CLOUD COMPUTING PARA PYMES

JENNIFER CÉLLERI-PACHECO / JAVIER ANDRADE-GARDA / SANTIAGO RODRÍGUEZ-YÁÑEZ

Editorial UTMACH

REDES 2017
COLECCIÓN EDITORIAL

Cloud Computing para PYMEs

Jennifer Célleri-Pacheco
Javier Andrade-Garda
Santiago Rodríguez-Yáñez
Coordinadores

Primera edición en español, 2018

Este texto ha sido sometido a un proceso de evaluación por pares externos con base en la normativa editorial de la UTMACH

Ediciones UTMACH

Gestión de proyectos editoriales universitarios

174 pag; 22X19cm - (Colección REDES 2017)

Título: Cloud Computing para PYMEs. / Jennifer Célleri-Pacheco / Javier Andrade-Garda / Santiago Rodríguez-Yáñez (Coordinadores)

ISBN: 978-9942-24-107-8

Publicación digital

Título del libro: Cloud Computing para PYMEs.

ISBN: 978-9942-24-107-8

Comentarios y sugerencias: editorial@utmachala.edu.ec

Diseño de portada: MZ Diseño Editorial

Diagramación: MZ Diseño Editorial

Diseño y comunicación digital: Jorge Maza Córdova, Ms.

Km. 5 1/2 Vía Machala Pasaje

www.utmachala.edu.ec

Machala - Ecuador

Índice

Dedicatoria

A nuestros familiares y amigos
Los autores

Introducción

En este libro se analiza al Cloud Computing desde un enfoque interdisciplinario y enriquecedor desde múltiples perspectivas como: ciencias de la información, ciencias de la comunicación, ciencias jurídicas y ciencias empresariales. Los autores identifican los riesgos y beneficios en el uso del Cloud como modelo de emprendimiento para pequeñas y medianas empresas, desde un enfoque social, tecnológico, jurídico y de negocio.

Esta propuesta editorial se ha desarrollado en las siguientes áreas del conocimiento: Tecnologías de la información y la Comunicación, Ciencias Humanas y Sociales, Ciencias Empresariales, entre otras.

En total, se han escrito siete capítulos con la participación activa de expertos en el área, e investigadores universitarios, quienes con entusiasmo han asumido el ejercicio novel de la escritura académica.

Con la coordinación de Santiago Rodríguez, Javier Andrade y Jénnifer Célleri, Cloud Computing para PYMEs espera convertirse en un material divulgativo y de fácil consulta para el lector ávido de conocimiento; en especial, se dirige hacia los emprendedores y microempresarios con intención de expandir su negocio y servicios hacia el Cloud.

Como autores colaborativos y en red del texto, esperamos satisfacer las necesidades de conocimiento en torno al Cloud en un intento de cumplir con la misión de informar, formar y educar de forma consciente, analítica y responsable.

Agradecemos la convocatoria de la Editorial UTMACH, Colección Redes, y desde ya esperamos que esta primera edición de Cloud Computing para PYMEs tenga la debida acogida y aceptación del lector.

04 Capítulo In-seguridad del Cloud Computing

Jennifer Celleri-Pacheco; Byron Ramirez Carrillo;
Santiago Rodríguez-Yánez

Se puede considerar al Cloud Computing como un aliado de aquellas empresas que no cuentan con la suficiente inversión monetaria para adquirir recursos tecnológicos y competir tecnológicamente con las grandes empresas. Este factor podría ser la principal razón por la que las empresas migran a este tipo de servicio.

Los avances en la capacidad de procesamiento, conexión a Internet y dispositivos móviles, junto a las importantes inversiones realizadas por las grandes empresas que dominan el panorama tecnológico mundial, han propiciado la rápida

Jennifer Celleri-Pacheco: Ingeniera en Sistemas, Especialista en redes de comunicación, Magíster en Informática Empresarial, Candidata a Doctora en Nuevas Tecnologías de la Información y Comunicación por la Universidad de A Coruña. Autora de artículos científicos. Ponente en congresos académicos. Directora del Grupo de Investigación GICOWEB. Profesora Titular de la Universidad Técnica de Machala. Experiencia de 10 años en la empresa privada en el área de sistemas.

Byron Ramirez Carrillo: Ingeniero en Sistemas. Analista de la Unidad de Tecnologías de Información (TIC) de la Universidad Técnica de Machala. Máster en Seguridad Informática por la Escuela Politécnica Superior de Litoral (ESPOL).

Santiago Rodríguez-Yánez: Diplomado, Licencia con Grado y Doctor en Informática por la Universidad de A Coruña, España. Profesor Titular de la Universidad de A Coruña. Coautor de capítulos de libros y publicaciones internacionales de prestigio sobre ingeniería de software y participante en diferentes proyectos y convenios de investigación y docencia. Sus intereses de investigación incluyen el modelado conceptual, la gestión del conocimiento y el e-learning.

evolución e implantación del Cloud Computing hasta tal punto que muchos usuarios ya disfrutan los servicios en la nube sin darse cuenta (INTECO, 2011).

Sin embargo, cuando una empresa decide migrar al cloud se enfrenta a varios factores relacionados a la seguridad de su preciada información: ¿Perdería el control de mis datos? ¿Estaría sujeto a la seguridad que el proveedor me pueda brindar y perdería la autonomía y el gobierno de seguridad de mi empresa? ¿Se pierde la gestión de los recursos tecnológicos? ¿Sigo siendo el dueño de la información? ¿Cómo se realizaría la identificación y el control de acceso a los recursos?. Estas dudas son muy comunes para quien entregará su información a terceras personas, de las que conoce muy poco. Por esta razón es de suma importancia que el usuario establezca requisitos mínimos que deben cumplir los proveedores de este servicio.

La información es uno de los activos más importantes para una empresa, tanto así que su evolución como tal y la evolución en su tratamiento ha llevado a que se escriban libros y estudios sobre cómo tratarla y aprovecharla, incluso sobre su estado y seguridad.

Para que una empresa pueda establecer una adecuada gestión de la información y su seguridad, puede apoyarse en herramientas como las normas ISO 27001 (ISO/IEC, 2013) e ISO 20000 (ISO/IEC, 2005), y la legislación existente en el país, además de implementar la infraestructura necesaria para la seguridad física. Para una empresa que no tenga el recurso humano y financiero suficiente para la implementación de las herramientas anteriormente mencionadas, es muy difícil establecer un nivel de seguridad óptimo para su información, acorde a las amenazas cibernéticas existentes en la actualidad, convirtiéndose de esta forma en un blanco fácil para ataques de cualquier tipo.

La NIST ha desarrollado varios documentos que sirven como guía para las empresas, pero no es la única organización que se ha dedicado a desarrollar textos que dan luces a quienes se inician en este mundo de orquestar recursos

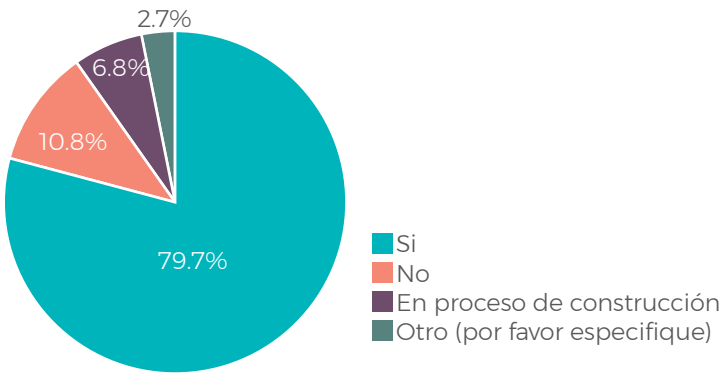
tecnológicos a través de Internet. También ENISA ha publicado grandes aportes referentes a esta tecnología, así como la Cloud Security Alliance y la consultora Gartner (INTECO, 2011).

Según la empresa auditora Deloitte en su estudio sobre Cyber Risk & information Security Study (2016), cuatro de cada diez organizaciones sufrieron una brecha de seguridad en los últimos 24 meses. Por otro lado, un estudio global realizado por el Ponemon Institute (2017) develó que el costo total promedio de una violación de datos fue de $3.62 millones de dólares y de $141 por pérdida o robo de registros. Con esos datos, seguramente, un ataque a la infraestructura de una pequeña empresa sería catastrófica.

Por este motivo, las empresas, entre ellas proveedoras de servicios en la nube, se han visto en la necesidad de tomar medidas para detectar eventos de amenaza en su información y la de sus clientes. Una de estas medidas es la creación de un Centro de Operaciones de Seguridad (SOC por sus siglas en inglés). El objetivo fundamental de un centro de operaciones de seguridad es el monitoreo, contención y remediación de amenazas a los sistemas de información de una empresa.

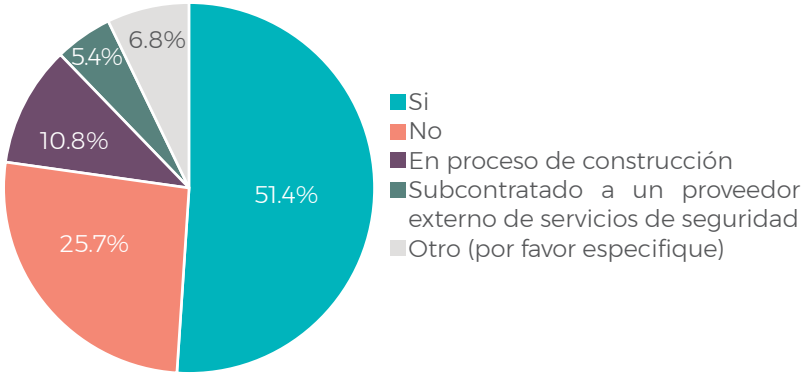
En el Cyber Risk Report 2016 desarrollado por la Hewlett Packard Enterprise, en un grupo de 299 empresas y responsables de respuesta ante incidentes, el 80% de los encuestados reportaron contar con funciones de operación de seguridad dentro de su organización (ver Gráfico 1). Asimismo, el 51% advierte la presencia de un SOC formal y el 11% reportó que está en proceso de construcción de uno (ver Gráfico 2).

Gráfico 1: Respuestas a la pregunta: "¿Su organización tiene una función de operaciones de seguridad?"



Fuente: Cyber Risk Report (Hewlett Packard Enterprise, 2016)

Gráfico 2: Respuestas a la pregunta: "¿Su organización tiene un centro de operaciones de seguridad (SOC)?"



Fuente: Cyber Risk Report (Hewlett Packard Enterprise, 2016)

Estos datos revelan la necesidad que tienen las empresas de buscar mecanismos alternos para garantizar la seguridad de la información, sin que esto implique altos costes de adquisición o actualización de hardware, contratación de personal y otros gastos que se pueden generar. Es entonces cuando las PYMEs fijan su mirada en las empresas proveedoras de servicios de cloud, quienes están mejorando su infraestructura para ofrecer un mejor servicio.

Riesgos en entornos Cloud Computing

Dado que cada PYME es diferente, sus oportunidades de seguridad también lo son (Dekker, 2015). Así, podemos distinguir entre:

- Pequeña oportunidad: el cliente podría aprovechar esta oportunidad, pero los beneficios serían limitados.
- Oportunidad media: El cliente debe explotar esta oportunidad, porque los beneficios serían significativos.
- Gran oportunidad: el cliente debe explotar esta oportunidad, ya que habría beneficios cruciales.

Según ISACA (2009) se pueden considerar los siguientes como posibles riesgos del Cloud Computing para las empresas:

- Al seleccionar un proveedor se debe tener en cuenta su reputación, antecedentes y la sostenibilidad. Esta última es muy importante ya que garantiza que los servicios estarán disponibles y que los datos se podrán rastrear.
- El proveedor del servicio tiene la responsabilidad de manejar la información y si no se actúa de conformidad con los niveles de servicio acordados perjudicarán la confidencialidad, la disponibilidad y consecuentemente las operaciones del negocio.
- Puede existir confusión sobre dónde reside la información lo que puede provocar demora cuando se requiere la recuperación de la información.
- El acceso por parte de terceros a información sensitiva compromete la confidencialidad de la información y esto puede representar una amenaza a la protección de la propiedad intelectual.
- En las Nubes Públicas un aspecto negativo es que es posible mezclar los activos de información con los de otros clientes de la nube, incluso de competidores. Para las empresas es desafiante cumplir con todas las regulaciones y leyes existentes en los diferentes países. Por lo tanto es absolutamente necesario que las empresas se

asesoren legalmente para que en el contrato se especifique la responsable legal y financiera del proveedor.

- En caso de un desastre puede suceder que la información no se encuentre de manera inmediata por lo tanto los planes de continuidad del negocio y de recuperación deben estar bien documentados y probados. Los tiempos de recuperación que debe cumplir el proveedor deben estar especificados en el contrato.

Si bien la Computación en la Nube está destinada a proveer muchos beneficios, los profesionales de aseguramiento y seguridad de la información deberían realizar análisis de impacto al negocio y evaluaciones de riesgos para informar a los líderes del negocio de los posibles riesgos para su empresa. Las actividades de gestión de riesgos se deben gerenciar a través del ciclo de vida de la información y los riesgos se deben volver a evaluar regularmente o en caso de que ocurra un cambio (ISACA , 2009).

Los directivos de las empresas deben considerar a la Computación en la Nube no como un proyecto de TI, sino más bien, como una estrategia tecnológica de negocio (ISACA, 2013).

Gobierno de seguridad en entornos cloud computing

Actualmente la Computación en la Nube (Cloud Computing) sigue llamando mucho la atención de las empresas, aunque su nivel de aceptación no sea el mejor debido a los problemas de confianza y seguridad que aún se perciben con respecto a sus plataformas. (Mohammed Alnuem, Hala Alrumaih, & Halah Al-Alshaikh, 2015)

No obstante, de los problemas mencionados, y según un estudio de Julio del 2016, el 81% de sus encuestados indicaron que las soluciones en la nube se volverán “muy importantes” o “importantes” en los siguientes dos años. Del mismo modo señalaron que el uso de recursos de Computación en la Nube crecerá del 36% a 45% en los próximos dos años (Ponemon Institute LLC, 2016).

Esto enfrenta a un gran reto a las empresas proveedoras de los servicios en la nube, ya que contarán con cada vez más información de sus clientes que sea considerada como crítica, obligándolas a buscar herramientas que les permitan mejorar sus servicios para la gestión de riesgos de la información, y con esto poder ofrecer a sus clientes entornos con alta seguridad para sus activos de información.

La seguridad ahora no es solo enfocarse en adquirir sistemas de seguridad como Firewalls, IPS, IDS, etc. Ya no solo basta el hardware y software, para que una empresa se pueda considerar como segura, sino que además debe contar con aspectos tales como marcos normativos, responsabilidades, asignación de roles y análisis de riesgos. Estos aspectos deben ser considerados siempre en conjunto con el personal y sus procesos.

El Gobierno de TI

El Gobierno de TI se define como "Los procesos que aseguran el uso efectivo y eficiente de TI para permitir que una organización alcance sus metas" (Gartner, 2017). En una definición más detallada, el Instituto de Gobernanza de TI (ITGI por sus siglas en inglés) la define como "La responsabilidad del consejo de administración y la dirección ejecutiva. Es una parte integral de la gobernanza empresarial y consiste en el liderazgo y las estructuras organizativas y el proceso que aseguran que la TI de la organización sostiene y extiende las estrategias y objetivos de la organización" (ITGI, 2013).

Tomando ambos conceptos, el gobierno de TI es un conjunto de procesos que permiten asegurar que la TI de una organización puede mantener y extender estrategias así como los objetivos de la organización.

Muchas veces las organizaciones funcionan de manera aislada, la comunicación entre las diferentes áreas es deficiente o nula terminando por afectar los objetivos establecidos para cada una, siendo de las más perjudicadas el área de TI. El propósito del gobierno de TI es alinear las tecnologías de la información de la organización con las necesidades

del negocio; pero probablemente el reto más grande para el gobierno de TI es alinear los objetivos estratégicos de la organización con los de TI.

El gobierno de seguridad de TI

Con la aparición de la nube, las organizaciones asisten con muchas expectativas al seguimiento y desarrollo del Cloud Computing, y, con cada vez más presencia de información crítica en la nube también prolifera las brechas de seguridad que ponen en riesgo los datos los clientes.

Si bien es cierto, la Computación en la Nube ha traído muchas facilidades y ventajas, pero debido al hecho de encontrarse asentada sobre las mismas tecnologías que existen actualmente, adoptó los problemas de estas infraestructuras, viéndose afectado el nuevo modelo de servicios (Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, & Bhavani Thuraisingham, 2010), a lo que se suma los mismos problemas de seguridad inherentes a sus propias características (Yanpei Chen, Vern Paxson, & Randy H. Katz, 2010).

La causa principal de desconfianza existente entre los posibles clientes de las soluciones cloud, se basa en que su infraestructura utiliza recursos de computación que no solo se mantienen dentro del perímetro controlado de las organizaciones sino que lo traspasan, causando que exista cierta pérdida de control sobre los activos de información. Ante estos inconvenientes es necesario que los temas de seguridad sean tratados a nivel de gobierno corporativo a través de adecuadas estrategias de seguridad (ISACA, 2011), involucrando no solo a los niveles intermedios de gestión y los inferiores de operación, también deben incluirse a los más altos de dirección (Anthony Bisong & Syed (Shawon) M. Rahman, 2011).

Cada modelo de Cloud Computing tiene un riesgo de seguridad asociado que varía y depende de un amplio conjunto de factores que incluyen, la sensibilidad de activos de información, arquitecturas de cloud y controles de seguridad involucrados en los entornos de cloud particulares.

Existen varias propuestas técnicas para mejorar la seguridad de los servicios Cloud Computing, pero prácticamente ninguna lo hace bajo una perspectiva de gobierno.

Entre los marcos (Frameworks) de referencia y estándares aceptados por la comunidad se encuentran el estándar ISO/IEC27001 (ISO/IEC, 2013) e ISO/IEC38500 (ISO/IEC, 2008), o el marco de gobierno COBIT IT 5 (ISACA, 2012). Estos contienen procesos relacionados con la seguridad de los sistemas de información, pero no han sido diseñados específicamente para los servicios Cloud Computing, por lo tanto, no son capaces de tratar con los continuos cambios a los que están sometidos.

Para los servicios de Cloud Computing se han diseñado diversos modelos de seguridad propios, como la guía de seguridad de la Cloud Security Alliance (Cloud Security Alliance, 2017) o los objetivos de control propuestos por ISACA (ISACA, 2011). Su debilidad es no incluir en sus modelos de seguridad un adecuado gobierno del mismo.

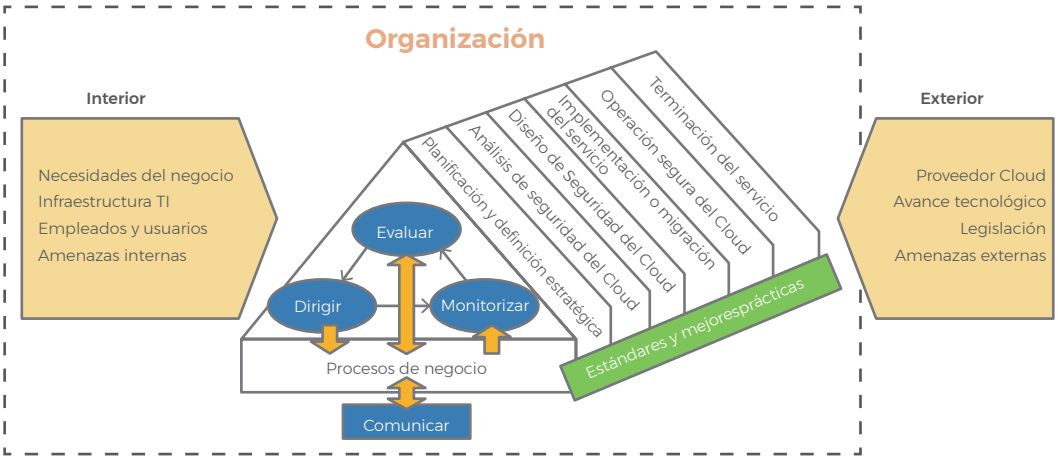
El marco de gobierno ISGCloud

En este apartado se ha considerado mencionar de manera general un marco de gobierno diseñado específicamente para el gobierno de seguridad en los entornos Cloud Computing. Este marco muestra un modelo a seguir para proveedores de servicios cloud y un modelo de evaluación que puede servir a los clientes para medir la calidad del servicio contratado, así como determinar el nivel de seguridad que se está brindando a sus activos de información.

ISGCloud (Information Security Gobernance for Cloud Computing Services) está orientado a garantizar la seguridad de los servicios Cloud Computing mediante la implantación de una estructura de Gobierno de Seguridad de la Información; y fue diseñado para llenar los vacíos en el tema de gobierno de seguridad de la información para entornos Cloud Computing (Rebollo, Daniel, & Fernandez-Medina, 2015).

Este marco de referencia se enfoca en procesos modelados empleando la especificación SPEM 2.0 (Software & Systems Process Engineering Meta-Model), lo que permite que pueda ser implementado por cualquier organización, utilizando nuevos procedimientos internos o modificando existentes. Está diseñado bajo una perspectiva de dos dimensiones (Gobierno de seguridad de la información y Seguridad de los servicios Cloud Computing) con lo que garantiza el cumplimiento de los aspectos de seguridad necesarios (ver Imagen 1).

Imagen 1: Estructura General de ISGCloud



Fuente: Adaptado de (Rebollo, Daniel, & Fernandez-Medina, 2015)

ISGCloud está basado en el estándar ISO/IEC38500 (ISO/IEC, 2008) en el ámbito de Gobierno de Seguridad de la Información, por lo que se enmarca en tres procesos y uno adicional agregado al final para este marco de gobierno, estos son:

- Evaluar el uso actual y futuro de las TI;
- Dirigir la preparación e implementación de políticas para asegurar que las TI cumplen con los objetivos del negocio;
- Monitorizar el cumplimiento de las políticas y el rendimiento de las acciones planificadas (ISO/IEC, 2008);

- Comunicar, enfatiza la importancia de la difusión del conocimiento de seguridad en el marco de gobierno (Rebollo, Daniel, & Fernandez-Medina, 2015).

Por otro lado, en el ámbito de la Seguridad de los Servicios Cloud Computing, ISGCloud se basa en el ciclo de vida propuesto por el estándar ISO/IEC 27036 (ISO/IEC, 2013-2016) que recoge aspectos de seguridad para la entrega de servicios por parte de proveedores, y permite adaptarse prácticamente a cualquier tipo de despliegue Cloud Computing, el ciclo de vida está compuesto por las siguientes fases:

1. Planificación y definición estratégica;
2. Análisis de seguridad del cloud;
3. Diseño de seguridad del cloud;
4. Implementación o migración del servicio;
5. Operación segura del cloud;
6. Terminación del servicio.

Este modelo es lo suficientemente flexible en cada una de sus fases, por lo que se puede adaptar a detalles específicos de implementación de cada servicio, según las necesidades de cada organización.

Características

Entre las principales características del modelo tenemos las siguientes:

- Procesos Iterativos: a nivel general (ciclo de vida del servicio) y a nivel de tareas, lo que ayuda a revisar y mejorar los detalles de las salidas de cada proceso;
- Reusabilidad del proceso: con el uso de SPEM 2.0 (OMG, 2008), cada proceso puede ser reutilizados en otros dominios y contextos, cualidades que son favorecidas por las interfaces del modelo y la modularidad de sus procesos.
- Reusabilidad de los productos: mediante un repositorio común de productos, resultado de cada proceso de

ISGCloud, estos pueden ser reutilizados en cada ciclo iterativo, mejorando cada producto y manteniendo el proceso de mejora continua.

- Alineación con estándares de seguridad y mejores prácticas de gobierno: uso de herramientas muy conocidas a nivel de los profesionales de TI, mantiene conformidad con los principales estándares de seguridad y las mejores prácticas de gobierno, entre estos se encuentran los siguientes (ver Tabla 1):

Tabla 1: Referencias de seguridad y enfoque para el marco ISGCloud.

Referencia de seguridad	Enfoque
ISO/IEC27001 (ISO/IEC2005b)	Gestión y controles de seguridad.
ISO/IEC38500 (ISO/IEC2008)	Gobierno de TI.
ISO/IEC 27036 (ISO/IEC draft)	Seguridad de servicios externalizados a proveedores.
COBIT 5 (ITGI 2012b)	Mejores prácticas de gobierno, adaptadas a Cloud Computing.
Guías de seguridad de la csa	Seguridad en la nube.

Fuente: Adaptado de (Rebollo, Daniel, & Fernandez-Medina, 2015)

- Trazabilidad y seguimiento del desarrollo: mediante el uso de indicadores y métricas se permite el uso de cuadros de mando para un seguimiento continuo por parte de la alta dirección, orientado a la consecución de los objetivos estratégicos del negocio.
- Flexibilidad de adaptación: tanto las actividades como las tareas del marco ISGCloud son parametrizables y modificables, lo que le permite ser altamente adaptable a cualquier escenario.

Roles

Para mantener una correcta estructura organizativa, en la que el personal sepa qué papel juega en los procesos de una organización, es necesario definir roles. Estos permiten conocer las responsabilidades, vías de comunicación y reporte que cada uno debe cumplir. ISGCloud tiene definidos un

conjunto de roles involucrados directamente, en cada proceso de gobierno, en relación a que estos cubren a toda una organización y la necesidad de que participe todo el personal de una organización incluida la alta dirección.

Es en el comité de dirección donde se inicia el ciclo Evaluar-Dirigir-Monitorizar para descender hasta el personal operativo y volver a ascender a la dirección cumpliéndose los procesos de ciclado.

Todas las funciones de un rol pueden dividirse entre varias personas, así como también una persona puede participar en varios roles debido a la flexibilidad del marco de gobierno. A continuación se detalla los roles y una pequeña descripción de cada uno:

- Comité de dirección: deben tener conocimiento de la misión/visión de la organización y participar en el desarrollo de estrategias que orienten a la organización. Puede incluir directivos de áreas técnicas como TIC, Seguridad, o de otras áreas relevantes. El rol siempre debe estar compuesto por personal de alta jerarquía.
- Ejecutivo de negocio: es el segundo nivel jerárquico debajo del comité de dirección, ayudan a transformar las estrategias de la dirección en tareas tácticas que permitan la consecución de objetivos a mediano plazo.
- Gestor de negocio: responsable del personal operativo de la organización, define cómo operar en base a plazos cortos, supervisa actividades y tareas diarias.
- Operador: son los encargados de la ejecución de las tareas programadas por los gestores, su participación con el servicio de cloud dependerá del departamento en el que se enmarquen.
- Recursos humanos: sus funciones son, además de las relacionadas a su cargo, asegurarse que el proceso de gobierno sea conocido por toda la organización, difun-

dir políticas y actividades de gobierno, formación en temas de seguridad y gobierno, etc.

- Gestor TI: es uno de los roles más involucrados en los aspectos técnicos del servicio Cloud Computing, definen soluciones técnicas, administran los sistemas y proyectos de desarrollo.
- Gestor de seguridad: es el responsable de garantizar la autenticación, confiabilidad y disponibilidad de la información de la organización.
- Auditor: se encarga del proceso de auditar, es recomendable que este sea personal completamente independiente no solo de la organización sino también del proveedor.
- Proveedor de servicio Cloud Computing: participa de manera conjunta con el cliente en los procesos de seguridad del proveedor, puede ser subdividido en varios sub-roles que se identifican con las funciones que asumirá el proveedor con su personal.

Implementación

Para la etapa de implementación ISGCloud propone dos criterios que evalúan si la organización cuenta con una estructura de gobierno de seguridad previa, y si el servicio que se estudia es ofrecido por la organización. Los escenarios son descritos en la Tabla 2 y 3.

Tabla 2: Escenarios y tareas en caso de disponibilidad de Gobierno de Seguridad de la Información

Escenario	Tareas propuestas
No dispone de una infraestructura de gobierno de seguridad del a información.	* Desarrollo profundo de actividad 1, para sentar bases de la implementación.
Dispone de una infraestructura de gobierno de seguridad de la información.	* Desarrollo superficial de actividad 1, revisar y evaluar la estructura de gobierno existente.

Fuente: Adaptado de (Rebollo, Daniel & Fernandez-Medina, 2015)

Tabla 3: Escenarios y tareas en caso de existencia del servicio

Escenario	Tareas propuestas
Servicio no existente	* Destinar más recursos a las actividades de diseño (Actividad 3) e implementación (Actividad 4) de la seguridad.
Servicio existente interno	* Evaluar la seguridad (Actividad 2) del servicio de cara al traslado del proveedor en la nube. * La implementación (Actividad 4), debe ejecutarse bajo la perspectiva de migración y no de creación de nuevo servicio, con el fin de adoptar medidas adicionales de seguridad en el traspaso.
Servicio existente en modo Cloud Computing.	* Se debe poner énfasis en el análisis de seguridad (Actividad 2) que permitan detectar y reforzar posibles debilidades * Revisar los procesos de seguridad (Actividad 5), durante las operaciones del servicio

Fuente: Adaptado de (Rebollo, Daniel & Fernandez-Medina, 2015)

En resumen, la Tabla 4 muestra lo planteado en la anterior descripción de los escenarios:

Tabla 4: Actividades prioritarias según criterios de implementación

	Servicio No existente	Servicio Existente interno	Servicio en modo Cloud Computing
Con Gobierno de Seguridad	1, 3, 4	1, 2, 4	1, 2, 5
Sin Gobierno de Seguridad	3, 4	2, 4	2, 5

Fuente: Adaptado de (Rebollo, Daniel & Fernandez-Medina, 2015)

Este modelo de criterios no indica que deben ejecutarse únicamente estas actividades, más bien hace notar que estas actividades deben ser tomadas muy en cuenta.

Es importante notar que el uso de otros criterios como NIST puede afectar la forma en la que se desarrollan las actividades de ISGCloud, derivando en características técnicas diferentes para los servicios cloud, pero esto solo afecta a los pasos de algunas tareas y no al enfoque general del marco ISGCloud. Sin embargo, este modelo promete ser una guía de implementación de gobierno de seguridad para las empresas que han decidido migrar al Cloud Computing.

En este capítulo se han presentado algunas concepciones genéricas que existen en la actualidad y algunos factores que se deben considerar en el contexto de la seguridad de la información al implementar el servicio del Cloud Computing. En el siguiente capítulo se establecerán aspectos de Gobierno de TI que deben ser considerados en entornos cloud.

Referencia bibliográfica

Anthony Bisong, & Syed (Shawon) M. Rahman. (2011). *An Overview of Security Concerns in Enterprise Cloud Computing.*

Cloud Security Alliance. (2017). *Security Guidance for Critical Areas of Focus in Cloud Computing v 4.0.*

Cyber Risk & information Security Study (2016)

Dekker, D. (2015). Cloud Security Guide for SMEs. Cloud computing security risks and opportunities for SMEs. ENISA. ISBN: 978-92-9204-122-9, DOI 10.2824/508412.

Ernst and Young Global. (2015). Encuesta Global de Seguridad de la Información. EY.

Gartner. (2017). Gartner. Retrieved from http://www.gartner.com/it-glossary/it-governance

INTECO. (2011). Guía para empresas: seguridad y privacidad del cloud computing. Instituto Nacional de Tecnologías de la Comunicación.

ISACA. (2009). Computación en la nube: Beneficios de negocio con perspectivas de seguridad, gobierno y aseguramiento, EE.UU., EE.UU.

ISACA. (2013). GOBIERNO EN LA NUBE: preguntas que los consejos directivos deben formular.

ISACA. (2011). IT Control Objectives for Cloud Computing.

ISACA. (2012). *COBIT 5.*

ISO/IEC. (2005). *ISO/IEC 20000-1:2005 Specification.*

ISO/IEC. (2008). *ISO/IEC 38500:2008 Corporate governance of information technology.*

ISO/IEC. (2013). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements.*

ISO/IEC. (2013-2016). *ISO/IEC 27036 - IT Security -Security techniques - Information security for suppliers relatioships.*

ITGI. (2013). ITGI. Retrieved from https://www.isaca.org/ITGI/Pages/default.aspx

Kevin Hamlen, Murat Kantarcioglu, Latifur Khan, & Bhavani Thuraisingham. (2010). Security Issues for Cloud Computing. *International Journal of Information Security and Privacy, 4(2), 39-51.*

Mohammed Alnuem, Hala Alrumaih, & Halah Al-Alshaikh. (2015). A Comparison Study of Information Security Risk Management Frameworks in Cloud Computing. CLOUD COMPUTING 2015 : *The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization,* 103.

OMG. (2008). *Software & Systems process Engineering Meta-Model Specification v.2.0.* Retrieved from http://www.omg.org/spec/SPEM/2.0/

Ponemon Institute LLC. (2016). *The 2016 Global Cloud Data Security Study.*

Ponemon Institute LLC. (2017). *2017 Cost of Data Breach Study*

Rebollo, O., Daniel, M., & Fernandez-Medina, E. (2015). *ISGcloud: a Security Governance Framework for Cloud Computing.* Computer Journal.

Yanpei Chen, Vern Paxson, & Randy H. Katz. (2010, Enero). What's New About Cloud Computing Security? EECS Department, University of California, Berkeley.

Cloud Computing para PYMEs
Edición digital 2017- 2018.
www.utmachala.edu.ec

Redes

Redes es la materialización del diálogo académico y propositivo entre investigadores de la UTMACH y de otras universidades iberoamericanas, que busca ofrecer respuestas glocalizadas a los requerimientos sociales y científicos. Los diversos textos de esta colección, tienen un espíritu crítico, constructivo y colaborativo. Ellos plasman alternativas novedosas para resignificar la pertinencia de nuestra investigación. Desde las ciencias experimentales hasta las artes y humanidades, Redes sintetiza policromías conceptuales que nos recuerdan, de forma empeñosa, la complejidad de los objetos construidos y la creatividad de sus autores para tratar temas de acalorada actualidad y de demanda creciente; por ello, cada interrogante y respuesta que se encierra en estas líneas, forman una trama que, sin lugar a dudas, inervará su sistema cognitivo, convirtiéndolo en un nodo de esta urdimbre de saberes.

UNIVERSIDAD TÉCNICA DE MACHALA
Editorial UTMACH
Km. 5 1/2 Vía Machala Pasaje
www.investigacion.utmachala.edu.ec / www.utmachala.edu.ec

ISBN: 978-9942-24-107-8