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

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

Departamento de Ciencias de la Administración. Universidad Nacional del Sur

Área temática: Investigación
Palabras claves: Seguridad – PyME – Sistemas - Administrativos – Cloud Computing – Computación en la Nube

RESUMEN

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.

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 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 recibirían con agrado una solución en materia de seguridad aplicable a su situación particular.

Siendo la Seguridad de la Información un tema muy amplio, este PGI está dirigido específicamente a la seguridad de los procesos desarrollados "en la nube".

1 INTRODUCCIÓN

OBJETIVO DEL PGI:

El objetivo del PGI es 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.

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.

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 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 recibirían con agrado una solución en materia de seguridad aplicable a su situación particular.

Siendo la Seguridad de la Información un tema muy amplio, este PGI está dirigido específicamente a la seguridad de los procesos desarrollados "en la nube".

2 REVISIÓN BIBLIOGRÁFICA

Se realizó una revisión bibliográfica del material más actualizado en el tema mientras que, simultáneamente, se evaluó el software del que puede 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.

A los efectos de adoptar definiciones y conceptos generales sobre los principales riesgos de seguridad y privacidad que pueden afectar los recursos en la nube y se optó por la Guía para empresas de INTECO [1].

3 ASPECTOS METODOLÓGICOS

Entre los pasos de la metodología, se realizó 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.

Para la realización del trabajo de campo se tomaron algunas decisiones

[1] *"Guía para empresas: seguridad y privacidad del cloud computing" ha sido elaborada por el equipo del Observatorio de la Seguridad de la Información de INTECO* (web: www. inteco.es)

y se concretaron las acciones correspondientes:

3.1 Adopción del modelo denominado "Guía para el trabajo de campo de Tecno1" elaborado en la UNC. *2*

Para ello mantuvimos una reunión personal en Bahía Blanca con la Mg. Carola Jones quién nos explicó la modalidad y alcance de ese modelo.

3.2 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.

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

3.3 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 en el 1º cuatrimestre de 2016 y 52 grupos de 3 a 4 alumnos en el 1º cuatrimestre de 2017.

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 instancias de desarrollo, revisión y evaluación.

3.3.1 Respuesta a los cuestionarios y entrevistas a las empresas

Una vez aceptada la empresa, cada grupo de alumnos invitó a su empresa a responder al formulario web. Este formulario se elaboró en forma conjunta con docentes de la Universidad Nacional de Córdoba, en la que también se aplicó el procedimiento.

Una segunda instancia fue la realización de una entrevista en la que completaron algunos aspectos planteados en el cuestionario.

Luego continuó el proceso programado para que cada grupo resumiera y presentara su caso.

Por otro lado, los docentes tabularon y analizaron los resultados obtenidos.

Sobra la base de todo este proceso que duró aproximadamente 2 años, teniendo en cuenta los cambios vertiginosos propios de la tecnología actual, es que pudimos ofrecer a las PyMEs las recomendaciones relacionadas con los procesos en la nube (cloud computing) que se detallan en el ANEXO II.

---

[2] Jones, C.; Ortega, F.; Peretti, F.; Aronica, S. "Guía para el trabajo de campo de Tecno1" (2015). Facultad de Ciencias Económicas, Universidad Nacional de Córdoba, Argentina.

4 RESULTADOS Y DISCUSIÓN

4.1 Análisis de resultados

El proyecto de Grupo de Investigación se llevó adelante mediante la metodología indicada en el punto anterior.

Del total de las empresas propuestas por los alumnos, se consideraron las respuestas de 84 de ellas que resultaron homogéneas en relación a las especificaciones realizadas (cantidad de equipos, tipos de procesos, etc.).

En forma simultánea, se utilizaron los resultados obtenidos en la UNC que permitieron incorporar 173 empresas más.

La tabulación de los resultados de las encuestas provocó un amplio intercambio de ideas entre los docentes que participaron del proyecto. De la misma manera le permitió a cada uno de ellos evaluar y proponer nuevos desafíos a los grupos de alumnos participantes del mismo.

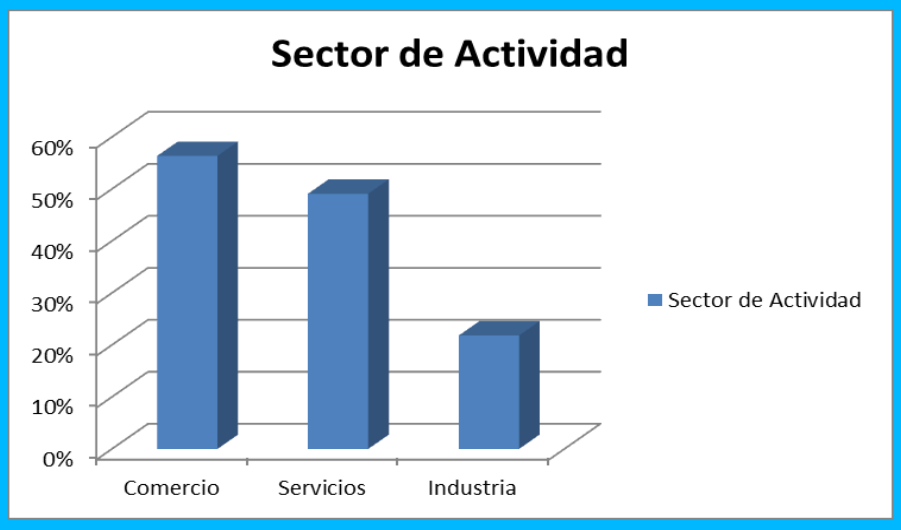
Los resultados obtenidos permitieron extraer conclusiones sobre la necesidad de continuar formando a los directivos de las PyMEs de tal manera que tomen acabada conciencia de la importancia de la Seguridad cuando se trata de la información de la cual depende su empresa.

- **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

.1 Sector de Actividad

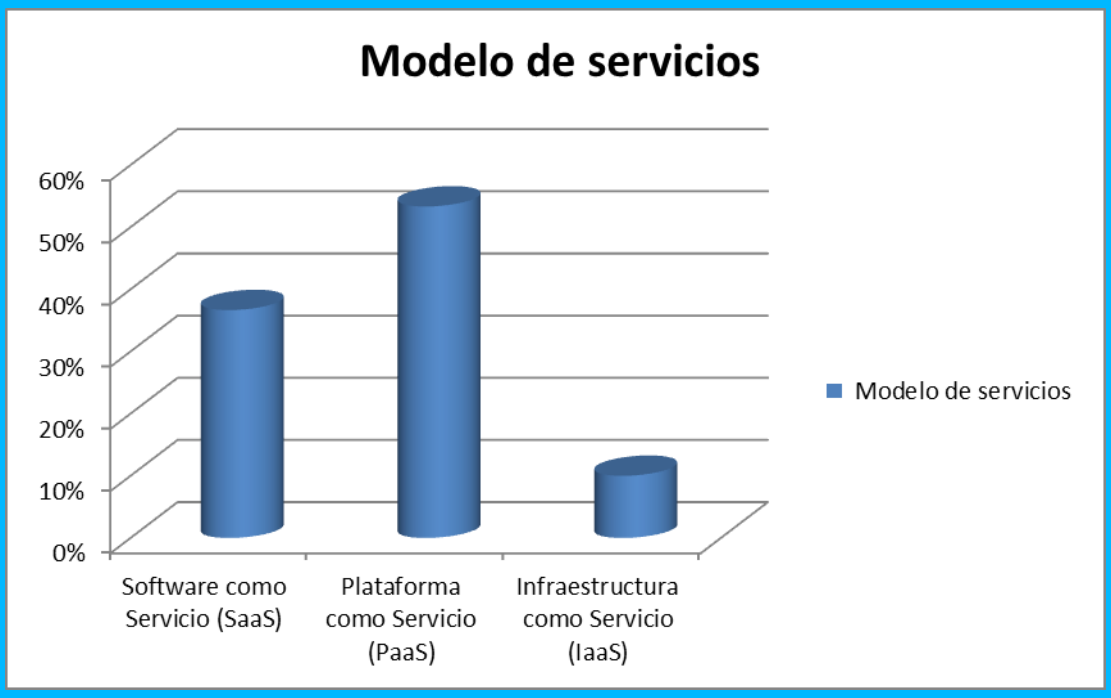
Comercio	56%
Servicios	49%
Industria	22%



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.

.2 Modelo de servicios

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



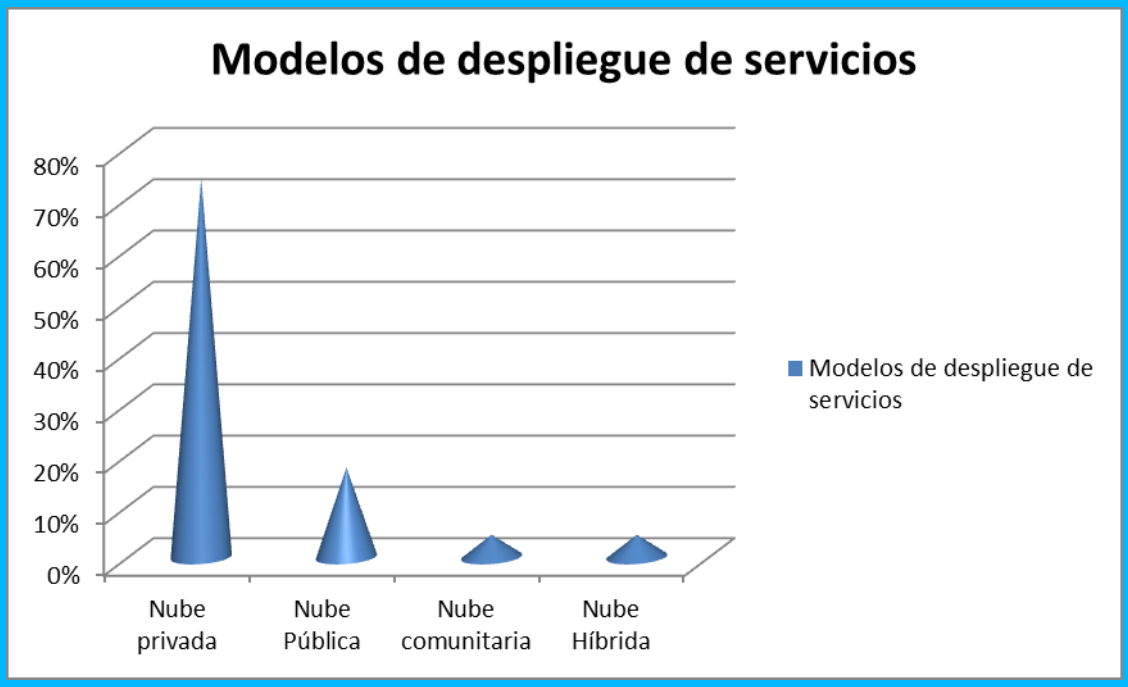
Se puede observar que la mayoría de las organizaciones utilizan Plataforma como Servicio (PaaS) y en segundo término Software como Servicio (SaaS).

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.

.3 Modelos de despliegue de servicios

Nube privada	74%
Nube Pública	17%
Nube comunitaria	4%
Nube Híbrida	4%
	100%

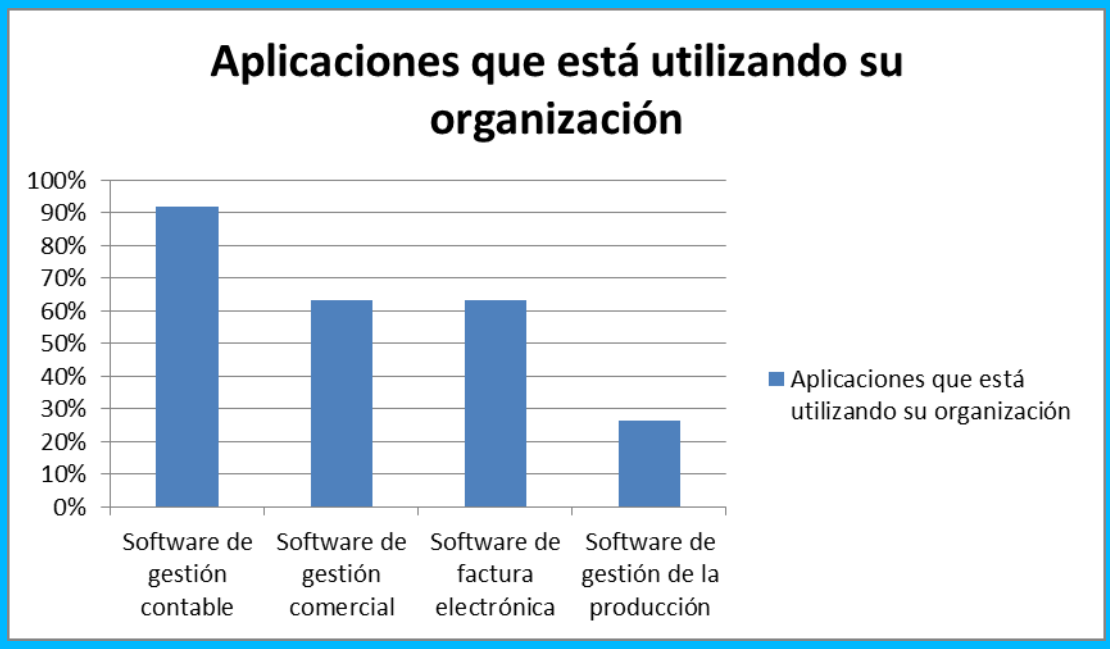


La respuesta mayoritaria de los modelos de despliegue de servicios tiene preponderancia la nube privada, que son creadas y administradas por un única entidad que decide donde y cuando se ejecutan los procesos dentro de la nube.

.4 *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%

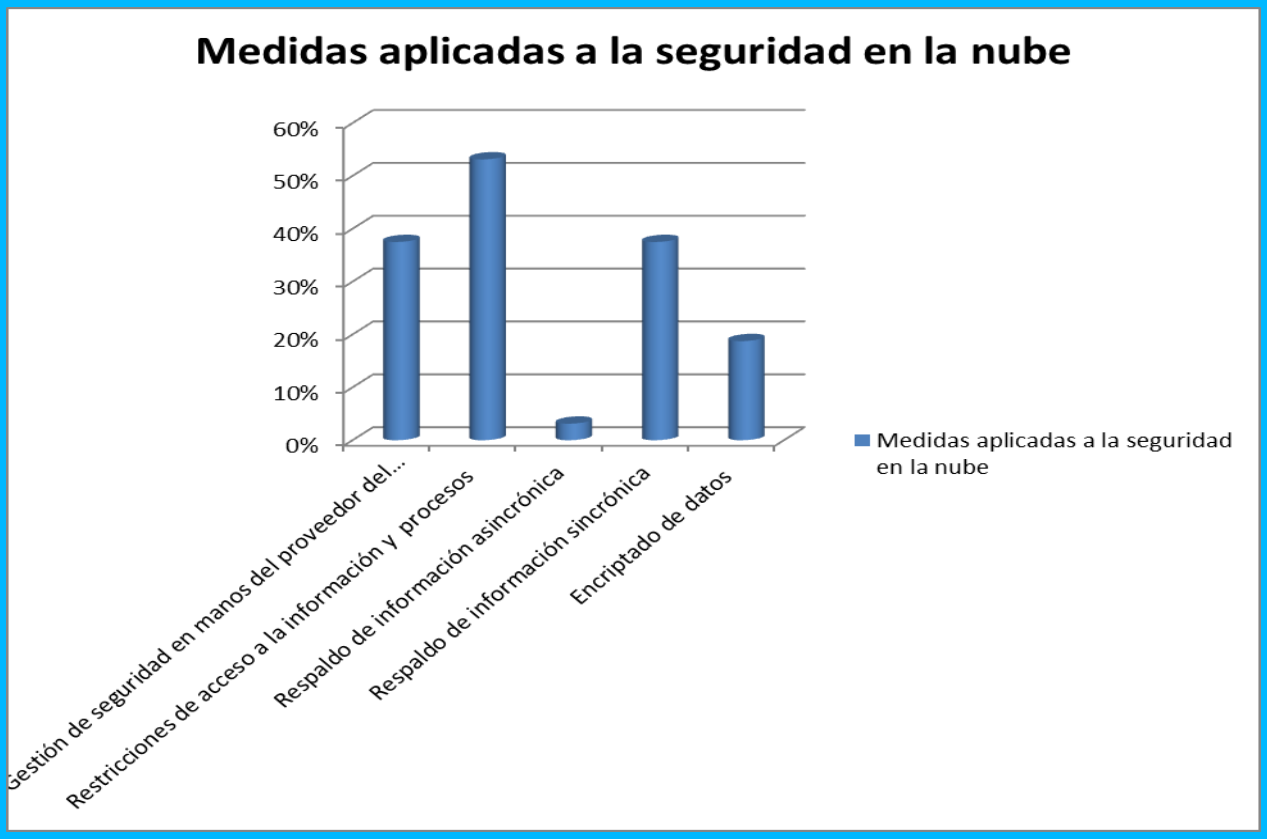
(más de una opción)



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.

.5 *Medidas aplicadas a la seguridad en la nube*

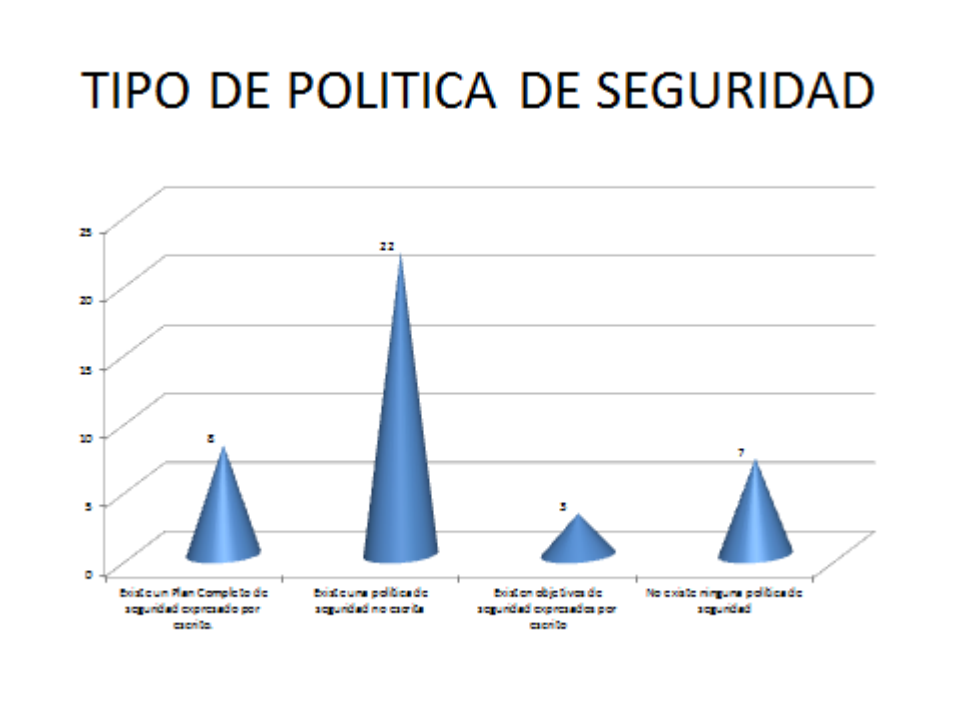
Gestión de seguridad en manos del proveedor del servicio	38%
Restricciones de acceso a la información y procesos	53%
Respaldo de información asincrónica	3%
Respaldo de información sincrónica	38%
Encriptado de datos	19%



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.

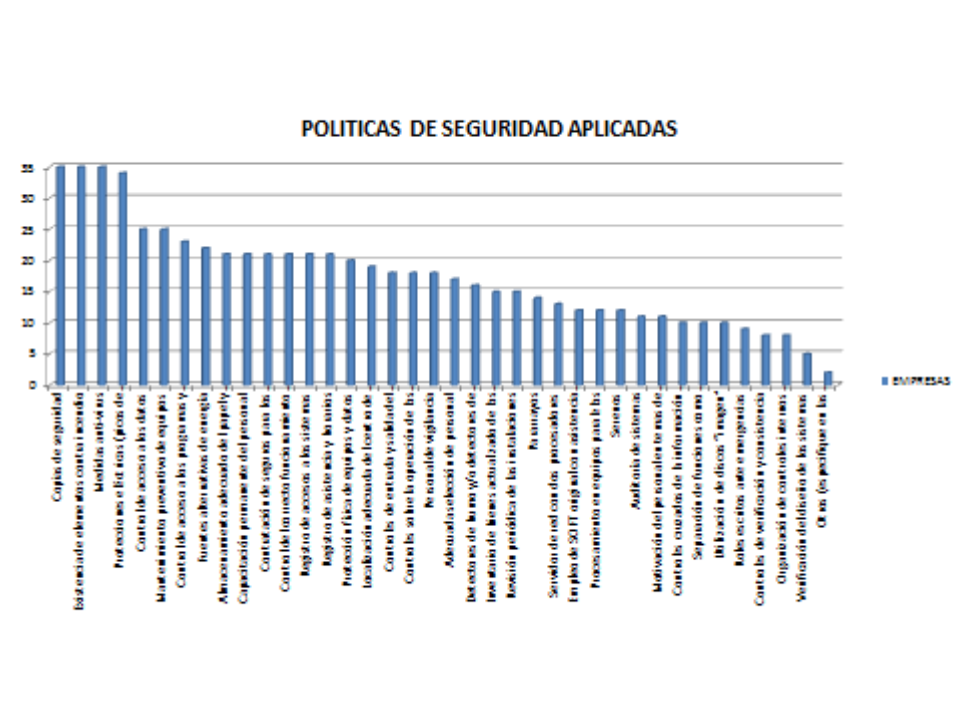
b) Respaldo de información sincrónica, se desarrolla en tiempo real.



.6 TIPO DE POLITICA DE SEGURIDAD

El 27% de las empresas encuestadas no respondió esta pregunta. De las restantes, el 55% señaló que Existe una política de seguridad no escrita, el 20% respondió que Existe un Plan Completo de seguridad expresado por escrito; el 18 % manifestó que no existe política de seguridad alguna, en tanto que el 7% expresó que Existen objetivos de seguridad expresados por escrito.

Nótese que la preocupación de las empresas por tener políticas de seguridad sobre los datos y recursos es generalizada (77% de las empresas), sin embargo, la inmensa mayoría de ellas no posee pautas de seguridad por escrito, claras e inequívocas .



.7 MEDIDAS DE SEGURIDAD ADOPTADAS

Teniendo en cuenta que para cada pregunta formulada la respuesta podía existir en algunos casos múltiples respuestas, se observó que por ejemplo el 31% de las empresas no ha adoptado ninguna medida de seguridad física o lógica sobre los recursos informáticos de la organización. A su vez, en los casos en que sí han implementado políticas de seguridad concretas, las mas populares fueron realizar copias de seguridad (backups), gestionar software antivirus, tomar medidas contra incendios y contra fallos de tensión eléctrica; todas ellas con casi el 90% de las respuestas.

Le siguieron políticas vinculadas con los controles de acceso a los datos, equipos y procesos, controles sobre el personal (también capacitación sobre el recurso humano en materia de seguridad informática), y mantenimiento preventivo de los equipos, con entre el 54% y 64% de las empresas relevadas. Sin embargo, a pesar del elevado porcentaje de empresas que capacitan a sus recursos humanos, sólo el 28% efectúa tareas de motivación del personal en materia de seguridad.

Políticas de seguridad mas complejas pero no por ello menos importantes como Controles cruzados de la información por medio de distintos procesos, Utilización de discos “imagen”, Controles de verificación y consistencia y Verificación del diseño de los sistemas fueron aplicados solo por el 22% promedio de las empresas encuestadas. Solo el 23% de las empresas prevee roles escritos a seguir por sus integrantes ante emergencias.

Llama la atención que menos de la mitad de las empresas que respondieron, gestionó una adecuada localización del centro de procesamiento de datos, política vital en materia de seguridad.

.8 EXISTENCIA DE PLAN DE CONTINGENCIAS ESCRITO

El 36% de las empresas no sabe/no contesta esta pregunta. De las restantes, casi un 72% afirmaron NO tener un plan de contingencias escrito para enfrentar las consecuencias de una amenaza concretada.

Es decir, si bien un alto porcentaje de organizaciones se preocupa por aplicar medias de seguridad sobre sus recursos físicos y lógicos, muy pocas preveen los pasos a seguir en caso de concreción de una amenaza.

.9 PRINCIPALES DIFICULTADES PARA IMPLEMENTAR UNA POLÍTICA ADECUADA DE SEGURIDAD

A esta pregunta (que era de respuesta múltiple), el 29% de las respuestas obtenidas fue FALTA DE TIEMPO.

Luego la selección de personal y las inversiones de capital representaron el 22% y el 21% de las respuestas.

En menor medida la complejidad de la tecnología, los gastos en personal y la falta de apoyo de la dirección.

Un dato importante es que entre selección de personal e inversiones de capital representan casi más del 40% de las respuestas obtenidas, lo que indica que la política de seguridad va en correlación con el presupuesto o con la economía del ente.

La Falta de tiempo pensamos que en general se debe a que las pymes dejan en terceros la decisión de la protección de sus datos o que se sienten absorbidas por otras cuestiones que no tienen que ver con los sistemas de información, aunque saben de la importancia de contar con una política de protección de datos.

4.2 Impacto sobre el aprendizaje de los alumnos en el dictado de la materia

Un resultado no incluido en la formulación del PGI se relaciona con el impacto que tuvo la propuesta en los alumnos al punto que alrededor de 20 de ellos fueron becados para participar de la apertura de las Jornadas DUTI 2016 y uno de los grupos tuvo la oportunidad de exponer y defender su propuesta en el transcurso de las mismas.

En esa misma línea, en el año 2017 se propuso nuevamente el trabajo de campo como parte de los contenidos de la materia.

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 enumeran los principales riesgos de seguridad y privacidad que pueden generar un impacto en los recursos en la nube y se realizan algunas recomendaciones[3].

4.3 Recomendaciones de seguridad a las empresas

4.3.1 Política de seguridad – Sistema de Gestión de la Seguridad de la Información (SGSI)

• 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.

• 3. Relación con el proveedor: 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.

4.3.2 Seguridad por parte del Proveedor

Una parte importante de la seguridad del sistema recae sobre la

[3] *"Guía para empresas: seguridad y privacidad del cloud computing" ha sido elaborada por el equipo del Observatorio de la Seguridad de la Información de INTECO* (web: www. inteco.es)

empresa que provee los servicios en la nube

El proveedor de servicios en la nube se encarga de garantizar la seguridad física en sus centros de procesos de datos.

Deberá impedir que personas no autorizadas entren en dichos edificios para, por ejemplo, robar sus equipos.

Deberá mantener sus equipos actualizados tanto a nivel hardware como software para hacer frente a las amenazas existentes en Internet

La virtualización puede ser vista como una forma de aumentar la seguridad de los procesos que se ejecutan en la nube. Varias máquinas virtuales pueden ser ejecutadas en un único servidor pero cada máquina virtual ejecuta un sistema operativo de forma aislada

La deslocalización de los datos es una característica que también puede ser explotada como un mecanismo de seguridad en sí misma. La segmentación de datos permite que los datos de un cliente residan en diferentes servidores, incluso en diferentes centros de datos.

4.3.3 Seguridad por parte de la PYME

Todos los sistemas administrativos requieren de medidas Preventivas, Detectivas y Correctivas para proteger la Integridad, Confidencialidad y Disponibilidad de sus recursos o activos informáticos, es decir el Hardware, el Software, las Instalaciones, los Datos y las Personas.

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.

Se debe considerar que, en las empresas encuestadas sobre las medidas aplicadas a la seguridad, hay preponderancia (casi 100 %) en la Restricciones de acceso a la información y procesos.

Debe mantener políticas de seguridad tradicionales

- control de usuarios
- revisión y cambio periódico de contraseñas seguras
- el borrado de cuentas de usuario que ya no se utilizan
- la revisión del software para comprobar que no tiene vulnerabilidades

Algunas otras políticas de seguridad específicas

- Control Perimetral

Para llevarlo a cabo, es recomendable la instalación y configuración de un firewall o cortafuegos.

- Criptografía

en el uso de los servicios en la nube proporciona un nivel superior de seguridad

- Control de accesos
  comprobar la actividad informática, detectar incidentes y formular un plan de acción

Copias de seguridad

- una correcta política de copias de seguridad permite recuperar los datos aún cuando todas las medidas de seguridad han fallado o cuando se produce una avería en un componente hardware.
- Existen diversas modalidades y mecanismos para hacerlas:
  - Copias en dispositivos físicos o en la nube
  - Realizadas en forma total, incremental o diferencial
  - Tomando períodos regulares de tiempo o según las necesidades
  - Programadas, automatizadas, manuales
  - Respaldo de información de forma asincrónica o sincrónica

No puede ignorarse que, cuando todo falle, la copia de seguridad realizada correctamente es la que nos permitirá recuperar la información perdida.

5 CONCLUSIONES

El cloud computing o computación en la nube es una forma de prestación de servicios globales que, apoyándose sobre una infraestructura tecnológica, permite a usuarios y empresas optimizar costos y recursos en función de sus necesidades de tratamiento de información.

Este paradigma, que se generalizó 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.

Se comprueba en las encuestas procesadas que las empresas van tomando conciencia del valor de la información e intentan resguardarla de diversas formas, sin perder su disponibilidad.

Debemos mencionar que hay que continuar trabajando para crear conciencia respecto de la importancia de contar con un Plan de Seguridad,

dentro de un Sistema de Gestión de la Seguridad de la Información que permita reducir el impacto de una amenaza que se concreta, permitiendo a la empresa volver a estar en condiciones de continuar trabajando en el menor tiempo posible y con el menor costo para la organización.

Cumpliendo con el objetivo inicial, el PGI culminó con la elaboración de un PLAN DE SEGURIDAD titulado **Recomendaciones de Seguridad para PYMES**, adecuado a este tipo de empresas que se puso a disposición de las mismas para su utilización. Se ha desarrollado en el punto **4.3 Recomendaciones de seguridad a las empresas**.

De la misma manera se realizó una conferencia especial para docentes, alumnos y empresas a la que asistieron varias de las empresas participantes.

6 REFERENCIAS BIBLIOGRÁFICAS

- PÉREZ, Pablo; GUTIÉRREZ, Cristina; RODRÍGUEZ, Susana. 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.
- Jones, C.; Ortega, F.; Peretti, F.; Aronica, S. “Guía para el trabajo de campo de Tecno1” (2015). Facultad de Ciencias Económicas, Universidad Nacional de Córdoba, Argentina
- BELTRÁN PARDO, Marta. SEVILLANO JAÉN, Fernando. Cloud computing, tecnología y negocio, Madrid, España, Ediciones Paraninfo S.A., 2014.
- TORRES, Jordi. Empresas en la nube Ventajas y retos del Cloud Computing, Barcelona, Libros de Cabecera, 2015.