

García, Eduardo Luis; Falzoni, Ariel Osvaldo; Guagnini, Juan Pablo; Biscaychipy, Ernesto; Otero, Sandra, Beryl; Dominguez, Martín Alberto; Iezzi, Ignacio

PLAN DE SEGURIDAD PARA PROCESOS ADMINISTRATIVOS EN LA NUBE (CLOUD COMPUTING) DE PEQUEÑAS Y MEDIANAS EMPRESAS

XI Jornadas DUTI (E-Book)

2016, pp. 206-222

García, E.L., Falzoni, A.O., Guagnini, J.P., Biscaychipy, E., Otero, S.B, Dominguez, M.A., Iezzi, I. (2016). Plan de seguridad para procesos administrativos en la Nube (Cloud Computing) de pequeñas y medianas empresas. En: García, L. E., compilador (2016). XI jornadas Duti. Bahía Blanca. En RIDCA. Disponible en:

<http://repositoriodigital.uns.edu.ar/handle/123456789/4781>



Esta obra está bajo una Licencia Creative Commons
Atribución-NoComercial-CompartirIgual 2.5 Argentina
<https://creativecommons.org/licenses/by-nc-sa/2.5/ar/>

Plan de seguridad para procesos administrativos en la Nube (*Cloud Computing*) de pequeñas y medianas empresas

Eduardo Luis García, Ariel Osvaldo Falzoni, Juan Pablo Guagnini,
Ernesto Biscaychipy, Sandra Otero, Martín Domínguez, Ignacio Iezzi
egarcia@criba.edu.ar; afalzoni@criba.edu.ar; jpguagnini@yahoo.com.ar;
biscaychipy@yahoo.com.ar; oterosandra_b@hotmail.com;
madomin@criba.edu.ar; ignacioiezzi@yahoo.com.ar;

Departamento de Ciencias de la Administración
Universidad Nacional del Sur

Área temática: Proyectos de Investigación: resultados parciales de proyectos en curso.

Palabras claves: Seguridad – PyME – Sistemas - Administrativos – *Cloud Computing* – Computación en la Nube

1. Resumen

3.b) Hipótesis de Trabajo

Todas las organizaciones, incluyendo a las pymes, dejan en esta “Nube” uno de los activos más importantes para ellas: La Información y los Procesos administrativos que permiten utilizarla.

Las PyME no siempre tienen conciencia del riesgo mencionado y, si lo tienen, no siempre están en condiciones de enfrentar por sí mismas este problema, por lo que recibirán con agrado una solución en materia de seguridad aplicable a su situación particular.

3.c) Objetivos

Desarrollar un Plan de seguridad específico, adecuado a la realidad de las Pequeñas y Medianas Empresas que utilizan computación en la Nube (*Cloud computing*), para proponerlo como modelo a implementar en las mismas.

3.d) Metodología de Trabajo

Entre pasos de la metodología, se realizará un relevamiento en empresas de la zona para determinar sus principales fortalezas y debilidades frente a las amenazas que pueden afectar los sistemas de información administrativos.

En este nuevo proyecto, se utilizará como herramienta para el relevamiento, además de encuestas y entrevistas, un formulario web para incluir a colegas de otras Universidades que han ofrecido su participación dentro de la Asociación de Docentes Universitarios de Sistemas y Tecnología de la Información —Ciencias Económicas— (DUTI).

Todo eso conducirá a la elaboración de un plan de seguridad en el tema objeto de estudio, adecuado a este tipo de empresas que se pondrá a disposición de las mismas para su utilización.

3.e) Formación de Recursos Humanos

Capacitación de los miembros del proyecto en investigación.

Formación de alumnos del Departamento de Ciencias de la Administración como colaboradores en el proyecto.

Integración de colegas de otras Universidades que han ofrecido su participación dentro de la Asociación de Docentes Universitarios de Sistemas y Tecnología de la Información —Ciencias Económicas— (DUTI).

2. Introducción

Nuevamente recurrimos a la presentación del PGI para realizar la introducción a este trabajo:

Debemos aclarar que la presentación a realizar en las DUTI se refiere a los resultados parciales del proyecto de investigación en curso y específicamente al informe del trabajo de campo.

2.1 Significado de la Investigación: Interés e importancia del tema

El uso de tecnología informática y el avance notorio de Internet sigue abriendo nuevos campos de trabajo e investigación.

Los sistemas administrativos de las organizaciones van aprovechando esos cambios desde los comienzos mismos del uso de las computadoras.

Sin duda que en este momento uno de los paradigmas más impactantes es el denominado Computación en la Nube (*Cloud Computing*). Ello implica que los procesos informáticos y el almacenamiento de datos ya no están físicamente en la propia organización sino en servidores de Internet accesibles desde cualquier lugar del mundo.

Todo parece indicar que el presente y el futuro de las empresas están en *Cloud Computing*, no sólo localmente (desde un servidor), sino también desde una PC, un teléfono o cualquier dispositivo con conexión a Internet.

Todas las organizaciones, incluyendo a las pymes, dejan en esta “Nube” uno de los activos más importantes para ellas: la información y los procesos administrativos que permiten utilizarla.

Ello potenciado por la vinculación de computadoras en redes dentro de la empresa (intranet), redes exclusivas con clientes y proveedores (extranet) y el acceso al resto del mundo por la vía de la vinculación entre redes de computadoras (Internet).

Es evidente que muchas transacciones no solo ya no quedan respaldadas en papel, sino que quedan almacenadas digitalmente y la validez de las mismas se ve refrendada por diversos sistemas de “firma digital”.

El avance en este sentido hace esperar que la mayoría de las operaciones se realicen de esta forma.

Esto plantea serios problemas de seguridad que puedan poner en riesgo la existencia misma de la empresa y su continuidad.

Podemos afirmar que las pymes no siempre tienen conciencia del riesgo mencionado y si la tienen, no siempre están en condiciones de hacer frente por sí solas a este desafío.

Al igual que en anteriores PGI, creemos que brindarles un modelo de plan de seguridad adecuado a su realidad es poner en sus manos una herramienta que puede dar lugar a solucionar esta situación.

2.2 Originalidad y finalidades específicas de la propuesta

En el PGI desarrollado durante 2012-2013 nos propusimos como finalidad desarrollar un plan de seguridad adecuado a la realidad de las Pequeñas y Medianas Empresas de la zona de influencia de la Universidad Nacional del Sur para proponerlo como modelo a implementar en las mismas.

Así se avanzó notablemente detectando las principales situaciones en las empresas a las que llegamos con el proyecto y finalizamos realizando recomendaciones de seguridad que provocaban el mayor impacto en el resguardo de los activos informáticos de la empresa.

Se utilizó para tal fin un procedimiento original consistente en estudiar por medio de un relevamiento, las Fortalezas, Oportunidades, Debilidades y Amenazas (FODA) que las afectan.

En este nuevo PGI, queremos concentrar nuestra tarea en lo que suele denominarse Computación en la Nube (*Cloud Computing*) por la magnitud que está teniendo este paradigma en el procesamiento de datos de todo tipo de organizaciones.

Nuevamente estará destinado específicamente a Pequeñas y Medianas Empresas que no siempre disponen de los medios para determinar en forma individual su propio plan de seguridad.

2.3 Plan a desarrollar

2.3.1 Revisión Bibliográfica

Como parte del plan a desarrollar se propone la recopilación y revisión de la bibliografía referida al tema objeto de este proyecto.

2.3.2 Hipótesis de Trabajo

Como quedó dicho en el punto 1, sin duda que en este momento uno de los paradigmas más impactante es el denominado Computación en la Nube (*Cloud Computing*). Ello implica que los procesos informáticos y el almacenamiento de datos ya no están físicamente en la propia organización sino en servidores de Internet accesibles desde cualquier lugar del mundo.

Todas las organizaciones, incluyendo a las pymes, dejan en esta “Nube” uno de los activos más importantes para ellas: la información y los procesos administrativos que permiten utilizarla.

Esto plantea serios problemas de seguridad que puedan poner en riesgo la existencia misma de la empresa y su continuidad.

Las pymes no siempre tienen conciencia del riesgo mencionado y, si lo tienen, no siempre están en condiciones de enfrentar por si mismas este problema, por lo que recibirían con agrado una solución en materia de seguridad aplicable a su situación particular.

2.3.3 Objetivos

Desarrollar un plan de seguridad específico, adecuado a la realidad de las Pequeñas y Medianas Empresas que utilizan Computación en la Nube (*Cloud Computing*), para proponerlo como modelo a implementar en las mismas.

2.3.4 Metodología de Trabajo

Los pasos siguientes de la metodología, ya utilizada exitosamente en el PGI anterior, están referidos específicamente al tema descrito en el objetivo: Computación en la Nube (*Cloud Computing*). Pueden considerarse como una continuidad del proceso anterior enfocando en un aspecto puntual de la seguridad de las pymes.

Por una parte se realizará una revisión bibliográfica del material más actualizado en el tema, simultáneamente, se evaluará el software del que pueda disponerse en materia de cifrado de información, auditoría de eventos, antivirus, control de claves de acceso, verificación de la asignación de recursos y prioridades, etc.

Por otro lado se realizará un relevamiento en empresas de la zona para determinar sus principales fortalezas y debilidades frente a las amenazas que pueden afectar los sistemas de información administrativos.

En forma paralela se estudiarán las oportunidades que están al alcance de las empresas en materia de hardware, software, instalaciones, capacitación del personal, proveedores de servicios de internet, etc.

En este nuevo proyecto, se utilizará como herramienta para el relevamiento, además de encuestas y entrevistas, un formulario web para incluir a colegas de otras Universidades que han ofrecido su participación dentro de la Asociación de Docentes Universitarios de Sistemas y Tecnología de la Información —Ciencias Económicas— (DUTI).

Todo eso conducirá a la elaboración de un plan de seguridad en el tema objeto de estudio, adecuado a este tipo de empresas que se pondrá a disposición de las mismas para su utilización.

2.3.5 Formación de Recursos Humanos

Capacitación de los miembros del proyecto en investigación.

Formación de alumnos del Departamento de Ciencias de la Administración como colaboradores en el proyecto.

Integración de colegas de otras Universidades que han ofrecido su participación dentro de la Asociación de Docentes Universitarios de Sistemas y Tecnología de la Información —Ciencias Económicas— (DUTI).

3. Desarrollo

Reiteramos que la presentación a realizar en las DUTI se refiere a los resultados parciales del proyecto de investigación en curso y específicamente al informe del trabajo de campo.

Por lo tanto describiremos todo lo relacionado con el mismo.

3.1 Descripción de la forma en que se realizó el trabajo de campo

Para la realización del trabajo de campo se tomaron algunas decisiones, en el mes de octubre del año 2015:

3.1.1 Adopción del modelo elaborado por la Mg. Carola Jones en la UNC.

Para ello mantuvimos una reunión personal en Bahía Blanca con ella quién nos explicó la modalidad y alcance de su modelo.

3.1.2 Preparación de formulario web

En el equipo se definió el contenido del formulario tomando textualmente el modelo propuesto pero agregando una cantidad significativa de preguntas relacionadas específicamente con el objetivo del PGI.

3.1.3 Distribución de los alumnos de Análisis de Sistemas Administrativos en equipos

Al comenzar el dictado de la materia, se constituyeron 56 grupos de 2 a 4 alumnos.

Cada grupo contactó una empresa y la presentó al docente responsable de su tarea, para su aceptación. El docente realizó una somera evaluación de la empresa presentada y evaluó si se encontraba dentro de las pautas propuestas.

El cronograma del trabajo de campo, dentro del cronograma general de la materia tuvo las siguientes instancias de desarrollo, revisión y evaluación

Trabajo de campo integrador de la asignatura. Este trabajo será una actividad grupal que se propone múltiples objetivos. Por un lado, pretende favorecer la integración de contenidos teóricos y su aplicación al abordaje e interpretación de una situación de la realidad. También procura propiciar el desarrollo de competencias transversales muy requeridas en el mercado laboral de los profesionales en ciencias económicas, tales como el trabajo en equipo, la gestión de proyectos, las capacidades de análisis, síntesis y de comunicación, tanto oral como escrita. Este trabajo se desarrollara a lo largo del cuatrimestre.

Práctico n.º 1. La actividad en éste punto, consiste en tomar contacto con una empresa, por los grupos, de envergadura acorde a las necesidades de este trabajo, con el objetivo de realizar una encuesta preliminar (puede ser vía e-mail) y una visita a la empresa para realizar una entrevista a un integrante de la empresa que tenga conocimiento y, en lo posible, haya participado en procesos de relevamiento de datos y procesos, selección, implementación y/o gestión de SI/TIC (Sistemas de Información y las Tecnologías de Información y Comunicación).

Se sugiere que la organización en cuestión cuente al menos con un sistema de aplicación (software de negocios) que de soporte a la actividad principal de la misma, como manera de asegurar que posee los elementos indispensables para que su estudio sea relevante.

- ° Quedan excluidas los monousuarios, las empresas cuya implementación de TIC se limita a herramientas de ofimática (procesador de texto, planillas de cálculo).
- ° Los sistemas informáticos pueden ser desarrollados y/o gestionados de forma interna, tercerizada o mixta.

Práctico n.º 2. Realizan el primer contacto con la empresa elegida, y completan la encuesta que servirá para obtener una descripción general de la misma y conocer en cierta medida los principales elementos inherentes a los SI (Sistemas de Información).

- ° Dicha encuesta podrá ser dirigida al contacto logrado dentro de la organización seleccionada en forma personal o vía e-mail.
- ° En la página web de la Universidad se encuentra el formulario de la encuesta, que será común a todos los grupos, y les servirá de base para evaluar cuál será la temática más pertinente para abordar en la entrevista.

Práctico n.º 3. Analizar las respuestas obtenidas en la encuesta del trabajo de campo y ayudados por la bibliografía sugerida a su disposición en la página de ésta asignatura, deben evaluar y redactar cuál será la temática más pertinente para abordar la entrevista.

Práctico n.º 4. Elaborar un resumen en dónde se identifiquen los conceptos en juego, estableciendo su importancia y el modo en que éstos se interrelacionan. Se sugiere completar el texto con algún esquema o mapa conceptual de su elaboración.

- ° Se valorará: consignar las referencias bibliográficas, colocando, autor y año, título de la obra y editorial. También tener presente que en el resumen no puede componerse exclusivamente de citas textuales, y cuando estas se utilicen deben aparecer entre comillas y con el autor referenciado (apellido, año).

Práctico n.º 5. habiendo estudiado en profundidad la temática, el equipo deberá utilizando el cuestionario; deberá procurarse entrevistar a la persona más idónea en relación a la temática seleccionada (práctico n.º 3) que pueda contactar en la organización y redactar un resumen de dicha entrevista con los temas abordados en la misma. El objetivo de la entrevista es doble: a) conocer ¿Cómo lo hacen?, esto es, registrar la forma en que las empresas visitadas abordan y resuelven la temática SI/TIC, b) comprender ¿por qué lo hacen de éste modo?, modo particular en que la empresa aborda y resuelve la temática SI/TIC.

Práctico n.º 6. En función de lo relevado y la investigación teórica realizada, se requiere que cada grupo elabore un texto en formato de historia o artículo periodístico (u otro formato sugerido por el docente), redactando detalladamente la situación de la organización en relación a la temática seleccionada.

Práctico n.º 7. La siguiente etapa será la elaboración de las conclusiones, donde se requiere que cada equipo analice la situación relevada en función de los conceptos teóricos estudiados y compare las similitudes y diferencias entre lo que dice la teoría con lo que pasa en la realidad del caso estudiado. Se pretende que en la conclusión:

- 1) El equipo realice una reflexión crítica, en base a:
 - La contrastación del caso particular con el marco teórico.
 - La contextualización del caso, en base a los datos relevados mediante la encuesta inicial.
 - En base al modelo de fases de crecimiento de Richard Nolan, identificar la fase en que se encuentra la empresa.
- 2) No se pretende que el equipo ofrezca una propuesta de mejora, aunque pueden dar su opinión al respecto, ofreciendo argumentos y fundamentos.
- 3) En ningún caso debe consistir en un resumen del trabajo.

El **trabajo de campo** deberá exponerse en forma oral y en dicha instancia, cualquier integrante del equipo debe ser capaz de sintetizar y transmitir las ideas y aspectos centrales del trabajo realizado con claridad y elocuencia.

Debe ser apoyada por una presentación sintética clara y representativa de los aspectos centrales del trabajo, en 5 diapositivas (opcional) que deberán contener:

- a- Integrantes del grupo, docente de la comisión, características generales de la empresa (sin dar necesariamente el nombre): mención del sector, rubro de la empresa y temática abordada.
- b- Aspectos salientes de la encuesta general: tamaño, organigrama, SI/TI.
- c- Esquema resumen de temática abordada.
- d- Resultados de la entrevista.
- e- Conclusiones.

La exposición oral es, a su vez, una instancia de intercambio intergrupar. Por lo que se pondrá en juego la capacidad de defender e intercambiar ideas y conclusiones.

Cada integrante del equipo debe responder y argumentar respecto de la totalidad del trabajo.

Gestión del proyecto y trabajo en equipo

El equipo deberá cumplir con las entregas pautadas, ya que éste aspecto también será evaluado. A fines de lograr un mejor desempeño, se recomienda distribuir roles y tareas; definir tiempos y medios de comunicación.

Cada uno pondrá a prueba su capacidad para generar aportes, ser flexibles para recibir sugerencias y colaborar con otros. Algunos pueden ser designados explícitamente o naturalmente cumplir roles de coordinación y/o liderazgo de grupo.

Al finalizar toda la tarea prevista en el cronograma del trabajo de campo, se seleccionaron los 5 mejores trabajos por su elaboración, contenido y exposición oral.

A esos alumnos (18 en total) se les otorgó un certificado de reconocimiento por su labor y una BECA para participar de la jornada de apertura de las IX DUTI 2016 a realizarse en Bahía Blanca, el 15 de septiembre.

3.1.4 Respuesta a los cuestionarios por parte de las empresas

Una vez aceptada la empresa, cada grupo de alumnos logró que su empresa responda al formulario web, para ello los docentes tuvieron en cuenta el desarrollo indicado en el punto

anterior, en especial indicaron que se excluyan los monousuarios, las empresas cuya implementación de TIC se limita a herramientas de ofimática (procesador de texto, planillas de cálculo), aunque los sistemas informáticos pueden ser desarrollados y/o gestionados de forma interna, tercerizada o mixta.

3.1.5 Entrevistas a las empresas

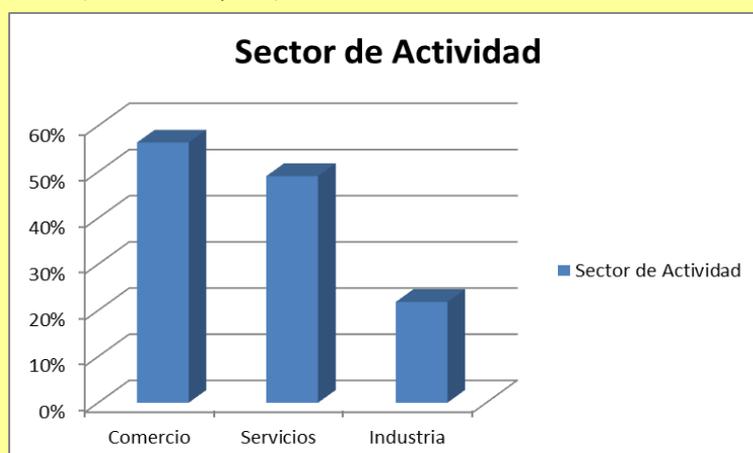
Objetivo del PGI, sobre Seguridad en los Sistemas de Información Administrativos, plasmados con encuestas a organizaciones de la zona, el desarrollo de cursos sobre el tema; permitiendo determinar que la seguridad se compone de un conjunto de elementos que se permeabiliza en el Plan de Seguridad de la organización. Siendo esta el conjunto de medidas preventivas, detectivas y correctivas que nos permiten asegurar la integridad, confidencialidad y privacidad de los recursos informáticos, tanto el software, hardware, instalaciones, información y personal.

4. Datos obtenidos a partir de las encuestas y entrevistas

A los efectos de esta presentación, hemos presentado únicamente los datos tabulados que se relacionan con el objetivo del PGI

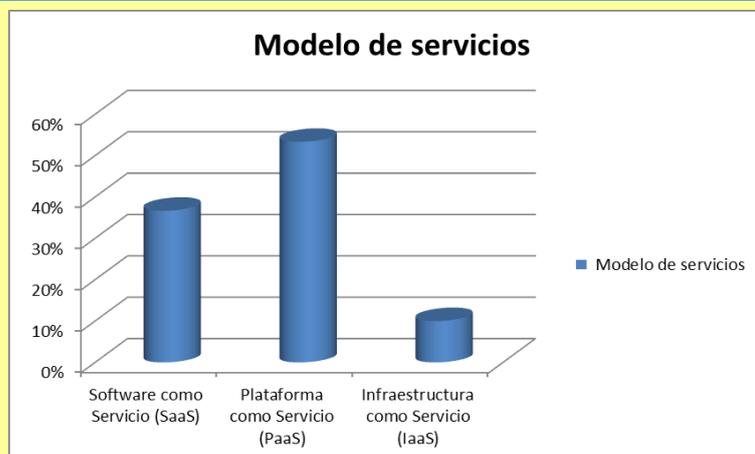
Sector de actividad	
Comercio	56 %
Servicios	49 %
Industria	22 %

(Más de una opción)



Nos permite determinar esta pregunta de las encuestas, que las actividades de la ciudad y su zona de influencia es principalmente comercial o de prestación de servicios.

Modelo de servicios	
Software como Servicio (SaaS)	37 %
Plataforma como Servicio (PaaS)	53 %
Infraestructura como Servicio (IaaS)	10 %
	100 %

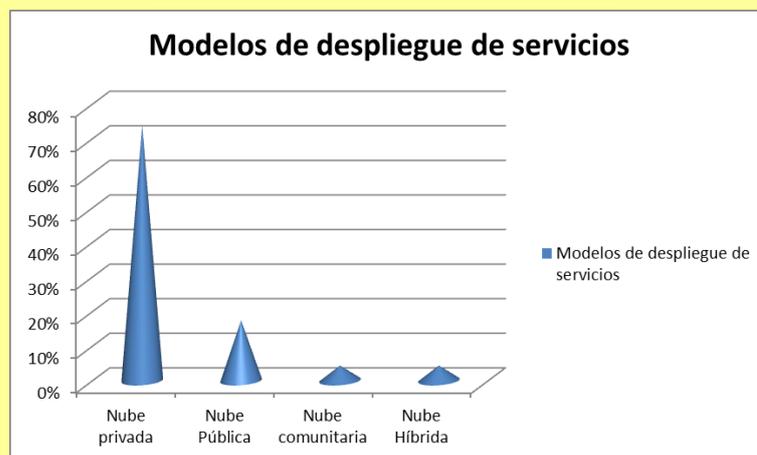


Se puede observar que la mayoría de las organizaciones utilizan Plataforma como Servicio (PaaS) y en segundo término Software como Servicio (SaaS).

El 53 % de las empresas utilizan Plataforma como Servicio (PaaS), dado que se trata de un nivel intermedio, en la cual se encarga de entregar una plataforma de procesamiento completa al usuario y sin tener que comprar y mantener el hardware y software.

Luego con un 37 % le sigue Software como Servicio (SaaS), en la cual se encarga de entregar el software como un servicio a través de internet siempre que lo demande el usuario. Permite el acceso a la aplicación utilizando un navegador web, sin necesidad de instalar programas adicionales.

Modelos de despliegue de servicios	
Nube privada	74 %
Nube pública	17 %
Nube comunitaria	4 %
Nube híbrida	4 %
	100 %



La respuesta mayoritaria de los modelos de despliegue de servicios tiene preponderancia la nube privada, que son creadas y administradas por un única entidad que decide donde y cuando se ejecutan los procesos dentro de la nube.

Aplicaciones que está utilizando su organización	
Software de gestión contable	92 %
Software de gestión comercial	63 %
Software de factura electrónica	63 %
Software de gestión de la producción	26 %

(Más de una opción).

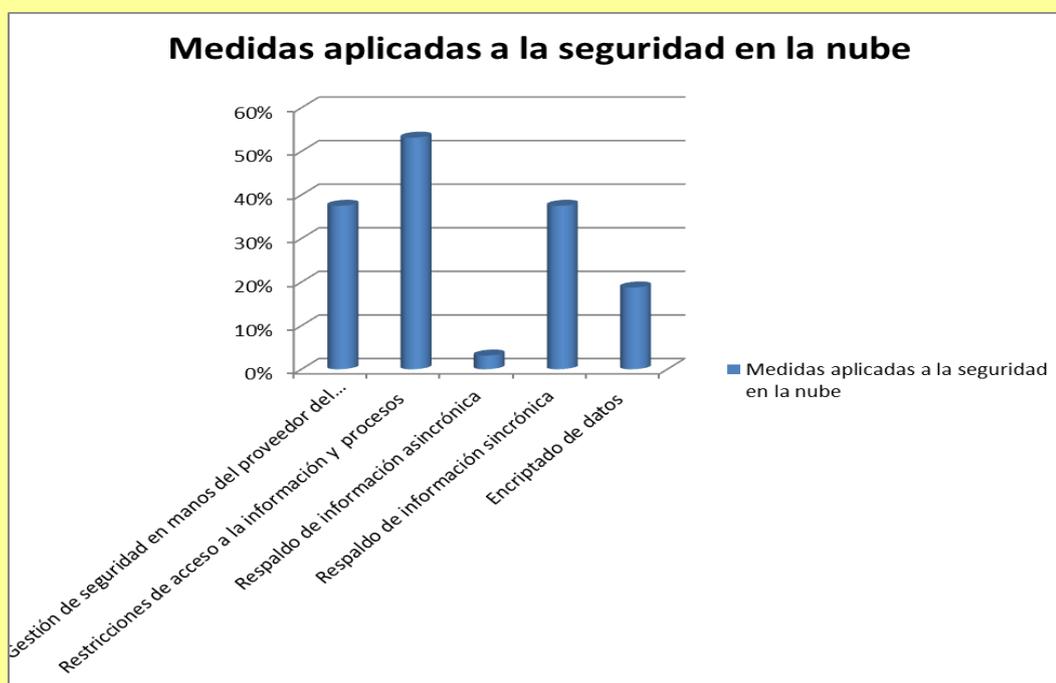


Dentro de las aplicaciones que están utilizando las organizaciones tiene preponderancia el software de gestión contable, seguido en igual proporción software de gestión comercial y de

factura electrónica. Esto se condice con las características principales de las empresas del sector comercial.

Medidas aplicadas a la seguridad en la nube	
Gestión de seguridad en manos del proveedor del servicio	38 %
Restricciones de acceso a la información y procesos	53 %
Respaldo de información asincrónica	3 %
Respaldo de información sincrónica	38 %
Encriptado de datos	19 %

(Más de una opción).



La respuesta mayoritaria con respecto a Medidas aplicadas a la seguridad en la nube es que tienen mayores restricciones de acceso a la información y procesos, medida preventiva que tendría a través de administración rigurosa de claves de acceso, un procedimiento automático de registro de accesos a los mimos y una auditoria que permita hacer un seguimiento de las situaciones posibles.

Siguiendo en igual medida:

- a) La Gestión de seguridad en manos del proveedor del servicio, dado que este se encargaría de garantizar la seguridad física en sus centros de procesos de datos; deberá impedir que personas no autorizadas entren en dichos edificios, a su vez deberá mantener sus equipos actualizados tanto a nivel de hardware como software para hacer frente a las amenazas existentes en internet.

b) Respaldo de información sincrónica, se desarrolla en tiempo real.

5. Conclusiones

El *Cloud Computing* o computación en la nube es una nueva forma de prestación de servicios globales que, apoyándose sobre una infraestructura tecnológica, permite a usuarios y empresas optimizar costes y recursos en función de sus necesidades de tratamiento de información. Este paradigma, que se está generalizando rápidamente debido a sus ventajas, supone también un reto importante para la protección y privacidad de datos.

La revolución tecnológica que actualmente estamos viviendo bien podría ser la más profunda de nuestra historia. Los servicios convergen y pasan del mundo físico al mundo digital, siendo accesibles desde cualquier dispositivo. Un hecho relevante es que nuestros datos ya no residen en nuestros ordenadores sino en una Internet Global que adquiere entidad propia y se convierte en mucho más que una simple infraestructura de conexión: es la plataforma que ofrece servicio a millones de dispositivos inteligentes conectados a la red.

Esto permite que los consumidores, empresas o particulares, no se tengan que preocupar de cómo se provee el servicio que necesitan. Las empresas no podrán evitar este cambio si no quieren perder el tren del avance tecnológico, y esto implicará tomar decisiones sobre la dirección a seguir para mejorar sus negocios.

Como toda tecnología, el *Cloud Computing* no está exento de riesgos. Cuanto más compleja es la infraestructura informática utilizada, más posibles vulnerabilidades aparecen. A continuación se describen los principales riesgos de seguridad y privacidad que pueden generar un impacto en los recursos en la nube:

Uno de los mayores riesgos a los que se enfrenta todo sistema informático es la pérdida de datos, ya sea porque un usuario ha borrado información accidentalmente, porque haya un fallo en algún dispositivo hardware o por culpa de un ataque informático. Perder los datos no solo significa tener que rehacer parte del trabajo realizado, sino que en muchos casos puede significar cuantiosas pérdidas económicas. La solución a este problema se enfoca desde dos puntos de vista principales.

- 1. Por un lado, una correcta política de seguridad limita la libertad de los usuarios para borrar elementos del sistema, protege los equipos ante el ataque de software malintencionado y además impide que personas ajenas a la organización accedan o corrompan los datos.

- 2. Por otra parte, una correcta política de copias de seguridad permite recuperar los datos aun cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware. La recuperación frente a un ataque puede ser tan sencilla como la restauración de una copia instantánea, anterior de la máquina virtual.

Como en todo acuerdo empresarial, la relación entre el proveedor de servicios en la nube y el cliente (en este caso, el contratante) debe estar regulada por un contrato. Este contrato debe definir claramente la posición de cada una de las partes así como sus responsabilidades y obligaciones.

Los términos de uso se encargan de definir las especificaciones técnicas más importantes relacionadas con la entrega y la calidad del servicio. Estas últimas establecen los niveles de rendimiento y disponibilidad garantizados por el proveedor.

Se vislumbra con las encuestas procesadas, una mayor utilización dentro del sector comercial (software sector comercial, contable y factura electrónica). Teniendo preponderancia la nube privada, que son creadas y administradas por un única entidad que decide donde y cuando se ejecutan los procesos dentro de la nube.

Se debe considerar que en las empresas encuestadas sobre las medidas aplicadas a la seguridad, hay preponderancia en la Restricciones de acceso a la información y procesos.

6 Referencias Bibliográficas

Pérez, Pablo; Gutiérrez, Cristina; y Rodríguez, Susana [s/f]. *Guía para empresas: Seguridad y privacidad del Cloud Computing*. Instituto Nacional de Tecnologías de la Comunicación (INTECO). Gobierno de España. Ministerio de Industria, Turismo y Comercio.

García, Eduardo (2016). *Seguridad en los Sistemas de Información Administrativa. Apunte de cátedra Análisis/Estudios de Sistemas Administrativos*. UNS.

Burch Grudnitski [s/f]. *Diseño de Sistemas de Información. Teoría y Práctica*. [s/l]: Editorial Megabyte.

Whitten, Jeffrey y Barlow, Victor [s/f]. *Análisis y Diseño de Sistemas de Información*. 3ra edición, [s/l]: Editorial Mc. Graw Hil.

Kendall y Kendall (2014). *Análisis y Diseño de Sistemas*. 3ra edición, Prentice Hall: Editorial PHH.

Beltrán Pardo, Marta y Sevillano Jaén, Fernando (2014). *Cloud Computing, tecnología y negocio*, Madrid: Ediciones Paraninfo.

Ruparelia, Nayan (2016). *Cloud Computing*. Cambridge: The MIT Press.

222

Puyol Montero, Javier (2013). *Algunas consideraciones sobre Cloud Computing*. Madrid: Boletín Oficial del Estado.

Muller, Hunter (2012). *On top of the cloud*. New York: John Wiley & Sons Inc.

Torres, Jordi (2015). *Empresas en la nube Ventajas y retos del Cloud Computing*. Barcelona: Libros de Cabecera.