

Guía de recuperación ante desastres en Pymes usando computación en la nube

Danilo José Mannella Lemos¹, Francis Salazar Pico²

¹*Maestrante del Departamento de Ciencias de la Computación; Escuela Politécnica del Ejército, Sangolquí, Ecuador*

²*Departamento de Ciencias Económicas, Administrativas y de Comercio; Escuela Politécnica del Ejército, Sangolquí, Ecuador*
danilo.mannella@gmail.com; fsalazar@espe.edu.ec

Resumen: Las pequeñas y medianas empresas (Pymes) deben cuidar hoy en día el que se considera en muchos negocios su activo más importante: su información. En caso de que se produzca un evento no previsto que pueda provocar una interrupción en el acceso a esta información – ya sea que se trate de errores humanos o de otros factores externos – se ve afectada la calidad del servicio y rentabilidad de la empresa. El objetivo general de este estudio consistió en 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 la ciudad de Quito. Para llevar a cabo el objetivo antes planteado se procedió a recopilar la información existente a nivel mundial y local, y a través de métodos científicos como el analítico-sintético, la recolección de información y triangulación, y mediante el uso de técnicas como las entrevistas y cuestionarios se realizó la fase de diagnóstico. Posteriormente se elaboró una guía de implementación para estas Pymes, que fue validada mediante el método de criterio de expertos. Los principales resultados que se obtuvieron de este trabajo fueron que se constató que las Pymes están poco preparadas ante un desastre tecnológico, y usualmente aplican métodos tradicionales de recuperación de información ante desastres que son costosos o ineficientes; adicionalmente se comprobó que existe poco conocimiento sobre la importancia en la elaboración de planes de recuperación ante desastres, y los beneficios que puede proveer la computación en la nube para las Pymes; finalmente, un resultado importante de este trabajo fue que se desarrollaron dos guías de implementación, la una para las Pymes y la otra para la microempresa, siendo ambas de fácil comprensión de términos y especificidad de contenidos, según los expertos.

Palabras clave: Computación en la nube, recuperación de desastres, Pymes

Abstract: Small and medium enterprises (SMEs) should care nowadays what is considered in many businesses to be their most important asset: their information. If an event occurs that can cause unforeseen interruption accessing this information - whether it's about human error or other external factors - the enterprises' service quality and profitability gets an impact. The main objective of this study was to structure a guide that could lead to the proper use of cloud computing and disaster recovery mechanism for SMEs technological services in the city of Quito. To accomplish the objective stated before we proceeded to compile existing information globally and locally, and through scientific methods such as analytic-synthetic, data collection and triangulation, and using techniques such as interviews and questionnaires it was performed the diagnostic phase. After that, a deployment guide was developed for these SMEs, which was validated by the expert judgment method. The main results obtained from this study were that it was found that SMEs are unprepared against technological disaster, and usually apply traditional methods of disaster recovery information that are costly or inefficient; further it was found that there is little knowledge about the importance in the development of disaster recovery plans, and the benefits that cloud computing can provide for SMEs; and finally, an important result of this work was the development of two implementation guides, one for SMEs and another

for microenterprise, being both easy to understand their terms and contents, according to experts.

Keywords: Cloud computing, disaster recovery, SME

I. Introducción

Hoy en día tanto grandes empresas como Pymes (pequeñas y medianas empresas) generan una gran cantidad de información que le son vitales, o críticas, y que deben ser protegidas. El almacenamiento y gestión de esta información debe considerar la posibilidad de que existan interrupciones en el servicio proporcionado al negocio, y éstas se pueden deber a errores humanos – sean éstos intencionados o no – o a factores externos de tipo climático (Rennels B., 2006), y todo esto se conoce como desastre tecnológico empresarial.

Con frecuencia las grandes empresas 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 (Disaster Recovery, 2012). 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, pero 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 (Cruz Mata F.et. All, 2011).

El problema a resolver en este estudio consistió en determinar si “Las Pymes no están preparadas para una recuperación ante desastres tecnológicos de cualquier índole, debiéndose esto al bajo grado de importancia otorgado por parte de sus ejecutivos, y/o debido al desconocimiento de mecanismos de recuperación ante desastres tecnológicos, lo que les provoca incluso pérdidas económicas sustanciales y hasta de cartera de clientes”. En nuestro medio no existen estudios directamente relacionados con la temática propuesta, y he ahí el aporte de este estudio.

Para resolver el problema propuesto el estudio de investigación pasó por diferentes etapas, con sus respectivos métodos, técnicas y resultados esperados, como se aprecia en la Tabla 1.

TABLA 1. Etapas del Estudio de Investigación.

ETAPAS	MÉTODOS	TÉCNICAS	RESULTADOS
FUNDAMENTACION TEÓRICA	<ul style="list-style-type: none"> • Analítico-sintético • Inductivo-deductivo • Sistémico 	<ul style="list-style-type: none"> • Revisión bibliográfica • Internet 	Bases teóricas para conocer el ámbito de aplicación de los DRP y computación en la nube a nivel mundial.
DIAGNÓSTICO	<ul style="list-style-type: none"> • Recolección de la Información • Matemático. • La Triangulación 	<ul style="list-style-type: none"> • Entrevistas • Encuestas 	Informe sobre el estado actual de la implementación de los DRP en PYMEs en Quito.

ETAPAS	MÉTODOS	TÉCNICAS	RESULTADOS
PROPUESTA	<ul style="list-style-type: none"> • Analítico-sintético • Inductivo-Deductivo • Modelación 	<ul style="list-style-type: none"> • Ficha de Resumen 	Presentación de guía de implementación de DRP usando computación en la nube en PYMEs de Quito.
VALIDACIÓN	<ul style="list-style-type: none"> • Criterio de expertos 	<ul style="list-style-type: none"> • Entrevista • Cuestionarios 	Propuesta validada

La principal contribución de este estudio consistió en la elaboración de las guías de implementación de un plan de recuperación ante desastres tecnológicos usando a la computación en la nube aplicado a las Pymes y microempresas de servicios en la ciudad de Quito, contando para ello con el valioso aporte de los expertos que participaron en el estudio, tanto en la fase de diagnóstico como en la validación del documento propuesto.

II. Metodología

El estudio fue organizado en 4 etapas o fases, que se describirán a continuación:

A. FUNDAMENTACIÓN TEÓRICA

a. Estado del arte

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: 1) 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; 2) 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; y 3) El 36% de las Pymes encuestadas manifestó que planea armar un plan de recuperación ante desastres.

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 (Vision Solutions, 2008) se pueden apreciar en la Tabla 2:

TABLA 2. Costos directos e indirectos de contar o no con un DRP.

Costos tangibles / directos	Costos intangibles / indirectos
<ul style="list-style-type: none"> • Pérdida de ingresos por transacciones 	<ul style="list-style-type: none"> • Pérdidas de oportunidades empresariales
<ul style="list-style-type: none"> • Pérdida de salarios 	<ul style="list-style-type: none"> • Pérdida de empleados o desmoralización de los mismos
<ul style="list-style-type: none"> • Pérdida de inventario 	<ul style="list-style-type: none"> • Disminución del valor de las acciones (si es que aplica)
<ul style="list-style-type: none"> • Costes laborales de saneamiento 	<ul style="list-style-type: none"> • Pérdida de los fondos de comercio de los clientes y de los socios
<ul style="list-style-type: none"> • Costos de marketing 	<ul style="list-style-type: none"> • Pérdida de negocio en favor de la competencia
<ul style="list-style-type: none"> • Tasas bancarias 	<ul style="list-style-type: none"> • Mala publicidad y prensa

Costos tangibles / directos	Costos intangibles / indirectos
• Multas legales	

La nube computacional en el Ecuador está dando sus primeros pasos y de acuerdo a Vicente Alonso Holmstron, gerente de Producto Virtual Data Center y Cloud Computing, de la empresa Telconet “en Ecuador se están dando servicios de nubes privadas e híbridas, en las cuales la contratación del servicio tiene una atención personalizada y en donde se dimensionan los requerimientos del cliente” (Computerworld, 2011).

De acuerdo a las estadísticas de la Superintendencia de Compañías del Ecuador¹, al 14 de octubre de 2011, en nuestro país existen 44,396 compañías registradas, y de ellas el 2.93% están en la categoría de grandes empresas, el 8.45% corresponden a medianas empresas, el 27.89% son consideradas pequeñas empresas y el restante 60.49% son microempresas. No existen datos difundidos acerca de un estudio que indique la utilización en el país por parte de las Pymes respecto de una recuperación de desastres usando la computación en la nube, y por ello este estudio permitirá adentrarse un poco más en conocer sobre esta temática. A continuación se mencionará sucintamente la fundamentación teórica en que se sustenta el estudio.

b. Plan 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. 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.

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

Un DRP se compone de los siguientes elementos (Disaster Recovery, 2012):

1. Conocimiento de las actividades de la organización
2. Evaluación de riesgos e impactos
3. Creación del DRP
4. Difusión del DRP
5. Mantenimiento del DRP

Estos componentes se los considera usando esquemas tradicionales de recuperación ante desastres, pero también son la base de la recuperación ante desastres usando a la computación en la nube, que es lo siguiente a tomar en cuenta en este marco teórico.

c. Computación en la nube

Una definición sobre la computación en la nube 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

¹ Tomado del sitio web de la Superintendencia de Compañías: www.supercias.gob.ec

liberados con un esfuerzo administrativo o provisión de administración de servicio mínimo.”(NIST, 2011)

El modelo de servicios de la computación en la nube se basa en tres componentes: IaaS (Infraestructura como Servicio), PaaS (Plataforma como Servicio) y SaaS (Software como Servicio) (INTECO, 2011). Para la recuperación de desastres en la nube, en el caso de las Pymes resulta conveniente usar el modelo llamado IaaS, que 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.

Ahora bien, hay que considerar así mismo que hay tres tipos de nubes: Nubes privadas (creadas y administradas dentro de la empresa, en donde se decide dónde y cómo se ejecutan los procesos dentro de la nube), nubes públicas (en donde todo el control de los recursos, procesos y datos está en manos de terceros) y nubes híbridas (una mezcla de las dos anteriores) (INTECO, 2011). En estos esquemas no hay que descuidar que es importante considerar al PSN (Proveedor de Servicios en la Nube).

d. Recuperación ante desastres en la nube

La computación en la nube, como se ha visto anteriormente, 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. La recuperación ante desastres en la nube presenta algunas ventajas y desventajas, tal como se muestra en la Tabla 3 (IDC, Marzo 2011):

TABLA 3. Ventajas y desventajas de la recuperación ante desastre en la nube.

Ventajas	Desventajas
<ul style="list-style-type: none"> • Reducción de la necesidad de comprar hardware caro (tal como unidades de respaldos, cintas y otros dispositivos de almacenamiento). 	<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Permite la ejecución de respaldos automáticos fuera de la empresa. 	<ul style="list-style-type: none"> • Dependencia.-Relacionado con pérdida de control: 1) Poca o ninguna penetración en los procedimientos de contingencias del PSN, 2) Migración a otro PSN no es fácil, 3) Recursos financieros atados a otra compañía, 4) Posibles problemas de calidad con el PSN.
<ul style="list-style-type: none"> • Incrementa la capacidad de tener acceso a los datos poco tiempo después de un desastre. 	<ul style="list-style-type: none"> • 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.
<ul style="list-style-type: none"> • Un DRP apropiadamente estructurado ofrece la posibilidad de tener desde el PSN el último respaldo restaurado (en minutos), con lo cual se recrea un servidor 	<ul style="list-style-type: none"> • Confianza en el PSN.- 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.

Ventajas	Desventajas
virtual funcional hasta el servidor local sea reemplazado.	
	<ul style="list-style-type: none"> • Inadecuado ancho de banda.- 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.

B. DIAGNÓSTICO

Para llevar a cabo el estudio se emprendió una fase de diagnóstico, con el fin de obtener información sobre el uso de planes de recuperación ante desastres mediante el uso de la computación en la nube en Pymes de servicios. Esta información se la obtuvo de fuentes primarias y secundarias, y metodológicamente se llevaron a cabo los siguientes pasos:

1. Uso de métodos de investigación.- A través del método conocido como criterio de expertos, aplicado a las Pymes de Servicios, se llevó 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.- La técnica usada en esta fase fue la entrevista, aplicadas a los gerentes y/o encargados de tecnología de las Pymes que fueron parte del estudio, en tanto que el instrumento usado fue el cuestionario, que apoyó la técnica antes citada. Aquí se incluyeron los objetivos que se pretendió cumplir, y que están relacionados con las preguntas de investigación.
3. Recopilación de información.- En esta etapa se efectuó la aplicación de la técnica e instrumento detallados en el punto anterior.
4. Análisis e interpretación de resultados.- Aquí se presentaron los resultados luego de la aplicación de los instrumentos de investigación y el análisis correspondiente, y que facilitó la emisión de conclusiones en esta fase. Para esto se usó el diagrama de espina de pescado, llamado también de Ishikawa, junto con el método de Pareto.
5. Hallazgos.- En esta parte final se emitieron las conclusiones a las que se llegó luego de aplicar el método y técnica antes descritos, y que permitieron responder las preguntas de investigación de este estudio, luego de lo cual se procedió a la elaboración de la propuesta de guía de implementación.

C. PROPUESTA

Luego de haber realizado la fase de diagnóstico se percibió que las Pymes, particularmente las medianas empresas tenían una estructura que difería de las pequeñas empresas, y que incluso quienes se podrían beneficiar de este estudio serían también las microempresas, y por ello se elaboraron dos guías. A continuación se menciona el contenido de cada una de las guías:

a. Guía de implementación para Pymes

A continuación se muestran los pasos que deben seguir las Pymes, con la finalidad de implementar soluciones de recuperación ante desastres usando computación en la nube:

1. **Paso 1** – Análisis de riesgos y BIA (qué se debe proteger)
2. **Paso 2** – Determinación de RTO y RPO (inactividad y disponibilidad)
3. **Paso 3** – Virtualizar las aplicaciones claves (migrar de lo físico a lo virtual)

4. **Paso 4** – Evaluación de los servicios y modelos en la nube (hacia un nuevo modelo de recuperación ante desastres)
5. **Paso 5** – Puesta en marcha del DRP en la nube (consideraciones prácticas del DRP)
6. **Paso 6** – Seleccionar el proveedor de soluciones (implementación de la solución con proveedores reales)

b. Guía de implementación para microempresas

La guía de implementación elaborada para Pymes era demasiado compleja para una pequeña empresa, y más todavía para microempresas, y por ello se decidió realizar un producto que sea más asequible para este tipo de negocios. Los pasos que deben seguir los microempresarios en la elaboración de un DRP orientado hacia la nube son:

1. **Paso 1** – Valoración de aplicaciones críticas
2. **Paso 2** – Conocer a la computación en la nube
3. **Paso 3** – Reconocimiento de las fases de una recuperación ante desastres
4. **Paso 4** – Respaldos y recuperación en la nube
5. **Paso 5** – Evaluación y mantenimiento

D. VALIDACIÓN

La validación de la guía se la llevó a cabo mediante el método de criterio de expertos, a través de un cuestionario, y cuyos aportes se detallará más adelante.

III. Evaluación de resultados y discusión

A. FASE DE DIAGNÓSTICO

La fase de diagnóstico fue muy importante para contrastar la realidad de otras Pymes a nivel mundial con la situación local, y fruto de ello se obtuvieron los siguientes hallazgos y consideraciones: 1) 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) También se encontró 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 PSN; 3) En cuanto al manejo de presupuesto para seguridad de TI, no existe un estándar, y hay desde empresas que invierten menos del 1% hasta aquellas que invierten hasta un 40% de su presupuesto, incluyendo aquellas de tipo reactivo que invierten en soluciones de protección de seguridad informática en caso de producirse algún problema; 4) El tiempo de recuperación ante un eventual desastre tecnológico varía en función del tipo de negocio de las Pymes entrevistadas, por ello, hay quienes manifiestan que su recuperación les tomaría de 24 a 48 horas, lo cual paralizaría las actividades del negocio, aunque algunas Pymes manifiestan que este tiempo es menor dado que su información se encuentra respaldada en servidores de PSN; 5) 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; y 6) Existe un conocimiento bastante escaso en cuanto a PSN, 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.

B. ELABORACIÓN DE LAS GUÍAS

Las guías de implementación elaboradas se las puso a consideración de varios profesionales vinculados con Pymes y/o servicios relacionados a la computación en la nube, y se obtuvieron los siguientes hallazgos y recomendaciones: 1) 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; 2) 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; 3) 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, tal y como se muestra en la Figura 1; y 4) 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.

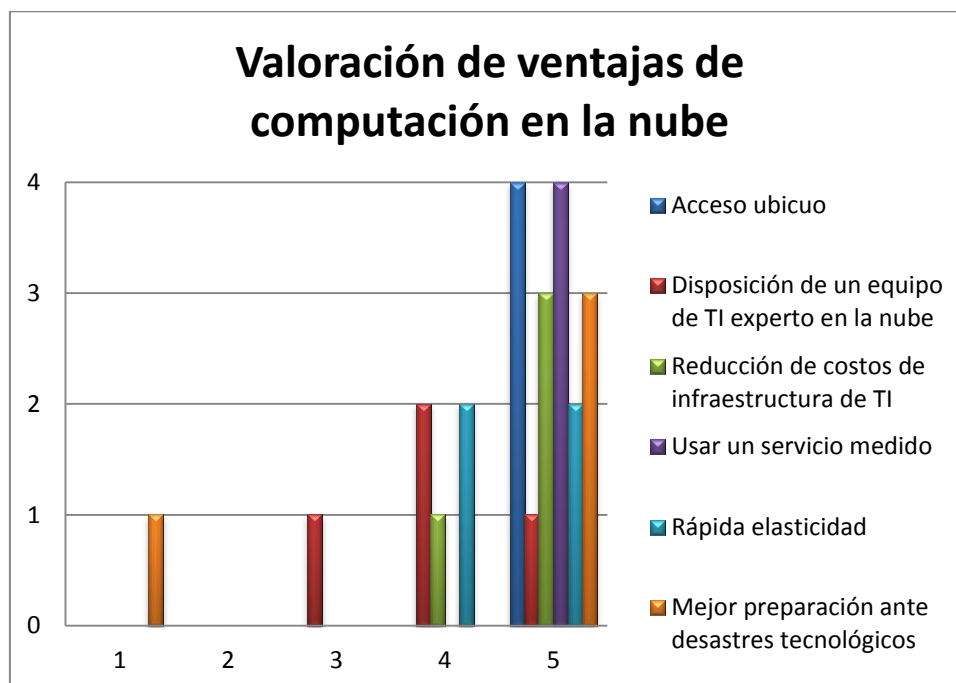


Figura 1. Valoración de ventajas de la computación en la nube de acuerdo a expertos.

IV. Trabajos relacionados

Como se mencionó anteriormente no existe un estudio formal en nuestro país que esté enfocado hacia la implementación de un plan de recuperación ante desastres tecnológicos usando a la computación en la nube con énfasis en las Pymes, sin embargo hay estudios sobre las ventajas del manejo de computación en la nube (Oviedo, A., 2011), así como una propuesta de una metodología para la preparación de un DRP para aplicaciones críticas (Torres, D., 1998).

V. Conclusiones y trabajo futuro

Fruto de esta investigación se ha podido llegar a las siguientes conclusiones:

- Las Pymes, 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, lo cual resulta ineficiente y/o costoso.
- Existe poco conocimiento sobre los beneficios que puede proveer la computación en la nube para las Pymes, 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.
- 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 que aquellas que no tengan contemplado ningún DRP, o que sigan un modelo tradicional que puede resultar costoso y/o ineficiente.
- La valoración usada por expertos en la validación de las guías de implementación claramente indican que las guías son de fácil comprensión de términos, y la especificidad del contenido contribuirá a una mejor implementación de las mismas.

Luego del estudio efectuado se recomienda tomar en cuenta lo siguiente:

- Las empresas que proveen servicios en la nube a nivel local deberán considerar a las Pymes como un potencial mercado a atender, analizando costos personalizados diseñados para este segmento que este mercado este momento no está siendo atendido.
- El presupuesto para seguridad de la información se sugiere incrementar en algo más del 10% de su presupuesto global, lo que les permitirá estar mejor preparados ante varios de los desastres tecnológicos citados en este estudio.
- 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, E-Vault, Rackspace, etc.
- Uno de los principales factores a tomar en cuenta por parte de las Pymes para la contratación de un PSN es la confiabilidad y esquemas de seguridad de la empresa,

por tanto se recomienda que se revise detalladamente el SLA que se firmará entre las partes.

- 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.

Agradecimientos

Para llevar a cabo este estudio se acudió a diversos actores relacionados con la temática tratada, lo cual incluye Pymes, empresas proveedoras de servicios en la nube así como desarrolladores de soluciones de computación en la nube, y de este modo deseo agradecer a todas aquellas instituciones que fueron parte del estudio, y cuyos criterios fueron de relevancia en el levantamiento de información así como en la validación de las guías propuestas tanto para microempresas como para Pymes.

Referencias bibliográficas

- Computerworld. (2011). La nube computacional un modelo de aprovechamiento de infraestructura que avanza para quedarse. Ediworl, Ed. Computerworld Ecuador (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. (2012). Disaster Recovery. Recuperado el 12 de Abril de 2012, de <http://www.disasterrecovery.org/index.html>
- IDC (Marzo, 2011). Improving Small Business Profitability by Optimizing IT Management. Whitepaper. MA, EE.UU
- INTECO. (2011). Guía para empresas: seguridad y privacidad del cloud computing. Madrid, España: INTECO.
- NIST. (2011). The NIST Definition of Cloud Computing. Whitepaper. NIST, U.S. Department of Commerce. Gaithersburg, EE.UU.
- Oviedo, A (2011). Estudio de las ventajas del manejo de Cloud Computing (computación en la nube) y propuesta de un modelo de uso para nuestro medio. Tesis. PUCE. Quito, Ecuador.
- Rennels, B. (2006). A practical guide to disaster recovery planning: The basics to getting started. Whitepaper, Southborough, MA.
- Symantec. (Marzo, 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
- Torres, D. (1998). Metodología para la preparación de un plan de recuperación de aplicaciones críticas y datos en casos de desastre. Tesis. EPN. Quito, Ecuador.
- Vision Solutions. (2008). La guía fundamental para la recuperación de desastres: Cómo garantizar la continuidad en equipos informáticos y actividades comerciales. Whitepaper, Irvine, California. EE.UU.