	• Amazon Simple Storage Service (Amazon S3) (Amazon Web Services, LLC) • Amazon SimpleDB (Amazon Web Services, Amazon SimpleDB) • Amazon Elastic Block Store (Amazon Web Services, Amazon Elastic Block Store (EBS)) • Microsoft SkyDrive (Microsoft Corporation) • Flicker (Flickr, LLC) • Youtube (YouTube, LLC) • Nirvanix Storage Delivery Network (Nirvanix) • Microsoft Live Mesh Beta (Microsoft Corporation, 2009)
Administraciónde sistemas	• Elastra (Elastra Corporation) • Engine Yard (Engine Yard, Inc.) • FlexiScalable (XCalibre Communications) • Grid Layer (Layered Technologies, Inc.) • Joyent (Joyent, Inc.) • Mosso (Rackspace, US Inc.) • Savvis Virtual Intelligent Hosting (Savvis, Inc.).
Administraciónde alojamiento	• Digital RealtyTrust (DigitalRealtyTrust, Inc.) • GoDaddy.com (GoDaddy.com, Inc.) • Layered Technology (Layered Technologies, Inc.).
Alojamiento autónomo	• Rackspace (Rackspace, US Inc.) • Savvis Virtual Intelligent Hosting (Savvis, Inc.) • Terremark Worldwide (Terremark Worldwide) • FlexiScalable (XCalibre Communications) • 1&1 Internet (1&1 Internet, Inc.).
VLAN (Virtual Local Area Network)	• CohesiveFT (Cohesive Flexible Technologies, Corp.).

Fuente: Cloud Computing – Una perspectiva para Colombia.
Elaborado por: Danilo Mannella L.

2.3.5 Impulsores y obstáculos de la computación en la nube

2.3.5.1 Impulsores

La computación en la nube se ha ido consolidando de acuerdo a algunos impulsores. Según Frost & Sullivan (2008) se tienen los siguientes impulsores:

- **Tercerización (o Outsourcing)**.- Las organizaciones acostumbradas al outsourcing como una manera de llevar a cabo los procesos de su negocio desean cada vez más expandir su campo para incluir computación por parte de terceros, por lo menos para ciertas aplicaciones.
- **Tiempo de Valoración y Desempeño**.- La computación en la Nube está orientada a entregar aplicaciones empresariales y servicios de mayor desempeño. Los Data Centers en la Nube están generalmente bien equipados para satisfacer las necesidades de cualquier Data Center privado. Los proveedores de la Nube prometen una capacidad de almacenamiento y de computación casi ilimitada y con una alta disponibilidad.
- **Ubicuidad**.- Las aplicaciones basadas en la Nube con acceso a Internet facilitan la naturaleza ubicua (a todo momento – en todo lugar) de los negocios actuales. Los empleados pueden acceder a las aplicaciones desde la oficina, desde la casa o desde cualquier otro lugar, a través de líneas fijas o dispositivos móviles. Los equipos de trabajo extendidos a lo largo del mundo pueden compartir acceso a una aplicación específica durante la ejecución de un proyecto. Los técnicos de TI pueden dejar la oficina, pues están en la capacidad de ampliar o reducir las aplicaciones de la nube a través de un buscador web.
- **Economía**.- Oportunidad de recortar costos mediante el uso y nivelación de facilidades compartidas. En el libro "*The Big Switch",* Nicholas Carr esboza un paralelo entre el incremento de la malla de distribución de potencia durante los inicios del siglo pasado y el movimiento actual hacia la computación basada en la nube. En ambos casos, él discute, que la economía – no el triunfo de la tecnología- es el factor preponderante

- **Maduración de las tecnologías de la virtualización**.- La maduración de las tecnologías de virtualización ha permitido a cloud computing asignar recursos y proveer servicios en forma eficiente, dinámica y elástica, diferenciando a cloud computing del escenario de centralización de recursos, propuesto hace más de 50 años con la aparición de servidores robustos compartidos por tiempo. Gracias a la virtualización, cloud computing ha brindando nuevas posibilidades para construir y desplegar infraestructuras computacionales y servicios complejos (Hwang, 2008), que pueden ser accedidos bajo demanda y ser utilizados desde cualquier lugar, a cualquier hora, ocultando las complejidades de la infraestructura base a los usuarios finales (Ohlman, Eriksson, & Rembarz, 2009).

Lo anterior lo complementa Carlos García, Director de Banca Móvil del Grupo Santander y ExDirector de Tecnología de Google para España y Portugal, quien señala que los principales impulsores de la computación en la nube son (Gracia Armendáriz, 2010): El impacto de la tecnología de consumo, a reducción de costes, la disponibilidad y escalabilidad del servicio, el efecto crisis y el efecto “garaje” o democratización de la empresa emprendedora.

2.3.5.2 Obstáculos

Si bien la computación en la nube ha dado grandes pasos en los últimos 3 años, no es menos cierto que este modelo presenta algunos obstáculos que todavía debe superar, particularmente si se desea que la computación en la nube sea mayoritariamente aceptada.

- **Seguridad**.- Sin lugar a dudas uno de los principales obstáculos que presenta la computación en la nube está relacionada con la seguridad.

Existe bastante desconocimiento sobre los mecanismos utilizados por las empresas que proveen de servicios en la nube, y se mantiene firmemente la creencia de que los datos están mejor resguardados dentro de la misma empresa que fuera de ella. “Con el objetivo de superar este obstáculo, Stratecast recomienda seguir los lineamientos de las mejores prácticas de seguridad como proteger los datos (24/7), asegurar y certificar todo el software, encriptar siempre los datos del suscriptor y validar prácticas de seguridad, entre otros; actividades que cumplen las nubes de cómputo en su gran mayoría” (Interactic. Mesa Sectorial de Cloud Computing, 2010).

- **Privacidad**.- En muchas empresas existe un alto nivel de preocupación por la privacidad de la información al interior de las empresas, en los centros de datos corporativos, no se diga en el caso de almacenarla fuera de la empresa en donde el peligro aumenta cuando se la pone en la “nube”.
- **Percepción sobre la conformidad con la regulación**.- Una de las características de la computación en la nube es su ubicuidad, pero esto implica que los datos pueden ser almacenados en cualquier parte del mundo, y esto conlleva a que se debe conocer y cumplir (tanto el consumidor como la empresa proveedora del servicio) las leyes y normas vigentes correspondiente a ese país respecto del manejo de información, almacenamiento y difusión, particularmente si se trata de transacciones comerciales. Es importante destacar que cuando la empresa contratante firma un contrato con la empresa contratista ambas se vinculan a aceptar una jurisdicción concreta.
- **Deslocalización de datos y procesos**.- Complementando los puntos anteriores, un obstáculo bastante común que enfrenta la computación en la nube, desde el punto de vista de las empresas que desean incurrir en este

modelo, consiste en el desconocimiento del lugar en donde se almacenan sus datos, puesto que en una empresa que almacene sus datos localmente sabe exactamente en qué servidor se encuentra su información, y qué procesos corren sobre el mismo, pero en la computación en la nube, si bien a las tecnologías de virtualización permiten no solamente hacer copias de seguridad de los datos sino de todo el servidor, y se pueden tener varias copias en diferentes sitios, la dificultad radica en que no se conoce en qué sitio se localizan los datos y procesos.

- **Restricciones de Internet**.- El tráfico de Internet puede ser un obstáculo para la computación en la nube debido a retardos en la transmisión de información pero sobre por el ancho de banda que puedan utilizar los consumidores, particularmente en el caso de las Pymes, en donde el presupuesto es reducido y más aún en países de economía emergente, en donde la infraestructura de Internet no está bien consolidada, en comparación con otras economías mundiales.
- **Pérdida sobre el control de los datos**.- Otro factor que preocupa a las empresas que incurren en la computación en la nube, sea que se trate de grandes empresas o de Pymes es la noción de pérdida de control sobre los datos, esto quiere decir que el consumidor no puede tener la certeza acerca de los planes de contingencia y recuperación ante desastres que tenga la empresa que provea los servicios de la computación en la nube, o incluso lo que pueda suceder en caso de que dicha empresa desaparezca del negocio. Es importante considerar este obstáculo en el SLA[15] establecido con el proveedor, tal y como lo manifiesta la guía de INTECO (INTECO, 2011): “El establecimiento de un nivel adecuado de transparencia en el

[15] El **SLA** se refiere al Acuerdo de Nivel de Servicio, por sus siglas en inglés, y que se firma entre la parte contratista y la contratante, en donde la primera establece a qué se compromete al ofrecer el servicio solicitado por el segundo, en definitiva, es un contrato en donde están las reglas del juego.

mercado a la hora de negociar los términos y condiciones en los contratos es fundamental para contrarrestar la falta de control derivada de la dependencia de terceros."

- **Interoperabilidad**.- Hoy en día existen una serie de estándares que no permiten la interoperabilidad entre servicios, por lo cual es importante que este obstáculo se lo examine, si se desea que la computación en la nube tenga una mayor aceptación.
- **Licenciamiento**.- En el mundo de la computación en la nube se debe tener bien claro cómo funcionarán los costos por licenciamiento de los servicios que utilizan las empresas y las aplicaciones que pudieran estar corriendo sobre varios servidores.

2.3.6 Situación actual en el mundo

Debido al auge y necesidad de contar con servicios de computación en la nube, sea cual fuere el modelo de servicios al cual acuden las empresas, hoy en día existen diferentes empresas a nivel mundial y local que prestan sus servicios y a continuación se enlista algunos de ellos, y se destacará sobre todo la situación por la que atraviesan las Pymes a este respecto.

2.3.6.1 Proveedores actuales de computación en la nube

Tal y como se mencionó en el capítulo 2.3.4 existen 3 tipos de modelos de servicios para la computación en la nube: SaaS, PaaS e IaaS, y las empresas que más sobresalen a nivel mundial de acuerdo a cada modelo son: Amazon, GoGrid, Google, Microsoft, Rackspace y Salesforce.com, tal y como se muestra en la **Ilustración 9**.

Ilustración 9. **Proveedores de computación en la nube en el mundo**

Fuente: Recopilación del autor.

Si bien cada una de las empresas antes citadas tiene un portafolio de productos amplio para servicios de computación en la nube a continuación se mencionan los servicios más representativos de estas empresas.

Cuadro 11. Empresas proveedoras de servicios de computación en la nube

Empresa	Producto	Modelo de servicio	Descripción
Amazon 	• Amazon Web Services (AWS)	SaaS	• Amazon Web Services (2006) proporciona una plataforma de infraestructura escalable de alta fiabilidad y de bajo coste en la nube. Es la base para los servicios mencionados más abajo.
	• Amazon Flexible Payments Service (Amazon FPS)		• Es un *Servicio Web de Amazon* (AWS) que permite la transferencia de dinero entre dos entidades. Existe un conjunto de herramientas básicas llamadas Amazon Simple Pay, que permite crear botones de pago a los desarrolladores de sitios web.
	• Amazon DevPay		• Es un servicio de administración de contabilidad y facturación en línea sencillo de usar que facilita a los negocios vender aplicaciones que están construidas dentro de AWS. Diseñado para ejecutar aplicaciones en la nube y a demanda para desarrolladores.
	• Amazon Simple Queue Service (Amazon SQS)	PaaS	• Este servicio ofrece un sistema de gestión de colas fiable y ampliable para almacenar mensajes a medida que se transfieren entre sistemas. Amazon SQS facilita la creación de un flujo de trabajo automatizado, junto con Amazon Elastic Compute Cloud (Amazon EC2) y los otros servicios web de la infraestructura AWS.
	• Amazon SimpleDB		• Amazon SimpleDB es un almacén de datos no relacionales de alta disponibilidad y flexible que descarga el trabajo de administración de bases de datos. Los desarrolladores simplemente almacenan elementos de datos y los consultan mediante solicitudes de servicios Web; Amazon SimpleDB se encarga del resto.
	• Amazon Elastic Compute Cloud (Amazon EC2)	IaaS	• Amazon Elastic Compute Cloud (Amazon EC2) es un servicio web que proporciona capacidad informática con tamaño modificable en la nube. Está diseñado para facilitar a los desarrolladores recursos informáticos escalables y basados en web.

Empresa	Producto	Modelo de servicio	Descripción
	• Amazon CloudFront		• Amazon CloudFront es un servicio web diseñado para la entrega de contenido. Se integra con otros Amazon Web Services para ofrecer a los desarrolladores y a las empresas una forma sencilla de distribuir contenido a los usuarios finales con baja latencia, altas velocidades de transferencia de datos y sin compromisos.
	• Amazon Simple Storage Service (Amazon S3)		• Amazon S3 es almacenamiento para Internet. Está diseñado para facilitar a los desarrolladores la informática a escala web. Proporciona una sencilla interfaz de servicios web que puede utilizarse para almacenar y recuperar la cantidad de datos que desee, cuando desee, y desde cualquier parte de la web.
	• Amazon Elastic Block Store		• Amazon Elastic Block Store (EBS) proporciona volúmenes de almacenamiento a nivel de bloque diseñados para utilizarlos con las instancias de Amazon EC2.
GoGrid 	• GoGrid	IaaS	• GoGrid (2008) es un servicio de infraestructura en la nube que hospeda máquinas virtuales de sistemas operativos Windows y Linux, administrados por un panel de control multi-servidor, en el que las empresas pueden construir y administrar infraestructura de nubes complejas.
Google 	• Google Maps	SaaS	• Es una tecnología y aplicación de servicio de mapeo web proporcionada por Google que ofrece mapas de calles, un planificador de rutas para viajar a pie, en auto, bicicleta (beta) o en el transporte público y urbano de negocios para la localización de numerosos países de todo el mundo.
	• Google Docs		• Google Docs es un suite gratis de ofimática y servicio de almacenamiento de datos basada en la Web, ofrecida por Google, la cual permite que los usuarios creen y editen sus documentos en-línea mientras colaboran en tiempo real con otros usuarios.
	• Google Talk		• Google Talk es una aplicación de mensajería descargable de Google, que permite enviar mensajes de texto instantáneos, transferir archivos, efectuar audioconferencias, conectar

Empresa	Producto	Modelo de servicio	Descripción
			mediante mensajería de voz a personas de todo el mundo mediante llamadas de PC-a-PC, y se integra con la aplicación GMail.
	• Google Calendar API		• La API (Interface de Programa de Aplicaciones) de Google Calendar permite desarrollar aplicaciones clientes para crear nuevos eventos, editar o eliminar eventos existentes y buscar eventos, dentro de los datos de calendarios de Google Calendar.
	• Google App Engine	PaaS	• Google App Engine permite ejecutar aplicaciones web en la infraestructura de Google. Las aplicaciones App Engine son fáciles de construir, mantener y escalar conforme se necesite crecer el tráfico y el almacenamiento de datos. Con App Engine no hay servidores que mantener. Simplemente se sube la aplicación, y está lista para servir a los usuarios.
	• YouTube		• YouTube permite que miles de millones de usuarios encuentren, vean y compartan vídeos creados de forma original. YouTube ofrece un foro para comunicarse con los usuarios de todo el mundo, para informarles y para inspirarlos y sirve como plataforma de difusión para creadores de contenido original y anunciantes de cualquier tamaño.
Microsoft 	• MS Office 365	SaaS	• Antiguamente llamado MS Office Live, el MS Office 365 ofrece un conjunto profesional y exhaustivo de herramientas de productividad de negocios, a través de versiones para uso en la nube de las herramientas de comunicación y colaboración de MS Office conocidas: o *Word, Excel, PowerPoint, Outlook*, además de o *Exchange Online* - correo electrónico empresarial con calendarios de uso compartido, correo de voz y mensajería unificada, correo electrónico móvil o *Lync Online* - para conferencias de audio y video de PC a PC, y o *SharePoint Online* - para crear sitios para compartir documentos e información con colegas y clientes,

Empresa	Producto	Modelo de servicio	Descripción
			extranet para compartir archivos de gran tamaño y acceso sin conexión a documentos a través de espacios de trabajo -
	• MS SQL Azure Database	PaaS	• SQL Azure es un servicio de base de datos en la nube altamente disponible y escalable basado en las tecnologías de SQL Server. Con SQL Azure, los desarrolladores no tienen que instalar, configurar ni administrar ninguna base de datos. La alta disponibilidad y la tolerancia a errores están integradas, y no se requiere administración física. SQL Azure es un servicio administrado que controla Microsoft y tiene un contrato mensual del 99,9 %.
Rackspace 	• Cloud Hosting • Managed Hosting • Hybrid Hosting • Email & Apps	SaaS PaaS IaaS	• Rackspace tiene dos principales segmentos de nivel de servicio: Gestionado y Intensivo. Ambos niveles de servicio reciben soporte a través de e-mail, teléfono, chat en vivo, y los sistemas de tickets, pero están diseñados para satisfacer las necesidades de diferentes empresas. Dentro de lo que son productos en la nube destacan: Cloud Servers, Cloud Servers Managed, Next Generation Rackspace, Cloud Databases, así como SaaS Application Hosting, Rackspace Cloud Drive, Rackspace Server Backup y Email Archiving. De igual manera hay soluciones Rackspace DR para recuperación ante desastres.
Salesforce 	• SalesForce AppExchange	SaaS	• AppExchange (2005) es un mercado para aplicaciones de computación en la nube construidas para la comunidad de Salesforce.com y que son entregadas por desarrolladores de terceros. Los usuarios pueden comprar estas aplicaciones y agregarlas a su entorno de Salesforce.com.

Fuente: Recopilación del autor

En el Ecuador existen algunas empresas que se dedican a ofrecer servicios de computación en la nube, a continuación se mencionan solamente algunas de ellas:

Cuadro 12. Empresas que ofrecen servicios de computación en la nube en Ecuador

Empresa	Servicio	Modelo de servicio	Descripción
Compuequip DOS	• Integración de soluciones con diferentes fabricantes	SaaS PaaS IaaS	• DOS por su conocimiento comercial del mercado y del modelo de computación en la nube desarrolla la visión comercial de estos modelos, basado en el conocimiento de sus consultores, y en servicios de sus partners, para desarrollar la visión del cliente y el catálogo de servicios Cloud de acuerdo al mercado potencial. (www.compuequip.com)
Kruger	• Implementación de Websphere IBM Cloudburst	PaaS	• Websphere IBM Cloudburst, es un paquete completo de *IBM Service Management* que complementa la infraestructura de IT ya existente, esto incluye hardware, software y servicios y proporciona un cloud computing seguro, fiable y privado. (www.kruger.com.ec)
New Access	• Continuidad de negocio y servicios data center	IaaS	• El servicio consiste en infraestructura de última generación para prestación de servicios de Data Center para implementar BCPs y DRPs de las empresas. (www.new-access.net)
Telconet	• Data Center de Alta Disponibilidad	IaaS	• El Data Center de Telconet proporciona a las empresas servicios de housing (alojamiento compartido, colocation, etc.) y hosting (servidores virtualizados, servicios en la nube, etc.) aprovechando su infraestructura de redes brindando servicios al mercado nacional e internacional (www.telconet.net)
VirtualIT	• Infraestructura virtual • Alta Disponibilidad de Aplicativos y Datos • Almacenamiento virtual	PaaS IaaS	• Virtual IT es una empresa líder en soluciones de Infraestructura Virtual, así como en el área de manejo, monitoreo y optimización del ambiente tecnológico de empresas que utilizan la informática para el manejo de los procesos de misión crítica de su negocio. • Virtual IT es representante para el Ecuador de empresas de prestigio mundial como VMware, DataCore, Vizioncore, NetSupport, entre otras. (www.virtualit.com.ec)

Fuente: Recopilación del autor

Algunos de los servicios que se proveen en Ecuador bajo el concepto de computación en la nube son: (Computerworld, 2011)

- Servicios de consultoría
- Respaldo On-line de información, desde cualquier lugar con conexión a Internet
- Gateway único de datos independiente de la conexión a Internet, manteniendo todos los servicios activos desde los Data Centers.
- Servidores virtuales para aplicaciones de clientes (Ej. Bases de datos, CRM, etc.)
- Servidores Privados Virtuales
- Aceleración de Servidores Web
- Licenciamiento SPLA de Microsoft
- Cloud Backup, OnSite Backup con replicación a la Cloud (Recuperación de desastres y Continuidad de negocios)
- Virtualización de Aplicaciones (entrega de aplicaciones vía Internet)

2.3.6.2 Casos de éxito a nivel mundial

Dentro de la computación en la nube quien ha adquirido una vasta experiencia es sin duda la compañía Amazon, que con su servicio AWS ha permitido implementar soluciones en la nube a una gran cantidad de empresas, por ello se detalla a continuación algunos de estos casos de éxito (Amazon Web Services, 2012):

Cuadro 13. Casos de éxito mundial de implementación de computación en la nube

Tipo	Logo	Empresa	Descripción del caso
1. Alojamiento de aplicaciones		GeneXus	• La empresa se puso en contacto con Amazon Web Services (AWS) cuando Artech necesitó un método económico y eficaz de implementación de productos a su base de clientes mundial. Amazon Elastic Compute Cloud (Amazon EC2) permite que Artech reduzca de manera significativa el tiempo de configuración del servidor mientras ajusta la capacidad para dar cabida a las necesidades fluctuantes. Come consecuencia, Artech ha reducido de manera considerable los gastos y el tiempo de comercialización del producto.
2. Copia de seguridad y almacenamiento		Hitachi Systems	• Hitachi Systems & Services, miembro de Hitachi Group, ha acudido a Amazon Simple Storage Service (S3) para afrontar la creciente demanda de almacenamiento para su nueva "Solución de Difusión para Móviles", el primer servicio de su clase en Japón.
3. Entrega de contenido		IMDb	• Internet Movie Database (www.imdb.com) es uno de los recursos más conocidos y con mayor autoridad del mundo para contenidos de películas, TV y de famosos, con más de 100 millones de visitantes únicos mensuales. IMDb utiliza Amazon CloudFront para alojar datos de búsquedas para la funcionalidad de búsqueda avanzada IMDb, que encuentra la película o la persona que se desea buscar con solo pulsar unas teclas. En el ámbito móvil, cada milisegundo cuenta mucho. Los clientes móviles valoran en especial acertar con la película que desean sin necesidad de teclear una consulta de búsqueda completa. CloudFront agiliza al máximo esta experiencia al distribuir contenido situado físicamente cerca de la base de usuarios mundial de IMDb.
4. Comercio electrónico		The Talk Market	• The Talk Market utiliza Amazon Flexible Payments Service para procesar su sistema de procesamiento de tarjetas de crédito.
5. Computación de alto rendimiento		Unilever	• Con la ayuda de Eagle Genomics, el equipo de investigación y desarrollo de Unilever creó un programa de datos digital para avanzar en materia de innovación biológica e informática. La arquitectura del programa combina Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Service (Amazon RDS) y Amazon Simple Storage Service (Amazon S3) con el sistema de flujo de trabajo de código abierto eHive. Desde que creó el programa, Unilever ha logrado mantener sus costes operativos, al mismo tiempo que ha conseguido procesar secuencias genéticas con una rapidez 20 veces superior y

Tipo	Logo	Empresa	Descripción del caso
			aumentar significativamente los flujos de trabajo simultáneos.
6. Alojamiento de medios		Sonico	• Sonico.com, sitio de redes sociales con más de 48 millones de usuarios inscritos, ha trasladado sus más de mil millones de imágenes a Amazon S3 y realiza toda la carga, procesamiento y almacenamiento por medio de Amazon EC2 y Amazon S3. La empresa también aprovecha Amazon Simple Queue Service (SQS) e instancias de MySQL que se ejecutan en Amazon EC2.
7. Personal según demanda		Channel Intelligence	• Gracias a Amazon Mechanical Turk, Channel Intelligence consiguió disponer de inteligencia humana en todo el planeta y reducir los costes específicos de tareas en un 85%.
8. Motores de búsqueda		Alexa	• Alexa ofrece servicios de información y búsqueda de grandes volúmenes, con una almacenamiento de más de 12 millones de objetos en Amazon SimpleDB y más de 5 millones de consultas cada día.
9. Alojamiento Web		Fútbol Club Barcelona	• El Fútbol Club Barcelona (FCBarcelona) es un equipo de fútbol muy popular con sede en Barcelona, España. A fin de mantener el sitio web del FCBarcelona —que aloja más de 6.000 páginas y más de 12.000 fotos digitales, que además se encuentra disponible en seis idiomas—, la empresa asociada del FCBarcelona, Gnuine, utiliza una serie de productos de Amazon Web Services (AWS) para alojar Ubiquo Sports, un sistema de gestión de contenidos (CMS) tipo plataforma de software como servicio (SaaS), entre los que destacan Amazon Route 53, Amazon CloudFront, Amazon Simple Storage Service (Amazon S3), Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Load Balancing (Amazon ELB), Amazon CloudWatch, Amazon Simple Notification Service (Amazon SNS), Amazon Relational Database Service (Amazon RDS) y Amazon CloudFormation.

Fuente: Casos prácticos de Amazon Web Services
Elaborado por: Danilo Mannella L.

2.3.6.3 Casos de éxito en Ecuador

En el país existen algunos casos en los cuales luego de aplicar soluciones de computación en la nube, sea a través de SaaS, PaaS o IaaS tuvieron los beneficios deseados.

Cuadro 14. Casos de éxito de computación en la nube en Ecuador

Empresa	Desafío	Solución	Resultados
Corporación Grupo Fybeca (Computerworld, 2011)	• El ahorro en costos, eficiencia operativa, disponibilidad y adecuada distribución de los servicios así como fortalecimiento de infraestructura llevaron a esta empresa a cambiar las herramientas de correo corporativo. • Aun cuando se contaba satisfactoriamente con Lotus Notes la empresa demandaba una solución más eficiente para fortalecer la colaboración con chat, video y compartición de documentos, y su versionamiento. • Lotus Notes implicaba adicionalmente un costo de aprovisionamiento desde la actualización de versiones, renovación de licencias de correo y antispam así como actualización en el PC de cada usuario, entre otros factores	• Luego de analizar herramientas de servicios de correo corporativo (Yahoo, Hotmail, Network Solutions, Google Apps) se deciden por Google Apps • Un factor preponderante para adquirir la solución fue también que el 75% de usuarios de la empresa contaban con Gmail como correo alterno	• Con Google Apps se consiguió un ahorro del 41% de este servicio proyectándolo a 3 años • Se eliminó costos por licenciamiento de antispam • En telefonía hubo un ahorro del 12% anual al utilizar la herramienta de chat de texto y video • Adicionalmente hay un evidente ahorro de 99.9% al no tener que invertir en recursos de hardware • Mayor capacidad de almacenamiento para los usuarios (25 GB) • El nivel de satisfacción del usuario es del 96%
Merck Ecuador (Computerworld, 2011)	• Contar con la mejor organización de TI en la industria Farmacéutica y Química. • Establecimiento de un acuerdo global entre el nivel de servicio del “backbone” de comunicaciones y enlaces de la red para atender incidentes en cualquier parte del mundo. • Trabajar con cada uno de los países (clientes de la nube) preparando desde las estaciones de trabajo, afinar sistemas y equipos de comunicaciones, implementar aplicaciones de medición de desempeño de los servicios, etc.	• Implementación de una nube corporativa propia. • Combinación de SaaS (ERP, CRM, correo electrónico, aplicaciones de RR.HH., entre otros), PaaS (aplicaciones de colaboración, workflows, documentales, intranets, extranets, entre otros) e IaaS, según cada aplicación.	• Estandarización • Mayor visibilidad • Mayor seguridad • Consolidación • Reducción de costos • Reorientación de planes de TI hacia el negocio

Fuente: Recopilación del autor

No obstante los ejemplos antes citados se debe recalcar que están son medianas empresas y que no hay datos documentados de pequeñas empresas que hayan todavía incursionado con éxito en la nube.

2.3.7 Modelos de negocios de computación en la nube

Existen básicamente 3 tipos de modelos de negocios de computación en la nube, tal y como se muestra a continuación en la **Ilustración 10**:

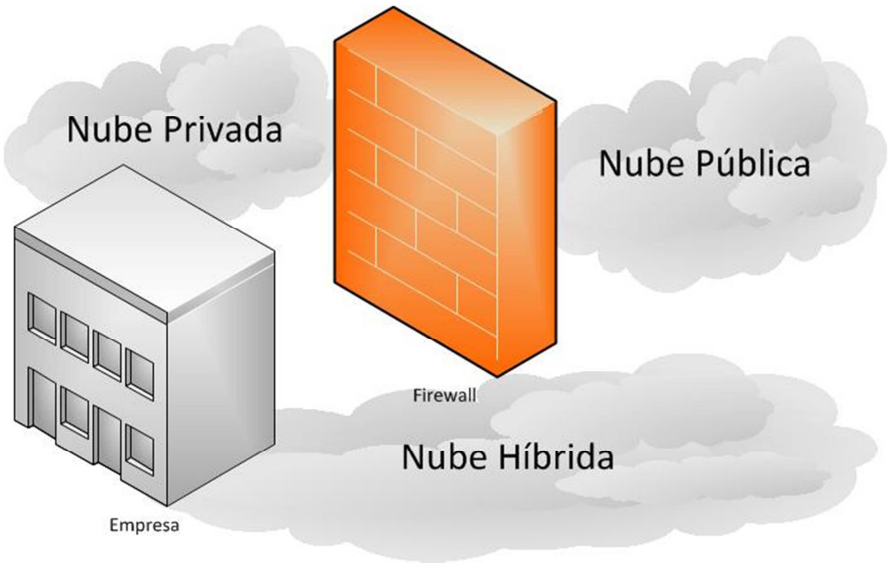


Ilustración 10. **Modelos de computación en la nube**

Fuente: Elaborado por el autor

- **Nubes privadas**.- Son aquellas creadas y administradas por una única entidad que decide dónde y cómo se ejecutan los procesos dentro de la nube. Supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, ya que los datos sensibles permanecen en la infraestructura informática de la entidad, mientras que controla qué usuario accede a cada servicio de la nube. Sin embargo, la entidad sigue siendo la encargada de comprar, mantener y administrar toda la infraestructura hardware y software de la nube.
- **Nubes públicas**.- Son aquellas en las que todo el control de los recursos, procesos y datos está en manos de terceros. Múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.

- **Nubes híbridas**.- Son aquellas en las que coexisten los dos modelos anteriores. Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web mientras que mantiene su servidor de bases de datos en su nube privada. De este modo, se establece un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo estricto control mientras que el servidor web es administrado por un tercero. Esta solución disminuye la complejidad y coste de la nube privada.

Algunos autores (INTECO, 2011) nombran a un cuarto tipo de nube conocidas como **nubes comunitarias**, las cuales son compartidas entre varias organizaciones que forman una comunidad con principios similares (*misión, requerimientos de seguridad, políticas y cumplimientos normativos*). Puede ser gestionada por la comunidad o por un tercero. Este modelo puede ser visto como una variación en el modelo de nube privada. Este estudio se centrará únicamente en las 3 primeras nubes.

2.3.8 Factores para la adopción de la computación en la nube

Las organizaciones a nivel mundial, y particularmente las Pymes están adoptando este modelo de computación en la nube principalmente debido al deseo de conectar a sus empleados a través de diferentes dispositivos que están a su alcance hoy en día. Existen algunos factores tanto en lo político, económico, social y tecnológico (PEST) que inciden para esta adopción (Cruz Marta, De Castro Neto, Neves, & Ramalho Correia, 2011):

Cuadro 15. Factores políticos, económicos, sociales y tecnológicos asociados con la adopción de computación en la nube por parte de Pymes a nivel mundial.

PEST	Factores
Político	• Se proporciona protección continua de datos, los requisitos legislativos son más necesitados, en particular aquellos relativos a las condiciones bajo las cuales los datos pueden ser almacenados y procesados; definición legal de la privacidad de información personal y de gestión.
	• Las iniciativas de políticas para acelerar el uso de la banda ancha de las Pymes podrían incluir un tratamiento fiscal favorable, en un entorno jurídico, político y fiscal.
	• Los políticos están buscando modelos de regulación, como alternativa a los monopolios del pasado, reconociendo que la infraestructura de regulación ha dado lugar a nuevos tipos de monopolios, controlados por los proveedores de servicios más fuertes.
	• Contribuye a reducir significativamente las emisiones de carbono.
Económico	• Permite pago flexible (por ejemplo, pago por uso), sin la necesidad de que los clientes posean las aplicaciones informáticas de infraestructura o software necesarios para las necesidades de su negocio (SaaS-Software as a Service). Esto significa que las Pymes, no necesitan mantener y actualizar los servidores, las aplicaciones diferentes (el software) y la seguridad. En su lugar, las PYME pueden confiar en el proveedor de servicios de nube que puede escalar fácilmente hacia arriba y hacia abajo a través de la asignación y re-asignación de recursos físicos y virtuales con el fin de satisfacer la necesidad real.
	• Permite el funcionamiento eficiente, con una reducción significativa del coste/ahorro; las soluciones de computación en la nube va a reducir al mínimo la inversión de las Pymes en el propio hardware (HW), software (SW) y el mantenimiento.
	• Debido a la limitada potencia financiera de las Pymes, en comparación con las grandes organizaciones, el factor de costo parece ser aún más relevante para las Pymes (que tienen una falta técnica y financiera de los recursos en comparación con las grandes empresas).
	• Ventaja competitiva y estrategia no parecen ser tan relevantes para las PYMES, como puede ser para las grandes empresas, porque su estrategia es de largo plazo en lugar de a corto plazo.
	• Muchas Pymes no tienen el conocimiento de SI (Sistemas de Información) y de TI y de todos sus temas, por lo que cualquier decisión depende de fuera de las organizaciones de TI de los proveedores.
	• La crisis económica actual ha llevado a respuestas de los gobiernos para limitar los efectos económicos de la crisis crediticia; la crisis no debe dañar los motores de crecimiento a largo plazo. Como resultado las Pymes deben invertir en infraestructura inteligente y en tecnología verde.
	• La necesidad de nuevas compras regulares de software se reduce o elimina.
	• En términos de costos/productividad en curso de las mejoras de las empresas, se estima una reducción del 50-75% en el tiempo y esfuerzo que se necesita para agregar nuevos productos.
	• Mayor seguridad es posible gracias a las economías de escala y la capacidad de pagar mejores expertos en seguridad.
	• La computación en la nube fomenta la innovación, y mejora de la competitividad empresarial
	• En general, los servicios de computación en la nube proporcionan una plataforma de negocios abierto para todos, en todas partes, para todos los países, para todas las empresas, para cada organización y para cada tipo de negocio.
Social	• Facilidad de uso
	• Nuevas oportunidades para la colaboración y las redes sociales entre los socios de trabajo, al permitir el acceso a fuentes de información que son independientes en tiempo y distancia.

PEST	Factores
	• Una comunidad de actores locales, distribuidos junto con las comunidades virtuales, contribuye al desarrollo de estrategias, soluciones tecnológicas, servicios digitales y modelos de negocio.
	• Oportunidad para los gerentes, ingenieros, personal de ventas y marketing para desarrollar nuevas habilidades, trabajar con tecnología nueva y potencialmente prestigiosa, que puede conducir a la progresión profesional y la satisfacción en el empleo.
	• Cooperación en tecnología de la información.
Tecnológico	• Proporciona un cierto nivel de personalización y permite una operación eficiente.
	• Proporciona una respuesta flexible a los cambios.
	• La fiabilidad se mejora a través del uso de sitios redundantes.
	• La escalabilidad se ofrece a través de aprovisionamiento dinámico de recursos. La ampliación de capacidad se realiza en la nube, y no en las instalaciones del cliente.
	• Servicio de alta calidad, siempre accesible en cualquier momento y en cualquier dispositivo (móvil y fijo), en cualquier conexión (a través de conexiones fijas e inalámbricas) y desde cualquier lugar.
	• Las Pymes no necesitan mantener y actualizar los servidores, aplicaciones (software) y la seguridad.
	• El gobierno de la red y el estado de TI, modelos flexibles de gestión de licencias, la comprensión de cómo las operaciones se realizan de acuerdo con los Acuerdos de Nivel de Servicio (SLA)
	• Los servicios genéricos básicos incluyen sistemas de pago electrónico, para la certificación y la confianza, la planificación de recursos empresariales (ERP), gestión de relaciones con los clientes (CRM), adquisiciones electrónicas
	• La puesta en marcha requiere un mínimo esfuerzo debido a la fácil migración de código para el nuevo entorno.

Fuente: The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors (2011).
Elaborado por: Danilo Mannella L.

Se hace evidente a partir del análisis de los factores PEST que los nuevos sistemas de computación en la nube tiene el potencial para multiplicar la productividad, la eficiencia y la rentabilidad de las empresas de pequeña escala. Sin embargo, algunas Pymes siguen siendo reacias a hacer uso de servicios de banda ancha, o considerar las posibles ventajas de Cloud Computing, debido a percepciones erróneas con respecto a posible inversión de capital, el miedo de la complejidad, la falta de comprensión de los beneficios potenciales, y la falta de técnica recursos. No obstante lo anterior, un creciente número de empresas (pequeñas y grandes) están empezando a ver algunos valores reales en el uso de la nube.

Como se ha visto anteriormente, hay muchas oportunidades y ventajas para las PYME en el uso de la computación en la nube. Muchas de las mismas funciones se pueden realizar más rápida y eficientemente mediante el uso de una moderna infraestructura de TI y el software de la nube que los tradicionales centros de datos. Como resultado, los factores antes citados son de consideración para la computación en la nube como una opción atractiva para muchas Pymes, sobre todo en la actual crisis económica mundial, debido a su estructura de costos flexible y escalabilidad.

Por último, hay que recordar que la decisión de incursionar en la computación en la nube en el caso de las Pymes no es una decisión netamente de Tecnología, sino de Modelo de Negocios, y el Gerente (o CEO) de la empresa en la PYME es quien mejor conoce las necesidades de su empresa, y debe tomar él la decisión de migrar a la nube, y no delegar esta decisión.

2.3.8.1 Interpretación de análisis PEST aplicado a las Pymes locales

El anterior análisis PEST (político, económico, social y tecnológico) efectuado a partir de un estudio internacional permite que se pueda revisar la situación en el ámbito nacional ecuatoriano, y de este modo a continuación se presenta un cuadro comparando los parámetros antes citados con la realidad ecuatoriana:

Cuadro 16. Factores políticos, económicos, sociales y tecnológicos asociados con la adopción de computación en la nube por parte de Pymes a nivel mundial.

PEST	Factores
Político	• Aunque está todavía pendiente de aprobación, el *Proyecto de Ley de Creación, Promoción y Fomento de Micro, Pequeñas y Medianas Empresas*, entregado a la Asamblea Nacional el 8 de marzo de 2010, en su Art. 8 habla sobre la reducción de trámites, requisitos e información que podrán tener las Pymes a través de Internet y otras formas electrónicas, con lo cual se busca tener información sobre plataformas de fácil acceso y transaccionalidad para las Pymes, y esto puede solventarse con los servicios de proveedores de servicios en la nube.
	• En la *Ley de Economía Popular y Solidaria*, publicada en el R. O. el 28 de abril de 2011 se menciona en el Art. 12 (Información) que dentro de las Formas de Organización de la Economía Popular y Solidaria, se deberá presentar a la Superintendencia información periódica relacionada con la situación económica y de gestión, con lo cual se requerirá de medios electrónicos eficaces para la conservación de los datos, y la computación en la

PEST	Factores
	nube coadyuva al cumplimiento de esta normativa en cuanto a la disponibilidad y confidencialidad de la información.
	• De igual manera, en la misma ley, en los Art. 94 (Información) y Art. 95 (Sigilo y Reserva) se menciona que las cooperativas de ahorro y crédito, que bien pueden considerarse Pymes en muchos casos, deben entregar información financiera y social de la entidad, con lo cual la incursión en la nube puede incluir un tratamiento político, jurídico y fiscal favorable para estas instituciones, al tener la información de manera confidencial, íntegra y a tiempo para los requerimientos de la Superintendencia.
	• Las estadísticas de la CAPEIPI (Cámara de Pequeños Industriales de Pichincha), en un estudio realizado en el 2010, señalan que un 23% de pequeñas empresas y un 27% de medianas empresas tienen problemas para acceder a tecnología de punta por la falta de incentivos fiscales, sin embargo el FONDEPYME (Fondo para el Desarrollo de las Pymes) ha otorgado créditos para 22000 emprendedores en 18 provincias, con lo cual se percibe un incentivo por parte del Estado para superar las brechas tecnológicas, y por ende, estos recursos se pueden usar en inversiones de aplicaciones que se puedan ejecutar en la nube.
	• La *Ley del Sistema Nacional de Registro de Datos Públicos*, publicada en el R.O. el 31 de marzo de 2010 busca mantener la protección de datos personales así como regular el sistema de registro de datos públicos y su acceso, en entidades públicas o privadas que administren dichas bases o registros, con lo cual las Pymes pudieran apoyarse en servicios en la nube para poder publicar de manera segura información que deba proveer a entidades del Estado.
Económico	• Aun cuando los precios de los computadores y servidores en general cada vez van disminuyendo (un buen servidor se puede encontrar en unos $2500 a $3000) las Pymes del Ecuador pueden tener una reducción de costos/ahorro en HW al no tener que cambiar de infraestructura si es que el negocio crece.
	• De acuerdo a Fundes (Fundación para el Desarrollo Sostenible) las Pymes en Latinoamérica generan el 88% de empleo en sus países frente al 10% de las grandes empresas, y en el Ecuador se ve como una gran oportunidad de negocio la incursión en cuanto al ahorro en tecnología, al utilizar servicios y/o infraestructura en la nube.
	• De acuerdo a algunos estudios en nuestro país la inversión en Tecnología dentro de las Pymes es baja, y aún se la considera un “gasto” más que una inversión, y consecuentemente la incursión en la nube, por un valor razonable es una opción a tomar en cuenta.
	• La legislación ecuatoriana exige que las compras públicas se las haga a través de un portal web (www.compraspublicas.gob.ec) lo cual abre un abanico de posibilidades para que las Pymes puedan ser parte de un proceso participativo en compras del Estado, y para ello la computación en la nube, a través de aplicaciones empresariales en línea, que permitan tener información actualizada.
	• El Instituto de Promoción de Exportaciones e Inversiones (Pro Ecuador), organiza con frecuencia charlas para Pymes para introducir a la tecnología como factor de crecimiento y diferenciador en la productividad de las mismas. En un estudio efectuado por HP y RGX (Sept. 2011) a 100 Pymes exportadoras ecuatorianas se descubrió que 1 de 4 empresas no usa herramientas ERP (*Enterprise Resource Planning*), y esto las desfavorece frente a la competencia, pero el argumento es que tienen un alto costo, con una implementación ERP en la nube estos costos se reducen drásticamente.
	• De acuerdo al mismo estudio solamente un 3% de Pymes exportadoras tiene un portal con ventas automatizadas, lo cual indica una oportunidad diferenciadora de competencia en el mercado el tener una plataforma en la nube a la que puedan acceder no solamente otros clientes sino otras empresas, y hacer negocios B2B (Business to Business).
	• Un negocio, dentro de las Pymes en Ecuador, que tiene aplicaciones en la nube posee una ventaja competitiva frente a la competencia, lamentablemente por lo pronto esto no es generalizado, y de hecho un 22% tiene un portal con posibilidad de hacer pedidos en

PEST	Factores
	línea, en tanto que otro 23% tiene solamente un sitio web meramente informativo.
	• Los ahorros en costos también se dan en cuanto al licenciamiento de productos, y en mantenimiento de aplicaciones para efectuar respaldos de información, por lo que las Pymes ecuatorianas no deberán invertir en ambos. La realidad indica que un 7% de ellas no realiza respaldos de datos ni aplicaciones.
	• Un estudio realizado en el 2010 por la Cámara de la Pequeña Industria de Quito (CAPEIPI) y la Pontificia Universidad Católica, revela que el 26% de pequeñas empresas ha realizado inversión tecnológica, frente al 23% de los medianos negocios. Con la incursión en la nube, la inversión en tecnología para la Pyme no debe ser abrumadora, sino que destinará recursos en su negocio.
Social	• Las Pymes ecuatorianas encontraron en Internet una oportunidad para publicitar sus productos y servicios. Las ventanas en la red para estas empresas son Facebook y Twitter.
	• Otra ventaja que presenta la computación en la nube para las Pymes ecuatorianas, y que la están usando es la colaboración a través de herramientas tales como Google Docs, en donde pueden editar documentos entre varias personas y mantener un versionamiento de los mismos, esto sin tomar en cuenta el uso de comunicación a través de Google Chat, que permite la intercomunicación en la misma empresa entre empleados de diferentes áreas.
	• Si bien las aplicaciones SaaS (software como servicio) son bastante intuitivas, las Pymes ecuatorianas no se han sumergido completamente en ellas, aunque la tendencia es irlo implementando poco a poco. Prueba de esto es que aplicaciones conocidas como MS Office, en su versión de computación en la nube (Office 365) están siendo evaluadas por Pymes ecuatorianas por su facilidad de uso, y conocimiento previo de la herramienta. Esto incluye no solamente la suite de ofimática, sino también correo electrónico, portales web y videoconferencias.
Tecnológico	• El mismo estudio de HP y RGX indica que tan solo un 9% de las Pymes encuestadas terceriza sus datos, el 46% tiene sus datos internamente y el 9% los tiene en un centro de datos alterno, con lo cual una implementación de planes de recuperación y desastres (DRP) puede resultar bastante costoso: por infraestructura, licenciamiento, personal técnico especializado, frente a reducción de costos de tenerlo en la nube.
	• En el Ecuador, la innovación tecnológica está cada vez más presente en las Pymes. Sin embargo la falta de información, capacitación para el personal e incentivos fiscales frenan su desarrollo, según un informe del Semanario de Economía y Negocios, LÍDERES (30/05/2011). Por lo anterior la computación en la nube presenta una oportunidad tecnológica importante por cuanto no se requiere de técnicos especialistas ni infraestructura especial para ofrecer los bienes y servicios de las Pymes.
	• Las Pymes ecuatorianas se pueden beneficiar – y muchas de ellas ya lo hacen – con tecnologías que no resultan onerosas pero sí útiles, tales como el uso de plataformas de telefonía virtual, videoconferencias o SMS, tal el caso de Skype o Google Voice, ambas son aplicaciones que residen en la nube, y que de PC a PC resultan gratis.
	• La gestión de relación con el cliente, conocido como CRM, por sus siglas en inglés, permite que se fidelice, retenga o encuentre clientes, y existen opciones gratuitas como SugarCRM, o de pago en la nube, como Salesforce.com, que las Pymes ecuatorianas no usan por falta de conocimiento.
	• Al igual que sucede con el CRM, existen sistemas de información gerencial, de tipo ERP (como se mencionó en el criterio económico) que permite que la Pyme ecuatoriana tenga un mejor manejo de sus recursos empresariales, y para ello no debe incurrir en altos costos, pues existen soluciones como OpenERP, de código abierto, que puede ser una opción, o también otras de tipo licenciada, como MS Dynamics, ambas pueden ser operadas desde la nube. En nuestro país son pocas las Pymes que sacan provecho de estas herramientas, por su costo y manejo, pero opciones en la nube pueden ser la solución.

PEST	Factores
	• Hoy por hoy las aplicaciones en la nube no se apalancan únicamente en los PCs de escritorio, sino – y sobre todo – en la computación móvil, que no involucra únicamente a las portátiles sino también a los teléfonos inteligentes (BlackBerry, iPhone, Samsung Galaxy, etc.) y tabletas (iPad, Samsung Galaxy, etc.) y las Pymes ecuatorianas están descubriendo en las aplicaciones móviles una gran oportunidad de mostrar información, particularmente para cerrar negocios, y aunque esto no se refleja en todas las Pymes poco a poco van apoyándose en estas aplicaciones.
	• Empresas como HP apoyan a las Pymes a través de servidores de bajo costo, tal como el modelo HP Proliant Microserver (PCWorld Ecuador, 2011), que en nuestro país hace uso de tecnología solamente un 30%, sin embargo la posibilidad de no comprar ni actualizar servidores en la nube es una ventaja que aún no es adoptada en su totalidad por las Pymes de nuestro país.
	• Existen aplicaciones dentro del modelo de la nube que les permite a las Pymes ecuatorianas guardar gran cantidad de información fuera de la empresa, y esto incluye a aplicaciones como MS Skydrive, Dropbox o Google Drive, con la consecuente facilidad de acceso desde cualquier dispositivo que tenga acceso a Internet. En el país esto va siendo una práctica común entre usuarios de Pymes aunque todavía no como política empresarial.
	• Un factor tecnológico importante para la adopción de la computación en la nube, ya sea usando un modelo privado, público o híbrido por parte de las Pymes es la seguridad de la información. Con frecuencia se tiene desconocimiento sobre los diversos mecanismos de seguridad, a través de algoritmos de encriptación de la información, pero las Pymes ecuatorianas deben ser conscientes de que los ataques que pueden sufrir en la nube son los mismos que existen en una infraestructura de TI tradicional, y lo que se debe proteger es identidades, infraestructura e información, lo cual está asociado al modelo de servicio (PCWorld Ecuador, 2012). A nivel mundial, y en particular en las pymes nacionales, todavía hay mucho por recorrer en este aspecto, y esto se lo hace a través de un SLA detallado, que proteja a las Pymes de cualquier brecha de seguridad.

Fuente: Recopilación del autor.

2.4 Recuperación ante desastres en la nube.

2.4.1 Ventajas y desventajas del uso de computación en la nube para una recuperación ante desastres

La computación en la nube, como se ha visto en capítulos anteriores, provee una serie de servicios que se pueden ajustar cómodamente a la realidad de cada empresa justificando su inversión en costos, ahorro de tiempo, disminución de la dependencia de personal de TI, mejora en el rendimiento de las aplicaciones, entre otros, sin embargo es hora de analizar cuál es la situación de este modelo de computación en cuanto a la recuperación ante desastres tecnológicos. A continuación se detallarán las ventajas y desventajas para este tipo de requerimiento.

Ventajas

1. Reduce la necesidad de comprar hardware caro, tal como unidades de respaldos, cintas y otros dispositivos de almacenamiento.
2. Ejecución de respaldos automáticos fuera de la empresa.
3. Capacidad de tener acceso a los datos poco tiempo después de un desastre.
4. Con un DRP apropiadamente estructurado, la empresa podría tener la capacidad adicional de tener el último respaldo restaurado (en minutos) al proveedor en la nube lo que permitiría que el servidor sea recreado (como un *servidor virtual*), y tener el servidor virtual funcional hasta que el servidor local sea remplazado.
5. No se requiere que tener una solución en la nube exclusivamente. El DRP puede ser una mezcla entre imágenes locales y respaldo fuera de la empresa.

Desventajas

1. Ante todo, las principales desventajas de la recuperación ante desastres usando la computación en la nube, están relacionadas con las mismas desventajas del uso de la computación de la nube per se, esto es:
    - *Seguridad*.- 1) No hay control sobre los datos de la empresa que están fuera de la misma, 2) ubicación física de HW y SW es desconocido, 3) se requiere de conectividad constante, 4) riesgo de pérdida de datos debido a respaldos inapropiados o fallas en el sistema virtualizado.
    - *Dependencia*.-Relacionado con pérdida de control: 1) Poca o ninguna penetración en los procedimientos de contingencias del CSP[16], 2) Migración a otro CSP no es fácil, 3) Recursos financieros atados a otra compañía, 4) Posibles problemas de calidad con el CSP

[16] CSP: Proveedor de Servicios en la Nube (*Cloud Service Provider*)

- *Costo*.-Relacionado con: 1) Costos ocultos (resolución de problemas relacionados con compatibilidad con regulaciones, respaldos, restauración y recuperación de desastres), 2) Riesgos de incrementos en costos en un futuro, 3) Estructura de costos no muy claro debido al uso flexible de servicios en la nube.
- *Flexibilidad*.-1) Personalización no siempre es posible
- *Conocimiento*.- 1) Se requiere de un conocimiento más profundo al implementar y administrar contratos momento de SLAs con el CSP, 2) Ya que todo el conocimiento sobre el trabajo en la nube recae sobre el CSP es difícil seguir el paso a la computación en la nube.
- *Integración*.-1) Es difícil lograr la integración con equipos hospedados en otros centros de datos, 2) La integración de periféricos, tales como impresoras locales y equipos de seguridad de TI, tales como sistemas de acceso, es difícil de lograr.

2. El proveedor de servicios en la nube podría retirarse del negocio o no tener la capacidad de operar según lo ofrecido (hay una variedad de razones para ello), y consecuentemente no poder un DRP funcional.
3. En caso de no contar con un apropiado ancho de banda y enlace de Internet cualquier esfuerzo por aplicar soluciones de recuperación ante desastres resulta en vano.
4. Las nubes privadas son un concepto relativamente nuevo en centros de datos empresariales. No hay estándares, y en la actualidad o un solo proveedor ofrece recursos limitados para habilitar una nube privada o hay demasiadas piezas de la solución que necesitan ser entrelazados. Incluso si una empresa se las arregla para construir una nube privada, la sincronización entre la nube privada y la nube pública no puede (aún) ser soportada. O podría ser apoyada por algunos vendedores en forma limitada.

5. Las distancias más grandes entre los centros de datos principales y los centros de datos cloud públicos introducen latencia para los usuarios durante la conmutación por error (fail-over). Las nubes públicas son vistas como inseguras y muchas empresas no quieren que sus datos sean expuestos a los proveedores de servicios externos. Una nube privada puede ser creada en un sitio de recuperación, pero es lo mismo que tener otro Centro de Datos de DR. Las tecnologías de almacenamiento utilizadas por la empresa y el proveedor de nube pública pueden tal vez ser incompatibles. Los ajustes de red o de propagación de DNS durante un failover necesitan ser tomados en cuenta.

2.4.2 Análisis comparativo entre DRP tradicionales y DRP con computación en la nube

En el capítulo 2.2.5.1 se pudo apreciar que los métodos tradicionales de recuperación ante desastres tecnológicos tenían una larga trayectoria en el mundo informático, sin embargo presentaban algunas falencias que se pueden compensar con la computación en la nube. A continuación se mostrará una comparación entre los métodos tradicionales y los de la computación en la nube:

1. **Protección casi continua de datos**.- Dentro de los DRPs tradicionales, en los respaldos de datos se tenían tiempos de recuperación de varias horas, e incluso de días, tomando en cuenta que los respaldos completos se hacen con cierta regularidad y los respaldos incrementales y diferenciales – si bien es cierto que ocupaban menos espacio – se los hace al menos una vez al día, y en ocasiones esto no era suficiente para recuperarse de un desastre tecnológico, en tanto que con la computación en la nube, y particularmente con la virtualización, existen mecanismos para determinar qué partes del disco duro han cambiado, para de ahí respaldar esa información, y que se lo puede

programar para que se lleve a cabo por minutos, lo cual posibilita una protección casi continua de los datos.

2. **Mejores RTO y RPO**.- Ligado al punto anterior tenemos que el objetivo de punto de recuperación (RPO) mejora considerablemente al tener una protección casi continua de datos, a través de soluciones de respaldo virtual, lo cual contrasta con los métodos tradicionales de recuperación. En el caso del objetivo de tiempo de recuperación (RTO), por ejemplo, en el caso de falla de hardware, esto se logra con una copia del respaldo del servidor virtual que se ejecuta inmediatamente sin necesidad de restauración.

3. **Facilidad de instalación y uso**.- En el caso de los DRPs tradicionales se contempla el uso de SW especializado para efectuar los respaldos de información de la empresa, y supone grandes desafíos para el administrador a cargo, pues un respaldo mal efectuado puede ser fatal en el momento necesario, sin tomar en cuenta los costos de los servidores de respaldos, el SW en sí, entre otros. En el caso de una solución virtualizada esto puede significar la aplicación de unos cuantos clics, y para esto la facilidad de uso es relevante, tomando en cuenta que se harán respaldos completos de todo el servidor con una restauración rápida en caso de ser necesario.

4. **Verificación y seguridad de los respaldos**.-Los métodos de respaldos tradicionales pueden “asegurar” que el respaldo se efectuó, pero no verificará su utilidad al momento de una restauración, y si bien algunos SW proveen de mecanismos de encriptación de la información – pues sería desastroso que los datos cayeran en las manos equivocadas – las empresas no deben olvidar que incluso por políticas internas o procedimientos regulatorios la seguridad de la

información debe ser mantenida a buen recaudo. En el caso de la computación en la nube la verificación de los respaldos se hace de manera automática, incluso en ambientes de prueba, todo esto con esquemas de encriptación tales como AES[17].

5. **Uso eficiente de almacenamiento**.- Características tales como compresión y deduplicación de se han usado por largo tiempo con soluciones tradicionales de respaldos. La compresión ha sido parte de las soluciones por más tiempo que la deduplicación, pero la deduplicación ha demostrado ser una adición estable a las soluciones de copia de seguridad. El espacio en disco puede ser barato, como regla general, pero las recientes alzas de precios de unidad de disco duro y el alto costo por gigabyte de almacenamiento SAN (Red de Área de Almacenamiento, por sus siglas en inglés) significa que el uso eficiente del espacio es crucial. Esto a menudo puede ser la justificación de costos lo suficiente para comprar una solución de compresión y/o deduplicación. Si se ahorra bastante espacio en el costo por gigabyte, a continuación, un modelo de costos se puede construir para justificar el gasto.

6. **Opciones de almacenamiento de respaldo flexible**.- Las copias de seguridad solían ser casi exclusivamente efectuadas en cinta. Luego los respaldos basados en disco llegaron con más velocidad y alta fiabilidad. La solución de copia de seguridad virtual tiene que ser aún más flexible. Las copias de seguridad basadas en la nube también deben ser consideradas como una opción para tener flexibilidad de almacenamiento. Inundaciones, incendios, robos, y una multitud de otros desastres naturales significa que las

[17] AES: *Advanced Encryption Standard*.- Consiste en uno de los algoritmos estándares más usados en criptografía, u ocultación de información.

copias de seguridad de servidor virtual se deben almacenar lejos de la infraestructura virtual. Históricamente, esto significaba tomar físicamente los discos o cintas fuera del sitio. Este enfoque es propenso a errores humanos y el riesgo de pérdida o robo de los medios de comunicación está siempre presente. La nube se ha convertido en una opción mucho más fiable y rentable para obtener copias de seguridad de servidores virtuales en un lugar seguro fuera del sitio.

Adicionalmente, algunos aspectos en los cuales un DRP en la nube es más conveniente que uno tradicional son (IBM Global Technology Services, 2012):

1. Gastos operativos mensuales más predecibles pueden ayudar a evitar los costos ocultos e inesperados de enfoques de hacerlo uno mismo, como sucede con esquemas tradicionales.
2. Reducidos requerimientos de gasto de capital por adelantado, debido a que la infraestructura de recuperación de desastres ya existe en la nube.
3. Los servicios administrados de capacidad de recuperación de negocios basados en la nube pueden ampliarse más fácilmente sobre la base de condiciones cambiantes.
4. El acceso al portal reduce la necesidad de viajar al sitio de recuperación lo cual puede ayudar a ahorrar tiempo y dinero.

2.4.3 Consideraciones para la implementación de un DRP en la nube

La computación en la nube podrá tener un sinnúmero de beneficios, sin embargo las Pymes todavía necesitan invertir en una solución en la nube para los respaldos y recuperación de datos, a menudo debido a consideraciones de seguridad,

asequibilidad, facilidad de uso y flexibilidad, tal y como se sintetiza en la **Ilustración 11**.

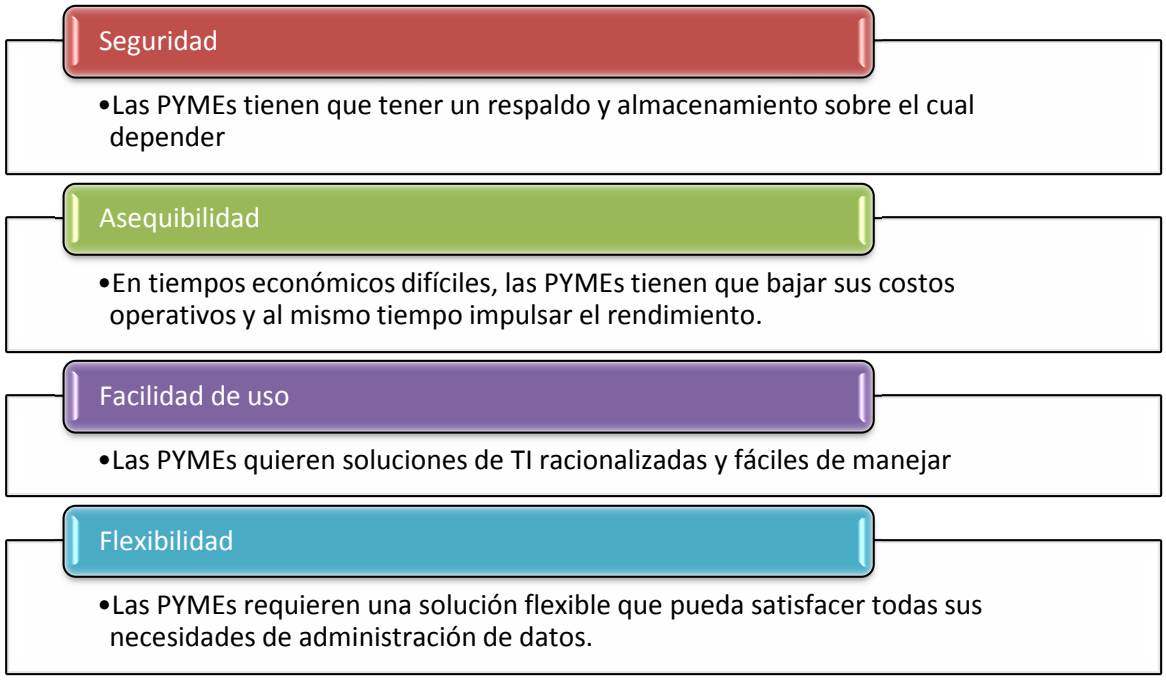


***Ilustración 11.*Consideraciones para la implementación de un DRP en la nube**

Fuente: Recopilación del autor
Elaborado por: Danilo Mannella L.

- **Seguridad**.- El tiempo de inactividad del sistema y la pérdida de datos puede paralizar a una PYME. Antes de invertir en una solución en la nube para copias de seguridad y recuperación de datos, muchos dueños de negocios quieren saber: ¿la nube es segura y confiable? ¿Cómo se aseguran los datos en las instalaciones de un proveedor de nube? ¿Cuánto tiempo se tarda en enviar y recibir datos a través de la WAN a la nube? Serán las empresas capaces de cumplir con sus ventanas de copia de seguridad?, ¿Hay una manera de combinar la protección local y la protección de la nube en una única solución?

- **Asequibilidad**.- La rentabilidad es una de las principales preocupaciones de las Pymes. Por esta razón, algunas organizaciones pequeñas se han mostrado

renuentes a invertir en una solución de nube privada para copia de seguridad y recuperación de datos, y muchas empresas están recurriendo a modelos SaaS - según una encuesta de Gartner, casi el 90 por ciento de las organizaciones esperan mantener o aumentar su uso de software como un servicio con el fin de ahorrar recursos financieros. Las soluciones SaaS para la copia de seguridad y recuperación de datos pueden ser muy rentables, ya que son fáciles y rápidas de implementar, reducen la necesidad de incrementar el personal de TI y el hardware, al tiempo que garantizan que los SLAs internos se cumplan y permitan a las empresas utilizar sus presupuestos de funcionamiento en lugar de gastos de capital para pagar solamente por el servicio que utilizan.

- **Facilidad de uso.-** En un esfuerzo por ahorrar recursos, las empresas de hoy buscan simplificar sus soluciones de TI. Muchas pequeñas empresas no tienen tiempo, recursos o el conocimiento para construir sus propias nubes privadas, y los que tienen equipos de TI desean alivianar sus cargas de trabajo en mantenimiento y gestión de TI – no añadirlos a los mismos. ¿Qué implica una solución en la nube para respaldo y recuperación?, ¿Realmente ahorra tiempo y recursos?

- **Flexibilidad.-** Cuando se trata de la gestión de datos, las Pymes están buscando una solución que sea lo suficientemente flexible como para satisfacer todas sus necesidades - desde una copia de seguridad y restauración rápida que pueda cumplir con sus ventanas de respaldos hasta la recuperación completa del sistema en caso de interrupciones no planificadas. Muchos propietarios de negocios se preguntan: ¿Necesitan la nube para la protección

de datos fuera de la empresa?, ¿Con el fin de almacenar viejos archivos?, ¿Para reducir los costos de almacenamiento in situ?, ¿O por los tres razones?

2.4.3.1 Recomendaciones de recuperación ante desastres en la nube para Pymes

La impresión general en la industria es que el tiempo de caída de los servicios en una empresa afecta únicamente a las grandes empresas y consiguientemente una recuperación rápida y la aplicación de un DRP es de algún modo un tema exclusivo de las grandes corporaciones, sin embargo esto no es verdad, pues si bien es cierto no considerar esto puede tener un alto impacto en términos económicos de manera absoluta el impacto relativo de una caída de los servicios en una PYME es exactamente igual que en las grandes empresas. A continuación, en la **Ilustración 12**, se muestran 5 recomendaciones que deberían adoptar las Pymes para estar prevenidos ante un desastre tecnológico:

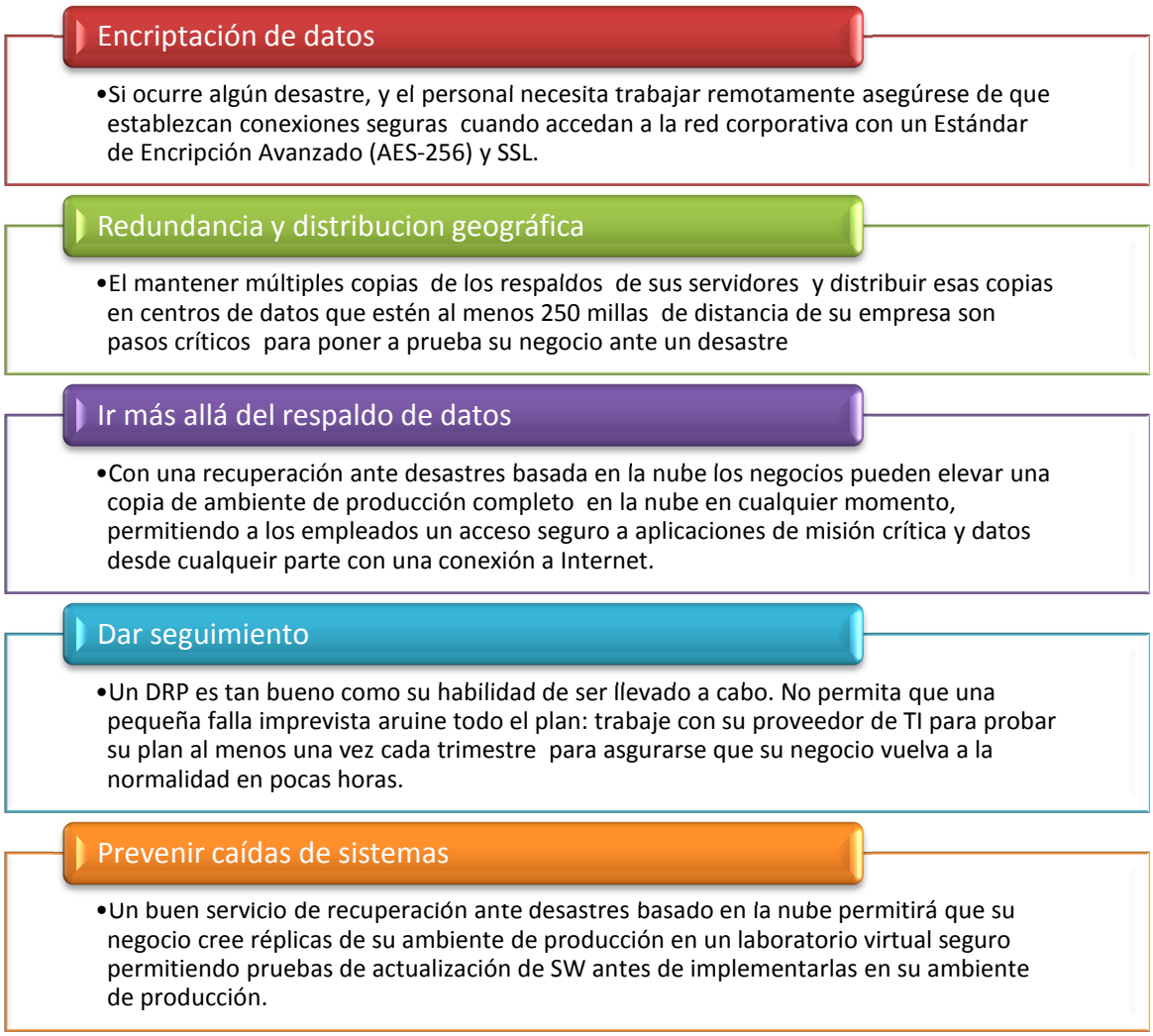


Ilustración 12. **Consejos a tomar en cuenta para recuperación ante desastres en la nube para Pymes**

Fuente: *5 Tips for your Small Business* (www.doyens.com)
Elaborado por: Danilo Mannella L.

2.4.3.2 Mejores prácticas para una recuperación de computación en la nube

La recuperación ante desastres mediante el uso de la computación en la nube ofrece los beneficios que aplican a los usuarios compartidos – esto es, una mayor eficiencia y a un costo más bajo – combinado con una velocidad de recuperación más rápida y una escalabilidad mejorada que va de la mano de la virtualización.

La experiencia en el uso de aplicaciones usadas para la recuperación ante desastres es fundamental para restaurar ambientes complejos sin incurrir en demoras

y tiempo de inactividad. Antes de escoger una solución de recuperación ante desastres en la nube, las Pymes deben analizar el valor de sus aplicaciones y el impacto que un tiempo de inactividad produciría en sus negocios, tal y como se mencionó anteriormente, y que va atado al BIA (Análisis de Impactos del Negocio). Una vez que se haya hecho este análisis, y se haya priorizado las aplicaciones que deberán ser tomadas en cuenta como parte de una recuperación ante desastres, considerando su nivel de criticidad, esto permitirá conocer el monto de inversiones que se usará y el tipo de solución de recuperación ante desastres.

De acuerdo a Sungard, empresa de reconocida trayectoria en la provisión de servicios de recuperación ante desastres, servicios de TI gestionados, servicios de consultoría sobre disponibilidad de la información, existen algunos consejos, o mejores prácticas para llevar a cabo la recuperación ante desastres usando la computación en la nube (Sungard, 2011):

1. **Determinar la implementación de nube apropiada**.- Las capacidades de la computación en la nube son amplias, y esto se debe a la variedad de modelos de negocios, que pueden ser públicos o privados, y administrados virtualmente de forma manual o completamente automatizados en la nube. Poder determinar la apropiada implementación de cómputo en la nube es una decisión de negocio que debe ser ampliamente considerada, basados en dos parámetros: seguridad y costo. La clave está en analizar la compensación entre ambos. A mayor seguridad mayor costo, en tanto que un mayor grado de automatización está ligado con frecuencia al uso de una infraestructura de computación pública.

   Se debe tener la suficiente flexibilidad para determinar, de entre una mezcla de opciones en la nube, la más idónea para cada negocio.

2. **Nunca poner en peligro la fiabilidad**.- Independientemente del tipo de implementación en la nube que se vaya a adoptar si hay algo que no debe quedar en entredicho es la confiabilidad de la solución de recuperación ante desastres en sí. Los siguientes elementos deben ser analizados cuidadosamente:
    - Datos coherentes
    - Suficiente capacidad
    - Personal disponible
    - Tiempo – para configuraciones, respaldos y pruebas
    - Experiencia en recuperación
    - Procedimientos que sean suficientemente probados para ser efectivos y mantenidos de forma actualizada conforme haya cambios

Para estar seguros de que los requerimientos antes citados se cumplan, las empresas deben contar con un proveedor de servicios externo, y más todavía cuando se recurre a la nube, al cual se le debe preguntar:

- ¿Quién posee los activos de cómputo?
- ¿Quién es el responsable de la recuperación?
- ¿Hay algún Seguro de Recuperación asociado con el servicio?

Debido a que el proveedor de servicios externo posee la experiencia y los recursos para llevar a cabo una recuperación completa se presume que las respuestas a las preguntas antes mencionadas recaen sobre el proveedor, y dado que la responsabilidad es asumida por éste, tanto los requerimientos de RTO/RPO se manifiestan en un SLA acorde.

3. **Clasificar en capas la recuperación ante desastres en la nube**.- El desarrollo de una estrategia de recuperación ante desastres basado en la nube requiere de un enfoque de capas en la disponibilidad de las aplicaciones. Lo primero es efectuar un BIA, luego priorizar y organizar las aplicaciones de acuerdo a su sensibilidad ante un tiempo de inactividad de las operaciones de la empresa. Cada capa está definida por el RTO/RPO de las aplicaciones en cuestión.

   Tecnologías modernas de movimiento de datos.- Tres categorías de tecnologías modernizan el movimiento de datos para apoyar mejor la amplia gama de requerimientos de recuperación de aplicaciones: replicación de servidor, replicación de almacenamiento y vaulting.

   Selección de un proveedor de servicios.- Cada una de las categorías anteriores puede ser utilizada en la nube, pero lo más crucial que deben pensar las empresas es en ¿Qué criterios deberían ser usados para seleccionar al proveedor de servicios? Si bien los bajos costos y la escalabilidad son beneficios importantes en la nube, para el caso de aplicaciones críticas lo que tiene más peso es la seguridad y la confiabilidad. Los servicios de recuperación administrados completamente en la nube deben estar respaldados por SLAs que garanticen contractualmente niveles de servicio de RPO/RTO.

   Finalmente, una amplia gama de opciones de infraestructura elimina el gasto adicional.

4. **Recuperación ante desastres en la nube completamente gestionada: Un modelo**.- El siguiente modelo ayuda a asegurar que los requerimientos de

seguridad, confiabilidad y efectividad en costos se cumplan, para una solución completamente gestionada.

Seleccionar la tecnología.- Con la recuperación basada en la nube, una vez que el BIA se completa y los niveles se definen, las aplicaciones datos pueden protegerse en una nube compartida y segura, utilizando la tecnología de movimiento de datos más adecuada.

Para las aplicaciones más críticas, las soluciones de replicación de servidor o almacenamiento son seleccionadas por su capacidad de entregar la recuperación en menos de cuatro horas a un punto de recuperación cercano a cero.

El SW del servidor de replicación encapsula los sistemas operativos, configuraciones de aplicaciones y aplicaciones de datos, y se replican tan pronto como los cambios se escriben en el disco.

Las aplicaciones que son menos sensibles al tiempo de inactividad, pero no menos críticas para el negocio, son encriptadas y almacenadas en un lugar seguro fuera del negocio utilizando la tecnología de vaulting para copia de seguridad en línea y recuperación. Los datos del vaulting se pueden restaurar a la última copia de seguridad en menos de 24 horas.

Entrega de la responsabilidad de la recuperación.- Con una solución completamente gestionada, el proveedor de servicios es responsable de la gestión y el mantenimiento del ciclo de vida de una recuperación total, con un monitoreo 24/7/365.

Para las pruebas, el proveedor de servicios ofrece guiones de recuperación personalizados a su medio ambiente, y la verificación de

suministros para el usuario final, como parte del ejercicio. Cuando el personal del proveedor de servicios hace el trabajo pesado necesario para las pruebas de recuperación, se alivia la carga sobre el personal de TI y puede eliminar los viajes y los gastos que normalmente se asocian con una prueba.

En el caso de una interrupción de corte de energía, desastre, o de otro tipo, el proveedor del servicio recuperará aplicaciones y datos en máquinas virtuales - y promoverá las máquinas virtuales como sistemas activos.

Automatizar tantos pasos en el proceso como sea posible acelera la recuperación y evita los errores y las dependencias humanas. Las tecnologías de replicación proporcionan máquinas virtuales listas para operar, y datos estando listos en el sitio de recuperación, mientras se lleva a cabo la restauración y reconstrucción de las máquinas virtuales a partir de los datos usados en el vaulting.

El proveedor de servicios coordina la recuperación en conjunción con otras aplicaciones en los sistemas físicos y equipos mainframe, y reconecta a los usuarios de negocio con las aplicaciones los datos recuperados. Cuando el incidente ha pasado, el entorno de producción retorna a la normalidad.

La **Ilustración 13** resume lo que se debería buscar en una solución de recuperación ante desastres en la nube:

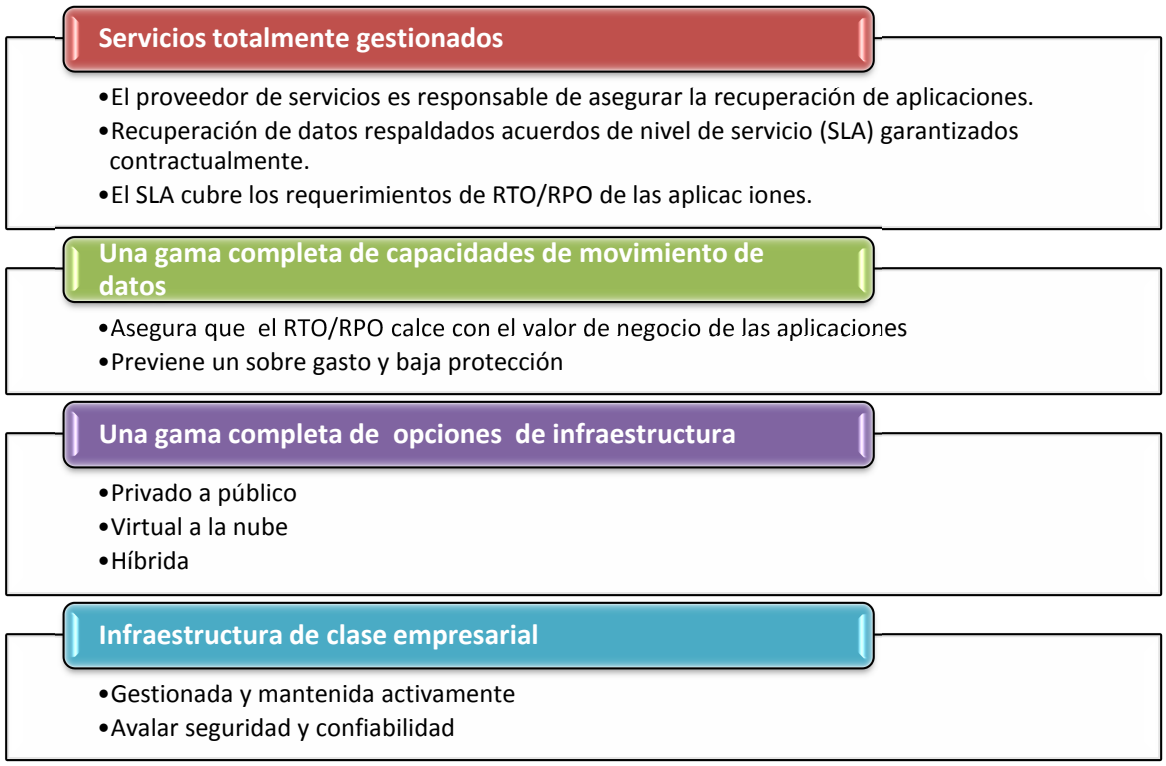


Ilustración 13. **Cuadro sinóptico de lo que se debe buscar en una solución de recuperación basada en la nube.**

Fuente: Whitepaper. Best practices for Cloud-based recovery. Sungard (2011).
Elaborado por: Danilo Mannella.

2.4.3.3 Opciones de recuperación ante desastres para Pymes

En general, para combatir los desastres tecnológicos las grandes empresas tienen como aliado planes de recuperación ante desastres (DRP) complejos y completos, en donde sus soluciones abarcan la creación de sitios secundarios en ubicaciones remotas en caso de que algún evento irrumpa sus actividades en su centro de datos principal, así mismo sus datos son replicados en caso de falla de hardware y poseen respaldos de información en cintas u otros medios fuera de sus empresas, pero la situación de las Pymes es distinta.

Si bien el estudio efectuado por Symantec indica que las Pymes no están preparadas para enfrentar un desastre tecnológico, y que las Pymes no sacan provecho de la tecnología, el principal argumento es que los costos son prohibitivos

para incursionar en un DRP que prácticamente los endeude enormemente, sin embargo existen opciones asequibles para enfrentar los desastres tecnológicos de forma tal que la información esté protegida oportunamente.

1. **Almacenamiento (o Hosting)**.- Una de las principales aplicaciones que pueden usar las Pymes son aquellas enmarcadas en SaaS (software como servicio), ya que, al ser servicios hospedados por un proveedor y accedidos a través de la Web, un buen plan de respaldos está siempre incluido en sus paquetes. En pocas palabras, los proveedores de servicios en la nube suministran una mayor protección de lo que regularmente se tiene al interior de las Pymes. En el caso de sitio web e infraestructura crítica las Pymes pueden rentar servidores y HW de almacenamiento en los centros de datos de alguien más.

2. **Respaldos en línea**.- Las Pymes siempre han batallado con los respaldos de datos. Son muchas las historias en las cuales el encargado se olvidó de sacar el respaldo, las cintas desaparecen o simplemente al momento de usarlas no sirven. Para esto las soluciones de respaldos en línea son más eficientes y útiles que los esquemas regulares de respaldos. Existen proveedores que tienen servidores que pueden sacar respaldos diarios delos servidores de la empresa, o incluso de PCs específicos. Los costos dependen de la cantidad de información a respaldar y el nivel de servicio deseado, de este modo estos costos varían entre $3.00 y $5.00 como tarifa mensual, más un adicional de $0.50/GB por equipo de escritorio, o hasta $7.00 más un adicional de $0.50/GB por servidor.

3. **Protección fuera de la empresa sin costo**.- Una solución que puede ser conveniente, y que la están llevando a cabo algunas Pymes sugiere que se asocien entre empresas con similares características de TI y provean un servicio de respaldo a la otra empresa. Esta solución puede ser tan sencilla como enviar al otro lado DVDs con datos críticos hasta la transferencia electrónica de datos en caso de un desastre tecnológico. El un sitio funciona como sitio alterno del otro.

4. **Mantener una copia extra dentro de la empresa**.- Otra opción barata para las Pymes es comprar un NAS[18] para almacenar copias de los datos dentro de la misma empresa. En general tienen un costo alrededor de $1000, y suelen venir con seguridad incorporada, protección de datos, y pueden ser manejados incluso por personas con poca experiencia en TI.

5. **Más allá de la tecnología**.- Finalmente, tanto grandes empresas como Pymes deben recordar que un DRP involucra algo más que tecnología, si bien es importante tener copias de respaldos, dentro o fuera de la empresa, de nada sirve si no existe un plan de comunicación que permita a los empleados, clientes y proveedores saber cuál es el plan de acción que lleva a cabo la empresa en casos de desastres tecnológicos. No hay que olvidar que un plan de recuperación de desastres no es un asunto de tecnología, es un asunto de negocios.

[18] NAS: *Network Attached Storage*, dispositivo para almacenamiento masivo de datos conectado a la red de datos.

2.4.4 Casos de éxito

Dentro de los servicios de computación en la nube, como se ha mencionado en capítulos anteriores, está la recuperación ante desastres tecnológicos, y para ello se ha revisado las empresas que proveen de estos servicios, los requerimientos para que las empresas de cualquier tamaño en general, y las Pymes en particular, puedan incursionar en el uso de estos servicios, ahora es momento de conocer la experiencia de algunas Pymes alrededor del mundo, que han hecho uso de estos servicios.

Cuadro 17. Ejemplos de Pymes que usan recuperación ante desastres en la nube

Proveedor	Empresa	Situación	Solución	Resultados
Mozy (www.mozy.com)	**United Way of the National Capital Area** UWNCA es el mayor proveedor de fondos de servicios de la salud humana dentro de las ONGs en el área metropolitana de Washington, y ha reunido a personas y recursos para mejorar la vida de personas por más de 30 años. www.unitedwaynca.org	La desventaja principal con su solución de copia de seguridad previa, ubicada fuera de las instalaciones de la empresa, fue que no era accesible por parte de la empresa. No tenían derechos administrativos en sus copias de seguridad, y tuvieron que ponerse en contacto con el proveedor para cualquier cosa a excepción de una simple restauración del cliente. Con el tiempo, su proveedor anterior de copia de seguridad decidió que no quería ofrecer más el servicio.	Uso de MozyPro	La UWNCA usa Mozy como una solución de recuperación de desastres, ya que tiene sentido tener algo fuera de sitio que está muy lejos de la oficina. En comparación con la solución usada anteriormente, MozyPro les ahorra cerca de $900 por mes, mientras les aumenta el control administrativo del servicio. Eso es un 75% de ahorro sobre su solución anterior, que costaba $1200 por mes para copias de seguridad de todos sus seis servidores. Además, ahora MozyPro ofrece a UWNCA el beneficio añadido de una solución automatizada, con acceso administrativo a-demanda.
Carbonite (www.carbonite.com)	**Foundation Real Estate Advisors** www.foundationrea.com La Foundation Real Estate Advisors (FRSA) representa exclusivamente a inquilinos y ocupantes de bienes raíces comerciales. La FRSA trabaja con los clientes para manejar bajos costos de	"Antes, sólo salíamos del paso de las copia de seguridad", dice Jeff Lerch, CEO. "Básicamente, teníamos que cruzar los dedos para que nada saliera mal. Eso no es realmente una gran manera de ejecutar tu negocio. " Como presidente de Foundation Real Estate Advisors Irvine, California, Lerch comenzó a	Uso de Carbonite	Confianza y tranquilidad en las características provistas por Carbonite: 1. Fácil instalación y uso 2. copia de seguridad automática 3. Copia de seguridad de varios equipos al mismo tiempo 4. Posibilidad de añadir más equipos ya que la empresa crece

Proveedor	Empresa	Situación	Solución	Resultados
	ocupación en menos tiempo. Los clientes de FRSA en general, logran una reducción del 20-25% en sus costos inmobiliarios, lo que equivale a decenas de miles de dólares al año. Su diferenciador es su experiencia colectiva en los ámbitos de la gestión de bienes raíces, inversión, propiedad, corretaje, y las operaciones.	preocuparse por la forma en que los datos de su compañía se estaban guardando. Debido a que la empresa utilizó dentro de la empresa discos duros externos, sentía que no eran más que un desastre natural y que tarde o temprano lo perderían todo. "Nadie se lleva las unidades externas a su casa en la noche", dice. "En esencia, nuestra estrategia de copia de seguridad sería inútil si algo le sucediera a nuestra oficina o nuestro equipo."		5. La confianza en la fiabilidad de copia de seguridad
VMWare (www.vmware.com)	**Myron Steves** (www.myronsteves.com) La aseguradora Myron Steves posee 200 empleados, y es una aseguradora mayorista que atiende a otras 3000 agencias en Houston, Texas, en EE.UU.	Myron Steves necesitaba remplazar su costoso y poco fiable servicio de outsourcing de recuperación de desastres con algo que pudiera confiar en el caso de un corte de servicios de su centro de datos.	La aseguradora virtualizó su infraestructura de servidores a VMware vSphere™, e implementó VMware vCenter™ Site Recovery Manager para responder a fallas sobre sus sistemas de producción en una ubicación de copia de seguridad. Un entorno de escritorio virtual VMware View ™ asegura que los empleados también puedan trabajar, incluso si son evacuados o no pueden trabajar desde las oficinas de la empresa.	1. El negocio puede recaer sus servicios a servidores en cuestión de horas, en lugar de días. 2. El servidor sobre el cual recae el servicio ahora es confiable. 3. El servicio de terceros de recuperación de desastres que costaba $400.000 por año, fue eliminado. 4. Se evitó la expansión futura de servidores, ahorrando $200.000 en costos de nómina y $150.000 en costos de mantenimiento anuales.

Proveedor	Empresa	Situación	Solución	Resultados
Egnyte **(www.egnyte.com)**	**Houston Christian High School** (www.houstonchristian.org) Houston Christian High School es una escuela secundaria privada con la misión de preparar a los estudiantes para la universidad. Con un evidente énfasis en lo académico, los profesores animan a los estudiantes para estar al día con las cambiantes tecnologías y ser líderes innovadores en sus comunidades.	Los huracanes amenazan regularmente a la zona de Houston, y los profesores y el personal necesitaban saber que sus documentos respaldados y de fácil acceso en caso de un desastre. Los servidores de archivos físicos requerían que los maestros y el personal respaldaran sus archivos cada vez que iniciaban sesión en sus equipos. La mayoría omitía el proceso de respaldos por completo. Michelle Vaughn, Director de TI del Colegio, no podía exigir el cumplimiento de la política de copia de seguridad, de modo que decidió buscar una solución que maximice la productividad de los miembros del personal y asegurar que los archivos se respaldaran de forma consistente.	El Colegio instaló Personal Local Cloud en los MacBooks de todo el personal y los maestros. Local Cloud proporciona a los maestros un acceso rápido y local a todos sus archivos, manteniendo al mismo tiempo respaldos de datos de forma rápida y eficiente. Los maestros y miembros del personal pueden estar seguros de que no sólo sus archivos están continuamente siendo respaldados en la nube, en el caso de un huracán podrían continuar trabajando de forma remota sin interrumpir su flujo de trabajo.	La utilización de una nube híbrida proporcionó los siguientes resultados: • Seguridad en los respaldos de la información de los servidores del Colegio a los servidores del proveedor. • Oportunidad de que los usuarios pudieran tener la información también fuera de línea • Accesibilidad de la información desde dentro o fuera de la institución.

Fuente: Recopilación del autor
Elaborado por: Danilo Mannella L.

2.5 Síntesis del Capítulo II

En este segundo capítulo se ha revisado los fundamentos teóricos acerca de lo que son las Pymes a nivel nacional y mundial, y de su importancia en la economía de los países. De igual modo se profundizó en el conocimiento de los métodos tradicionales de recuperación ante desastres y la importancia de tener un DRP. A continuación se estudió a la computación en la nube, sus características, componentes, modelos de servicios, proveedores y algunos casos de éxito a nivel mundial y nacional. Finalmente se hizo un análisis sobre el uso de la computación en la nube como mecanismo de recuperación ante desastres tecnológicos.

En el siguiente capítulo se efectuará un diagnóstico de la situación actual de las Pymes de Servicios en la ciudad de Quito, con lo cual se podrá conocer, a través de una metodología, métodos, técnicas e instrumentos de investigación seleccionados el nivel de conocimiento sobre recuperación ante desastres tecnológicos así como el uso de la computación en la nube para proteger a las Pymes de pérdidas de información.

3 Capítulo III: Diagnóstico de la situación de las Pymes de Servicios en el uso de planes de recuperación ante desastres tecnológicos en el DMQ

3.1 Levantamiento de Información

3.1.1 Metodología de la investigación

Se conoce que la investigación es un proceso:

- **Sistemático.-** Se obtiene información a partir de un plan prestablecido que, una vez asimilada y examinada, modificará o añadirá conocimientos a los ya existentes,
- **Organizado.-** Es necesario especificar los detalles vinculados al estudio, y
- **Objetivo.-** Sus conclusiones no se amparan en un parecer subjetivo, sino en episodios que previamente han sido observados y evaluados)

En el caso de una investigación científica se debe identificar si se trata de una investigación pura o aplicada. La presente investigación es de tipo aplicada.

De acuerdo al nivel de conocimientos (exploratorio, descriptivo o explicativo) esta investigación, en esta fase de diagnóstico, es de tipo:

- Exploratorio.- Ya que se trata de tener una visión general aproximada de la realidad de las Pymes de Quito en cuanto a su conocimiento y uso de DRPs a través de mecanismos de computación en la nube, partiendo de la premisa mencionada en capítulos anteriores, de que se tiene un nivel superficial de conocimiento sobre este tema.
- Descriptivo.- Debido a que la preocupación primordial de este diagnóstico radica en describir características fundamentales de los grupos homogéneos a ser evaluados, como lo son las Pymes de Servicios en Quito, en cuanto al tema

de estudio, de uso de DRPs y a la computación en la nube como el vehículo para llevar a cabo esto. Dado que la descripción hace uso de la fundamentación teórica y para ello es necesario medir los resultados esta investigación se apoyará en las diferentes técnicas que se indicarán más adelante.

- Explicativo.- Por cuanto buscará conocer las causas que determinan las razones por las cuales en las Pymes de Quito no se tiene planes de recuperación ante desastres, y peor aún a través de modelos de computación en la nube, y qué efecto tiene esto en la estabilidad del negocio.

3.1.2 Procedimiento para realizar la investigación

3.1.2.1 Investigación de fuentes primarias

Para esta etapa de diagnóstico de la investigación se debe tomar en cuenta que la primera etapa, que consistió en obtener las bases de la fundamentación teórica, fue importante porque a través de los métodos (Analítico-Sintético, Inductivo-Deductivo y Sistémico) y técnicas usados (recopilación de información e Internet) se pudo tener los criterios para esta siguiente fase.

Esta siguiente fase se caracteriza por los siguientes pasos:

1. **Uso de métodos de investigación**.- A través del método conocido como criterio de expertos, aplicado a las Pymes de Servicios del DMQ, se llevará a cabo el diagnóstico de la situación de las Pymes en el uso de DRPs usando a la computación en la nube como el mecanismo adecuado para ello.

2. **Técnicas e instrumentos para la obtención de datos**.- Esta parte tiene relación con las técnicas e instrumentos que se aplicará en el estudio. La técnica más idónea en esta fase es la entrevista, aplicadas a los gerentes y/o encargados de tecnología de las Pymes que serán parte del estudio, en tanto que el instrumento usado será el cuestionario, que apoyará la técnica antes citada. Aquí se incluirán los objetivos que se pretende cumplir, y que están relacionados con las preguntas de investigación.

3. **Recopilación de información**.- En esta etapa se efectúa la aplicación de la técnica e instrumento detallados en el punto anterior.

4. **Análisis e interpretación de resultados**.- Aquí se presentan los resultados luego de la aplicación de los instrumentos de investigación y el análisis correspondiente, y que facilitará la emisión de conclusiones en esta fase.
5. **Hallazgos**.- En esta parte final se emitirán las conclusiones a las que se llegó luego de aplicar el método y técnica antes descritos, y que permitirán responder las preguntas de investigación de este estudio, luego de lo cual se procederá a la elaboración de la propuesta que podrá ayudar a las Pymes a que puedan recurrir a la computación en la nube como mecanismo idóneo para la recuperación ante desastres tecnológicos.

3.1.2.2 Investigación de fuentes secundarias

Este trabajo de investigación se nutre en esta fase de diagnóstico de fuentes primarias, sin embargo es importante recalcar que, para afianzar el estudio, es de vital importancia recurrir también a fuentes secundarias que permitan corroborar los datos obtenidos respecto de la realidad de las Pymes en cuanto al uso de tecnologías de la información, y particularmente respecto del personal que se usa en este tipo de

negocios, el presupuesto destinado para TI, y su realidad frente a los esquemas de respaldo de información frente a una contingencia en el evento de un desastre tecnológico.

El uso de fuentes secundarias se utilizó en los primeros dos capítulos, y ahora permitirá obtener información que aporte en el conocimiento de la realidad a través de la información recolectada por terceras personas, y que apoyarán los datos obtenidos de la fuente primaria, de manera que no se tenga que “reinventar la rueda”, siendo una importante fuente de enriquecimiento para la demostración de las hipótesis planteadas.

Este estudio tomará, como fuente de información secundaria datos estadísticos de los censos poblacional y económico, estudios de mercado recientes en el ámbito de las TICs así como de tesis de estudios relacionados con el tema de investigación.

3.1.2.3 Uso de Métodos de investigación

En esta etapa de diagnóstico es importante definir los métodos de investigación que se usarán para esta tesis. El método escogido en esta fase es de Criterio de Expertos juntamente con el Método de Pareto.

El Criterio de Expertos puede definirse como un método en el cual un grupo de especialistas independientes y reputados, en al menos uno de los campos concernidos por el tema de estudio que se va a evaluar, emite un juicio colectivo y consensuado sobre dicho estudio. Según se les solicite, el juicio emitido puede hacer referencia a la puesta en práctica o a los efectos del conjunto de una parte del estudio.

Para determinar al grupo de expertos hay que considerar un aspecto fundamental, cual es la experiencia profesional en el campo de estudio, y esto es un requisito indispensable; el experto debe estar muy cualificado en el área objeto de evaluación, y ser reconocido y respetado por sus pares.

El Método de Pareto de manera general dice que el 80% de los efectos es ocasionado por el 20% de las causas, es decir, se trata de un método que ayuda a definir las causas más importantes de un problema particular y luego de lo cual se decide las prioridades sobre las acciones a seguir.

La utilización del Método de Pareto contribuirá con el método de Criterio de Expertos en cuanto a que se expondrán las causas prioritarias en los problemas que presentan las Pymes al momento de implementar un DRP en general, y en la nube en particular, y el uso de estos métodos contribuirán en el análisis de la hipótesis planteada en esta investigación.

3.1.2.4 Técnicas e instrumentos para la obtención de datos

Las técnicas que se usarán con el método de investigación seleccionado son: la observación directa y la entrevista.

La observación es un instrumento utilizado con mucha frecuencia en cualquier tipo de investigación. Esta técnica es así mismo adecuada para una posterior interpretación y análisis de los resultados, lo cual se complementa con la entrevista.

La entrevista es una técnica de recopilación de información mediante una conversación profesional con ciertos actores escogidos con antelación, y cuyo objetivo es el de adquirir información acerca de las variables de estudio, con lo cual se elaborará un cuestionario adecuado con preguntas que tengan un determinado fin y que son imprescindibles para esclarecer la tarea de investigación, así como las preguntas de apoyo que ayudan a desenvolver la entrevista.

Como se indicó en el párrafo anterior el instrumento que se utilizará será el cuestionario, en el cual se formulará una serie de preguntas que permitirán medir una o más variables. El cuestionario posibilitará observar los hechos a través de la

valoración que hace de los mismos el entrevistado, limitándose la investigación a las valoraciones subjetivas de éste.

Dado que se desea abarcar de una manera muy amplia las apreciaciones de los entrevistados, el cuestionario contará con preguntas abiertas, en donde se alcanzará a obtener una opinión del tema de estudio.

Formulación del cuestionario

Las preguntas formuladas en este cuestionario fueron de carácter evaluativo descriptivo, y destinadas a obtener información sobre el uso de planes de recuperación ante desastres mediante el uso de la computación en la nube en Pymes de servicios del DMQ.

El cuestionario está compuesto por preguntas de tipo abierto, lo que proporcionó un análisis cualitativo en la investigación.

Las preguntas fueron realizadas de forma tal que se pudiera conocer, a través de los expertos seleccionados, el conocimiento que han tenido en sus negocios respecto de la manera como manejan la seguridad de la información, lo que incluye el presupuesto que asignan al área de TI para llevar a cabo planes de recuperación ante desastres, y conocer las consecuencias que tiene para sus *stakeholders* la interrupción de servicios en el evento de un desastre tecnológico. Finalmente se busca entender su conocimiento acerca de empresas que pudieran proveerles de servicios para recuperación ante desastres, en particular usando a la computación en la nube para ello.

Cuadro 18. Ficha de entrevista para expertos de Pymes

FICHA DE ENTREVISTA	
Nombre del Entrevistado:	
Cargo:	
Empresa:	
Cantidad de empleados o facturación anual:	
Fecha:	
Descripción de la entrevista	
1. ¿Cuál es la experiencia que tiene respecto del manejo de seguridad de la información de su empresa?	
2. Para el manejo de TI (Tecnología de la Información) en su negocio, ¿cuenta con personal propio o tercerizado?	
3. ¿Qué porcentaje de su presupuesto lo asigna a seguridad de la información al área de TI?	
4. En caso de que sucediera un desastre tecnológico en su empresa (*corte de electricidad, daño en el servidor, sabotaje por parte de exempleados, etc.*), ¿en qué tiempo y a qué costo recupera la información?	
5. ¿Cuáles serían las consecuencias en su negocio para los *stakeholders* (empleados, proveedores, accionistas, etc.) en caso de producirse un desastre tecnológico?	
6. Sabiendo que, de manera general, la computación en la nube se refiere a servicios que están en algún lado en Internet, ¿Está incursionando su empresa en algún proyecto de computación en la nube (*o cloud computing*)?	
7. ¿Conoce usted sobre alguna empresa que le pueda proveer de servicios de recuperación ante desastres tecnológicos en la nube? De ser afirmativa la respuesta indicar el nombre de la empresa y su experiencia con la misma.	
8. ¿Estaría dispuesto a contratar a una empresa externa para que se hiciera cargo de su plan de recuperación ante desastres (DRP), lo que incluiría el uso de computación en la nube?	

Fuente: Elaboración del autor.

Esta toma de datos será de importancia porque a partir de la información recolectada se dará inicio al estudio de investigación, y permitirá definir, a partir de los resultados encontrados la guía que les permitirá profundizar mejor en este tema y

acceder, a través de un proceso ordenado, a un DRP mediante un proveedor de servicios en la nube.

3.1.2.5 Recopilación de información

A través del uso del método de criterio de expertos, y de la aplicación de la entrevista mediante el cuestionario mencionado en el capítulo anterior se procedió a conocer la opinión de los expertos.

En el **Anexo 1** se puede revisar la carta de invitación enviada a los expertos para que colaboren con el estudio, en tanto que en el **Anexo 2** se muestra el detalle de cada una de las entrevistas, y a continuación se procederá a efectuar el análisis e interpretación de los resultados.

3.1.2.6 Análisis e interpretación de resultados

Para efectuar el análisis e interpretación de resultados se usará el Diagrama de espina de pescado, llamado también **Diagrama de Ishikawa**, que permite analizar un problema el cual puede provenir de diversos ámbitos, esto es lo que se conoce como un análisis causa-efecto.

Esta técnica gráfica es útil porque permite:

- Visualizar, en equipo, las causas principales y secundarias de un problema.
- Ampliar la visión de las posibles causas de un problema, enriqueciendo su análisis y la identificación de soluciones.
- Analizar procesos en búsqueda de mejoras.
- Modificar procedimientos, métodos, costumbres, actitudes o hábitos, con soluciones - muchas veces - sencillas y baratas.

- Educar sobre la comprensión de un problema.
- Ofrecer una guía objetiva para la discusión y la motiva.
- Mostrar el nivel de conocimientos técnicos que existe en la empresa sobre un determinado problema.
- Prever los problemas y ayuda a controlarlos, no sólo al final, sino durante cada etapa del proceso.

A continuación se analiza las preguntas efectuadas a los expertos, a través de esta técnica:

1. **¿Cuál es la experiencia que tiene respecto del manejo de seguridad de la información de su empresa?**

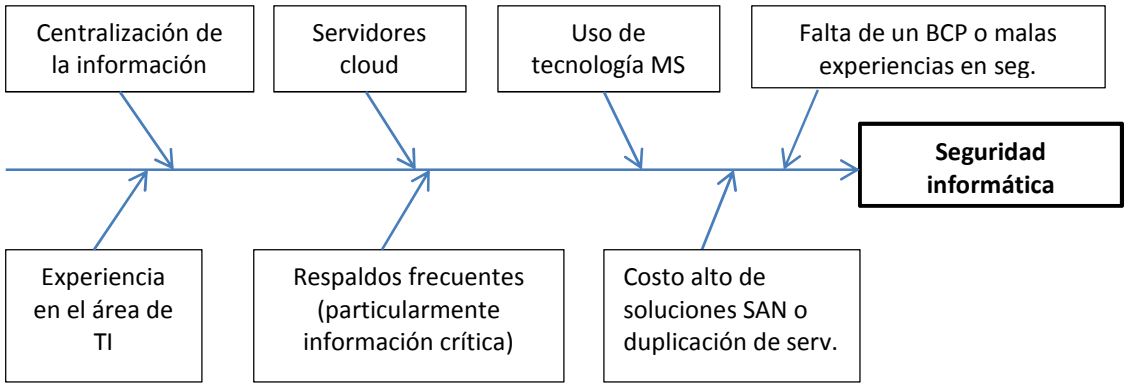


***Ilustración 14*. Diagrama de Ishikawa – Pregunta 1**

Fuente: Elaboración del autor

Conclusiones:

- La mayoría de Pymes cuenta con soluciones de respaldo tradicional como respaldos frecuentes en medios magnéticos al interior de la empresa, ya sea en discos externos, servidores duplicados u otros mecanismos.

- Se requiere de personal con experiencia para el manejo de los respaldos de la información, y de esta manera evitar pérdida de información crítica.
- Hay un consenso bastante generalizado en cuanto a la falta de implementación de un BCP (plan de continuidad del negocio) aunque se utilizan procesos de seguridad informática básicos para minimizar el impacto de una posible pérdida de información.
- Existen muchas Pymes que se afianzan en tecnología de proveedores reconocidos para minimizar el impacto de pérdidas de información debidas a malware (virus, troyanos, gusanos, spyware, etc.)
- Un porcentaje reducido de empresas está delegando la seguridad de su información en empresas con servidores en la nube.
- De acuerdo al método de Pareto se encuentra que unas pocas Pymes presentan malas experiencias de seguridad informática o que su costo de inversión es alto.

2. Para el manejo de TI (Tecnología de la Información) en su negocio, ¿cuenta con personal propio o tercerizado?

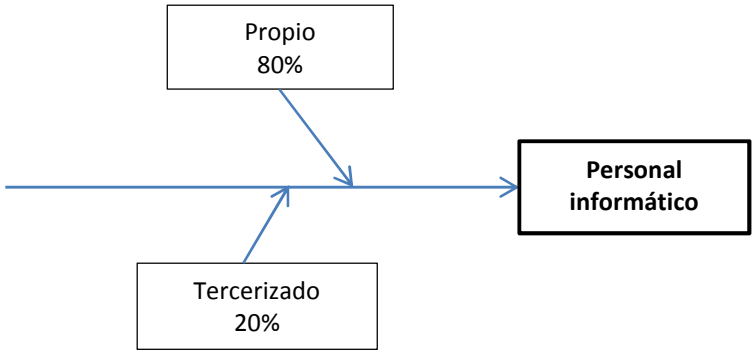


Ilustración 15. **Diagrama de Ishikawa – Pregunta 2**

Fuente: Elaboración del autor

Conclusiones:

- Un gran porcentaje de Pymes cuenta con al menos una persona para el área de tecnología.
- Usando el método de Pareto se concluye que tan solo un pequeño porcentaje se encarga de contratar los servicios de una empresa externa para el manejo de TI.

3. ¿Qué porcentaje de su presupuesto lo asigna a seguridad de la información al área de TI?

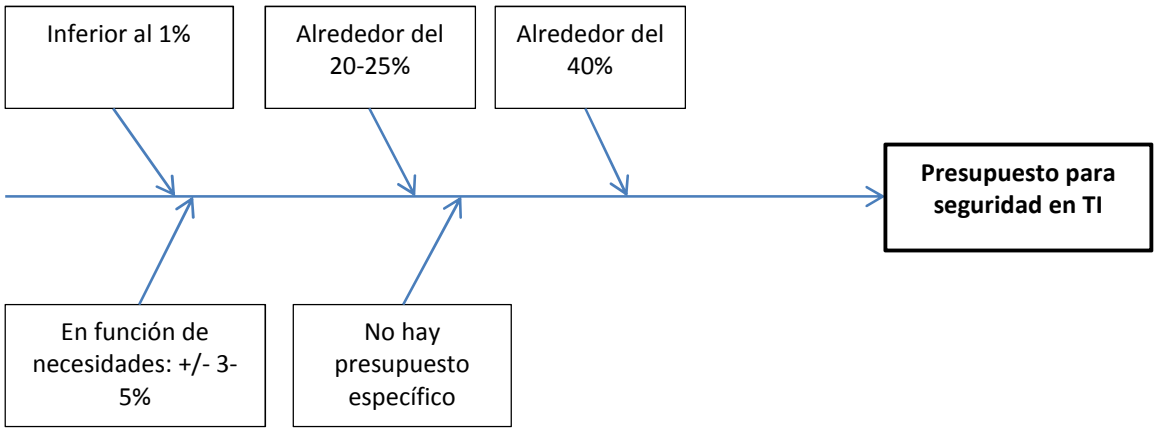


Ilustración 16. **Diagrama de Ishikawa – Pregunta 3**

Fuente: Elaboración del autor

Conclusiones:

- Conforme el uso del método de Pareto se puede concluir que una gran parte de Pymes destina de 1 a 5 % (o menos) de su presupuesto para seguridad de la información.
- Existen casos aislados de empresas que destinan una cantidad bastante grande (20 a 40%) para la seguridad del área de TI.

- De igual manera hay Pymes que no tienen un presupuesto específico, pero que destinan un rubro por debajo de la media en caso de alguna eventualidad.

4. **En caso de que sucediera un desastre tecnológico en su empresa (*corte de electricidad, daño en el servidor, sabotaje por parte de exempleados, etc.*), ¿en qué tiempo y a qué costo recupera la información?**

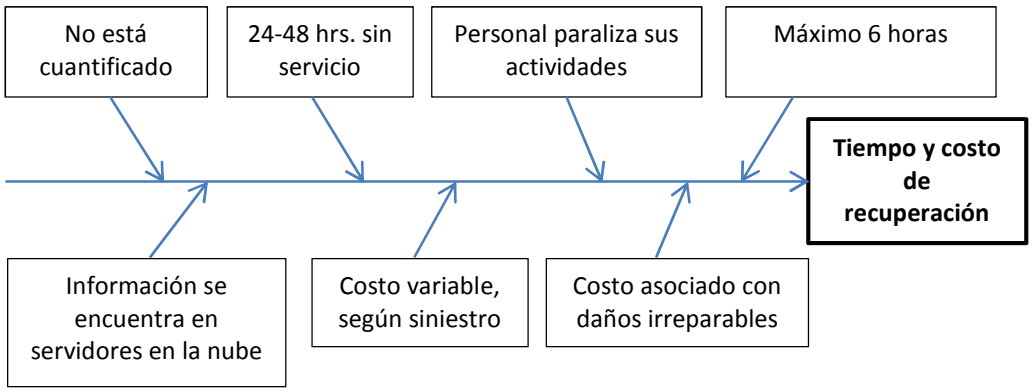


Ilustración 17. **Diagrama de Ishikawa – Pregunta 4**

Fuente: Elaboración del autor

Conclusiones:

- Usando el método de Pareto se encuentra que existen unas pocas Pymes que podrían recuperar su información desde algún sitio en Internet.
- En otros casos el costo es variable dependiendo del desastre tecnológico producido y el tiempo de recuperación va desde unas pocas horas hasta dos días.
- Uno de los mayores costos que se tiene en las Pymes es la paralización de actividades por parte del personal.

5. **¿Cuáles serían las consecuencias en su negocio para los *stakeholders* (empleados, proveedores, accionistas, etc.) en caso de producirse un desastre tecnológico?**

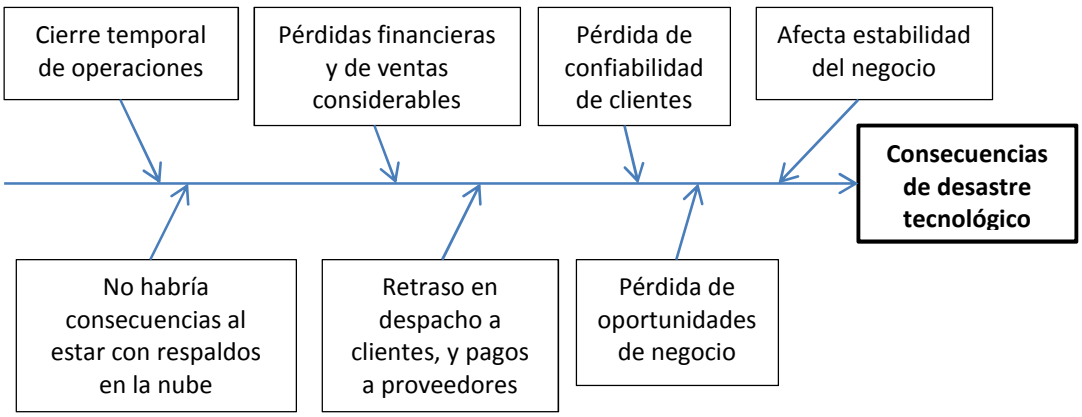


Ilustración 18. **Diagrama de Ishikawa – Pregunta 5**

Fuente: Elaboración del autor

Conclusiones:

- Una primera conclusión, con el uso de Pareto es que solamente unas pocas Pymes afirman tener poco impacto en caso de un desastre tecnológico, debido a que tienen respaldos en servidores en la nube.
- La gran mayoría de Pymes manifiesta que las consecuencias de un desastre tecnológico está asociado con costos directos en cuanto a pérdidas financieras y de ventas considerable.
- Así mismo se mencionan temas operativos como retrasos en la relación con los clientes y proveedores.
- De importancia, conforme las Pymes consultadas son los costos indirectos como consecuencia de un desastre tecnológico, tal como la pérdida de oportunidades de negocio, pérdida de confiabilidad de los clientes, lo cual afecta a la estabilidad del negocio.

6. **Sabiendo que, de manera general, la computación en la nube se refiere a servicios que están en algún lado en Internet, ¿Está incursionando su empresa en algún proyecto de computación en la nube (*o cloud computing*)?**

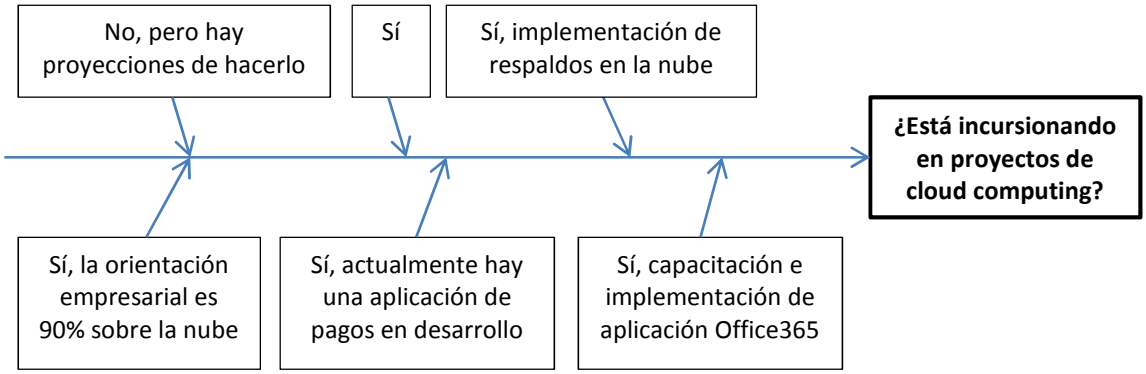


Ilustración 19. **Diagrama de Ishikawa – Pregunta 6**

Fuente: Elaboración del autor

Conclusiones:

- Las Pymes entrevistada mencionaron mayoritariamente que la incursión en la nube es un hecho en sus empresas, a través de implementación de aplicaciones en-línea, tales como Microsoft Office 365.
- Otra de las aplicaciones en la nube a la que apunta una de las Pymes está relacionada con pagos en línea de sus clientes.
- Adicionalmente, una de las Pymes mencionó que sí está incursionando en la implementación de respaldos en la nube.
- La Pyme que mencionó que no está incursionando en la nube subrayó que sí tiene proyecciones de hacerlo.
- Como una conclusión fundamental, usando el método de Pareto tenemos que uno de los pocos vitales importantes es que hay Pymes que no incursionan todavía en la nube.

7. **¿Conoce usted sobre alguna empresa que le pueda proveer de servicios de recuperación ante desastres tecnológicos en la nube? De ser afirmativa la respuesta indicar el nombre de la empresa y su experiencia con la misma.**

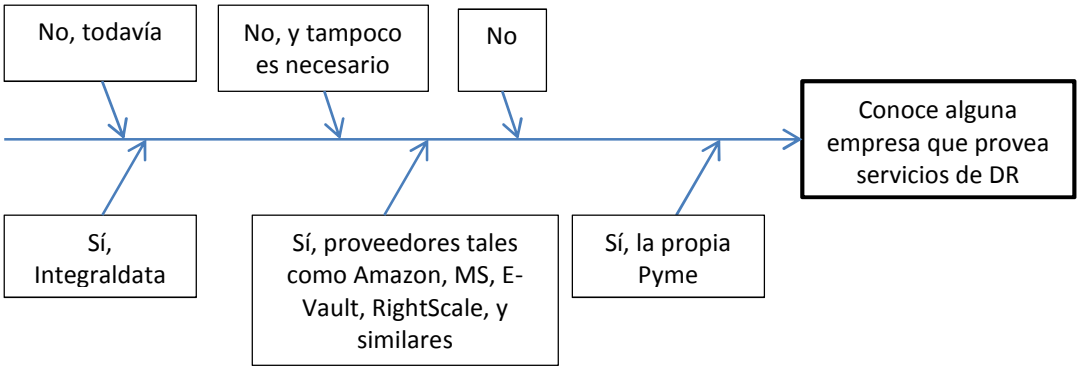


Ilustración 20. **Diagrama de Ishikawa – Pregunta 7**

Fuente: Elaboración del autor

Conclusiones:

- Existe una gran cantidad de Pymes, alrededor de la mitad, que aún desconocen sobre empresas locales o foráneas que provean de soluciones de recuperación ante desastres en la nube.
- Con el uso del método de Pareto se concluye que una de las causas por las que no se emplea a empresas en la nube es el desconocimiento de la existencia de las mismas por parte de las Pymes.
- Una sola Pyme conoce de un proveedor local, una sola Pyme conoce de un proveedor extranjero y una Pyme es su propio proveedor.

8. **¿Estaría dispuesto a contratar a una empresa externa para que se hiciera cargo de su plan de recuperación ante desastres (DRP), lo que incluiría el uso de computación en la nube?**

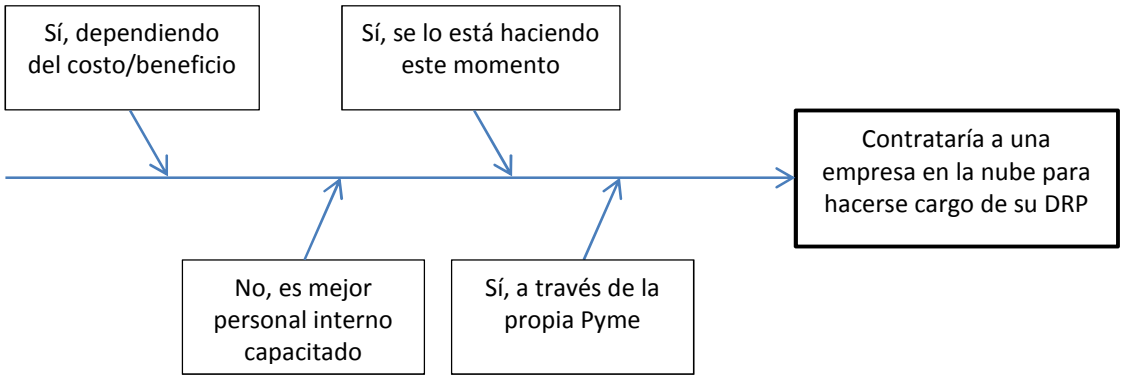


Ilustración 21. **Diagrama de Ishikawa – Pregunta 8**

Fuente: Elaboración del autor

Conclusiones:

- Conforme el uso del método de Pareto se concluye que una gran mayoría de Pymes prefiere contar con personal de la misma empresa en lugar de contratar una empresa externa para hacerse cargo de su DRP
- Pocas Pymes lo efectúan este momento con empresas externas, pero de amplia trayectoria, como Amazon.
- Una sola Pyme comentó que sí se arriesgaría a contar con una empresa que se hiciera cargo de su DRP, siempre y cuando el costo/beneficio sea conveniente.

3.1.2.7 Hallazgos

Una vez que se ha recogido las principales respuestas de las Pymes consultadas como parte del estudio mediante el criterio de expertos se procede en

esta etapa a recopilar las conclusiones personales, y que contrastan con las hipótesis planteadas al inicio de esta tesis de investigación:

1. En primer lugar se puede concluir que en las Pymes entrevistadas existe una concienciación sobre la importancia de mantener la información protegida y respaldada, mediante el uso de medios tradicionales y en períodos diarios (para la información crítica) y semanales (para información menos crítica).
2. Respecto de la seguridad informática también se puede concluir que aún son pocas las Pymes que tienen sus respaldos en la nube, siendo las Pymes de Servicios informáticos aquellas que recién están incursionando en el uso de respaldos de información en servidores de proveedores externos en la nube.
3. Aun cuando las Pymes entrevistadas son conscientes de la importancia del manejo de seguridad informática se percibe todavía como un gasto alto al que deben recurrir, al tener que invertir en infraestructura y capacitar a su personal al interior de la empresa, en el manejo de programas que permitan efectuar respaldos de manera que se pueda mantener centralizada la información.
4. En cuanto al manejo de TI se percibe claramente que el 90% de las Pymes entrevistadas todavía prefiere contar con personal propio para el manejo de su negocio en el área de Informática y Telecomunicaciones, lo cual indica que todavía no se confía el manejo de la información en una empresa externa.
5. De igual manera se puede concluir en cuanto al manejo de presupuesto para seguridad de TI que no existe un estándar, y que hay empresas que invierten menos del 1% hasta aquellas que invierten hasta un 40% de su

presupuesto, pasando por aquellas de tipo reactivo que invierten en soluciones de protección de seguridad informática en caso de producirse algún problema.

6. El costo que implica recuperarse de un desastre tecnológico, conforme los datos extraídos de las entrevistas permite concluir que existen Pymes que no se han puesto a cuantificar los posibles daños, pero también hay Pymes que asocian este costo a daños irreparables que podrían sufrir en su negocio y que incluso paralizaría las actividades de su personal.
7. El tiempo de recuperación ante un eventual desastre tecnológico varía en función del tipo de negocio de las Pymes entrevistadas, es por ello que hay quienes manifiestan que su recuperación les tomaría de 24 a 48 horas, lo cual paralizaría las actividades del negocio, aunque algunas Pymes de Servicios informáticos manifiestan que este tiempo es menor dado que su información se encuentra respaldada en servidores de proveedores en la nube.
8. La conclusión a la que se llega, para varias de las Pymes, respecto de las consecuencias de un desastre tecnológico está íntimamente ligado con la pérdida de confiabilidad de los clientes, así como de pérdidas financieras y de ventas así como la estabilidad del negocio, al producirse incluso pérdidas de oportunidades de negocio.
9. No obstante lo anterior las pocas Pymes que respaldan su información en la nube comentaron que las consecuencias serían mínimas debido a la facilidad con la que podrían recurrir a su información en el proveedor en la nube.
10. Es de relevancia el destacar que hay varias Pymes que de una u otra manera están ya incursionando en proyectos en la nube, ya sea a través

del uso de aplicaciones, capacitando a su personal o incluso teniendo respaldos en la nube

11. Aun cuando la gran mayoría de Pymes del estudio afirmó estar incursionando en la nube aquellas que todavía no lo hacen tienen planes de hacerlo eventualmente, lo cual permite visualizar que no se trata únicamente de un tema de moda, sino de una realidad acuciante en los pequeños y medianos negocios.
12. Existe un conocimiento bastante escaso en cuanto a proveedores de servicios en la nube, y menos aún para efectuar respaldos de información en caso de desastres tecnológicos, e incluso existen Pymes que consideran que no es un tema necesario el contar con empresas externas que se hagan cargo del tema.
13. Las pocas Pymes que conocen sobre proveedores en la nube recomiendan el uso de proveedores conocidos a nivel internacional, tal el caso de Amazon, E-Vault, RightScale, etc.
14. La disponibilidad de contar con una empresa externa que se hiciera cargo del DRP en la empresa estaría supeditada a un análisis costo/beneficio, aunque aquellas que respondieron en la pregunta anterior mencionan que este momento ya lo están haciendo con estas empresas, o forma parte de su plan corporativo.
15. Mediante este estudio, y con la ayuda del método de Pareto, se determinó que las principales causas para que las Pymes no estén preparadas ante un desastre tecnológico son la baja inversión en tecnología y seguridad informática, la baja prioridad otorgada por parte de altos directivos en el tema, el desconocimiento de mecanismos de recuperación ante desastres (sean estos tradicionales o en la nube), la desconfianza en proveedores externos para manejar la información interna y el desconocimiento de

empresas – nacionales o extranjeras en la web - que pudieran hacerse cargo de la recuperación ante desastres de una manera sistemática y automatizada.

3.1.3 Relación de fuentes primarias con fuentes secundarias

Un aspecto importante en esta fase de diagnóstico es la de contrastar los resultados preliminares de este estudio, en tanto que son una fuente primaria, con fuentes secundarias y empezar a verificar las hipótesis planteadas para esta tesis, y para ello se tomará en cuenta en cuenta datos estadísticos de los censos poblacional y económico del país efectuados hace un par de años, así como de estudios de mercado recientes en el ámbito de las TICs, y otros estudios relacionados, en donde se procurará cruzar la información de estos estudios.

Las preguntas de este estudio, como se detalló en la Formulación del cuestionario (capítulo 3.1.2.4) se relacionarán con algunas de las preguntas del estudio de mercado antes citado:

1. **Para el manejo de TI (Tecnología de la Información) en su negocio, ¿cuenta con personal propio o tercerizado?**
    a. De acuerdo a la fuente secundaria más del 50% de Pymes a nivel nacional cuentan con personal interno para el manejo Informático del negocio, lo cual coincide con las Pymes de Servicios de Quito de esta investigación, y consecuentemente se concluye que las Pymes aún desconfían de personal externo para sus proyectos de TI. Esto se aprecia en la **Ilustración 22**.

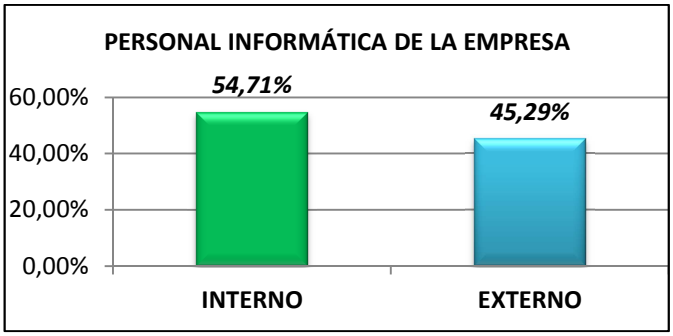


Ilustración 22. **Porcentaje de personal informático (fuente secundaria)**

Fuente: Estudio de mercado Parra y Benalcázar (2012)

2. **¿Qué porcentaje de su presupuesto lo asigna a seguridad de la información al área de TI?**

   a. De acuerdo a la fuente secundaria citada, apenas un poco más de la mitad de las Pymes a nivel nacional manejan un presupuesto anual, y de éstas, el monto asignado para TI es completamente variable, lo cual se confirma también con esta investigación, en donde hay empresas que asignan un 1% o menos de su presupuesto frente a otras – particularmente las de servicios informáticos – que destinan hasta un 40% de su presupuesto. Esto se aprecia en las **Ilustraciones 23** y **24**.

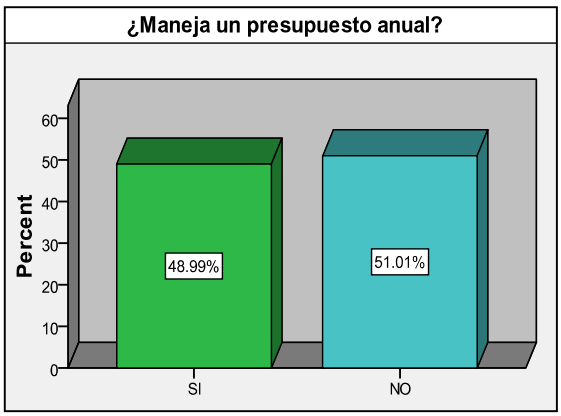


Ilustración 23. **Manejo de presupuesto informático (fuente secundaria)**

Fuente: Estudio de mercado Parra y Benalcázar (2012)

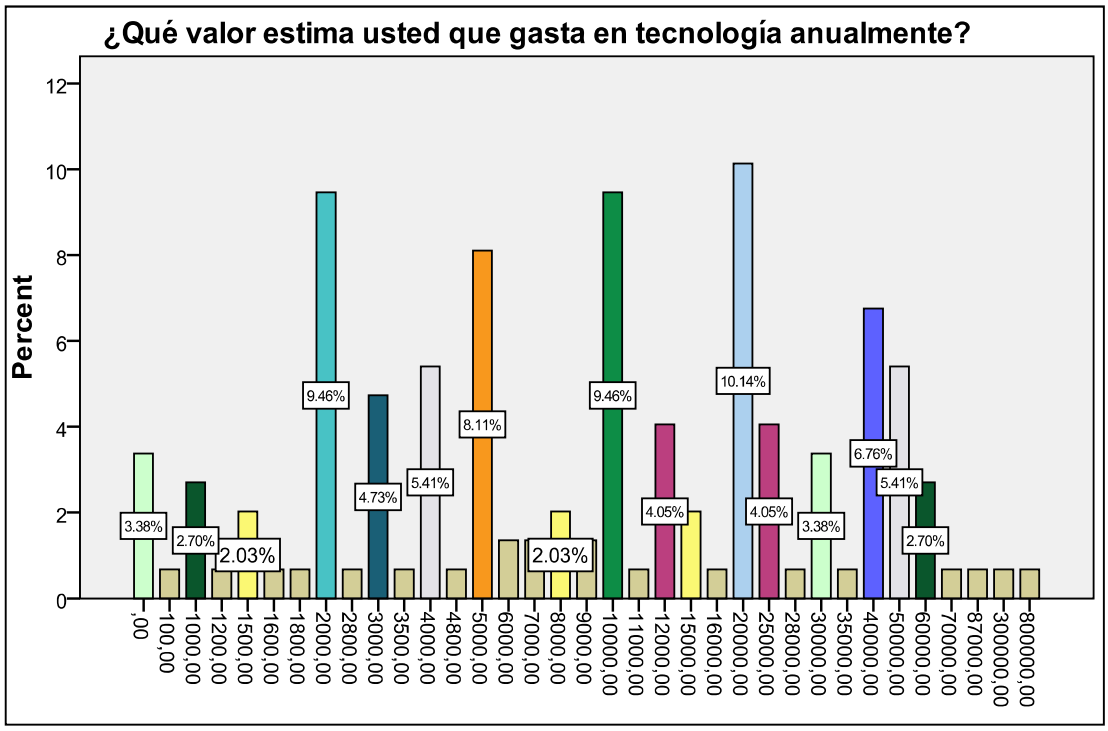


Ilustración 24. **Porcentaje de presupuesto informático (fuente secundaria)**

Fuente: Estudio de mercado Parra y Benalcázar (2012)

3. **¿Estaría dispuesto a contratar a una empresa externa para que se hiciera cargo de su plan de recuperación ante desastres (DRP), lo que incluiría el uso de computación en la nube?**

    a. De acuerdo a la fuente secundaria, aproximadamente ¾ partes de las Pymes a nivel nacional estarían dispuestas a contratar una empresa externa que les brinde asesoría informática, sin embargo esto contrasta con las Pymes de servicios de Quito, en el caso puntual de dejar en manos de una empresa externa el manejo de sus datos, concretamente en la recuperación ante desastres tecnológicos. Esto se aprecia en la **Ilustración 25**.

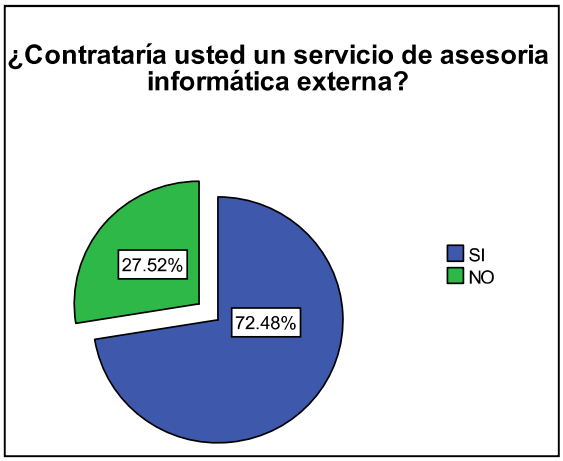


Ilustración 25. **Contratación de empresa informática externa (fuente externa)**

Fuente: Estudio de mercado Parra y Benalcázar (2012)

b. Así mismo, en esta pregunta se contrasta el que de acuerdo a la fuente secundaria hay una gran variedad de empresas de tecnología informática que pueden brindar sus servicios a las .Pymes, pero de acuerdo a este estudio, salvo aquellas Pymes de servicios informáticos, existe poco conocimiento sobre aquellas empresas que pueden dar un buen soporte en cuanto a recuperación ante desastres, y menos aun usando como mecanismo a la nube. Esto se aprecia en la **Ilustración 26**.

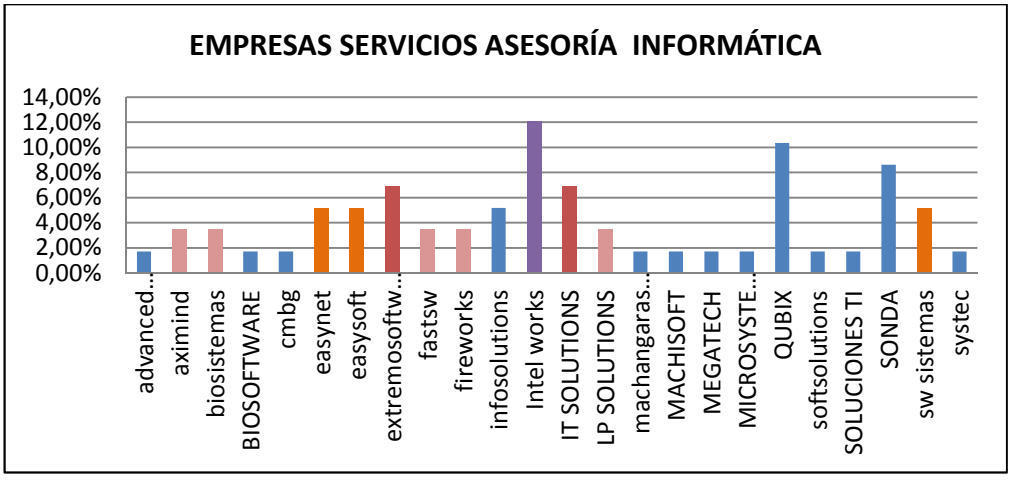


Ilustración 26. **Empresas de servicios informáticos (Fuente secundaria)**

Fuente: Estudio de mercado Parra y Benalcázar (2012)

3.2 Síntesis del Capítulo III

En este tercer capítulo se ha efectuado un diagnóstico de la realidad de las Pymes de servicios en el Distrito Metropolitano de Quito en cuanto al uso de planes de recuperación ante desastres tanto mediante el uso de métodos tradicionales como de computación en la nube.

Para la recopilación de información en la investigación de fuentes primarias se utilizó los métodos de Criterio de Expertos, a través del uso de la técnica de entrevistas, y para afianzar el estudio se recurrió a fuentes secundarias, con las cuales se cruzó información y se usó el método de Pareto.

Los hallazgos que se obtuvieron de este capítulo determinaron que la hipótesis nula planteada en este estudio se cumple, y consecuentemente las Pymes sí son afectadas considerablemente en el evento de un desastre tecnológico, pudiendo provocarles pérdidas económicas, disminución en la cartera de clientes e incluso el cierre de la empresa.

El siguiente capítulo permitirá – con los resultados de este capítulo – formular la guía de implementación de un DRP utilizando a la computación en la nube como el mecanismo más idóneo para las Pymes.

4 Capítulo IV: Elaboración de la guía de implementación

Debido a que en la fase de diagnóstico se identificaron las necesidades de las Pymes, pero también de las microempresas, se ha decidido efectuar la elaboración de la guía de implementación tanto para Pymes como para Mipymes.

4.1 Guía para Pymes

4.1.1 Introducción

Las Pymes a nivel mundial, tal y como se mostró en la fundamentación teórica en el Capítulo II, y particularmente las Pymes a nivel nacional y local, según se pudo evaluar en el capítulo anterior, no se encuentran preparadas para afrontar un desastre tecnológico en sus empresas o actúan de manera reactiva cuando es demasiado tarde, o no dimensionan las pérdidas a las que se pueden enfrentar ante tales eventos, a pesar de que son conscientes de la necesidad de contar con un DRP (Plan de Recuperación ante Desastres, por sus siglas en inglés) que les permita mitigar los riesgos a los que se pueden enfrentar, ya sean éstos desde ataques maliciosos producidos por malware hasta cortes de electricidad o fallos en los discos duros de sus servidores, pasando por catástrofes climáticas.

La presente guía de implementación permitirá ofrecer a los gerentes de las Pymes una visión acerca de los pasos que deben tomar en consideración para implementar un DRP que coadyuve a minimizar los impactos de una pérdida en la productividad, estabilidad y reputación de las empresas, tomando en cuenta que los esquemas tradicionales de recuperación ante desastres no son los más idóneos, y que incursionar en la computación en la nube, a través de un proveedor que ofrezca un servicio para enfrentar los desastres tecnológicos, a un precio razonable, es la solución que mejor satisface a la Pyme en el largo, mediano e incluso corto plazo.

4.1.2 Descripción general de la guía

Esta guía, que tiene un enfoque para Pymes, se encuentra estructurada de forma tal que sea fácilmente comprensible para el gerente, o dueño de una Pyme, o que en su defecto se la pueda transmitir al CIO o Gerente de Tecnología, de manera que le resulte sencillo transmitir sus requerimientos al proveedor de servicios en la nube.

La guía está dividida en una secuencia de pasos, en donde se puede revisar tanto la parte gerencial como la parte técnica, a grosso modo, y con ello que la guía sea lo suficientemente flexible como para que cada Pyme pueda seguir a su propio ritmo esta implementación.

4.1.3 Características

La guía poseerá las siguientes características:

- **Facilidad de uso**.- Aun cuando la guía está orientada al área técnica será de fácil comprensión para los gerentes empresariales, quienes podrán darle seguimiento a los procesos que se deban efectuar para llevar a cabo tanto el DRP como su implementación en la nube.

- **Fácil interpretación de términos**.- La guía permitirá a los dueños de Pymes o CEO y a los CIO una fácil interpretación de los términos usados tanto para la elaboración de un DRP como del conocimiento de la terminología usada en la computación en la nube.

- **Fácil comprensión de procedimientos**.- Tanto los altos directivos como el personal técnico de TI de las Pymes podrán comprender de manera sencilla

los procedimientos que se deban emprender para poder implementar esta guía.

- **Flexibilidad**.- La idea de esta guía es que sea adaptable a la circunstancia de cada Pyme y no se transforme en una *receta* o *camisa de fuerza*, sino que se vaya acoplando a la situación específica de cada negocio.

- **Escalable**.- De igual manera, la guía a ser propuesta será escalable, y esto se refiere a que cada Pyme irá implementando su DRP en la nube en una transición que puede ir desde tener una solución local, o en sus instalaciones, pasando por una solución híbrida, es decir, con parte de su DRP implementado localmente y otra en la nube, y eventualmente tener todo en la nube.

4.1.4 Secuencia de pasos

4.1.4.1 Introducción

Las Pymes hoy en día dependen en gran medida de sistemas computacionales y de telecomunicaciones, y cuando éstos fallan, por cualquier motivo, su negocio puede cerrar sus operaciones en cuestión de días. En estos tiempos modernos se debe dar una mayor prioridad al manejo o gestión de desastres tecnológicos, y para esto es necesario establecer procesos de gestión de respaldos de manera formal, así como de estrategias para recuperación ante este tipo de desastres.

Ya sea que se trate de recuperar solamente un archivo o implementar un plan de recuperación ante desastres tecnológicos a través de sistemas que sean seguros, rápidos y confiables en el evento de un desastre natural o provocado por el hombre, las Pymes enfrentan los mismos retos que las grandes empresas.

Los **centros de datos** en donde se alojan los componentes de TI críticos – datos, hardware, software y comunicaciones – de las Pymes, y de los cuales dependen sus negocios, normalmente no están protegidos de desastres naturales o de accidentes (tales como el daño inesperado de un disco duro o corte de energía) ni tan siquiera de desastres provocados por el hombre (ex empleados disgustados que se roban la información, virus informáticos, entre otros), de manera que los siguientes pasos están estructurados para que las Pymes puedan tener un panorama más amplio de lo que la tecnología actual les permite hacer sin tener que invertir exorbitantes sumas de dinero, y sin tener que recurrir a métodos tradicionales (como los respaldos en cintas de datos) que han probado no ser ni eficaces ni eficientes en el momento de la verdad.

Lo primero que hay que darse cuenta es que se requiere de un DRP. La implementación de un DRP se lo ha asociado con una actividad exclusiva de grandes empresas, sin embargo – y como se mencionó anteriormente – las Pymes enfrentan los mismos retos que sus similares más grandes, y en algunos casos las Pymes, al encontrarse ante un reto que puede ser sobrecogedor, presentan temor o incluso relegan esta tarea para una próxima oportunidad, la cual no llega sino hasta que haya sufrido pérdidas económicas de las cuales muchas veces no se pudieron recuperar. De hecho, las Pymes no suelen implementar un DRP debido a que:

- Resultaba excesivamente caro implementar un segundo centro de recuperación ante fallos con recursos dedicados.
- Los planes de recuperación eran demasiado complejos.
- Los procedimientos de recuperación ante desastres eran demasiado poco fiables.

La presente guía ayudará a los Gerentes de Pymes a garantizar la continuidad y la preservación de sus negocios orientándolos a través de pasos fundamentales, desde la comprensión de los conceptos de recuperación de desastres y disponibilidad de la información hasta los motivos por los cuales la implementación de un DRP, usando a la computación en la nube, es el mecanismo más idóneo para reducir los riesgos a los que pueda enfrentarse la Pyme, y mejorar la capacidad de recuperación ante un desastre manteniendo la productividad de los usuarios y del negocio durante estas situaciones adversas.

La guía está estructurada en 6 pasos, lo cual se visualiza de mejor manera en la **Ilustración 27**:

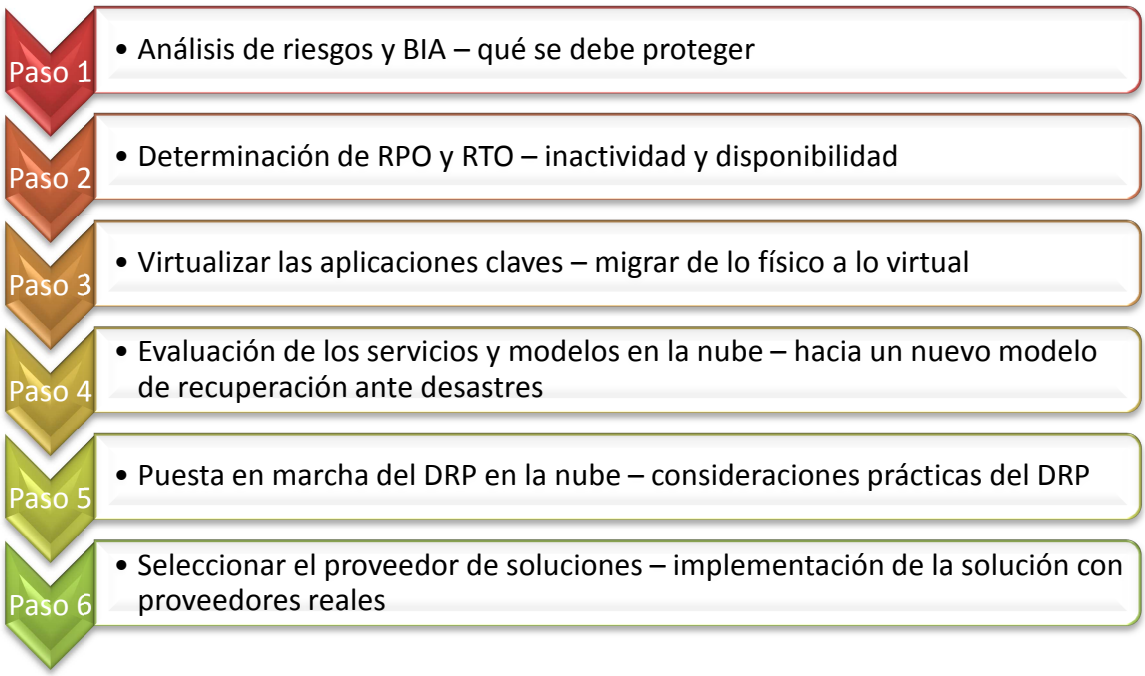


Ilustración 27. **Secuencia de pasos de la guía para la recuperación ante desastres usando a la computación en la nube**

Fuente: Elaboración del autor
Elaborado por: Danilo Mannella

Alcance de la guía

Es importante tomar en cuenta que, si bien un DRP y una estrategia de recuperación ante desastres tecnológicos forman parte importante de un Plan de Continuidad de Negocio (BCP) y está íntimamente relacionada con esta última, en esta guía no se abordará ningún tópico relacionado con el BCP.

La implementación de un DRP requiere de un trabajo mancomunado entre la alta gerencia de las Pymes y el departamento de TI de la empresa, o en su defecto de una empresa tercerizada que ayude a la organización a implementar esta guía, pero en este estudio se mostrará qué se debe hacer, y en algunos pocos casos los cómos, de forma tal que los gerentes puedan saber qué solicitar y dejen al área técnica buscar las mejores alternativas de implementación.

4.1.4.2 Paso 1: Análisis de riesgos y BIA – qué se debe proteger

Toda Pyme debe conocer cuál es su ámbito de negocio y los procesos que le permiten desarrollar su actividad. Dentro de la misma es necesario y crítico identificar:

1. Los procesos críticos del negocio
2. El apoyo de los mismos en las Tecnologías de la Información (TI)
3. El conocimiento de personas clave para la organización, los productos y servicios
4. La estrategia de negocio o las metas de la organización, los procesos internos, etc.

Tomando en cuenta los puntos anteriores, es necesario efectuar un análisis de impacto del negocio (BIA) que consiste simplemente en calcular las pérdidas potenciales a las que podría verse avocado el negocio por las diferentes amenazas que pueden interrumpir sus actividades, y para ello se debe cuestionar:

- ¿Qué aplicaciones generan beneficios directamente, mantienen la seguridad, o son fundamentales de cualquier otro modo, para la continuidad del negocio?
- ¿Qué datos son absolutamente críticos para los clientes, la contabilidad interna o las finanzas, o son de obligado cumplimiento?

Este análisis permite identificar los datos y aplicaciones más importantes que deberán ser respaldados porque no todo puede y debe ser respaldado, al menos no desde un principio, más aun considerando el presupuesto limitado que usualmente manejan las Pymes. Adicionalmente a esto, las Pymes deben enfrentar factores tales como la recesión global, una creciente competencia que requiere de procesos justo-a-tiempo, el incremento explosivo de datos, y requerimientos regulatorios, que resaltan la necesidad de un plan de recuperación ante desastres.

Un DRP ofrecerá una solución efectiva que se puede utilizar para recuperar todos los procesos de negocio vitales en el marco de tiempo requerido usando registros críticos que se almacenan fuera de la empresa. No contar con un DRP puede traer como consecuencias algunos costos directos e indirectos, tal y como se aprecia en el **Cuadro 19**.

Cuadro 19. Costos directos e indirectos de no contar con un DRP

Costos tangibles / directos	Costos intangibles / indirectos
• Pérdida de ingresos por transacciones	• Pérdidas de oportunidades empresariales
• Pérdida de salarios	• Pérdida de empleados o desmoralización de los mismos
• Pérdida de inventario	• Disminución del valor de las acciones (si es que aplica)
• Costes laborales de saneamiento	• Pérdida de los fondos de comercio de los clientes y de los socios
• Costos de marketing	• Pérdida de negocio en favor de la competencia
• Tasas bancarias	• Mala publicidad y prensa

Costos tangibles / directos	Costos intangibles / indirectos
• Multas legales	

Fuente: Guía fundamental para la recuperación de desastres – Novell (Whitepaper)
Elaborado por: Danilo Mannella L.

Este primer paso lo debe ejecutar la Gerencia con sus unidades de negocio, a fin de determinar los requisitos de disponibilidad de cada proceso, y con esto poder determinar el costo que tendría el fracaso en la consecución de los objetivos de disponibilidad de cada proceso, tal y como se indicó en párrafos anteriores. Usualmente se sugiere hacer un borrador a nivel de capas para priorizar qué información es más importante y prioritaria proteger, puesto que no es lo mismo proteger las aplicaciones de negocios o un servidor de correo electrónico, que los datos que tengan los empleados en una portátil. La ventaja de esta estrategia es que permite optimizar los costos de recuperación ante desastres, que puede variar, dependiendo del tipo y profundidad de plan que se quiera implementar. Más adelante, en el Paso 5, se analizará dentro del DRP cómo manejar los riesgos, y la relación entre éstos y las amenazas y vulnerabilidades a las que pueda estar expuesta la Pyme.

4.1.4.3 Paso 2: Determinación de RPO y RTO – inactividad y disponibilidad

Una vez que se ha determinado cuáles son las aplicaciones y procesos de negocios críticos es momento de preguntarse:

1. ¿Cómo maneja la empresa el tema de recuperación ante desastres en la actualidad?
2. ¿Qué pasaría si y cuándo sucede un desastre en la empresa?
3. ¿Qué tan rápido se puede recuperar el negocio en caso de un desastre?
4. ¿Cuánto tiempo sobreviviría la empresa si se perdiera toda la información?

5. ¿Con cuánta rapidez y seguridad se recupera la información?

Lo anterior constituye algunas de las inquietudes a resolver en esta fase, de hecho es una de las cosas a tomar en cuenta en la elaboración de un plan de recuperación ante desastres, para lo cual se incluye el **objetivo de tiempo de recuperación** (*RTO, por sus siglas en inglés*) y el **objetivo de punto de recuperación** (*RPO, por sus siglas en inglés*) de la información, así como la necesidad de tener acceso remoto a los datos desde fuera de la empresa. Este momento se analizará en detalle la utilidad de considerar los objetivos de tiempo y punto de recuperación.

- **RTO (Objetivo de Tiempo de Recuperación)**.- Describe la cantidad de tiempo, o qué tan rápido se puede recuperar información a partir de que acontezca un desastre. La clave aquí es la velocidad con la que la información en el medio de respaldo se restaura en el sistema. P. ej. Si se pierde, o desea recuperar un archivo, ¿en cuánto tiempo lo tiene de vuelta?, ¿5 minutos?, ¿una hora?, ¿un par de días? Si bien es cierto que esto depende – entre otras cosas – del tamaño del archivo, es importante considerar esto de antemano.

- **RPO (Objetivo de Punto de Recuperación)**.- Se refiere al punto en el tiempo en donde los datos son restaurados y refleja la cantidad de datos que en última instancia se perderán durante el proceso de recuperación. P. ej. Si se efectúa un respaldo del sistema una vez al día, a medianoche, el RPO será de 24h. En caso de algún desastre o fallo tecnológico, cualquier dato cambiado o ingresado entre la medianoche y las 23h59 se perderá, de

modo que la exposición de pérdida es de 23h59, y si bien esto podría ser admisible en PCs caseras, en el caso de un negocio, como de las Pymes, esta ventana debe reducirse, quizás a 5 minutos.

El RTO y RPO están asociados a la “disponibilidad”, que se la define como algún punto de un continuo entre varias horas de “inactividad” con pérdida de datos importantes y el funcionamiento ininterrumpido en tiempo real sin pérdida de datos. Su definición depende de las necesidades de cada Pyme, sus requisitos de datos y aplicaciones y su estructura organizativa. Sin embargo, el objetivo debe ser impedir que el inevitable tiempo de inactividad del sistema afecte al funcionamiento de la empresa.

El importe que se puede asignar a cada hora de inactividad varía mucho en función de la naturaleza de su negocio, el tamaño de la Pyme y la importancia de los sistemas informáticos para los principales procesos de generación de ingresos, y por ello es importante que se establezca el RPO y RTO que está dispuesto a tener cada negocio, en base a sus particularidades, y aunque frecuentemente las Pymes optan por usar métodos tradicionales de recuperación ante desastres estos suelen tener más debilidades que ventajas.

A continuación se muestra un cuadro comparativo con los enfoques de sistemas tradicionales de recuperación ante desastres, desde el punto de vista del RTO. RPO, costo y sus debilidades:

Cuadro 20. Ventajas y debilidades de los enfoques de recuperación ante desastres tradicionales

Solución	RPO	RTO	Costo	Debilidades
Uso de cintas	24h+	Días	$	• Difícil de administrar • Lento, propenso a errores
Captura de imágenes	24h	Horas	$$$	• Restauración limitada y flexible
Replicación	Min.	Min.	$$$$$	• Configuración complicada • HW duplicado
Agrupamiento de	0	0	$$$$$$	• HW duplicado

Solución	RPO	RTO	Costo	Debilidades
servidores				• Configuración complicada

Fuente: Consolidated Disaster Recovery – Novell (Whitepaper)
Elaborado por: Danilo Mannella L.

Las Pymes usualmente han usado modelos de recuperación ante desastres tecnológicos tradicionales, en donde deben compensar entre costo y velocidad de recuperación, ya sea que tengan una solución dedicada o compartida, tal y como se ve a continuación, en la **Ilustración 28**.

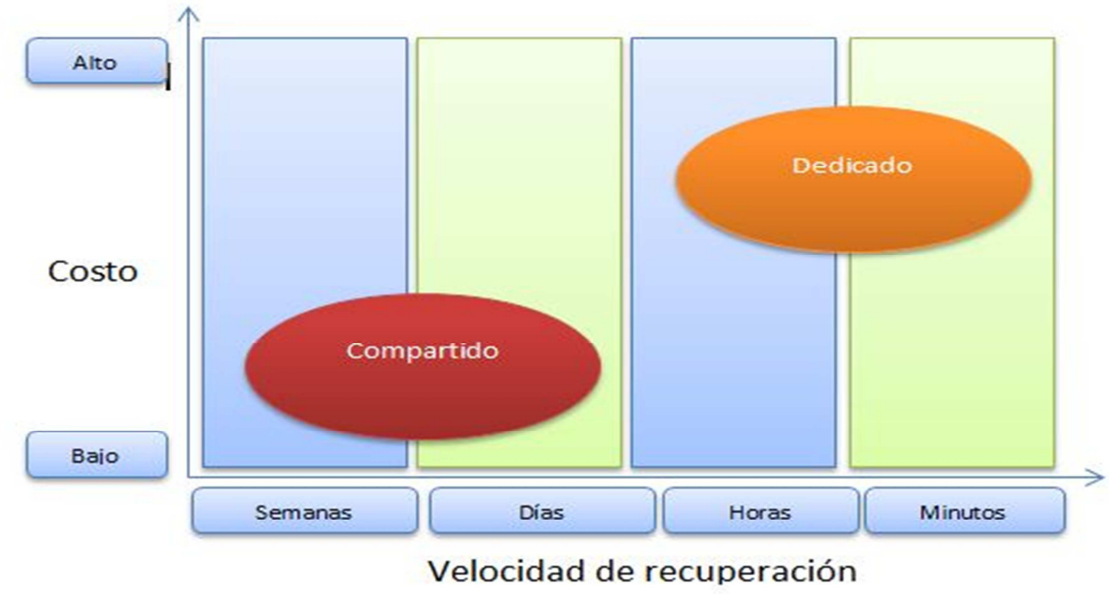


Ilustración 28. **Modelos compartidos y dedicados en DRPs tradicionales**

Fuente: Virtualizing Disaster Recovery using Cloud Computing.
Elaboración: Danilo Mannella L.

En un **modelo dedicado**, la infraestructura está dedicada a una sola organización. Este tipo de recuperación de desastres puede ofrecer un tiempo más rápido de recuperación en comparación con otros modelos tradicionales, ya que la infraestructura de TI se ve reflejada en el sitio de recuperación ante desastres y está lista para ser llamada en caso de un desastre. Si bien este modelo puede reducir el RTO, porque el hardware y el software están preconfigurados, no elimina todos los

retrasos. El proceso sigue dependiendo de recibir una imagen de datos actualizada, lo que implica el transporte de las cintas físicas y un proceso de restauración de datos.

Este enfoque también es costoso porque el hardware se encuentra inactivo cuando no se utiliza para la recuperación de desastres. Algunas organizaciones utilizan la infraestructura de respaldo para el desarrollo y pruebas para mitigar el costo, pero esto no aplica en el caso de las Pymes.

Finalmente, el proceso de restauración de datos añade variabilidad en el proceso. La restauración de datos puede tardar hasta 72 horas, incluyendo el proceso de recuperación de la cinta, los viajes y de carga.

En un **modelo compartido**, la infraestructura es compartida entre múltiples organizaciones. La recuperación de desastres compartida está diseñada para ser más rentable, ya que la infraestructura de copia de seguridad fuera del sitio se comparte entre varias organizaciones. Después de que se declara un desastre, el hardware, sistema operativo y software de aplicación, en el lugar del desastre, se debe configurar desde el principio para que coincida con el sitio de TI que ha declarado un desastre, y este proceso puede durar horas o incluso días. Además de eso, el proceso de restauración de datos debe ser completado, resultando en un promedio de 48 a 72 horas a la recuperación.

En esta guía la propuesta para las Pymes es utilizar a la computación en la nube ya que ofrece una alternativa atractiva a la recuperación de desastres tradicionales. "La Nube" es de por sí una infraestructura compartida: un conjunto agrupado de los recursos con los costos de infraestructura distribuidos a través de todas las personas que contratan el servicio en la nube.

Esta naturaleza compartida hace que la nube sea un modelo ideal para la recuperación de desastres. Incluso cuando se amplíe la definición de la recuperación de desastres para incluir las interrupciones de servicios más corrientes, la necesidad de recursos de recuperación de desastres es esporádica. Puesto que es muy

improbable que todas las organizaciones que confían en la nube para respaldo y recuperación necesiten la infraestructura al mismo tiempo, los costos pueden reducirse y la nube puede acelerar el tiempo de recuperación, lo cual se muestra en la **Ilustración 29**.

Ilustración 29. **Enfoque de uso de computación en la nube para recuperación ante desastres**

Fuente: Virtualizing Disaster Recovery using Cloud Computing.
Elaboración: Danilo Mannella L.

4.1.4.4 Paso 3: Virtualizar las aplicaciones claves – migrar de lo físico a lo virtual

Hoy en día las Pymes deben pensar más en términos de interrupciones en lugar de desastres, y desde hace algunos años la virtualización se ha constituido en una opción viable para lograr esto.

La virtualización es una tecnología que consiste en que una máquina física (usualmente un servidor), llamado computador “anfitrión”, puede ser configurada para ejecutar varias máquinas virtuales, en donde cada instancia del sistema operativo ejecuta sus propias aplicaciones, como si fuera el único sistema operativo en dicha máquina. La virtualización se realiza mediante una capa de software denominada

"monitor de máquina virtual" (VMM), “Gestor de máquinas virtuales” o "hipervisor" que se encuentra entre el hardware y los 'anfitriones' a los sistemas operativos. En la **Ilustración 30** se puede apreciar de manera gráfica esta explicación.

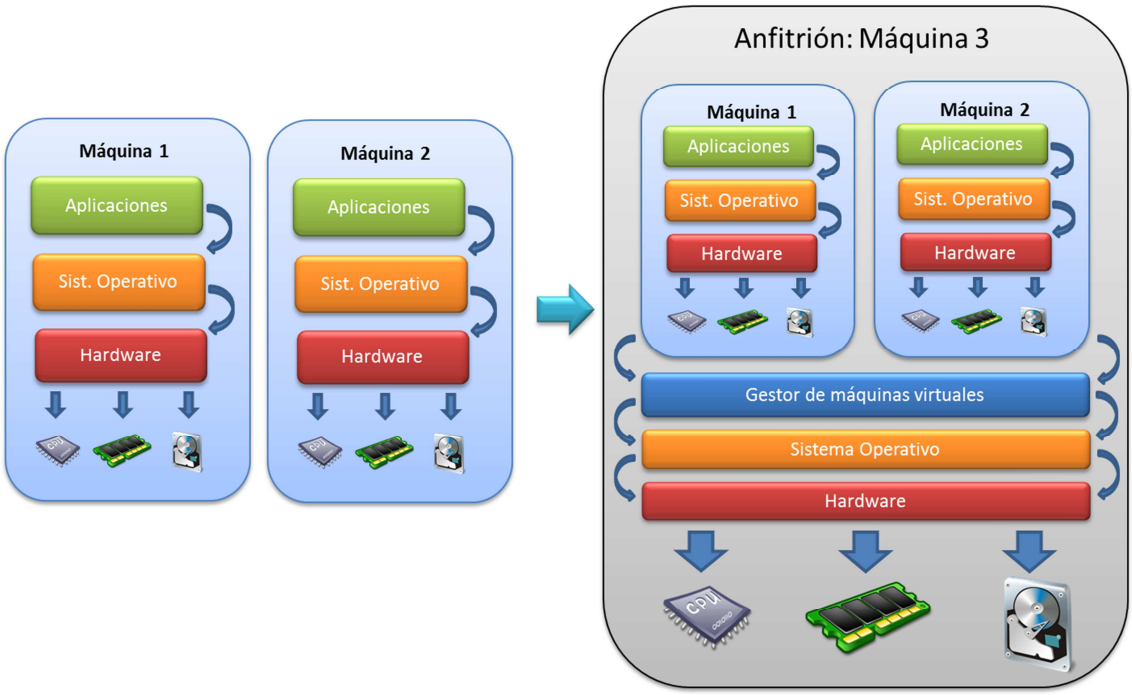


Ilustración 30. **Ejemplo de uso de virtualización**

Fuente: Virtualización, una solución para la eficiencia, seguridad y administración de intranets (Whitepaper)
Elaborado por: Danilo Mannella L.

La virtualización se usó por primera vez de manera generalizada en los escenarios de desarrollo y pruebas de software, lo que permitió a las organizaciones proveer rápidamente de diferentes entornos operativos virtuales en los cuales se podía probar un nuevo software antes de sacarlo a producción. Más recientemente, las organizaciones han recurrido a la virtualización para la *consolidación de servidores* como un medio para reducir los gastos de hardware y reducir el coste por servidor de la energía, espacio físico y recursos humanos. La virtualización permite una mayor utilización de los recursos de infraestructura y la disminución de los costos de

hardware y mantenimiento, así como la instalación del servidor y la configuración de aceleración.

Una de las grandes ventajas de la virtualización es que las máquinas virtuales pueden ser usadas para ejecutar diferentes tipos de cargas de datos, y esta flexibilidad puede y es aprovechada para la recuperación ante desastres.

El proceso típico para recuperar un servidor físico a menudo es:

1. Buscar o comprar servidores físicos equivalentes o compatibles
2. Instalar un sistema operativo
3. Instalar los parches y actualizaciones
4. Instalación de aplicaciones aplicables
5. Instalar los parches y actualizaciones
6. Carga de datos de copia de seguridad

Con el uso de la recuperación virtual, casi todos esos pasos son cosa del pasado. El proceso para recuperar un servidor físico puede ser tan simple como:

1. Encender el equipo virtual equivalente
2. Agradecer que ya no se tiene que hacer frente a los servidores físicos

La rápida adopción de las tecnologías de virtualización ha cambiado fundamentalmente en las organizaciones en general, y en las Pymes en particular la manera ver al centro de datos. Al ayudar a disolver los lazos entre software y hardware, la virtualización ha alentado a las organizaciones para ver el centro de datos ya no como una mezcla heterogénea de diferentes servidores, sistemas operativos,

aplicaciones y datos, sino como un conjunto de unidades de carga de trabajo portátiles.

Una carga de trabajo encapsula los datos, aplicaciones y sistemas operativos que residen en un servidor físico o virtual. La capacidad de perfil, mover, copiar, proteger y reproducir las cargas de trabajo de todo el servidor como unidades globales entre los servidores físicos y virtuales está ayudando a muchas organizaciones a alcanzar nuevas eficiencias operativas y ahorros de costes en el centro de datos, y la apertura de nuevas opciones para la recuperación de desastres y protección de la carga de trabajo consolidada.

Al reconocer la flexibilidad inherente de esta tecnología, las organizaciones están empezando a extender el uso de la virtualización de servidores a nuevas áreas de operaciones del centro de datos, y aprovechar los beneficios de las infraestructuras virtuales de forma más fácil y rentable de proteger las cargas de trabajo del servidor que se ejecutan en entornos físicos o virtuales.

La protección de la carga de trabajo es la tarea de copiar o reproducir las cargas de trabajo de servidores físicos o virtuales a un lugar secundario (usualmente fuera de la empresa) para su uso como un medio de espera *caliente* en el caso de una interrupción del servidor principal o un desastre en todo el sitio.

La virtualización permite a las Pymes lograr la protección de la carga de trabajo mediante la creación de un archivo de arranque de la carga de trabajo en una plataforma virtual en el que la recuperación puede ser rápidamente restaurada. La virtualización permite un ahorro significativo de costes y ventajas de rendimiento sobre las opciones de recuperación de desastres más tradicionales, tales como copia de seguridad de cinta, las imágenes, la reproducción o agrupación.

4.1.4.5 Paso 4: Evaluación de los servicios y modelos en la nube – hacia un nuevo modelo de recuperación ante desastres

Como ya se ha mencionado en capítulos anteriores la computación en la nube (*Cloud Computing*) es un nuevo modelo y entrega de servicios de Tecnología Informática, cuyo acceso es ubicuo, conveniente y a demanda, a través de esquemas de virtualización.

La computación en la nube presenta 5 características importantes para las Pymes, y que se resume brevemente a continuación:

1. **Autoservicio por demanda**.- La Pyme puede solicitar la provisión de un servicio sin necesidad de interacción humana con el proveedor de servicios.

2. **Acceso de red ubicuo**.- Las diferentes prestaciones se pueden acceder a través de una plataforma heterogénea de dispositivos, que van desde las tradicionales PCs hasta dispositivos móviles como teléfonos inteligentes y tabletas

3. **Fuente común de recursos**.- Los recursos provistos por parte de los proveedores de servicios benefician a varios usuarios o empresas, y en el caso de las Pymes esto quiere decir que los costos se abaratan al no tener que preocuparse de infraestructura propia (procesador, memoria, discos duros, etc.) y se abstrae incluso de la ubicación de estos recursos. Además, al aprovechar la infraestructura de una empresa mejor equipada se gana en eficiencia.

4. **Rápida elasticidad**.- Dependiendo de la demanda de servicios las Pymes pueden tener elasticidad en la adquisición de más o menos recursos de

acuerdo al uso que hagan de los servicios, lo cual hace que los costos no sean fijos, sino variables, y en el caso de un esquema de recuperación ante desastres esto puede resultar sumamente beneficioso.

5. **Servicio medido**.- En cierto modo relacionado a lo anterior, se paga lo que se consume, y las Pymes pueden conocer de manera transparente el manejo de estos recursos a través de un monitoreo permanente.

Las características de la computación en la nube, y para la implementación de un plan de recuperación ante desastres están atadas al tipo de modelos de servicio con el cual deberá interactuar la Pyme, tal y como se manifestó en capítulos anteriores estos modelos son:

1. SaaS (Software como Servicio)
2. PaaS (Plataforma como Servicio)
3. IaaS (Infraestructura como Servicio)

En el caso de las Pymes, y para efecto de esta guía, se sugiere que se considere inicialmente al modelo SaaS en cuanto al uso de aplicaciones (tanto de aplicaciones web como de colaboración y aplicaciones de oficina) y IaaS como modelo de servicio que se deberá profundizar en su conocimiento y solicitar al proveedor para lo que tiene que ver con la recuperación ante desastres y que algunos llaman RaaS (Recuperación como Servicio).

El servicio de tipo RaaS debe tomar en cuenta que la información y aplicaciones que deben ser analizadas para ser respaldadas y restauradas se las debe hacer en base una priorización, o modelo por capas, en donde es importante efectuar

como parte del DRP una ejecución de pruebas con cierta frecuencia, para justificar la validez de este esquema.

Un aspecto fundamental que deben tomar en cuenta las Pymes es el tipo de nube sobre la que se llevará a cabo el DRP.

Aun cuando la computación en la nube es un modelo que ha venido tomando fuerza en los últimos 3 años, y tiene aspectos positivos y negativos a continuación se detallará algunas variables que las Pymes deben considerar antes de saltar a la nube:

1. **¿Qué aplicaciones o cargas de trabajo se llevará a la nube?**

   En un principio los gerentes de las Pymes deben estar conscientes de que no todo puede y/o debe estar en la nube. Las aplicaciones que se usarán serán exclusivamente para todo lo relacionado con la recuperación ante desastres, y se sugiere que se migre la información o carga de trabajo que es crítica de ser respaldada. No existen recetas predefinidas, y cada Pyme es diferente, por lo que se sugiere que se haga una identificación de las aplicaciones y que serán parte del DRP y que aporten los mayores beneficios a la organización. Si bien las grandes empresas pueden darse el lujo de implementar nubes privadas, en el caso de las Pymes se sugiere aprovechar las nubes públicas, pero esto se tratará más adelante.

2. **¿Cómo debe ser la infraestructura deseada?**

   Antes de considerar al proveedor con el cual se deseará llevar a cabo el DRP en la nube es fundamental que éste cuente con una infraestructura dinámica, con capacidad de virtualización, estandarización de servicios y provisión automática de recursos de TI, y sobre todo, que se apoye en esquemas de seguridad que siga las mejores prácticas de la industria para proteger la información de la empresa.

3. ¿Cuáles son sus requisitos de seguridad?

Indudablemente la seguridad es uno de los temas más delicados y que más preocupan a todas las empresas que incursionan en la nube, y las Pymes no son la excepción. Aun cuando el nivel de exposición de los datos y compartición de recursos es mayor en una nube pública que en una privada los gerentes de las Pymes deberán buscar a proveedores que usen algoritmos de encriptación fuertes (tales como AES-256) y que en base a su solvencia, seriedad y transparencia afronte los niveles de seguridad requeridos, esto es parte del Acuerdo de Nivel de Servicios (SLA) que es el siguiente factor a considerar.

4. Definición del SLA

Las Pymes deben enfocar sus esfuerzos en la seguridad de la información cuando ésta suba a la nube, y parte de esta seguridad se logra con la negociación de niveles de servicio, los cuales no se limitan únicamente a considerar diferentes indicadores sino también el cómo serán medidos. El SLA la ayuda a la Pyme a conocer cómo será la interacción entre el proveedor y el consumidor del servicio. Dado que se sugiere en esta guía la utilización de una nube pública debe tomarse en cuenta que el SLA muy posiblemente es común para varios usuarios y que no tendrá la misma flexibilidad que en el uso de una nube privada, en donde se ajusta a las necesidades del cliente.

5. ¿Cuál será el nivel de portabilidad?

Las barreras de entrada a un modelo en la nube público son muy bajas, sin embargo cuando se trata de la barrera de salida la cosa cambia. Cuando se

habla de portabilidad se refiere a la capacidad de cambiar de entorno luego de implementar un modelo en la nube, es decir que se debe analizar lo que sucede cuando la empresa desea cambiar de proveedor, o desea agregar nuevos proveedores, pasar de una nube pública a una privada, o incluso salirse de un esquema en la nube para usar otro esquema. Cuando un proveedor ofrece alta portabilidad, está asegurando al cliente flexibilidad, libertad y capacidad de decisión.

6. Nube pública o privada

Como se ha mencionado reiteradamente en esta guía cada tipo de nube presenta sus pros y contras, pero la nube pública es la que mejor se ajusta a la realidad de nuestras Pymes, por flexibilidad, costos, uso eficiente de recursos, entre otros. Sin embargo no hay que olvidar que esto es un proceso, y como tal, se puede tener un esquema hibrido en donde se tenga cierta información respaldada localmente, y otra información respaldada en la nube pública.

Ahora sí, en el siguiente capítulo, se va a revisar la estructura de un DRP en la nube.

4.1.4.6 Paso 5: Puesta en marcha del DRP en la nube – consideraciones prácticas del DRP

El ciclo de vida de un DRP en la nube es bastante similar a aquel que se usa con métodos de recuperación tradicionales, aunque con la flexibilidad, escalabilidad, seguridad de la computación en la nube.

Si un DRP no ha sido implementado todavía será necesario iniciar la preparación de la primera versión del plan. Para esto el Directorio (o altos ejecutivos) de la Pyme deberán recibir una propuesta. Cuando se trata de proyecto de desarrollo

de un DRP debe ser aprobado por las más altas instancias de la empresa, de manera que se pueda asegurar que el nivel requerido de compromiso, recursos y gestión administrativa se apliquen a todo el proceso.

La propuesta debería incluir las razones por las que se debe efectuar este plan, lo cual incluye:

1. La creciente dependencia del negocio, en los últimos años, en cuanto a mecanismos de entrega de producción y ventas computarizadas, consecuentemente se identifica un creciente riesgo en la pérdida de servicios regulares.
2. La creciente dependencia del negocio, en los últimos años, respecto de los sistemas de información, lo cual abarca entre otros a los ERP[19] y CRM[20].
3. El creciente reconocimiento acerca del serio impacto que un incidente puede tener en el negocio.
4. La necesidad de establecer un proceso formal a seguir cuando se presenta un desastre tecnológico.
5. Una intención de reducir costos y pérdidas que surjan de serios incidentes.
6. La necesidad de desarrollar estrategias efectivas de respaldo y restauración de datos para mitigar el impacto de eventos que interrumpan las normales actividades del negocio.
7. Evitar el fracaso, e incluso cierre de las operaciones del negocio, debido a eventos disruptivos.

<u>Evite las complejidades</u>

[19] ERP: *Enterprise Resource Planning*.- Herramienta gerencial de administración de información que permite el manejo de todos los recursos empresariales

[20] *Customer Relationship Management*.- De igual manera es una herramienta empresarial que permite conocer y administrar de mejor manera la relación con los clientes

Algunas Pymes, al querer tratar de adaptar un plan de recuperación ante desastres de grandes empresas se pierden en las complejidades del mismo, debido a que no saben cómo funciona para su realidad. El plan en sí mismo debe ser lo más simple de entender. Hay que imaginarse lo duro que debe ser tratar de interpretar un plan en medio de un desastre.

De modo que, la primera regla de oro es ENTENDER el plan. Al inicio, hay que tener claro cómo es creado el plan. Aquellos planes considerados exitosos son aquellos que siguen una secuencia lógica.

Uso de herramientas de soporte

En esquemas tradicionales de recuperación ante desastres, e incluso en algunos en la nube, existen productos que ayudan en esta área, sin embargo muchos de ellos requieren de un gran esfuerzo para comprender su funcionamiento, y se pierde la razón del uso de estas herramientas: la simplicidad. Adicionalmente a este factor también entra en consideración el costo de la herramienta, los procesos que usan, y algunos otros. De ser posible hay que buscar herramientas que permitan la automatización del DRP, de lo contrario habrá que hacerlo a través de hojas electrónicas y/o procesadores de texto, siempre y cuando la documentación sea clara y principalmente, sea conocida, difundida y aplicada por todos los involucrados.

Elaboración del DRP

El DRP, plan de recuperación ante desastres, es el ítem más importante en todo este asunto. Se trata de la herramienta a la cual dirigirse al momento de ocurrir algún desastre tecnológico.

Como empresario uno esperaría no tener que usar este plan nunca, pero en caso de que ocurriera algo, este plan podrá marcar la diferencia entre la pérdida del

negocio o su supervivencia. Por eso, es crítico que este plan sea operativo, de manera que sea de suficiente calidad para guiarlo en el momento de crisis.

Un DRP está compuesto de los siguientes elementos:

1. Análisis del entorno
2. Tipos de operación ante un desastre
    a. Operación normal
    b. Operación alternativa
    c. Operación durante el desastre
    d. Operación normal restablecida
3. Valoración de criticidades
4. Determinación de prestaciones mínimas
5. Análisis de riesgos
    a. Matriz de riesgos
    b. Diagrama de riesgos
6. Determinación del nivel de desastre
    a. Desastre total
    b. Desastre parcial
    c. Desastre menor
7. Análisis, selección y presentación de estrategias de recuperación
    a. Descripción de la estrategia
8. Requerimientos para llevar a cabo el DRP
    a. Establecimientos de esquemas técnicos
    b. Conformación de equipos de recuperación
    c. Desarrollo de procedimientos
9. Pruebas y revisión del DRP

A continuación se analiza cada uno de estos componentes:

1. Análisis del entorno

Lo primero que se debe realizar es un análisis del entorno empresarial para determinar el alcance del plan, y esto incluye levantar el inventario de los dispositivos físicos que se desea proteger, para más adelante, y con apoyo de la computación en la nube, determinar cómo recuperar la información. Los elementos que se deben tomar en cuenta, pueden ser:

- Las condiciones físicas del entorno
- Levantamiento de las aplicaciones y servicios existentes
    - ERP
    - CRM
    - Aplicaciones desarrolladas
    - Servicio de correo electrónico
    - Servicio de Internet
- Elementos activos de la red:
    - Servidores de datos
    - Servidores de aplicaciones
    - Servidores de comunicaciones
    - Servidores
    - Switches, ruteadores, etc.
    - Elementos tradicionales de respaldo (cintas, unidades ópticas externas, etc.)

2. Tipos de operación ante un desastre

Ante una emergencia es vital conocer de antemano los diferentes estados por los que atraviesan las operaciones de la empresa. Básicamente la idea es saber cómo se desarrollan las actividades de la Pyme, antes, durante y después de la contingencia. A continuación en la **Ilustración 31** se muestra esta situación:

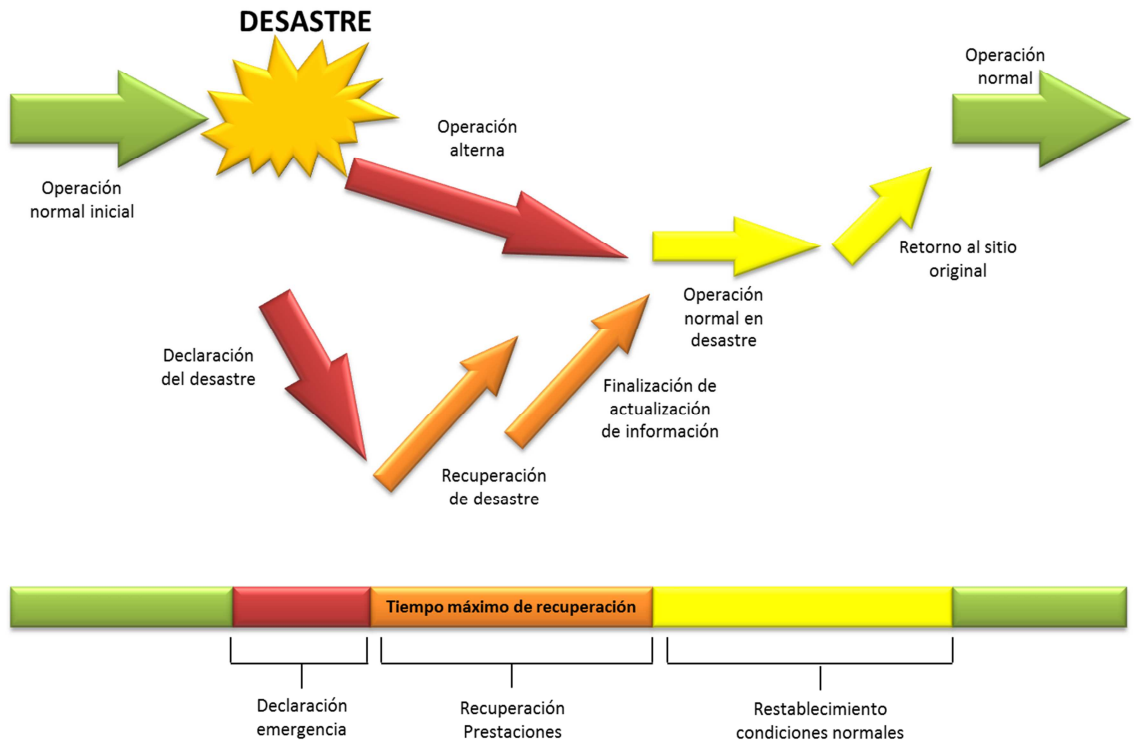


Ilustración 31. **Estados de situación en una recuperación ante desastres**

Fuente: Elaboración del Plan de Recuperación ante Desastres (PRD) – Cidicom. Argentina
Elaborado por: Ing. Danilo Mannella

Los estados principales que se debe considerar son:

- **Operación normal**.- Consiste en la operación que lleva a cabo la Pyme antes de que se presente un desastre. Así mismo, define las condiciones que se deben alcanzar con el DRP mediante la ejecución de este plan.

- **Operación alternativa**.- El momento en que se produce el desastre el personal deberá trabajar de una manera alternativa, hasta que se restablezcan la operación normal, y consecuentemente se generará información que deberá ser almacenada en otros medios distintos a los normales, pero que deberá ser incorporada una vez que se restablezcan operaciones. Esto está asociado al RPO y RTO mencionado anteriormente.

- **Operación durante el desastre**.- El momento que se da la "alarma" de que ha ocurrido un desastre, dependiendo de la severidad del mismo, se disparan una serie de procedimientos que buscan regularizar el restablecimiento de las operaciones, y en este caso la información, que se encuentra en la nube, es aquella a la que accederá el personal de la Pyme, mientras se soluciona el problema ocurrido dentro de la empresa. Una vez que los servicios y aplicaciones de la empresa están en estado de "activo" en la nube los empleados vuelven a trabajar en un estado de "operación normal durante el desastre". El tiempo desde la declaración de la emergencia hasta el restablecimiento de operaciones debe estar dentro de los límites definidos de RTO.

- **Operación normal restablecida**.- Una vez que el problema ha sido resuelto se vuelve a operar en condiciones normales, en donde todas las aplicaciones y servicios se encuentran operando con regularidad en las condiciones en las que se encontraban antes del desastre.

3. Valoración de criticidades

Este siguiente paso, dentro del DRP establece el nivel de criticidad de los activos que se desea proteger. Estos activos se refieren a los equipos, aplicaciones y servicios que son vitales para el funcionamiento del negocio, y sin los cuales se pueden producir pérdidas o incluso el cierre de la empresa.

La criticidad se determina en función del impacto que produciría el contar con determinado equipo, aplicación o servicio y el tiempo máximo permitido de no contar con los mismos debido a la suspensión de sus prestaciones.

En este punto se deben llenar tablas que contengan este análisis, y que se describen a continuación, con ejemplos prácticos:

Tabla de Criticidades – Por Equipos

La siguiente tabla contiene información relativa a 3 servidores (uno de comunicaciones, otro de aplicaciones y otro de datos de la intranet), con distinta tolerancia máxima de pérdida según su utilización e impacto en el negocio.

Cuadro 21. Tabla de criticidades – por equipos

No. Ítem	Equipo	Descripción	Criticidad	Tolerancia máxima	Impacto
1	Srv-comm	- Permite la comunicación y transacciones en línea de la Pyme hacia el Internet	Alta	3 horas	1. Pérdida de transacciones 2. Pérdida de imagen
2	Srv-aplicac	- Permite el manejo de aplicaciones desarrolladas internamente en la empresa para seguimiento de clientes	Media	1 día	1. Pérdida / inconsistencia de información 2. Reprocesamiento de formularios cargados manualmente
3.	Srv-intranet	- Permite la publicación de noticias internas de la empresa	Baja	2 días	1. Demora en actualización de noticias de la empresa

Fuente: Elaboración del Plan de Recuperación ante Desastres (PRD) – Cidicom. Argentina
Elaborado por: Ing. Danilo Mannella

En el ejemplo anterior se puede apreciar que el equipo de comunicaciones, debido a las prestaciones que ofrece, tiene un nivel de criticidad alto comparado con los otros servidores, y por tanto se debe enfocar mayor atención al momento de definir la estrategia apropiada dentro de la recuperación ante desastres.

Tabla de criticidades – Por Servicios

En el siguiente ejemplo se analiza el impacto y criticidad desde el punto de vista de servicios prestados a la Pyme, tomando al archivo de datos y correo electrónico como servicios ofrecidos a todos los empleados de la Pyme.

Cuadro 22. Tabla de criticidades – por servicios

No. Ítem	Servicio	Criticidad	Período crítico	Alternativa	Tolerancia máxima	Usuarios involucrados
1	Almacenamiento de archivos	Media	Cierre a fin de mes	- Guardar archivos localmente	1 semana	Todos
2	Correo electrónico	Alta	Todos los días	- Toma de pedidos telefónicos o por fax	1 día	Compras, Ventas, Despacho

Fuente: Elaboración del Plan de Recuperación ante Desastres (PRD) – Cidicom. Argentina
Elaborado por: Ing. Danilo Mannella

En este ejemplo se puede ver que, si bien ambos servicios son importantes dentro de la Pyme, el servicio de correo electrónico es más crítico, y la tolerancia máxima permitida debe ser menor que aquella del servicio de almacenamiento de archivos. Todo esto hay que tomar en cuenta al establecer el RTO y RPO.

4. Determinación de prestaciones mínimas

A través de distintas técnicas, tales como entrevistas a miembros de las principales unidades de negocio se debe recabar la información acerca de cuáles son

las aplicaciones, servicios o prestaciones mínimas que se considera críticas de proteger para que pueda funcionar el negocio, y que deberán ser recuperadas de manera prioritaria al momento de presentarse un desastre tecnológico, de forma que se pueda preservar la continuidad del negocio. Asociado a esto, como siempre, está el tiempo máximo para recuperar estas prestaciones.

5. Análisis de riesgos

Tal y como se mencionó en el Paso 1 de esta guía (Análisis de riesgos y BIA), hay que efectuar un análisis de riesgos e impacto en el negocio. Hay que determinar qué riesgos se pueden mitigar, cuáles se pueden transferir y cuáles se deben asumir.

En tecnología, al igual que en otras áreas en las cuáles existe gestión de riesgos se sabe que los riesgos no se eliminan, sino que se gestionan, y dado que no es posible eliminarlos hay que buscar la manera de *mitigarlos*, es decir de buscando medidas para reducir su impacto; se los puede *transferir*, y esto se refiere a que la responsabilidad se la cede a otra persona u organización, o finalmente se lo *asume*, y esto involucra que se va a correr el riesgo con las consecuencias que esto pueda acarrear.

Los riesgos pueden ser de tipo tecnológicos, si afectan aspectos técnicos del entorno, tales como el deterioro de los equipos, indisponibilidad de recursos, etc. o funcionales, si – tal y como su nombre lo indica – afecta aspectos funcionales del entorno, tales como falta de precaución por parte de usuarios al no modificar su contraseña establecida por omisión, o lo que se conoce como ingeniería social.

Los riesgos son inherentes a cualquier actividad humana, y en el caso de la tecnología de las Pymes, esto es independiente de la infraestructura tecnológica (servidores, cableado, cortafuegos, IPS, IDS, etc.), o aplicaciones usadas para evitar intrusión por parte de terceras personas que deseen afectar los negocios o la reputación de la empresa. No hay que olvidar que un BIA consiste en un análisis de

los impactos que pueden tener los negocios en el caso de incurrir en cualquier tipo de riesgo, y que su relevancia está dada por la criticidad de no contar con un servicio o aplicación para el normal desenvolvimiento del negocio.

Un par de términos que los dueños deben conocer, y están relacionados con los riesgos de seguridad informática son las amenazas y las vulnerabilidades:

- Las **amenazas** se refieren a toda acción o evento que puede afectar la seguridad, en pocas palabras, las amenazas son violaciones potenciales de seguridad.

- Las **vulnerabilidades** no son otra cosa que la existencia de una debilidad, diseño o error de implementación que puede conducir a un evento no deseado o esperado, que compromete la seguridad del sistema.

Con todo lo anterior es importante destacar, para el DRP, que existe una relación entre los diferentes tipos de desastres, su probabilidad de ocurrencia y el impacto en el negocio que puede causar un determinado riesgo que se desea mitigar, transferir o asumir.

Aquellos riesgos que presentan una probabilidad de ocurrencia no despreciables están relacionados con factores que van desde aspectos climáticos o meteorológicos hasta factores humanos de la Pyme.

Un método usualmente utilizado para medir el riesgo puede ser un diagrama de probabilidad vs. Impacto del riesgo, tal y como se muestra a continuación en la **Ilustración 32**:

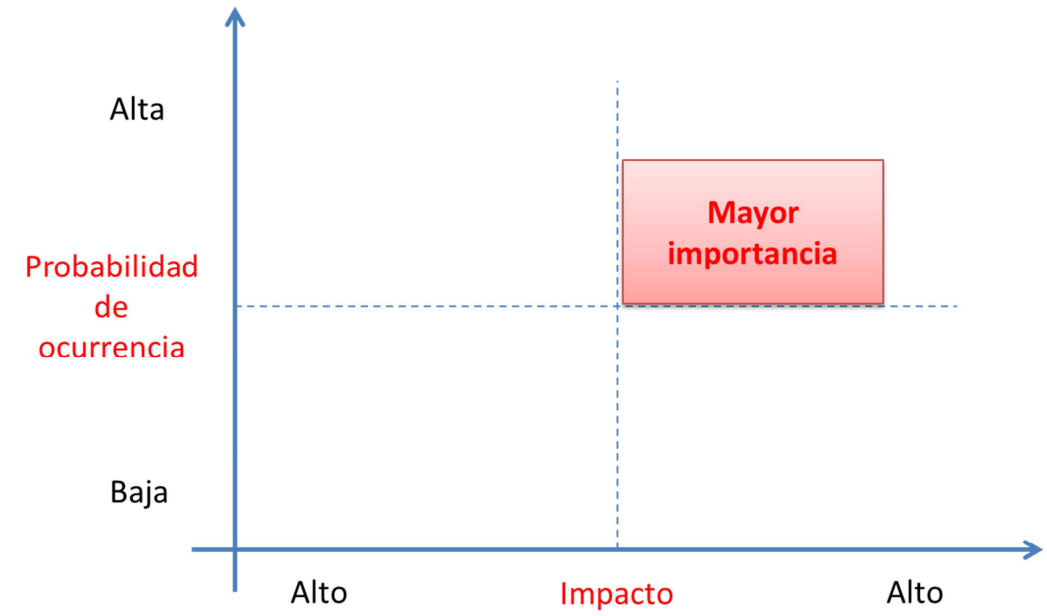


Ilustración 32. **Diagrama de probabilidad de ocurrencia versus impacto en el negocio**

Fuente: Elaboración del Plan de Recuperación ante Desastres (PRD) – Cidicom. Argentina
Elaborado por: Ing. Danilo Mannella

Independientemente de la técnica utilizada lo imprescindible en el análisis de riesgos, que debe efectuarse en todos las áreas de la empresa, para determinar los requerimientos de seguridad del sistema objetivo y las prioridades que se desprendan de esta información. Usualmente a través de entrevistas se puede lograr recabar esta información por parte de los usuarios.

Matriz de riesgos

Un documento que ayuda a la formalización del análisis de riesgos es la **Matriz de riesgos**, que toma en cuenta la amenaza, la valoración del riesgo, la criticidad, la ocurrencia y el impacto. En el siguiente cuadro queda explicado esto con más claridad:

Cuadro 23. Matriz de riesgos

No.	Amenaza	Riesgo	Criticidad	P (ocurrencia)	Impacto
1	Existencia de material inflamable en el cuarto	Fuego en el Data Center	Alta	0.5	Destrucción de equipos y espacio físico

No.	Amenaza	Riesgo	Criticidad	P (ocurrencia)	Impacto
	de servidores				
2	Ubicación física en zona inundable	Inundación	Media	0.1	Posibles cortocircuitos, equipos quemados
3	Falta de mantenimiento de los equipos servidores	Fallas en los equipos	Media	0.5	Indisponibilidad de los servicios
4	Exposición de los equipos a personal no autorizado	Actos de vandalismo	Alta	0.1	Pérdida de equipos y/o información, negación de servicios, pérdida de confiabilidad, mala reputación
5	Administración de los equipos por personal no autorizado	Errores humanos no intencionados	Baja	0.5	Indisponibilidad de los servicios, pérdida de datos
6	Falta de mantenimiento en central eléctrica o UPS	Corte de suministro eléctricos	Media	0.7	Indisponibilidad de los servicios, pérdida de datos
7	Exposición de los equipos a terceros	Actos de sabotaje o robo de información	Alta	0.5	Pérdida de confiabilidad, pérdida de información

Fuente: Elaboración del Plan de Recuperación ante Desastres (PRD) – Cidicom. Argentina
Elaborado por: Ing. Danilo Mannella

Diagrama de riesgos

Otra herramienta que es de utilidad, y que está relacionada con la anterior es el Diagrama de riesgos, en donde de una forma visual se esquematiza el impacto que tiene el riesgo en función de la probabilidad de ocurrencia.

Cuanto mayor sea el impacto y la probabilidad de ocurrencia, mayores deberán ser los controles que se deban aplicar para mitigar el riesgo. Los riesgos más altos, por ende, deberán ser gestionados en primer lugar, tomando en cuenta que los riesgos a ser considerados en el DRP son aquellos que presentan una probabilidad de ocurrencia que no sean despreciables.

6. Determinación del nivel de desastre

Existen 3 tipos o niveles de desastres de los cuales hay que recuperarse en caso de producirse en cualquier organización, y en la Pyme en particular. Estos son:

1. **Desastre total**.- Ocurre en el caso en el que el lugar físico no pueda estar disponible dentro del tiempo máximo permitido para la interrupción de la prestación de servicios, o que el tiempo de restablecimiento de las operaciones normales sea mayor al tiempo permitido máximo aceptable.

2. **Desastre parcial**.- En el caso en el que los equipos hayan sufrido daños menores y cuyo funcionamiento o prestación de servicios sea realizados por equipos alternos ubicados en la misma empresa y se requiera de la intervención del departamento de TI de la empresa o de una tercera empresa pero en un tiempo razonable, de acuerdo al RTO establecido.

3. **Desastre menor**.- Esto se da en el caso en el cual los equipos presenten desperfectos que se puedan solucionar a través de la reinstalación o reconfiguración de los mismos, y consecuentemente no sea necesaria la intervención de una tercera empresa externa.

En el caso de este DRP, que usa como mecanismo a la computación en la nube, se puede aplicar tanto para los desastres totales como para desastres parciales, tomando en cuenta las políticas de seguridad informáticas definidas y el alcance del contrato con el proveedor de servicios en la nube, pero de esto se tratará en los siguientes capítulos.

7. Análisis, selección y presentación de estrategias de recuperación

Con todos los antecedentes de este DRP evaluados anteriormente, es fundamental tener claro que el tipo de recuperación ante desastres que suministrará el proveedor de servicios en la nube será orientado a desastres totales (del centro de datos) y/o parciales (de determinados equipos) de la Pyme, por lo tanto, y como se

verá en el Paso 6, la selección del proveedor de servicios debe ser ajustado a las necesidades del negocio, y tomando en cuenta la realidad tecnológica y económica de la Pyme.

Dado que la estrategia en sí de recuperación ante desastres tecnológicos está enfocado en la utilización de la computación en la nube lo siguiente que se debe aclarar es que la mitigación de los riesgos serán llevados a cabo con la tecnología y experiencia del proveedor de servicios de la nube, aunque es fundamental recordar que el punto débil y con el cual se deberá lidiar es el tener un buen enlace de comunicaciones y suficiente ancho de banda para poder acceder a los datos que están en la nube, es decir, que no solamente es importante el proveedor de servicios en la nube sino también el ISP (Proveedor de Servicios de Internet). De ser posible se debería asegurar un enlace de comunicaciones de respaldo, con la misma u otra empresa, para posibilitar que el acceso a la red de Internet sea permanente.

Descripción de la estrategia

Para la eficaz recuperación del entorno luego de un desastre, la Pyme deberá considerar los pasos anteriores y el alcance de este plan. En muchos casos la implementación del DRP se lo hace por etapas:

- Comenzando con los servidores de datos
- Pasando por los servidores de correo electrónico (si es que aplica)
- Posteriormente se procede con los servidores de aplicaciones
- Luego las comunicaciones, y
- Finalmente el centro de datos como tal.

Hay que recordar que existen empresas que, dado que su tamaño es pequeño deciden implementar el DRP en una sola etapa, más aun considerando las opciones de virtualización que se ofrecen hoy en día, y que se detalló en el Paso 3, considerando los beneficios en costo, tiempo y productividad, que ahí se mencionaron.

En la descripción de la estrategia del DRP se debe tener claro las siguientes medidas:

1. Conformación del Equipo de Recuperación ante Desastres.
2. Recuperación de las prestaciones de servicios conforme los acuerdos firmados con el proveedor de servicios en la nube.
3. Exigencia del cumplimiento de los tiempos de respuesta especificados en el SLA con el proveedor de servicios en la nube.

8. Requerimientos para llevar a cabo el DRP

Los requerimientos que se mencionan a continuación constituyen las principales características y condiciones que debe cumplir el DRP, de manera que puedan ser utilizados en procedimientos de mantenimiento e incluso auditoría.

Estos documentos establecen las condiciones de:

- Características que debe presentar el proveedor de servicios en la nube respecto de la infraestructura requerida para la recuperación ante desastres
- Miembros del equipo de recuperación ante desastres, tanto en lo administrativo como técnico

Establecimientos de esquemas técnicos

Los esquemas técnicos definen los pasos generales a seguir en la parte operativa para la ejecución de una determinada tarea. Para esto, se debe tener el conocimiento técnico de la tarea que se está ejecutando y tiene por objetivo brindar un marco integral de rápida referencia. Todas estas tareas deben estar predefinidas y documentadas al momento de enfrentar una recuperación ante desastres. Si la Pyme no contara con una persona o departamento técnico de TI, podrá contratar un consultor externo para contribuir con esta tarea.

Algunos de los esquemas que se deben desarrollar son:

1. Contacto con el proveedor de servicios en la nube
2. Recuperación de equipos
3. Restablecimiento de servidores
4. Restablecimientos de aplicaciones y bases de datos
5. Ejemplos de notificación de emergencia al resto de la empresa

Conformación de equipos de recuperación

La conformación de los equipos de recuperación tiene como finalidad determinar y asignar distintas responsabilidades con el fin de obtener una exitosa recuperación ante desastres de acuerdo al DRP establecido.

Para lograr lo anterior se deben establecer roles y responsabilidades de las personas que componen este equipo, lo cual incluye:

- Definir las medidas preventivas necesarias y factibles de aplicar, de manera que se disminuya de algún modo la probabilidad de ocurrencia de los desastres.

- Definir, probar, ajustar y mantener actualizado el DRP
- Ante un desastre que afecte el centro de datos debe:
    - Recuperar las prestaciones en el menor tiempo posible, y dentro del RTO establecido
    - Restablecer la operatividad del negocio a como estaba antes del desastre
    - Analizar las causas que produjeron el desastre, y documentarlo a través de un informe formal, en donde se indique cómo se procedió, y con ello modificar las medidas preventivas y el plan de recuperación de acuerdo a las conclusiones a las que se haya llegado.

El equipo de recuperación está conformado por:

- Equipo de dirección estratégica y coordinación
- Equipo de recuperación técnica
- Equipo de comunicación a usuarios

Obviamente, cada equipo tiene ciertas responsabilidades que llevar a cabo, y dependiendo del tamaño y estructura de la Pyme puede estas responsabilidades pueden recaer en una o varias personas del departamento de TI, si lo hubiera, de lo contrario se procedería a contactar a la empresa tercerizada encargada de la gestión de TI en la empresa. A continuación se detalla las responsabilidades de cada equipo:

<u>Equipo de dirección estratégica y coordinación</u>

- Dirigir y coordinar las actividades del resto de equipos

- Efectuar las declaraciones del estado del desastre (emergencia, contingencia y restablecimiento de actividades)
- Determinar el nivel de desastre (total, parcial o menor)
- Elaborar el DRP
- Controlar la ejecución del DRP y realizar los ajustes de acuerdo a las novedades encontradas en la aplicación del mismo
- Interactuar con el equipo de recuperación técnica para la resolución de contingencias físicas del centro de datos

Es importante recordar que quien preside este equipo debe ser alguien de la alta gerencia.

Equipo de recuperación técnica

- Identificar los elementos de HW que hayan sido dañados a causa de un desastre
- Coordinar con los proveedores de HW el cumplimiento de los contratos mantenimiento, garantía y niveles de soporte
- Verificar el correcto funcionamiento de los dispositivos de HW que hayan sido reemplazados o restaurados por los proveedores
- Verificar que la información almacenada en la máquina virtual del proveedor de servicios en la nube se reinstale correctamente en los servidores de la empresa.
- Identificar los elementos de comunicaciones que hayan sido dañados por el desastre
- Detectar los problemas de conectividad de los equipos del centro de datos y determinar sus causas

- Verificar el correcto funcionamiento de los elementos de comunicaciones y conectividad general para que los usuarios puedan acceder a los recursos del centro de datos.

Equipo de comunicación a usuarios

- Efectuar las comunicaciones oficiales a los stakeholders ante un desastre (antes, durante y después del mismo).
- Realizar las comunicaciones a los usuarios internos.

Desarrollo de procedimientos

Si bien el alcance del DRP es importante se debe desarrollar los procedimientos que ayuden a alcanzar el restablecimiento de las condiciones normales del entorno de TI de la Pyme, y los principales procedimientos a definir son:

1. **Declaración de la emergencia**.- Abarca desde la detección del desastre hasta que el mismo es comunicado a los afectados. En este punto únicamente se evalúan los daños causados

2. **Recuperación de las prestaciones**.- Consta del diseño y ejecución del DRP conforme a lo acontecido en el desastre, junto con el ajuste del mismo cuando aparezcan imprevistos que puedan modificar el plan inicialmente armado.

3. **Restablecimiento de las operaciones normales**.- Consiste en el diseño y ejecución del restablecimiento de las condiciones normales de operación, y que culmina con el análisis de la situación ocurrida a fin de ajustar el DRP

en función de los errores, demoras e inconvenientes acontecidos, así como la posible toma de nuevas medidas preventivas.

9. Pruebas y revisión del DRP

Una de las últimas fases, y que de hecho resulta en una medida preventiva, dentro de la elaboración del DRP es la de pruebas. El plan debe ser probado en su totalidad al menos una vez al año, de acuerdo a las mejores prácticas y estándares internacionales, y probado parcialmente en distintas oportunidades mediante un esquema continuo de mejoras y revisión, que contribuyan al mantenimiento vigente del plan a lo largo del tiempo.

El DRP debe ser revisado con regularidad para garantizar su adecuación a los cambios que sufre el entorno, manteniendo vigente su aplicabilidad frente a desastres.

Tanto en las pruebas y revisión del DRP cuanto en su aplicación en un evento disruptivo verdadero, las Pymes deberán coordinar con el proveedor de servicios en la nube para que las aplicaciones y datos se recuperen en máquinas virtuales que pasarán a estar activas al momento del desastre. Por eso es importante seleccionar al proveedor más adecuado, particular que se verá en el siguiente, y último paso.

4.1.4.7 Paso 6: Seleccionar el proveedor de soluciones – implementación de la solución con proveedores reales

La selección de un proveedor de soluciones para recuperación ante desastres no siempre es fácil, y hay que tener mucho cuidado con aquellas empresas que presionan sobre la adquisición de determinado hardware, sistema operativo u otras opciones limitadas que no se alineen bien con las necesidades del entorno de la Pyme. Se recomienda estudiar el nivel de experiencia requerido por parte de su equipo para mantener la solución o la cantidad de recursos que se necesita adquirir. Es vital

asegurarse que con el proveedor se puedan efectuar pruebas de la solución antes de que suceda un desastre real.

Finalmente, hay que recordar que los acuerdos firmados en el SLA se cumplan y estén a nivel de detalle que sea fácil de comprender e implementar, con expectativas reales de cumplimiento.

A continuación se mencionan 10 aspectos a tomar en cuenta antes de seleccionar a un proveedor en la nube que pueda ayudar a la migración de servicios, como los de recuperación ante desastres tecnológicos:

1. **Experiencia técnica**.- Un servicio de computación en la nube no es una comodidad, y no se tan simple como proveer de una computadora que acceda a una *granja de servidores*. Requiere de una gran cantidad de experiencia técnica para configurar el sistema apropiado que garantice a las empresas de seguridad para sus datos y que pueda ejecutar sus negocios sin interrupciones. Por tanto, lo primero en lo que se debe fijar la Pyme que busca un proveedor es la calidad del equipo de trabajo y su habilidad técnica.

2. **Confianza**.- Las Pymes que deseen migrar sus datos en un proveedor externo, como parte de su plan de recuperación ante desastres deben poder confiar en él. Es importante efectuar una serie de entrevistas para determinar si se puede confiar en el equipo del proveedor para depositar su información corporativa confidencial. Hay que preguntar por referencias y testimonios de otros clientes. Se sugiere hacer una investigación completa de la trayectoria del vendedor antes de entregarles sus datos. También se puede indagar si tienen membresías y acreditaciones en la industria.

3. **Garantía de tiempo de actividad**.- Dado que las Pymes confiarán su información a un proveedor externo en la recuperación ante desastres es importante solicitar al proveedor acerca de cuál es su compromiso en la garantía de tiempo de actividad (*uptime*, en inglés) para con la empresa, pues el servidor que servirá de respaldo no puede estar con los servicios abajo por horas en medio de un desastre. De ser posible hay que averiguar con otros clientes del proveedor acerca de cortes previos, y cuánto tiempo les tomó restablecer los servicios.

4. **Herramientas disponibles**.- ¿Tiene el proveedor un buen conjunto de herramientas para ayudarlo a monitorear el estado de sus datos, estadísticas, seguridad, etc.? Un buen conjunto de herramientas le puede ayudar a la Pyme a reducir sus costos en operaciones del personal de TI.

5. **Facilidad de migración**.- ¿Qué tan fácil es el proceso de migración hacia la nube? Tomando en cuenta que la Pyme efectuará un respaldo de su información en la nube, qué tan fácil o doloroso es la migración de esta información hacia la nube, es lo que hay que aclarar con el proveedor. Lo ideal es que se cuente con herramientas y técnicas que puedan hacer lo menos complicado posible esta migración.

6. **Garantía de rendimiento**.- Del mismo modo en que el tiempo de actividad es importante así mismo lo son las métricas de rendimiento. Hay que preguntar al proveedor – o averiguar de algún modo – acerca de los servidores que usan, la velocidad de acceso del disco, el tipo de procesador, uso de ancho de banda y la disponibilidad de uso de tecnología de punta, tal y como los discos de estado sólidos (SSD).

7. **Soporte al cliente**.- Las Pymes que incurrirán en la nube pondrán toda su confianza en el proveedor, pero ¿qué sucede si el servidor local colapsa al inicio del día debido a un malware o alguna aplicación mal configurada, o a un problema físico?, ¿se puede recurrir al proveedor en la nube lo antes posible? El soporte técnico es un factor crítico, y es importante que el proveedor pueda asistirlo en un esquema 24x7x365. Si el soporte no es el adecuado, se gastará un montón de dinero y esfuerzo con el equipo de TI interno, si es que lo hay. En muchas ocasiones el proveedor apoya a la Pyme en el ciclo de vida de la recuperación ante desastres.

8. **Seguridad**.-La seguridad es un tópico de alta prioridad al momento de seleccionar el proveedor de servicios en la nube. Hay que preguntarles acerca de las técnicas y pasos que toman para asegurar los datos y aplicaciones de la empresa.

9. **Cumplimiento con auditorías externas**.- Un aspecto que resulta importante, aunque en muchos casos no prioritario, es conocer si el proveedor de la nube ha tenido auditorías de cumplimiento. Existen organismos que acreditan a un proveedor en la nube como apto de acuerdo a normas internacionales.

10. **Costo**.-Finalmente, siempre se trata de costo. Hay que verificar todos los importes (aquellos que se pagan por una sola vez, costos mensuales, cuotas de uso, etc.) y estar claros que estén especificados en el contrato.

De todos los criterios antes mencionados, en el caso de las Pymes es importante no solamente considerar el costo, sino sobretodo la seguridad y confiabilidad.

4.1.5 Mejores prácticas

Las mejores prácticas consisten en un conjunto de acciones, técnicas o métodos, y en algunos casos estándares, que han sido llevados a cabo con éxito – y en muchos casos superando las expectativas – en algunas empresas, y que se recomiendan para su uso en otras empresas con características similares: en pocas palabras, lo que funciona para determinadas empresas se puede adoptar en nuestra propia empresa. A continuación se mencionan algunas “mejores prácticas” para la implementación del DRP en la nube.

1. **Virtualizar**.- Los entornos virtuales son más ágiles y fáciles de migrar. La virtualización esconde la complejidad de un sistema al proteger los componentes individuales y movimiento de partes, y de este modo simplificando el planeamiento e incrementando la visibilidad en el proceso de recuperación de desastres. Permite también usar la replicación basada en hipervisores que es mucho más flexible que la replicación basada en almacenamiento.

2. **Automatizar**.- Hay que evitar, lo más posible, que los errores humanos se interpongan en la recuperación ante desastres. Se debe usar planes de recuperación automáticos en lugar de una pila de notas a mano. Con una automatización apropiada, un plan de recuperación puede ser hecho en unos pocos minutos, en lugar de semanas. La automatización protege a los usuarios de tener que gestionar muchos de los pasos de la recuperación, y

coordinar automáticamente actividades tales como la preconfiguración de las redes y máquinas virtuales, configurar la infraestructura de recuperación, y reiniciar las aplicaciones.

3. **Verificar y probar**.- Se debe probar el plan de recuperación ante desastres a menudo. Hay que usar pruebas que no afecten los planes de recuperación y *failback*. Se debe estudiar los reportados detallados de los resultados de las pruebas, lo cual incluye el cumplimiento del RTO. Con esta información se puede tener la confianza de que el plan de protección contra desastres cumple con los objetivos del negocio. Así mismo provee del entrenamiento necesario al personal y muestra cualquier posible inconveniente de manera temprana, de forma que pueda ser manejado apropiadamente.

4. **Alcanzar metas logrables**.- Una recuperación ante desastres automatizado puede ser muy poderoso, pero no se trata de magia. Por ejemplo, 100 máquinas virtuales que contengan servidores de correo electrónico (p. ej. MS Exchange), o servidores de bases de datos (p. ej. Oracle), ERPs u otros no pueden ser restaurados y puestos en funcionamiento en 30 minutos. Hay que establecer el RTO de manera realista. Para establecer una línea base, hay que ejecutar pruebas bajo diferentes condiciones y ver qué resultados se obtienen.

5. **Anticipar**.-Si se tienen advertencias, hay que tomarlas en cuenta. Se debe actuar tempranamente para ejecutar el plan de recuperación ante desastres que ha sido probado anteriormente antes de que un desastre real se produzca, para impedir un evento de desastres del todo. La confianza que

debe tener el área de TI se basa en un plan de recuperación de desastres sólido que ha sido probado. Un ejemplo de esto puede ser la amenaza de un corte de electricidad en la red.

6. **Ser proactivo cuando se presente el riesgo**.- La mayoría de cortes de servicio no son causados por desastres en sí, sino por procedimientos planeados mal ejecutados. Por ejemplo, actualizaciones de SW o de red, mantenimiento de datos, reparación de infraestructura, etc. Al efectuar un respaldo de aplicaciones críticas en la nube, de manera progresiva, se puede mitigar el riesgo y reducir enormemente una posibilidad de corte o degradación de servicios.

7. **Asignar responsabilidades**.- Se debe asignar una tarea específica a cada una de las personas involucradas en el DRP. No hay que esperar que el personal relevante esté en el sitio del desastre o que tome el control de la situación inmediatamente. Es importante implementar un respaldo o redundancia no solo de los datos, sino también de las personas.

8. **Mantener la información restaurada lo más actualizada posible**.- Es una buena práctica efectuar un respaldo de toda la información crítica una sola vez, aunque esto conlleve un poco de tiempo, dinero y esfuerzo, pues en adelante solo se actualizará aquella información que ha sido modificada, y no todos los datos. Esto permitirá que se enfoque en adelante solamente en los cambios de la información crítica, y podrá cumplirse el RTO con menos esfuerzo.

9. **Prepararse para los fallos**.- Hay que crear y probar un plan de recuperación ante desastres en un ambiente de pruebas lo más real posible. Hay que estar de acuerdo, al interior de la empresa, respecto de cuándo se ha terminado la alerta, de manera que el negocio pueda volver a la normalidad.

10. **Optimizar recursos en el DR**.- El uso de SaaS (software como servicio) o IaaS (infraestructura como servicio) es solamente una parte de lo que se puede lograr para el plan de recuperación ante desastres, sin embargo existen otras alternativas que pueden verse como medios no técnico y que pueden ayudar, esto incluye el uso de UPS, generadores de energía eléctrica, mejor protección ante incendios, entre otras.

4.1.6 Estrategias para la utilización de la guía

Para que esta guía propuesta sea efectiva se recomienda **ser riguroso con las etapas planteadas en el fondo más que en la forma**. Debido a que cada Pyme sigue ciertos estándares particulares, el presente documento no pretende ser una "camisa de fuerza" sobre la cual deberán regirse, sino que queda a criterio de cada negocio adaptar de la mejor manera posible a la realidad de cada una.

Como se mencionó en el párrafo anterior la realidad de cada Pyme es distinta, y si bien lo óptimo es que cada Pyme incursione en la nube con un modelo en el cual pueda aplicar su DRP en un 100% en la nube se sugiere que se siga los siguientes lineamientos para no crear falsas expectativas, y para que el negocio como tal vaya escalando de acuerdo a sus necesidades y posibilidades económicas, tomando en cuenta la priorización de información que deberá ser respaldada en la nube, luego de haber pasado por las etapas mencionadas en el capítulo anterior.

4.2 Guía de implementación para Mipymes

4.2.1 Introducción

Las Pymes a nivel mundial, tal y como se mostró en la fundamentación teórica en el Capítulo II, y particularmente las Pymes a nivel nacional y local, conforme se pudo evaluar en el capítulo anterior, no se encuentran preparadas para afrontar un desastre tecnológico en sus empresas o actúan de manera reactiva cuando es demasiado tarde, o no dimensionan las pérdidas a las que se pueden enfrentar ante tales eventos, a pesar de que son conscientes de la necesidad de contar con un DRP (Plan de Recuperación ante Desastres, por sus siglas en inglés) que les permita mitigar los riesgos a los que se pueden enfrentar, ya sean éstos desde ataques maliciosos producidos por malware hasta cortes de electricidad o fallos en los discos duros de sus servidores, pasando por catástrofes climáticas.

La presente guía de implementación permitirá ofrecer a los gerentes de las Mipymes (micro, pequeñas y medianas empresas) una visión acerca de los pasos que deben tomar en consideración para implementar un DRP que coadyuve a minimizar los impactos de una pérdida en la productividad, estabilidad y reputación de las empresas, tomando en cuenta que los esquemas tradicionales de recuperación ante desastres no son los más idóneos, y que incursionar en la computación en la nube, a través de un proveedor que ofrezca un servicio para enfrentar los desastres tecnológicos, a un precio razonable, es la solución que mejor satisface a la Mipyme en el largo, mediano e incluso corto plazo.

4.2.2 Descripción general de la guía

Esta guía, que tiene un enfoque para Mipymes, se encuentra estructurada de forma tal que sea fácilmente comprensible para el gerente, o dueño de una Mipyme, o que en su defecto se la pueda transmitir al Gerente de Tecnología Informática, o a una

tercera empresa, de manera que le resulte sencillo transmitir sus requerimientos al proveedor de servicios en la nube.

La guía está dividida en una secuencia de pasos, en donde se puede revisar tanto la parte gerencial como la parte técnica, a grosso modo, y con ello que la guía sea lo suficientemente flexible como para que cada Mipyme pueda seguir a su propio ritmo esta implementación.

4.2.3 Características

La guía poseerá 5 características, tal y como se muestra en la **Ilustración 33**:

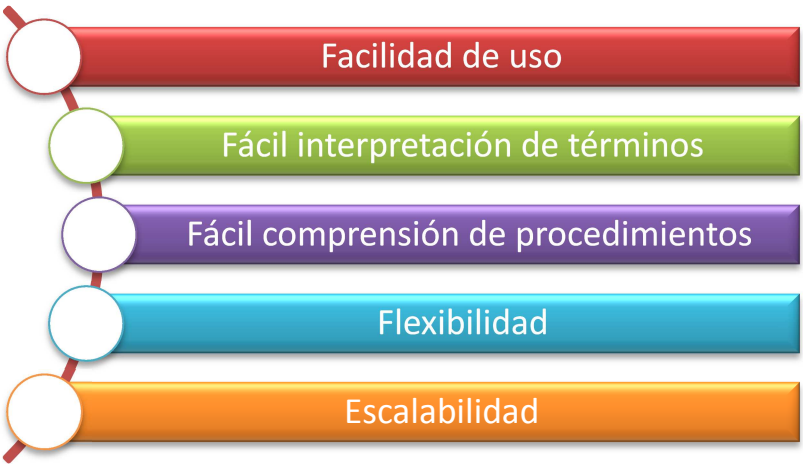


Ilustración 33. **Resumen de características de la guía para Mipymes**

Elaborado por: Danilo Mannella L.

- **Facilidad de uso**.- Aun cuando la guía está orientada al área técnica, será de fácil comprensión para los gerentes empresariales, quienes podrán darle seguimiento a los procesos que se deban efectuar para llevar a cabo tanto el DRP como su implementación en la nube.

- **Fácil interpretación de términos**.- La guía permitirá a los dueños de Mipymes y a los encargados de TI, una fácil interpretación de los términos

usados tanto para la elaboración de un DRP como del conocimiento de la terminología usada en la computación en la nube.

- **Fácil comprensión de procedimientos**.- Tanto los altos directivos como el personal técnico de TI de las Mipymes podrán comprender de manera sencilla los procedimientos que se deban emprender para poder implementar esta guía.

- **Flexibilidad**.- La idea de esta guía es que sea adaptable a la circunstancia de cada Mipyme y no se transforme en una *receta* o *camisa de fuerza*, sino que se vaya acoplando a la situación específica de cada negocio.

- **Escalabilidad**.- De igual manera, la guía a ser propuesta será escalable, y con esto nos referimos a que cada Mipyme irá implementando su DRP en la nube en una transición que puede ir desde tener una solución local – o en sus instalaciones – pasando por una solución híbrida, es decir, con parte de su DRP implementado localmente y otra en la nube, y eventualmente tener todo en la nube.

4.2.4 Secuencia de pasos

4.2.4.1 Introducción

Las microempresas son el motor de la economía de cualquier país, y más aún en la ecuatoriana. Su capacidad para beneficiarse de la tecnología es enorme, tomando en cuenta que puede proporcionarle innovación, expandir sus horizontes desde un mercado local a uno global, o simplemente proveerle de maneras para hacer mejor las cosas.

Lamentablemente la tecnología no siempre es tomada en cuenta en este tipo de empresas. Sus hermanas mayores, las grandes empresas invierten una enorme cantidad de tiempo y energías en seguridad de la información, y esto se debe a que tienen mucho que proteger: bases de datos de clientes, propiedad intelectual invaluable, inversiones de negocios, etc. Las microempresas también tienen activos que proteger, pero la diferencia entre estas últimas y las primeras es que las microempresas no están en muchos de los casos en posibilidades económicas de invertir en programas de seguridad informática, y de recuperarse de una brecha de seguridad. Tener seguridad para una microempresa puede ser incluso más importante que para una grande, por cuanto en descuido en la misma pudiera provocarle daños graves de toda índole (económicos, legales, etc.) incluyendo el cierre de la empresa.

Muchas microempresas se enfrentan constantemente a presiones de mantener bajos los costos y los servicios siempre operativos, los desafíos son varios: Sus clientes esperan que sus servicios estén disponibles 24x7x365 (24 horas del día, los 7 días de la semana y los 365 días del año) y sin pérdidas de datos. Concurrentemente el crecimiento de datos cada vez es exponencial, los ambientes son cada vez más heterogéneos y complejos. Incluso un simple corte de electricidad por tiempo extendido puede provocar daños en los ingresos de la compañía – y eso sin mencionar la reputación y marca de la empresa.

Por todo lo anterior, la necesidad de elaborar un plan de recuperación ante desastres que asegure que los servicios tecnológicos se lleven a cabo ininterrumpidamente con una pérdida mínima de datos no es ni fácil ni barata. Los métodos tradicionales de recuperación ante desastres obligan a escoger entre costo y velocidad, dejando que muchas aplicaciones de las microempresas queden desprotegidas. Ejecutar planes de recuperación ante desastres tecnológicos usando la computación en la nube ofrece a las empresas de cualquier tamaño, y a las

microempresas en particular, una alternativa que les permita una rápida recuperación y con una mínima pérdida de datos, y a un costo asequible.

La presente guía dará a conocer los pasos que deben seguir las microempresas de manera que conozcan qué información deben respaldar y restaurar cuando se produzca un evento no deseado, así como las características de la computación en la nube, a través de la cual podrán implementar un plan de recuperación ante desastres adecuado para la realidad de su negocio.

4.2.4.2 Alcance de la guía

La presente guía tiene como finalidad que las microempresas puedan evaluar de manera general la información que consideren crítica y tengan una alternativa para respaldar y restaurar su información con una pérdida mínima de información y optimizando los costos de una inversión de una solución de computación en la nube, sin embargo aquí se no se efectúa un análisis minucioso sobre las características de medios tradicionales de respaldos.

Es importante destacar que cuando se habla de recuperación ante desastres generalmente se hace alusión a incidentes provocados por la naturaleza (terremotos, inundaciones, incendios, etc.) y a aquellos provocados por fallas en los sistemas informáticos (corte de electricidad, fallas en los equipos, etc.) y los que son provocados intencionalmente por el hombre (sabotaje, robo de información, difusión de malware, etc.). En esta guía se prescindirá de los desastres naturales y se enfocará en los otros dos casos.

Muchos autores destacan una serie de análisis respecto de las bondades de diversos mecanismos para llevar a cabo un plan de recuperación ante desastres, en el caso de esta guía se dejará de lado los métodos tradicionales para enfocarse exclusivamente en aquellos provistos por la computación en la nube.

Así mismo se sugerirán los nombres de algunas empresas que pueden ser usados para seguir esta guía, pero esto no implica que sean los únicos ni que sean necesariamente los mejores.

4.2.4.3 ¿Por dónde empezar?

Previamente a elaborar un DRP es importante tomar en cuenta los siguientes 6 aspectos mostrados en la **Ilustración 34**, que ayudarán en gran medida para que esta guía sea útil y práctica:

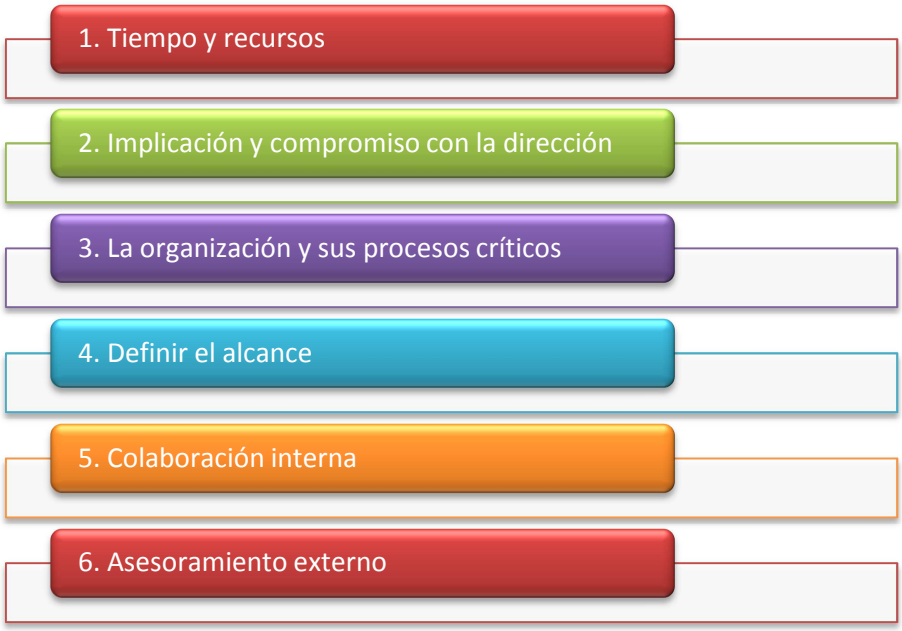


***Ilustración 34*. Resumen de aspectos a considerar por las Mipymes antes previo la elaboración de un DRP**

Elaborado por: Danilo Mannella L.

1. **Tiempo y recursos**.- Cualquier estrategia que permita mejorar a la organización, independientemente de su tamaño, requerirá de la asignación de tiempo y recursos (económicos, humanos y tecnológicos), y se necesita que la dirección de la microempresa, que muchos casos consiste en una empresa familiar, apoye la gestión y dote de los recursos necesarios.

2. **Implicación y compromiso de la dirección**.- Este punto refuerza el punto anterior, y toma en consideración que quien dirige (o dirigen) la microempresa deben tomar en serio la implementación de un DRP que coadyuve a mejorar la seguridad de la información del negocio, y para ello la dirección o gerencia debe ser concienciada y convencida de este tipo de planes.
3. **Conocer la organización y sus procesos críticos**.- La microempresa, independientemente de su tamaño debe conocer cuáles son sus procesos críticos, aquellos que le agregan valor al negocio, y saber qué personas son claves en el negocio, de igual modo conocer de qué manera las Tecnologías de la Información y Comunicación contribuyen al negocio. La esperanza de que una microempresa se recupere de un desastre es nula, si no dispone previamente de un conocimiento de su organización.
4. **Definir el alcance**.- Un punto importante en la implementación de un DRP para las microempresas es el alcance del plan, por cuanto si se espera proteger la información de toda la organización, o si no se conoce qué áreas son críticas para el negocio se terminará fracasando. No existe una receta mágica que aplique a todas las organizaciones y por ello es vital conocer qué procesos, productos, servicios y/o áreas son críticas proteger, e incluso el alcance está determinado por el impacto que podría producir una interrupción en los servicios o procesos del negocio.
5. **Colaboración con las áreas que componen la empresa**.- Las microempresas pueden estar compuestas por varias áreas, y se requiere que el apoyo no sea solamente desde el punto de vista tecnológico, sino de negocio, y por eso es importante contar con el apoyo de áreas tales como recursos humanos, atención al cliente, marketing, recursos logísticos, etc.

6. **Considerar la posibilidad de asesoramiento externo**.- Finalmente, es importante saber que la implementación de un plan ante desastres no se trata de una actividad, sino de un proceso, y si bien las microempresas pueden empezar con procesos simples, el crecimiento de las mismas podrá requerir de la asistencia de terceros que podrán guiar de mejor manera la implementación de un DRP conforme la microempresa crezca. En muchos casos es mejor no reinventar la rueda, y acudir a quien ya ha transitado por esa vía.

Recordar: La meta de un DRP es la de restaurar servicios de TI críticos lo más pronto posible y minimizar el tiempo de interrupción de los servicios del negocio.

La guía está dividida en 5 pasos, tal y como se muestra en la **Ilustración 35**:

***Ilustración 35*. Resumen de pasos de la guía para Mipymes**

Elaborado por: Danilo Mannella L.

4.2.4.4 Paso 1: Valoración de aplicaciones críticas

Ilustración 36. **Paso 1: Valoración de aplicaciones críticas**

Muchas microempresas se arriesgan a grandes pérdidas de información debido a fallas en los sistemas y a desastres de diferente índole, y sin embargo la idea de incursionar en la implementación de un plan de recuperación ante desastres les resulta abrumadora, al punto de dejar esta implementación para más tarde, pero lamentablemente 'más tarde' es algo que no llega, y cuando lo hace el negocio ha sufrido una pérdida económica considerable de la cual no se puede recuperar.

Cuando se producen eventos no deseados en las organizaciones se dan cuenta que conocen poco de la misma, o de que no se tiene claro qué procesos, productos, servicios e incluso personal, son los que constituyen la razón de ser del negocio, y por ello el primer paso es efectuar un BIA (análisis de impacto del negocio, por sus siglas en inglés), y esto está relacionado con identificar cuáles aplicaciones, sistemas y recursos son absolutamente críticos para llevar adelante el negocio, y a los cuales se les deberá dar un mayor enfoque en protegerlos. No todos los sistemas requieren el mismo nivel de protección, de hecho algunos de ellos posiblemente no requieran ser protegidos del todo, por ejemplo, la información personal que guarde cada empleado en sus computadores o portátiles no tendrá la misma prioridad que el servidor en donde se guarde información relacionada con la administración de la gestión de clientes, o la base de datos de los proveedores. Un análisis de costo beneficio que permita reconocer qué información es prioritaria de proteger ayudará a que la microempresa se recupere de un desastre lo antes posible.

4.2.4.5 Paso 2: Conocer a la computación en la nube

Ilustración 37. **Paso 2: Conocer a la computación en la nube**

La forma más rápida y fácil de asegurarse de que el negocio de una microempresa se pueda recuperar de un desastre tecnológico y que sufra por la pérdida de información es mantener los datos fuera del sitio de trabajo. Si una pérdida o falla de datos ocurre, se debería estar en capacidad de recuperarse de la misma, incluso si esto involucra el que la restauración se la haga fuera de la empresa, con lo cual al menos los datos estarían a salvo.

Tradicionalmente las empresas, y particularmente las microempresas han utilizado mecanismos como el respaldo y restauración de datos y aplicaciones en medios tales como cintas de datos, unidades de disco externas o, en el mejor de los casos, a través de imágenes de servidores o hasta usando el *clustering* de servidores, que consiste en tener la información replicada (o duplicada) en equipos exactos a los que usualmente se usan en la empresa.

Estos métodos han presentado dificultades debido a la lentitud en el respaldo/restauración de datos y/o falta de confiabilidad en los medios de respaldo (como el caso de las cintas), el costo o subutilización de recursos (en el caso del uso de *clustering*). Por lo anterior las empresas han tenido que escoger entre costo y velocidad de recuperación, lo cual para las microempresas en muchos casos no ha habido por dónde escaparse: no se efectúan respaldos con estos esquemas. La **Ilustración 38** muestra esta situación, en donde compartir recursos de respaldos

puede tener un costo bajo, pero un tiempo de recuperación alto, o si se adquiere una solución dedicada el tiempo de recuperación es rápido, pero el costo es casi prohibitivo:

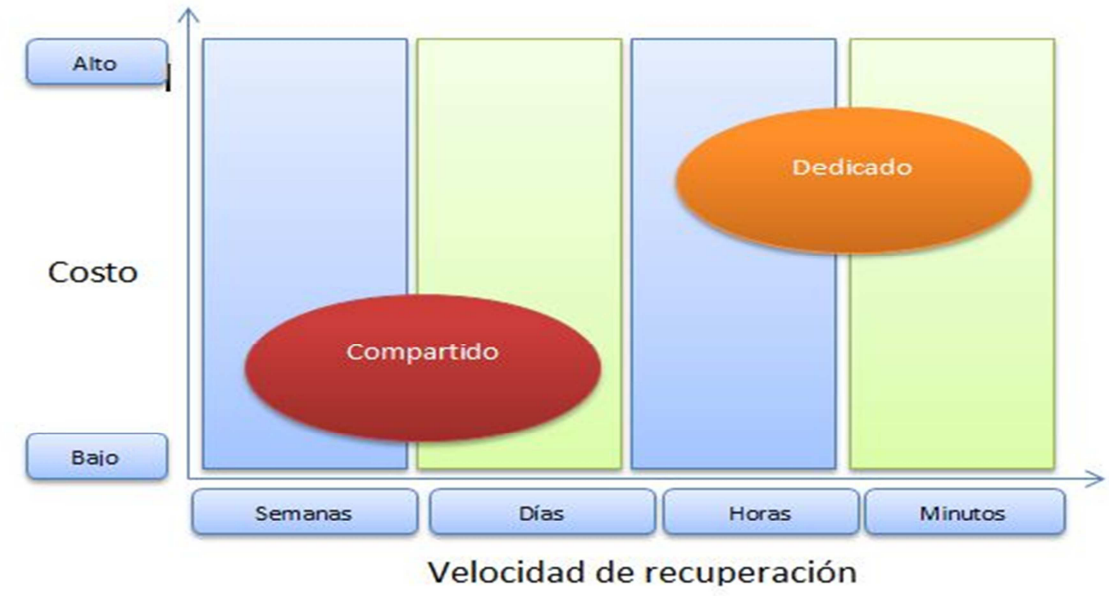


Ilustración 38. **Modelos compartidos y dedicados en DRPs tradicionales**

Fuente: Virtualizing Disaster Recovery using Cloud Computing.
Elaboración: Danilo Mannella L.

Hoy en día muchos negocios y organizaciones están orientando sus planes de recuperación ante desastres hacia la computación en la nube ya que ofrece un sinnúmero de beneficios. Con la computación en la nube las empresas en general, y particularmente las microempresas no requieren mantener sus servidores y aplicaciones dentro de sus instalaciones, no se requiere mantener un personal altamente técnico para mantener la infraestructura de TI, en pocas palabras, mediante la computación en la nube las microempresas pueden rentar un espacio en un servidor localizado en algún lugar del mundo, en Internet, de manera que puedan acceder a sus aplicaciones de software.

A continuación se detalla un poco más los beneficios a los que pueden acceder las microempresas con la computación en la nube:

1. **Libertad en adquisición de hardware**.- En esquemas tradicionales de TI se debe adquirir cierta infraestructura de HW determinada para que se ejecuten las aplicaciones. Con la computación en la nube se puede tener una variedad más amplia de dispositivos en los cuales ejecutar las aplicaciones y servicios, sin estar atado a determinadas marcas, disminuyendo gastos innecesarios.
2. **Adquisición de un buen equipo de TI**.- Para las microempresas, la contratación de un experto en seguridad, desempeño, o escalabilidad puede ser un asunto impensable y oneroso; sin embargo, con la utilización de la computación en la nube se puede contar con estos recursos para administrar los requerimientos antes mencionados sin necesidad de tener a un experto a tiempo completo de TI en la organización.
3. **Reducción de costos de TI**.- La premisa fundamental de la computación de la nube pública (ver más adelante) se basa en economías de escala. En lugar de tener un servidor metido en la oficina, administrado por un equipo dedicado, los PSN (Proveedores de Servicios en la Nube) pueden proveer servicios a miles de clientes aprovechando recursos comunes.
4. **Incremento en la eficiencia de las microempresas**.- En muchas microempresas los requerimientos de TI empresarial sobrepasa la infraestructura de TI rápidamente. No es fácil planificar y predecir el crecimiento que tendrá el negocio, a diferencia de lo que sucede en las grandes empresas, y tarde o temprano se subutiliza o sobredimensiona el tamaño apropiado de la infraestructura. Con el uso de computación en la nube se hace un uso eficiente de recursos, y esto se hace posible a través

del uso de tecnologías como la virtualización[21], que ya no son exclusivas de las grandes empresas.

5. **Se paga lo que se consume**.- Muchas microempresas tienen problemas de liquidez, y efectuar una inversión de capital pesado para la infraestructura de TI puede paralizar la inversión en otros lugares. Al pasar los gastos de capital a gastos de funcionamiento, se llega a utilizar su precioso capital en las otras áreas de la empresa.
6. **Mejor preparación ante desastres tecnológicos**.- Con ciertas herramientas de la nube, se puede configurar fácilmente un servicio para manejar desastres locales, sin tener una gran cantidad de servidores redundantes por ahí. También se puede configurar con eficacia las copias de seguridad y tener un programa de DR/BC (recuperación de desastres / continuidad del negocio) al igual que las grandes empresas.

Precisamente a partir de estos beneficios es que se puede contar con un esquema de recuperación ante desastres en donde se puede tener una recuperación relativamente rápida – dependiendo de varios factores, tales como el ancho de banda y la cantidad de información que se quiera recuperar – y a un costo asequible, esto debido a que, como se anotó anteriormente, los recursos del PSN son compartidos con otras empresas. La **Ilustración 39**, mostrada a continuación, permite visualizar esta situación, aunque en el siguiente paso se lo trata con un poco más de detalle.

[21] La **virtualización** es una tecnología que consiste en que una máquina física (usualmente un servidor), llamado computador "anfitrión", puede ser configurada para ejecutar varias máquinas virtuales, en donde cada instancia del sistema operativo ejecuta sus propias aplicaciones, como si fuera el único sistema operativo en dicha máquina.

Ilustración 39. **Enfoque de uso de computación en la nube para recuperación ante desastres**

Fuente: Virtualizing Disaster Recovery using Cloud Computing.
Elaboración: Danilo Mannella L.

Como se ha podido ver hasta ahora, la computación en la nube no es otra cosa que un modelo que permite ofrecer servicios informáticos a través de Internet en donde los recursos (HW, SW y aplicaciones) se ofrecen bajo demanda. Este modelo se generó debido a varios factores, entre los cuales se destacan el aumento en la capacidad de procesamiento de los equipos, el incremento en el ancho de banda y penetración del Internet en el mercado, y claro está, gracias a la amplia difusión de dispositivos móviles (teléfonos inteligentes, tabletas, ultraportátiles, etc.), que ha hecho que los negocios sean ubicuos.

Un aspecto fundamental a tener en cuenta cuando se habla de computación en la nube es que existen varios modelos de servicios a los que se puede recurrir en la nube, y estos se muestran en la **Ilustración 40**:

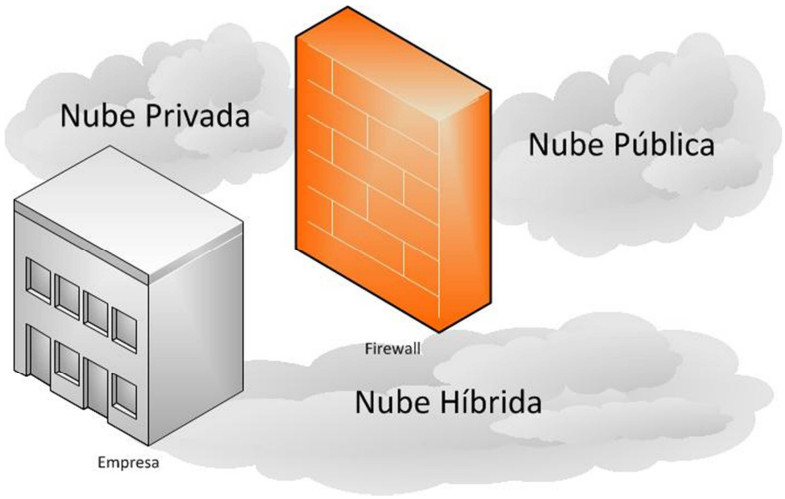


Ilustración 40. **Explicación de tipos de nubes para Mipymes**

Elaborado por: Danilo Mannella L.

1. Nubes **públicas**.- Son aquellas en las que todo el control de los recursos, procesos y datos está en manos de terceros. Múltiples usuarios pueden utilizar servicios web que son procesados en el mismo servidor, pueden compartir espacio en disco u otras infraestructuras de red con otros usuarios.
2. Nubes **privadas**.- Son aquellas creadas y administradas por una "única" entidad que decide dónde y cómo se ejecutan los procesos dentro de la nube. Supone una mejora en cuanto a la seguridad y privacidad de los datos y procesos, ya que los datos sensibles permanecen en la infraestructura informática de la entidad, mientras que controla qué usuario accede a cada servicio de la nube. Sin embargo, la entidad sigue siendo la encargada de comprar, mantener y administrar toda la infraestructura hardware y software de la nube.
3. Nubes **híbridas**.- Aquí coexisten los dos modelos anteriores. Por ejemplo, una empresa hace uso de una nube pública para mantener su servidor web mientras que mantiene su servidor de bases de datos en su nube privada.

De este modo, se establece un canal de comunicación entre la nube pública y privada mediante el cual los datos sensibles permanecen bajo estricto control mientras que el servidor web es administrado por un tercero. Esta solución disminuye la complejidad y coste de la nube privada.

Para el caso de las microempresas el modelo más apropiado a seguir es el de nube pública, si bien en algunos casos – particularmente de Pymes – se suele empezar por un modelo híbrido.

Curiosamente la computación en la nube pública ha estado presente desde hace varios años o incluso décadas, a continuación se presentan algunos ejemplos que los usuarios ordinarios han echado mano, y que algunos microempresarios quizás conozcan:

1. **Correo electrónico**.- través del correo electrónico "gratuito", pues servicios de correo tales y como Hotmail, Yahoo, Gmail, entre otros ofrecen un mecanismo de acceso ubicuo a mensajería.
2. **Almacenamiento de datos**.- De igual modo existen hoy en día servicios de almacenamiento de datos, tales como MS Skydrive, Dropbox, Google Drive, o iDrive, entre los más conocidos.
3. **Herramientas de colaboración**.- Posiblemente hoy en día sea muy conocida la suite de ofimática llamada Google Docs, con la cual se puede no solamente crear archivos, sino compartirlos. Microsoft no se ha querido quedar atrás y está impulsando su Office 365, que incluye no solamente herramientas de colaboración, sino también de mensajería.
4. **Comunicaciones**.- Probablemente el ejemplo más conocido es Skype, que permite comunicar de manera gratuita a dos PCs que tengan instalada esta aplicación, pero también se permite efectuar llamadas a teléfonos, mediante el

uso de un protocolo de comunicaciones llamado VoIP (Voz sobre IP), pero también está el caso de Google Voice, que también tiene buenos resultados. De igual manera la mensajería instantánea tiene a MS Live Messenger, Google Talk y Yahoo Messenger entre las plataformas de Internet más conocidas, y que en el caso de Microsoft se apalanca en una solución para empresas llamada Lync Server.

Una estrategia interesante para las microempresas sería que puedan acceder a muchos de estos servicios como usuarios ordinarios, y luego dar el salto en planes corporativos.

Preguntas básicas antes de lanzarse a la nube

La transición a la nube, particularmente para las microempresas, puede ser una de las decisiones más importantes que se haga en cuanto a gestión de infraestructura de TI, y consecuentemente es importante que se lo haga correctamente, y a continuación se presenta una lista de consideraciones a tomar en cuenta antes de contratar servicios con un PSN:

Cuadro 24. Aspectos a tomar en cuenta previa incursión en la nube

Parámetro	Preguntas
1. Precio	• ¿Cuál es el costo de instalación inicial? • ¿Cuáles son los costos vigentes? • ¿Hay alguna cuota de uso (de pago según el ancho de banda utilizado o el número de usuarios)? • ¿Existe un límite las tasas que el proveedor pueda incrementar? Si el proveedor aumenta las tasas más allá del límite, ¿puede esto ser una justificación válida para la cancelación del servicio? • ¿Cuál es el costo total de su infraestructura de TI existente descontados al valor presente? ¿Es más alto que el costo total de la infraestructura de nube?
2. Disponibilidad	• ¿Cuál es el tiempo de funcionamiento garantizado (*uptime*) por el proveedor? • ¿Cómo calcula el proveedor el tiempo de actividad (*uptime*)? • ¿Existe alguna compensación por no satisfacer la garantía de

Parámetro	Preguntas
	operatividad? • ¿Cuál es el costo por minuto de tiempo de inactividad de servicio? Por ejemplo, si se tiene una tienda en línea, se podría incluir la pérdida de ventas, el costo del incremento de llamadas de soporte y una estimación de la pérdida de buena voluntad (*goodwill*) de la marca.
3. Almacenamiento de datos	• ¿Qué tan sensibles son los datos a ser almacenados? • ¿Dónde se encuentran los servidores de datos? • ¿Qué métodos de cifrado se utilizan para proteger los datos? • ¿Hay garantías para proteger los datos contra las fugas? • ¿Quién puede acceder a los datos en el centro de datos? • ¿Está el proveedor permitido el uso de los datos y / o metadatos? Por ejemplo, en Gmail el contenido de su correo electrónico puede ser leído por los algoritmos de Google con fines publicitarios. • ¿En qué formatos se almacenan los datos? ¿Son esos formatos fácilmente convertibles al formato de almacenamiento de datos que se utiliza en la empresa? • ¿Con qué frecuencia son programadas las copias de seguridad? • ¿Utilizan algún tipo de arquitectura RAID para mejorar la fiabilidad?
4. Rendimiento y escalabilidad	• ¿Cuáles son las especificaciones de los discos, memoria RAM y procesadores utilizados en los servidores? • ¿Utilizan los SSD[22], dispositivos flash o técnicas de optimización para mejorar el rendimiento? • ¿Cuál es el ancho de banda máximo que ofrece? • ¿Están sus buses de datos y discos compartidos con otros usuarios? • ¿Qué tan pronto puede el PSN añadir recursos de computación cuando sea necesario? • ¿Cuáles son los resultados de las garantías ofrecidas en el SLA?
5. Cláusulas de terminación	• ¿Se puede rescindir el contrato en cualquier momento y sin una sanción importante? • ¿Se puede rescindir el contrato sin penalización alguna si hay un fallo de seguridad u otras circunstancias tenues? • ¿Por qué motivos puede el proveedor rescindir su contrato? • ¿Qué tan pronto podrá devolver el proveedor sus datos después de la terminación del contrato?
6. Soporte	• ¿Está la ayuda de emergencia disponible 24/7? • ¿Qué tipo de canales de soporte están disponibles (Línea de teléfono / email / chat basado en la Web)? • ¿Qué tan útil es el servicio de asistencia al cliente (*helpdesk*)? • ¿Tiene el proveedor una amplia KB (*Knowledge Base*) para ayudar a su personal a manejar asuntos simples?

Fuente: Basic Checklist For Cloud Computing Customers.
Elaboración: Danilo Mannella L.

[22] SSD es el acrónimo de *Solid State Disc* (disco de estado sólido), el cual consiste en una unidad de almacenamiento de datos no volátil, como las memorias flash, y que se diferencias de los discos duros convencionales en que estos utilizan platos giratorios magnéticos, y al ser dispositivos mecánicos son más susceptibles de falla.

El siguiente paso permitirá conocer las fases por las que se incurre en la recuperación ante desastres tecnológicos, de modo que en la microempresa se difunda lo que podría ocurrir, y cómo salir adelante.

4.2.4.6 Paso 3: Reconocimiento de las fases de una recuperación ante desastres

Ilustración 41. **Paso 3: Reconocimento de las fases de una recuperación ante desastres**

Cuando se produce una situación de desastre tecnológico en la microempresa es necesario reconocer 3 instancias: 1) Declaración de la emergencia, 2) Recuperación de las prestaciones y 3) Restablecimiento de las operaciones normales.

En la **Ilustración 42** se aprecia de mejor manera estas fases:

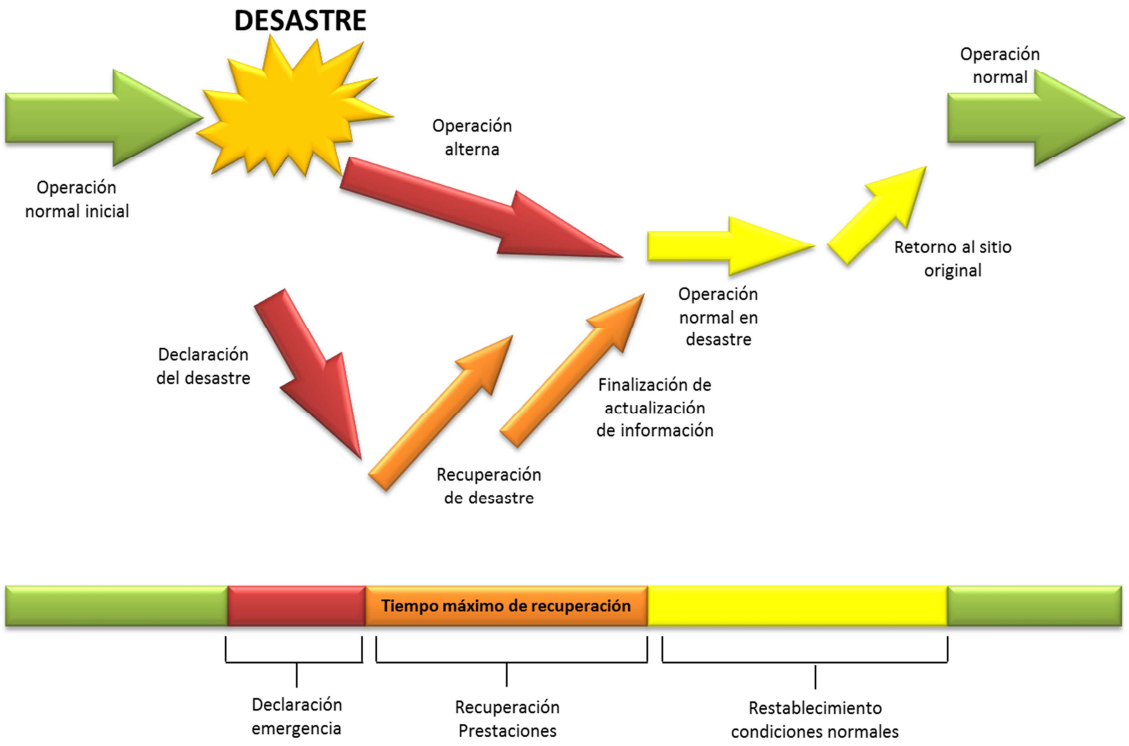


Ilustración 42. **Estados de situación en una recuperación ante desastres**

Fuente: Elaboración del Plan de Recuperación ante Desastres (PRD) – Cidicom. Argentina
Elaborado por: Ing. Danilo Mannella

A continuación se detalla cada etapa:

4. **Declaración de la emergencia**.- Abarca desde la detección del desastre hasta que el mismo es comunicado a los afectados. En este punto únicamente se evalúan los daños causados.

5. **Recuperación de las prestaciones**.- Consta del diseño y ejecución del DRP – que en este caso se lo hace mediante el esquema de recuperación en la nube – conforme a lo acontecido en el desastre, junto con el ajuste del mismo cuando aparezcan imprevistos que puedan modificar el plan inicialmente armado.

6. **Restablecimiento de las operaciones normales**.- Consiste en el diseño y ejecución del restablecimiento de las condiciones normales de operación, y que culmina con el análisis de la situación ocurrida a fin de ajustar el DRP en función de los errores, demoras e inconvenientes acontecidos, así como la posible toma de nuevas medidas preventivas.

En el siguiente paso se conocerá la manera de llevar a cabo los procedimientos y consideraciones para efectuar respaldos y restauraciones usando la computación en la nube.

4.2.4.7 Paso 4: Respaldos y recuperación en la nube

Ilustración 43. **Paso 4: Respaldos y recuperación en la nube**

En el pasado, una solución completa de recuperación de desastres requería significativos costos iniciales y gastos (CAPEX), además de mantenimiento continuo, lo cual lo hacía inalcanzable para muchas pymes, y peor aún para microempresas. Pero gracias a los modelos de nube de prestación de servicios, hoy en día, los clientes pueden aprovechar las operaciones de copia de seguridad y recuperación directamente desde la nube con un servicio de respaldo y recuperación en línea, una forma de software como servicio (SaaS[23]).

Al igual que otras aplicaciones SaaS, la copia de seguridad en línea es una alternativa a una aplicación de software dentro de la empresa. En este caso, tanto la

[23] SaaS: El Software como Servicio (*Software as a Service*, por sus siglas en inglés) consiste en un modelo de servicios provistos al consumidor a través de aplicaciones del proveedor, que se ejecutan en una infraestructura de la nube. El cliente accede desde un navegador web o un cliente ligero especializado, que se encuentra en diversos dispositivos tales como teléfonos inteligentes, tabletas, etc.

aplicación de respaldo como el almacenamiento de información residen fuera del sitio de trabajo. Este enfoque permite a los clientes reemplazar costosas inversiones iniciales en hardware de respaldo, software y personal con un precio asequible mensual o anual basado en la suscripción de servicio, de este modo se reducen de manera significativa el costo total de propiedad (TCO) al eliminar la gran inversión inicial y mover estos grandes costos CAPEX a los pequeños gastos de funcionamiento recurrentes.

Conforme una organización crece y utiliza más aplicaciones, los respaldos pueden llegar a ser complejos, costosos y difíciles. Los respaldos en línea le permite a la empresa dejar esta tarea a los expertos, optimizando las - ya de por sí muy limitadas - conexiones de ancho de banda entre las ubicaciones de las empresas y el PSN. Como tal, es ideal para los clientes de uno a dos servidores por sitio y para los usuarios itinerantes. Por último, la seguridad es un criterio más importante para los compradores. Este esquema es una de las mejores soluciones provistas por los principales proveedores al asegurar la transmisión y almacenamiento de datos en centros de datos de clase empresarial.

¿Cómo funciona la recuperación ante desastres en la nube?

1. **¿De qué manera funciona realmente la recuperación de desastres en la nube?** Se comienza al respaldar con regularidad los servidores de misión crítica a un lugar fuera de las instalaciones-una nube segura. Para la recuperación que es fácil y completa, hay que asegurarse de que la captura inicial sea una copia completa de la imagen de todo el sistema, a partir de ese momento, hay que asegurarse de que el proceso transferencia sólo datos cambiados. Esta transferencia de datos fuera del sitio puede ser también una copia de seguridad incorporada.

2. **¿Qué sucede si ocurre un desastre?** Si alguna vez sucede un desastre, los sistemas se reconstruyen con la información que ha sido regularmente enviada a la nube. Esta información es reconstruida en un entorno virtualizado, lo que permite un aprovisionamiento rápido y fácil de máquinas. Una vez que todos los datos y las aplicaciones se han recuperado, a los empleados se les da un acceso seguro y remoto a los sistemas recuperados a través de una red privada virtual. Todo lo que necesitan es una conexión estándar de Internet.
3. **¿Cómo se logra el menor tiempo de recuperación, digamos, cuatro horas o menos?** Si sus sistemas críticos o de datos requieren el RTO[24] más riguroso, un sitio caliente[25], basado en la nube usando la tecnología de replicación – en lugar de copia de seguridad tradicional – es el camino a seguir. Con la replicación, el sistema transfiere continuamente datos a una máquina pasiva de espera, ofreciendo un espejo completo de sus sistemas de producción, lo que garantiza la recuperación más rápida posible. En estos casos, por supuesto, también se utiliza la deduplicación de datos, que de inmediato reconstituye los datos una vez que "cruza el cable." Los sistemas de espera requieren altos niveles de seguridad, lo que los datos normalmente se entrega a través de Túneles IPSec y firewalls de aplicación.

Los proveedores de respaldos en la nube también:

1. **Aseguran respaldos regulares y consistentes**.- Con las soluciones de respaldos en línea, las copias de seguridad pueden ser completamente automatizadas y el vendedor asume la mayor parte (pero no toda) de la responsabilidad por el éxito de las copias de seguridad y restauraciones. Si

[24] RTO: Proviene de Objetivo de Tiempo de Recuperación, (por sus siglas en inglés), y describe la cantidad de tiempo, o qué tan rápido se puede recuperar información a partir de que acontezca un desastre.
[25] Un “sitio caliente”, o *hot site*, consiste en un sitio de recuperación ante desastres en donde se duplica exactamente el entorno de producción de la empresa.

algo va mal con la conexión de red y no con la copia de seguridad, la responsabilidad es compartida. Sin embargo, los vendedores ofrecen soporte las 24 horas al día, siete días a la semana y proporcionan un portal basado en Web para: ver las copias de seguridad completas y el historial de las versiones de los respaldos, iniciar restauraciones y ejecutar informes.

2. **Ayudan a manejar costos**.- Con un modelo basado en suscripción, el costo de construir y mantener la infraestructura para apoyar la aplicación de copia de seguridad se extiende a numerosos clientes, permitiendo que el proveedor de servicios pueda ofrecer el servicio a un costo menor que de otro modo no sería posible.
3. **Proveen protección asequible, confiable y fuera de las instalaciones**.- Los respaldos en la nube eliminan la necesidad de transportar físicamente cintas o unidades externas extraíbles. Los datos de los respaldos de información se copian electrónicamente a través de Internet al centro de datos del proveedor. Además, los datos están cifrados, ya que se transmiten al proveedor ("cifrado en vuelo") y son cifrados de nuevo en el centro de datos del proveedor ("cifrado en reposo"), lo que garantiza la seguridad de sus datos.
4. **Ofrecen a las sucursales la misma protección que a la matriz**.- Muchas sucursales tienen poca o ninguna copia de seguridad en el sitio. Un servicio de respaldo en línea para las oficinas remotas proporciona copias de seguridad periódicas y automáticas para los sitios que carecen de personal local o ancho de banda significativo. También puede reducir los requerimientos de infraestructura en el sitio remoto, como los sistemas de cinta locales, servidores de medios y profesionales de TI.

A continuación se brindan algunos ejemplos de empresas que, si bien prestan sus servicios de respaldo y recuperación ante desastres en la nube a personas, a través de planes individuales, también lo hacen a microempresas:

- SugarSync (www.sugarsync.com)
- LiveDrive (www.livedrive.com)
- RightScale (www.rightscale.com)
- Jungle Disc (www.jungledisc.com)

En nuestro país existe un proveedor llamado Ecuador Cloud (www.ecuadorcloud.com), que opera desde el año 2003, y que es especializado en soluciones de telecomunicaciones, y cuyas divisiones de negocio incluyen ISP Corporativo, Infraestructura de Telecomunicaciones, Soluciones Satelitales, Servicios Data Center, e Integración de Soluciones. Dentro de esta integración de soluciones se encuentran los planes de contingencia y respaldo de información, así como recuperación de información ante desastres.

4.2.4.8 Paso 5: Evaluación y mantenimiento

Ilustración 44. **Paso 5: Evaluación y mantenmiento**

Una de las últimas fases, y que de hecho resulta en una medida preventiva, dentro de esta guía de pasos, y considerando la elaboración previa del DRP, es la de pruebas. El plan debe ser probado en su totalidad al menos una vez al año, de acuerdo a las mejores prácticas y de ser posible siguiendo estándares internacionales, y debe ser probado parcialmente en distintas oportunidades mediante un esquema continuo

de mejoras y revisión, que contribuyan al mantenimiento vigente del plan a lo largo del tiempo.

El DRP debe ser revisado con regularidad para garantizar su adecuación a los cambios que sufre el entorno, manteniendo vigente su aplicabilidad frente a desastres.

Tanto en las pruebas y revisión del DRP cuanto en su aplicación en un evento disruptivo verdadero, las microempresas deberán coordinar con el PSN para que las aplicaciones y datos se recuperen en máquinas virtuales que pasarán a estar activas al momento del desastre. Por eso es importante seleccionar al proveedor más adecuado, tal y como se mencionó anteriormente.

4.2.5 Unas últimas palabras

Hoy en día, todas las empresas, incluyendo las microempresas, deben asegurarse de que se puedan recuperar de forma rápida y fiable a partir de un fallo del sistema, corrupción de datos, ataques de virus, y mucho más.

La información se puede perder en cualquier momento, por lo que es imprescindible el asegurar que los datos estén siempre protegidos y se puedan recuperar. Conforme los retos de respaldos y recuperación evolucionan, los principales fabricantes están respondiendo con nuevos enfoques para la protección de datos adaptada a empresas de cualquier tamaño. Las copias de seguridad y de recuperación robustas para entornos físicos y virtuales pueden encontrar un gran aliado en los servicio ofrecidos por proveedores de respaldos en la nube.

Ahora usted puede aprovechar de esta guía para implementar un plan de recuperación ante desastres mediante copias de seguridad y recuperación

de una forma rápida, sencilla y moderna de la manera que mejor se adapte a sus necesidades.

4.3 Validación de las guías de implementación

Para llevar a cabo la validación de las guías de implementación, tanto de las Pymes como de las microempresas se envió a las empresas que participaron de la fase de diagnóstico una carta en donde se les agradecía por su colaboración en la fase inicial del estudio y se les invitaba a que evaluaran las guías de implementación dependiendo de si eran microempresas o Pymes. Esta carta se la encuentra en el **Anexo 3**.

Adjunto a las guías de implementación se les hizo llegar igualmente un cuestionario con preguntas relativas a la guía, las cuales permitieron conocer el grado de aplicabilidad de las mismas en sus empresas o para que juzgaran sobre la aplicabilidad en Pymes que tuvieran contacto con ellas, a continuación se muestra la ficha que contiene la validación de las guías por parte de estos expertos

Cuadro 25. Ficha de validación de las guías de implementación por parte de expertos

Ficha del experto	
Nombre del Entrevistado:	Haga clic aquí para escribir texto.
Cargo:	Haga clic aquí para escribir texto.
Empresa:	Haga clic aquí para escribir texto.
Fecha:	Haga clic aquí para escribir una fecha.
Criterios de evaluación	
Indicaciones Las siguientes preguntas están relacionadas con la guía de implementación de un plan de recuperación ante desastres tecnológicos usando a la computación en la nube que usted recibió, y para ello es importante conocer sus apreciaciones en función de su negocio. *¡Se le agradece mucho por su tiempo y sinceridad en esta parte final del estudio!*	

1. Señale con una “X” si su evaluación corresponde a: **Pyme** ☐ **Mipyme** ☐

2. Valore en la escala del 1 al 5 – siendo 1 lo menos importante y 5 lo más importante – la **importancia** que tiene en su negocio las siguientes categorías de aplicaciones críticas que le gustaría recuperar en caso de un desastre tecnológico:

Categoría	1	2	3	4	5
Correo electrónico corporativo	☐	☐	☐	☐	☐
CRM (Gestión de relación con clientes)	☐	☐	☐	☐	☐
ERP (Planeación de recursos empresariales)	☐	☐	☐	☐	☐
Aplicaciones de relación con proveedores	☐	☐	☐	☐	☐
Portal interno (intranet)	☐	☐	☐	☐	☐
Otro (cuál):_Haga clic aquí para escribir texto.	☐	☐	☐	☐	☐

3. Señale qué aplicaciones estaría dispuesto a migrar en la nube (*ya sea privada, pública o híbrida*):

Aplicación	Señale con una “X”
Correo electrónico	☐
Aplicaciones desarrolladas internamente	☐
Portal interno	☐
Almacenamiento de datos	☐
Otro (cuál):_Haga clic aquí para escribir texto. ___	☐

4. Una vez analizada la guía y aplicándola a su negocio, valore en la escala del 1 al 5 – siendo 1 lo menos importante y 5 lo más importante – los **medios** que usaría en adelante en su empresa para recuperar su información en caso de un desastre tecnológico:

Categoría	1	2	3	4	5
Respaldos en cinta	☐	☐	☐	☐	☐
Redundancia de información (*duplicación de información en otros servidores*)	☐	☐	☐	☐	☐
Uso de imágenes de servidores	☐	☐	☐	☐	☐
Servicios de Respaldo y Recuperación como servicio en la nube	☐	☐	☐	☐	☐

5. Valore en la escala del 1 al 5 – siendo 1 lo menos importante y 5 lo más importante – las **ventajas** que puede tener en su negocio la **computación en la nube**, de acuerdo a los siguientes parámetros:

Ventaja	1	2	3	4	5
Acceso ubicuo (*es decir, desde cualquier dispositivo*)	☐	☐	☐	☐	☐
Disposición de un equipo de TI experto en la nube	☐	☐	☐	☐	☐
Reducción de costos de infraestructura de TI	☐	☐	☐	☐	☐
Usar un servicio medido (*pagar por los servicios que se usan*)	☐	☐	☐	☐	☐
Rápida elasticidad (*capacidad de aumentar o disminuir los servicios a usar en la nube*)	☐	☐	☐	☐	☐
Mejor preparación ante desastres tecnológicos	☐	☐	☐	☐	☐

6. Ahora que conoce la **importancia del DRP** (Plan de recuperación ante desastres) valore en la escala del 1 al 5 – siendo 1 lo menos importante y 5 lo más importante – las acciones a tomar en su empresa, de acuerdo a los siguientes parámetros:

Acciones	1	2	3	4	5
Buscar compromiso de los ejecutivos de la empresa	☐	☐	☐	☐	☐
Análisis de riesgos y vulnerabilidades del negocio	☐	☐	☐	☐	☐
Elaboración del DRP	☐	☐	☐	☐	☐
Conformación de un equipo a cargo del DRP	☐	☐	☐	☐	☐
Revisión anual del DRP	☐	☐	☐	☐	☐

7. Un factor importante para la aplicación de un DRP en la nube es la **selección del PSN** (Proveedor de servicios en la nube), valore en la escala del 1 al 5 – siendo 1 lo menos importante y 5 lo más importante – la importancia de los siguientes criterios en su negocio:

Criterio	1	2	3	4	5
Experiencia técnica	☐	☐	☐	☐	☐
Confiabilidad del PSN	☐	☐	☐	☐	☐
Garantía de tiempo de actividad	☐	☐	☐	☐	☐
Facilidad de migración	☐	☐	☐	☐	☐
Soporte técnico	☐	☐	☐	☐	☐
Seguridad en la nube	☐	☐	☐	☐	☐
Costo de la solución	☐	☐	☐	☐	☐

8. Finalmente, valore en la escala del 1 al 5 – siendo 1 lo menos útil y 5 lo más útil – el grado de utilidad de esta guía para llegar a implementarla en su negocio y en cualquier otra Pyme.

Criterio	1	2	3	4	5
Explicación de términos técnicos	☐	☐	☐	☐	☐

Especificidad del contenido	☐	☐	☐	☐	☐
Profundización de la computación en la nube	☐	☐	☐	☐	☐
Profundización del DRP	☐	☐	☐	☐	☐
Profundización del DRP en la nube	☐	☐	☐	☐	☐
Otro (cuál):_Haga clic aquí para escribir texto.	☐	☐	☐	☐	☐

Elaborado por: Ing. Danilo Mannella

En el siguiente apartado se apreciarán las conclusiones a las que se llegó luego de la validación por parte de los diferentes expertos en la evaluación de las guías.

4.3.1 Conclusiones de la validación de las guías

1. En primer lugar se concluye que dentro de las aplicaciones críticas que poseen las Pymes y microempresas resultan de mayor importancia enfocar la protección en el correo electrónico, y luego resulta importante el CRM para las microempresas, en tanto que las Pymes resaltan la importancia del ERP, aplicación de relación con proveedores y el portal interno, tal y como se aprecia en la **Ilustración 45**.

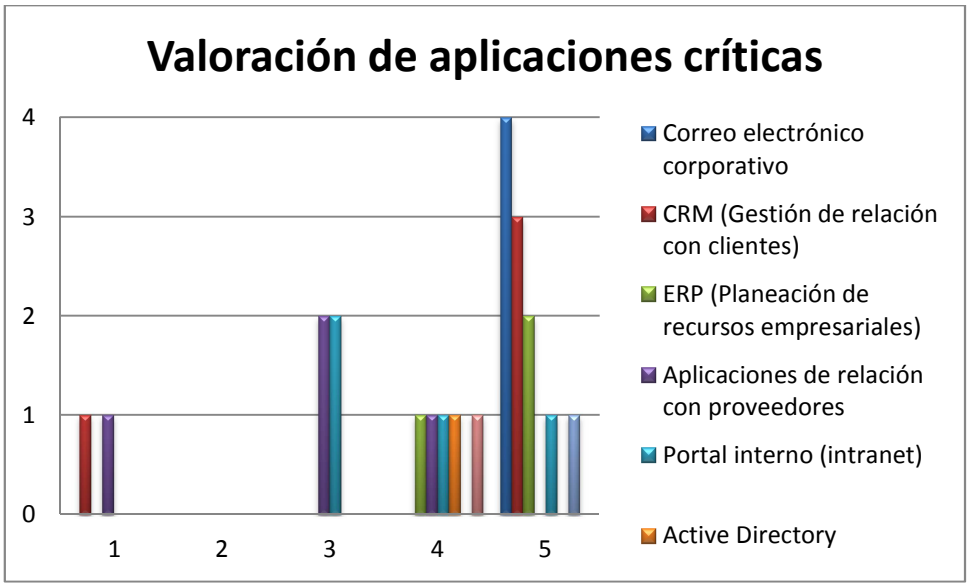


Ilustración 45. **Valoración de aplicaciones críticas a ser recuperadas ante un desastre tecnológico**

Elaborado por: Ing. Danilo Mannella

2. Cuando se trata de evaluar qué aplicaciones estaría dispuesto a migrar a la nube tanto Pymes como microempresas resaltan la disponibilidad de migrar el correo electrónico, y luego el portal interno y el almacenamiento de datos, como se muestra en la **Ilustración 46**.

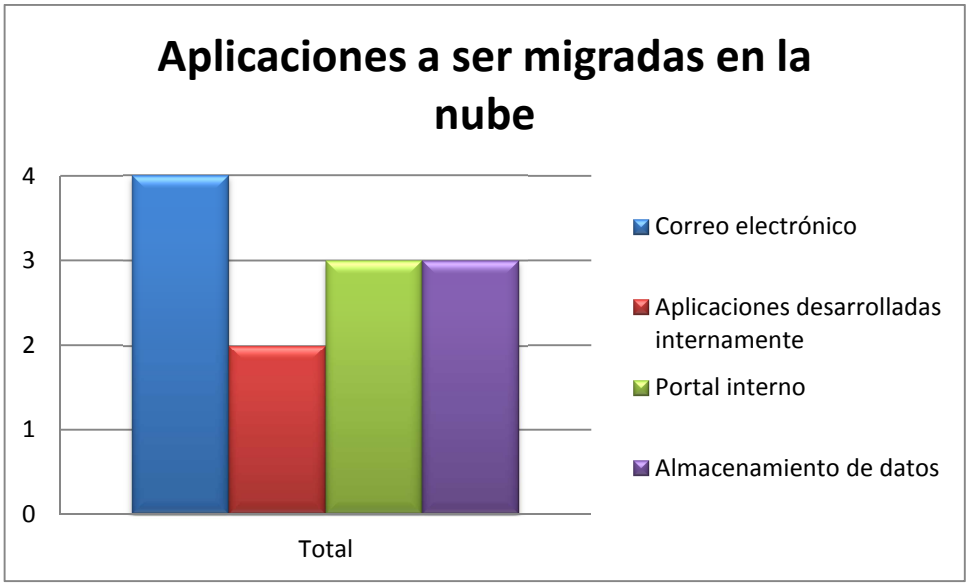


Ilustración 46. **Aplicaciones a ser migradas en la nube (pública, privada o híbrida)**

Elaborado por: Ing. Danilo Mannella

3. Es de gran importancia destacar que cuando se trata de valorar los medios que usarán las Pymes y Mipymes hay un consenso bastante generalizado en cuanto a usar servicios de respaldo y recuperación en la nube, sin embargo el resto de medios siguen siendo todavía tan importantes como el mencionado anteriormente, es decir el uso de respaldos en cintas y la redundancia de información aún es vista como necesaria para mantener un esquema de seguridad apropiado, principalmente para las Pymes, según se aprecia en la **Ilustración 47**.

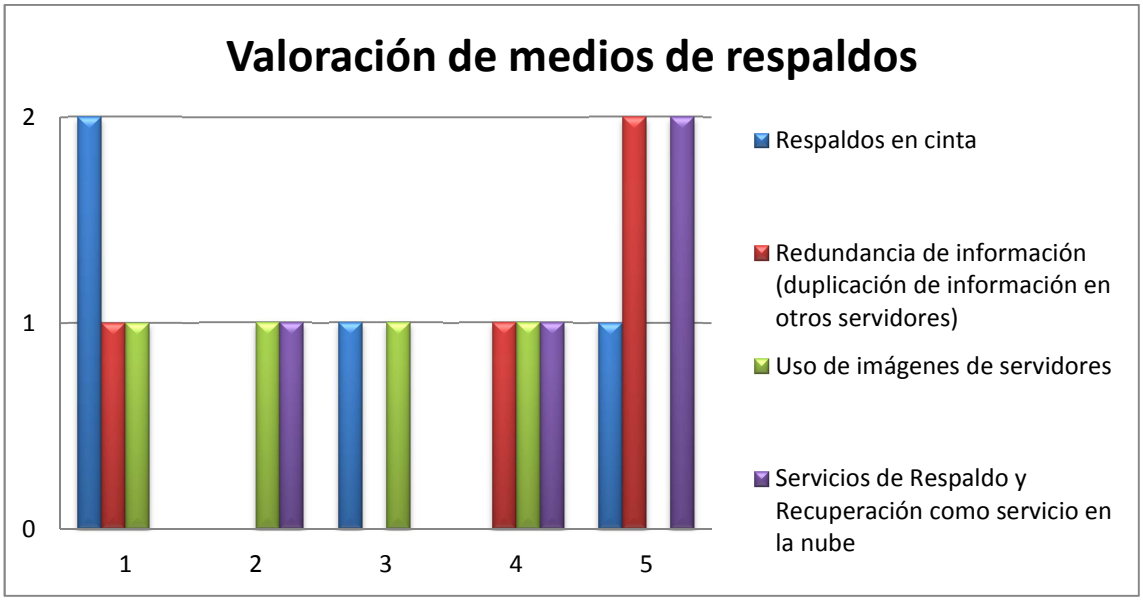


Ilustración 47. **Medios a ser usados por las Mipymes para recuperar información en adelante.**

Elaborado por: Ing. Danilo Mannella

4. Las guías de implementación han servido para destacar las ventajas que puede tener para el negocio la computación en la nube, y es un consenso que tiene la mayor importancia el acceso ubicuo y el usar un servicio y medido, luego de lo cual es de relevancia la reducción de costos de infraestructura de TI y también el permitir a la organización estar mejor preparado ante desastres tecnológicos, siendo los otros factores importantes pero en menor grado, conforme se visualiza en la **Ilustración 48**.

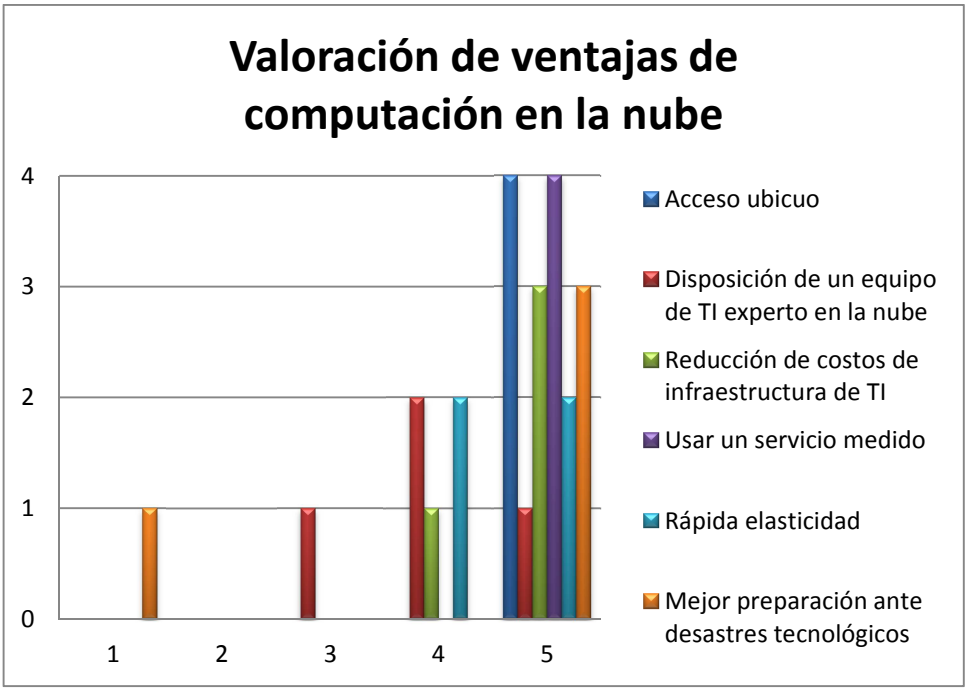


Ilustración 48. **Valoración de ventajas de la computación en la nube para la Pyme**

Elaborado por: Ing. Danilo Mannella

5. En cuanto a la importancia de contar con un DRP, las Pymes y Mipymes consideran que lo más importante es buscar el compromiso de los ejecutivos de la empresa para la implementación de este plan, así como llegar a elaborar el mismo, siendo el análisis de riesgos y vulnerabilidades y la conformación de un equipo que lidere el DRP un factor menos importante, aunque necesario, de acuerdo a la gráfica mostrada en la **Ilustración 49**.

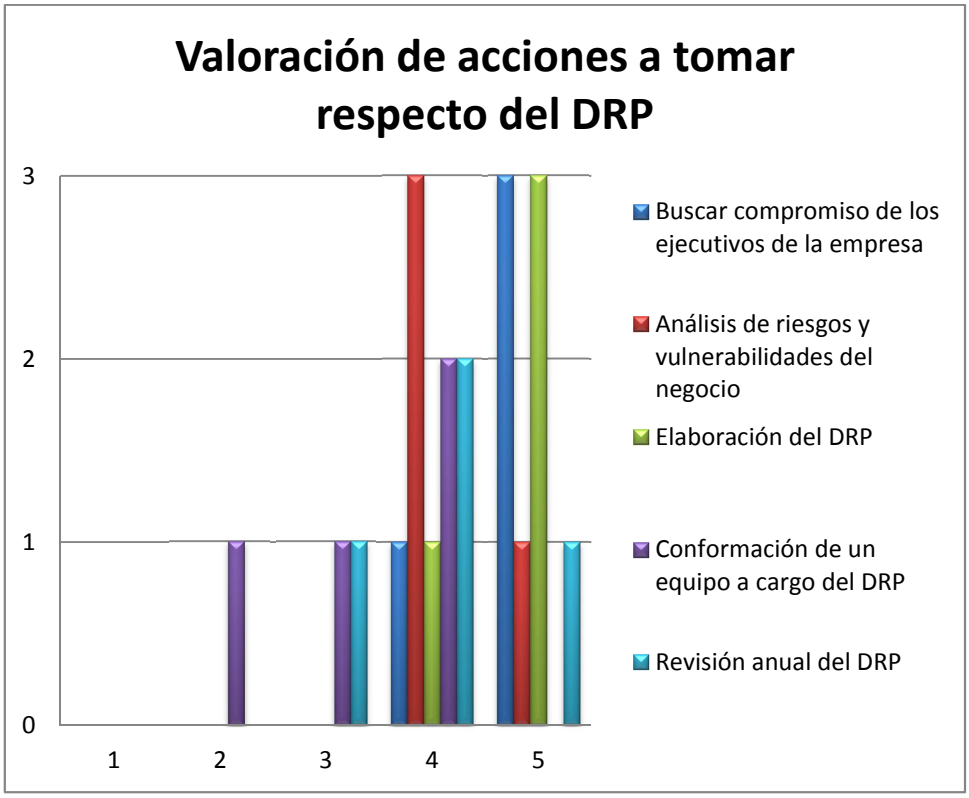


Ilustración 49. **Valoración de acciones a tomar en la empresa respecto del DRP**

Elaborado por: Ing. Danilo Mannella

6. Respecto de la selección del PSN (proveedor de servicios en la nube) los factores que más sobresalen a ser tomados en cuenta por las Pymes y Mipymes son la confiabilidad del PSN tanto como la seguridad que pueden brindar en los servicios que se ofrece en la nube, luego de lo cual los otros factores son también importantes, pero en menor grado, y esto se muestra en la **Ilustración 50**.

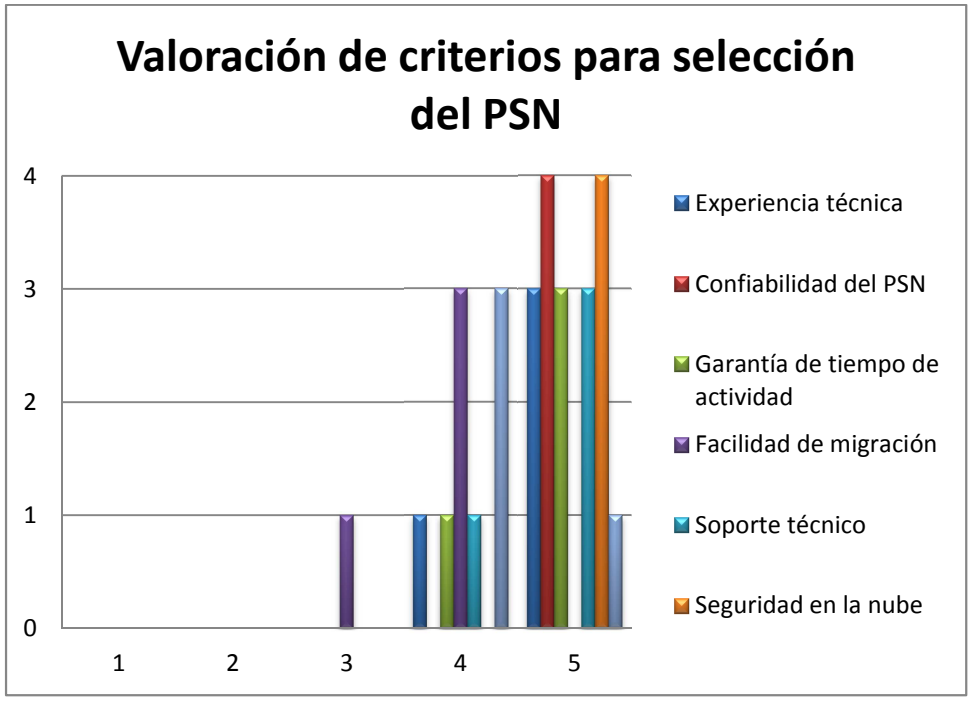


***Ilustración 50*. Valoración de criterios para escoger un proveedor de servicios en la nube**

Elaborado por: Ing. Danilo Mannella

7. Finalmente, respecto de la utilidad de la guía, se concluye de esta valoración por parte de los expertos que lo más útil para llegar implementarla en su negocio, así como en cualquier otra Pyme, es la especificidad del contenido, seguido de la explicación de los términos técnicos así como la profundización del DRP.

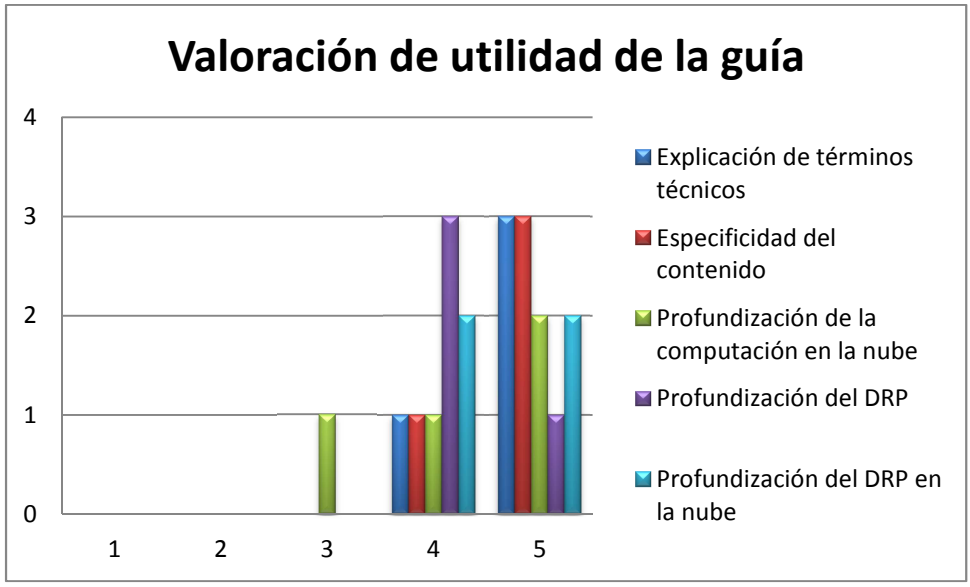


Ilustración 51. **Valoración del grado de utilidad de la guía de implementación**

Elaborado por: Ing. Danilo Mannella

5 Capítulo V: Conclusiones y Recomendaciones

5.1 Conclusiones

Fruto del trabajo de investigación de esta tesis se ha podido llegar a las siguientes conclusiones:

- La hipótesis nula (Ho) planteada fue que “Las Pymes son afectadas considerablemente en el evento de un desastre tecnológico, pudiendo provocarle pérdidas económicas, disminución en cartera de clientes y hasta el cierre de la empresa.”, lo cual fue demostrado con el análisis llevado a cabo en el Capítulo III, es decir, en caso de no hacer nada al respecto las Pymes cumplen con esta hipótesis.
- No obstante lo anterior, la hipótesis alternativa (Ha) propuesta menciona que “las Pymes que formulen un DRP utilizando un modelo de computación en la nube tendrán un menor impacto en recuperación ante desastres que aquellas que utilizan un modelo tradicional, o que no lo tengan siquiera contemplado, con una inversión relativamente baja.”, cuyo cumplimiento se demuestra en los criterios emitidos por los expertos cuando evaluaron las guías de implementación, y cuyos aportes se encuentran en ese capítulo, y sintetizado más adelante en este capítulo.
- Adicionalmente se puede concluir de este trabajo de investigación que el levantamiento de información llevada a cabo en la fase de investigación previa, o de fundamentación teórica, permitió conocer de manera global la situación de las Pymes a nivel mundial, nacional y local respecto de los mecanismos utilizados para proteger su información ante desastres tecnológicos, y la implementación de planes de recuperación ante estos desastres utilizando a la computación en la nube.

- Las pequeñas y medianas empresas, así como las microempresas, de acuerdo a los resultados arrojados en la fase de diagnóstico, están poco preparadas ante eventos producidos debido a desastres tecnológicos, y al momento se usan mayoritariamente medios tradicionales de respaldos, tales como unidades de cintas (u otros medios como CD-S y DVDs), duplicación de infraestructura, lo cual resulta ineficiente y/o costoso.
- Existe poco conocimiento sobre los beneficios que puede proveer la computación en la nube para las Pymes de manera general, y en cuanto a los mecanismos que se pueden usar para beneficio de éstas en cuanto a servicios como los de recuperación ante desastres tecnológicos.
- Dentro de los beneficios que se tiene al utilizar a la computación en la nube para una recuperación ante desastres tecnológicos se destaca el acceso de red ubicuo, es decir desde cualquier dispositivo, así como el poder contar con una mejor infraestructura que la que se puede tener dentro de la empresa y con el respaldo de personal técnico mejor preparado para manejar la infraestructura de TI que su requeriría si estuviera dentro de las instalaciones de la empresa.
- Se puede concluir así mismo que tanto las Pymes, y sobretodo las microempresas todavía deben sensibilizar a la alta gerencia sobre la importancia de contar con planes de recuperación ante desastres, y que pueden apalancarse en estos planes usando a la computación en la nube.
- La elaboración planes ante recuperación de desastres tecnológicos usando a la computación en la nube benefician no solamente a las grandes empresas sino también a las pequeñas y medianas empresas, así como a las microempresas, cuya implementación se reflejará en la disminución en el porcentaje de quejas

por parte de usuarios, incremento en el porcentaje de clientes satisfechos, y una mejora en la imagen de la empresa.

- A raíz del levantamiento de información en la fase de diagnóstico se vio la necesidad de elaborar una guía de implementación no solamente para las Pymes, sino también para las microempresas, en un formato más simple, pero con la profundidad suficiente para llevarlo a cabo.
- Las guías de implementación ante desastres tecnológicos son propuestas que irán madurando en las Pymes conforme se difunda al interior de estos negocios que la inversión en seguridad no es un gasto.
- Las Pymes y microempresas que implementen la guía de DRP propuesta tendrán un menor impacto en la recuperación de información ante desastres tecnológicos que aquellas que no tengan contemplado ningún DRP o que sigan un modelo tradicional que puede resultar costoso y/o ineficiente.
- Conforme la valoración usada por expertos en la validación de las guías de implementación para las Pymes y microempresas se aprecia claramente que las guías son de fácil comprensión de términos y la especificidad del contenido contribuirá a una mejor implementación de las mismas.

5.2 Recomendaciones

Luego del estudio efectuado se recomienda considerar lo siguiente:

- Es importante tener un acercamiento entre la oferta y la demanda, es decir, las empresas que proveen servicios en la nube a nivel local deberán considerar a las Pymes como un potencial mercado a atender no solamente en la provisión de aplicaciones del tipo SaaS, sino para ofrecer servicios de recuperación ante desastres, considerando costos personalizados diseñados para este segmento que son distintos a los de otras industrias, pero que este mercado este momento no está siendo atendido.

- Desde el punto de vista de las Pymes es recomendable que se empleen planes de recuperación ante desastres fáciles de implementar en tiempo y costo, y que cuenten con el apoyo de los altos directivos, y cuya difusión se dé a toda la organización, de lo contrario será una iniciativa que podría fracasar.
- Dado que el presupuesto para seguridad de la información en general es bajo tanto en las Pymes como en las microempresas se recomienda que se incremente este valor en un porcentaje superior al 10% de su presupuesto global, ya que esto les permitirá estar mejor preparados ante varios de los desastres tecnológicos citados en esta tesis.
- De igual manera se sugiere que las organizaciones que agrupan a las diferentes Pymes y microempresas organicen asistencias técnicas y capacitaciones a estos pequeños y medianos negocios sobre esta temática de seguridad de la información y respaldos y recuperación de información.
- Adicionalmente es muy recomendable que exista apoyo del Estado, juntamente con la empresa privada para proveer lineamientos que permitan que se pueda acceder a una mejor prestación de servicios de Internet para llevar a cabo DRPs usando la computación en la nube.
- Es recomendable que se implemente la guía de implementación correspondiente a la Pyme o microempresa, respectivamente, de forma tal que se pueda establecer una línea base de la situación actual en términos de seguridad informática en el negocio, e ir mejorando el DRP inicial.
- Hoy en día existen varias empresas locales proveedoras de servicios en la nube que están incursionando en la entrega de soluciones SaaS, y se recomienda que también provean de soluciones IaaS a las Pymes ya sea directamente o tercerizando servicios de proveedores más grandes como Amazon, Google, Microsoft, HP, IBM, E-Vault, Rackspace, etc.

- La computación en la nube puede ser implementada en las empresas usando esquemas de nubes privadas, públicas o híbridas, pero para las Pymes se recomienda que se inicien con nubes públicas debido a la menor inversión inicial y aprovechamiento de la infraestructura de PSN externos.
- Dado que uno de los principales factores a tomar en cuenta por parte de las Pymes y microempresas para la contratación de un PSN es la confiabilidad de la empresa así como la seguridad que puedan ofrecer a sus clientes, se recomienda que se revise detalladamente el SLA que se firmará entre las partes, de manera que se conozcan los deberes y derechos de cada uno.
- Finalmente, se recomienda que se haga un seguimiento continuo a la evolución de la adopción de la computación en la nube como mecanismo de recuperación ante desastres tecnológicos, y cuyos resultados beneficiarán a las Pymes que constantemente no están preparadas para una eventualidad en la pérdida de su información.

6 Bibliografía

Agencia Andes. (23 de Junio de 2011). *Las empresas pequeñas son las que dan más trabajo en Ecuador* . Recuperado el 14 de Abril de 2012, de http://andes.info.ec/2009-2011.php/?p=70157

Amazon Web Services. (2012). *Casos prácticos*. Recuperado el 24 de Abril de 2012, de http://aws.amazon.com/es/solutions/case-studies/

Barrera, M. (2001). *Seminario- Taller: Mecanismos de promoción de exportaciones para las pequeñas y medianas empresas en los países de la Aladi.* Ponencia, CAPEIPI, Montevideo, Uruguay.

Benalcázar, C., & Parra, L. (2012). *Plan de negocio para la creación de una empresa de servicios tecnológicos basados en outsorcing y colaboración, enfocado a pequeñas y medianas empresas .* Tesis, ESPE, Quito.

CIO. (s.f.). *Business Continuity and Disaster Recovery Planning Definition and Solutions*. Obtenido de http://www.cio.com/article/40287/Business_Continuity_and_Disaster_Recovery_Planning_Definition_and_Solutions

Computerworld. (2011). CIO conocimientos y experiencias de TI para manejar la eficiencia en las empresas. *Computerworld Ecuador*, 14.

Computerworld. (2011). CIO Forum - Conocimientos y experiencias. *Computerworld Ecuador*(224), 14.

Computerworld. (2011). La nube computacional un modelo de aprovechamiento de infraestructura que avanza para quedarse. (Ediworld, Ed.) *Computerworld Ecuador*(230), 19-21.

Computerworld. (15 de Mayo de 2011). Servicios en la nube crecieron en A.L. *Computerworld Ecuador*(6), 6.

Computerworld. (2011). Una nube privada apoya la definición estratégica de negocio en Merck. *Computerworld Ecuador*(230), 22-23.

Computerworld. (14 de Agosto de 2012). La nube computacional un modelo de aprovechamiento de infraestructura que avanza para quedarse. *Computerworld*(230), 19-21.

Cruz Marta, F., De Castro Neto, M., Neves, F. T., & Ramalho Correia, A. (2011). *The Adoption of Cloud Computing by SMEs: Identifying and Coping with External Factors.* Paper, Lisboa, Portugal.

Disaster Recovery. (s.f.). *Disaster Recovery Plan Maintenance*. Recuperado el 12 de Abril de 2012, de http://www.disasterrecovery.org/maintenance.html

Exforsys. (5 de Abril de 2009). *Cloud Computing Basic Components.* Recuperado el 15 de Abril de 2012, de http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-basic-components.html

Gartner, Inc. (2012). *Top 10 Strategic Technology Trends for 2012.* Recuperado el 13 de Marzo de 2012, de http://www.gartner.com/technology/research/top-10-technology-trends/

Gracia Armendáriz, C. (8 de Octubre de 2010). A Internet tal y como la conocemos hoy le quedan cinco telediarios. 1. (I.-C. I. Empresas, Entrevistador) España.

Halscott, J. (2011). *10 Must-Have Features for Every Virtualization Backup and Disaster Recovery Solution.* Realtime Publishers.

IBM Global Technology Services. (2012). *Virtualizing disaster recovery using cloud computing.* Somers, NY: IBM Corporation.

IBM Global Technology Services. (2012). *Virtualizing disaster recovery using cloud computing. Transition your applications quickly to a resilient cloud.* Somers, NY: Enero.

INTECO. (2011). *Guía para empresas: seguridad y privacidad del cloud computing.* Madrid, España: INTECO.
Interactic. Mesa Sectorial de Cloud Computing. (2010). *Cloud Computing - Una perspectiva para Colombia.* Recuperado el 17 de Abril de 2012, de http://www.interactic.com.co/dmdocuments/clud_computing.pdf
Lock, T., Bennett, M., & Vile, D. (2010, Octubre). *Freeform Dynamics.* Retrieved from Disaster Recovery in European SMBs: http://www.freeformdynamics.com/fullarticle.asp?
Myerson, J. (3 de Marzo de 2009). *Cloud computing versus grid computing.* Recuperado el 20 de Abril de 2012, de http://www.ibm.com/developerworks/web/library/wa-cloudgrid/
NIST. (2011). *The NIST Definition of Cloud Computing.* NIST, U.S. Department of Commerce. Gaithersburg, MD: NIST.
PCWorld Ecuador. (14 de mayo de 2012). Seguridad en la nube. ¿La información de mi empresa está a salvo? *PCWorld Ecuador*(238), 22-23.
Platespin, Microsoft y Dell. (2007). *Using Virtualization to Achieve Affordable Disaster Recovery: Physical-to-virtual Disaster Recovery from Microsoft, PlateSpin, and Dell.* EE.UU.: Microsoft.
Real Academia Española. (s.f.). *pyme*. Recuperado el 4 de Abril de 2012, de http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=pyme
Rennels, B. (2006). *A practical guide to disaster recovery planning: The basics to getting started.* Whitepaper, Southborough, MA.
Saavedra García, M. L., & Hernández Callejas, Y. (2006). *Caracterización de las MPYMES en Latinoamérica: Un estudio comparativo.* Paper, Universidad Autónoma del Estado de Hidalgo, Estado de Higaldo.
Salazar Villalobos, J. (2008). *Guía para crear un Plan de Recuperación en caso de Desastre en el sistema informático del Centro de Datos de un grupo financiero.* Tesis de Maestría en Administración de Proyectos, San José, Costa Rica.
Slater, D. (2 de Abril de 2012). *CSO Online.* Recuperado el 7 de Abril de 2012, de Business Continuity and Disaster Recovery Planning: The Basics: http://www.csoonline.com/article/204450/business-continuity-and-disaster-recovery-planning-the-basics
SRI. (s.f.). *PYMES*. Recuperado el 12 de Marzo de 2012, de http://www.sri.gob.ec/web/10138/32@public
SRI. (s.f.). *Pymes - Servicio de Rentas Internas del Ecuador.* Recuperado el 4 de Abril de 2012, de http://www.sri.gob.ec/web/10138/32@public
Sungard. (2011). *Best practices for cloud-based recovery.* Whitepaper.
Superintendencia de Compañías del Ecuador. (2011). *DISPOSICIONES LEGALES Y REGLAMENTARIAS SOBRE IMPLEMENTACIÓN DE NIIF.* Resolución, Superintendencia de Compañías del Ecuador, Quito.
Symantec. (Enero de 2011). *Las PyMEs No Están Preparadas Ante Desastres y Deben Actuar Antes de que Sea Tarde.* Obtenido de http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20110110_01
The Disaster Recovery Guide. (2002). *The Disaster Recovery Guide*. Recuperado el 7 de Abril de 2012, de http://www.disaster-recovery-guide.com/doclist.htm
Vargas Palacios, M. d. (2009). *Estudio de factibilidad para la implementación de una empresa de asesoría financiera organizacional, para las PYMEs en la ciudad de Quito.* Tesis de Ingeniería Empresarial, Escuela Politécnica Nacional, Quito.
Vision Solutions. (2008). *La guía fundamental para la recuperación de desastres: Cómo garantizar la continuidad en equipos informáticos y actividades comerciales.* Whitepapaer, Irvine, California. EE.UU .

Viteri Velasco, L. O. (1 de Marzo de 2010). *Proyecto de Ley de Creación, Promoción y Fomento de Micro, Pequeñas y Medianas Empresas*. Recuperado el 13 de Marzo de 2012, de http://asambleanacional.gob.ec/tramite-de-las-leyes.html

Webopedia. (s.f.). *BCP*. Obtenido de http://www.webopedia.com/TERM/B/Business_Continuity_Planning_BCP.html

Wikipedia. (29 de Febrero de 2012). *Computacón grid.* Recuperado el 20 de Abril de 2012, de http://es.wikipedia.org/wiki/Computaci%C3%B3n_grid