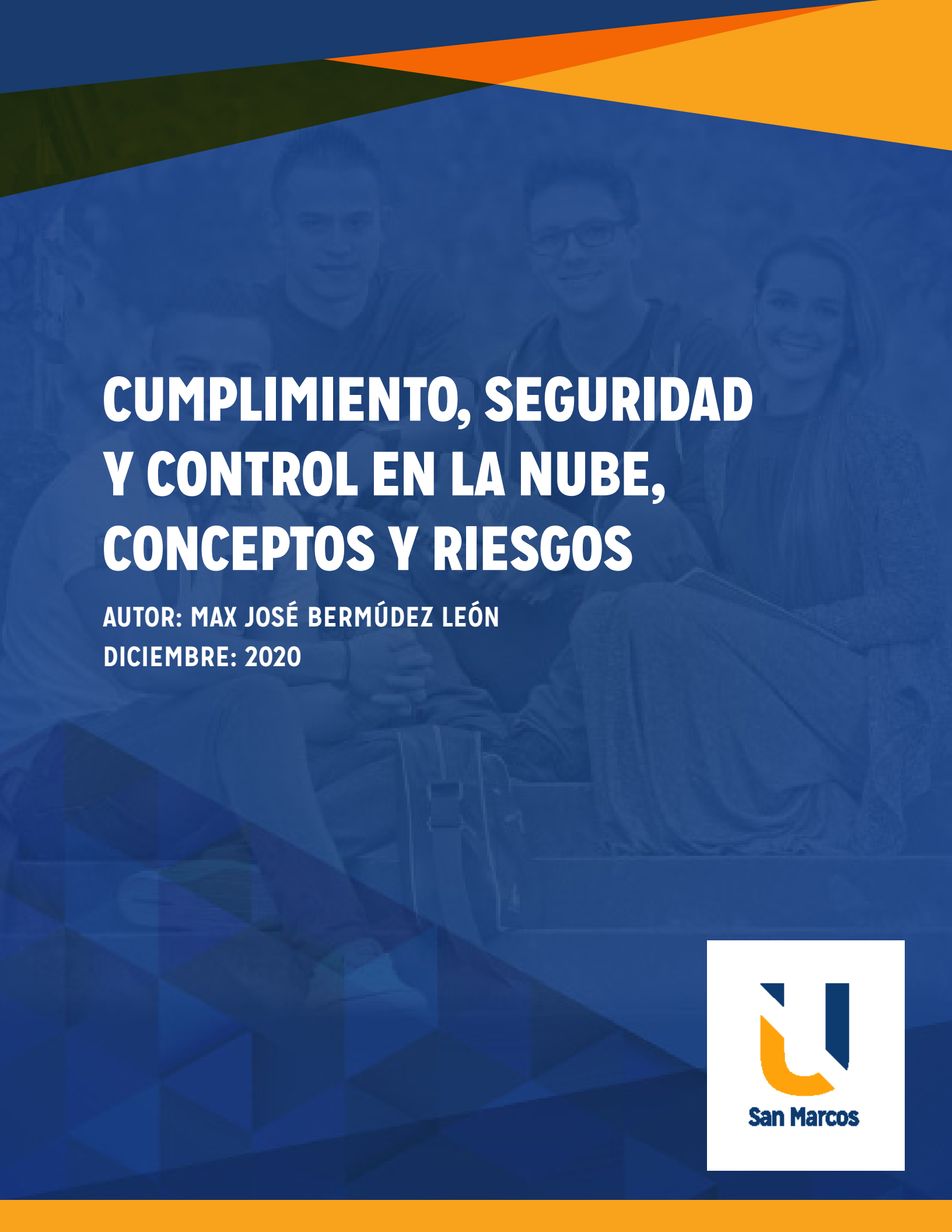

CUMPLIMIENTO, SEGURIDAD Y CONTROL EN LA NUBE, CONCEPTOS Y RIESGOS

AUTOR: MAX JOSÉ BERMÚDEZ LEÓN

DICIEMBRE: 2020

San Marcos

Introducción

Nuevos acrónimos aparecen para ilustrarnos las diferencias y nuevas capacidades que se promulgan con este cambio: Cumplimiento, seguridad y control en la nube. SaaS – Software as a Service, IaaS – Infrastructure as a Service, PaaS – Plataform as a Service. Estas nuevas palabras, responden a una marcada necesidad de las organizaciones para hacer las cosas de manera más eficiente, con un acceso universal y pagando sólo por aquello que utilizan. Si bien, la crisis financiera internacional ha llevado a replantear muchos elementos de la gestión de tecnologías de información, ya en este escenario, los Chief Information Officers – CIO, habían detectado previamente la necesidad de hacer más efectivo y eficiente el tratamiento de la información, con mínimos de inversión y máximos niveles de retorno. Por tanto, como consecuencia natural de esta necesidad, la industria del hardware y software, desarrolla alternativas donde se tienen los recursos de TI – Tecnologías de Información, disponibles todo el tiempo, con la calidad deseada y asegurando las características requeridas por las organizaciones.

Tabla de contenido

Aseguramiento de la nube

Hablar de computación en la nube o Cloud Computing, es presentar un concepto de computación por demanda, una democratización del uso de los recursos de tecnología, una reconceptualización de los modelos de consumo y distribución de recursos de tecnología, una transformación de llamados a funciones remotas por una invocación de servicios y una abstracción total de las infraestructuras de computación asociadas.

La única vía para asegurar los recursos de computación son un cifrado fuerte y una administración escalable de llaves.

Las nuevas exigencias de los modelos de seguridad y control requeridos, se hace necesario dar respuesta a preguntas que surgen en este cambio de paradigma computacional y porqué no empresarial:

- ¿Quién la administra?
- ¿Quién es su dueño?
- ¿Dónde esta localizada?
- ¿Quién tiene acceso?
- ¿Cómo se tiene acceso?
- ¿Qué regulaciones, normas o buenas prácticas le son aplicables?
- ¿Cómo se adelantan investigaciones?

En este sentido, este documento presenta un análisis de las consideraciones de seguridad y control de la información requerida para esta estrategia de computación tercerizada y basada en servicios, de tal forma que, tanto los entes de control organizacional como el gobierno y administración de tecnologías de información cuenten con un lenguaje base para balancear las decisiones que se concreten, de cara al tratamiento de los riesgos que se derivan de asumir la computación en la nube como una estrategia corporativa.

Aclarando el lenguaje en la nube La computación en la nube, sigue algunas de las características de estilo de los que promueven los cambios:

- Pueden aparecer desorganizados, indisciplinados, no convencionales y espontáneos
- Prefieren cambios que cuestionen las estructuras actuales

- Disfrutan el riesgo y la incertidumbre
- Pueden ser imprácticos y olvidar detalles importantes
- Pueden aparecer como visionarios y sistémicos en sus pensamientos.

Estas características nos indican que una nueva raza de empresarios e innovadores están tratando de generar una forma diferente de hacer las cosas y, por tanto, se hace necesario revisar con detalle y claridad los impactos que ello representa para la realidad actual y cómo avanzar ágilmente y de manera confiable en la conquista de esta propuesta de servicios en computación.

Si bien no existe con claridad una definición para la computación en la nube, si se tienen algunos acuerdos respecto a los servicios que se entregan en la nube: software como servicio, plataforma como servicio e infraestructura como servicio.

Como vimos en temas anteriores,

Software como servicio – (SaaS) se traduce como la capacidad provista al consumidor o cliente de utilizar las aplicaciones del proveedor que se ejecutan una infraestructura tecnológica en la nube, la cual es accesible desde varios dispositivos tecnológicos, a través de un cliente de interfase liviana como lo puede ser un navegador web. Esto es, el cliente no tiene que preocuparse del software, tipo de sistema operativo o lenguaje en que está construida la aplicación. Adicionalmente no se requiere ninguna instalación de software adicional.

Plataforma como servicio – (PaaS) es la capacidad provista al consumidor o cliente para desplegar en una infraestructura tecnológica en la nube las aplicaciones creadas por éste utilizando para ello lenguajes y herramientas de programación que son soportadas por el proveedor. Esto es, que el cliente final no controla o administra las redes, servidores, sistemas operativos o almacenamiento de las aplicaciones, pero si el despliegue de sus aplicaciones y posibles consideraciones del entorno de alojamiento de éstas. (idem)

Infraestructura como servicio – (IaaS) nos habla de la capacidad provista al consumidor o cliente para alquilar recursos computacionales (capacidad de procesamiento, almacenamiento, redes, entre otros) donde éste tiene la posibilidad de desplegar y ejecutar software de manera libre, lo cual incluye tanto sistemas operativos como aplicaciones. Esto es, el cliente no administra o controla la infraestructura en la nube, pero si lo hace sobre los sistemas operativos, el almacenamiento, el despliegue de las aplicaciones y posiblemente la selección de algunos componentes de red (p.e, firewalls, balanceadores de carga). (idem)

Por un lado, el utilizar, cuando se utiliza una infraestructura asumimos o previamente acordamos con el proveedor de servicios, las condiciones en las cuales vamos a consumir sus servicios; esto implica unos acuerdos de nivel de servicio y las necesidades de seguridad y control requeridas para que los clientes hagan uso del software disponible en la nube. Si ocurre alguna falla en el uso de esta aplicación, el cliente no tendrá control para avanzar en el análisis de la misma, la cual estará supeditada a la reacción del proveedor del servicio. Cuando hablamos de desplegar aplicaciones en una infraestructura, el cliente tiene el control y administración de los códigos fuente de sus aplicaciones y las interacciones de cada una de las piezas de software que dispone en las máquinas del proveedor. En este contexto, si existe alguna falla a nivel de sistema operativo, redes o almacenamiento, el cliente no tendrá margen de maniobra, pues estará limitado por la oportunidad del proveedor para soportar dicha falla.

Finalmente, el alquilar, nos dice que tenemos algo en préstamo que podemos utilizar según lo pactado con el proveedor. En este contexto, el cliente puede controlar y administrar en los recursos computacionales elementos como el sistema operativo, el almacenamiento y sus aplicaciones, nuevamente dejando en manos del proveedor los temas de continuidad y acceso a los servidores y demás componentes tecnológicos.

Luego de revisar cada una de estas estrategias, observamos que el proveedor de los servicios tiene una alta responsabilidad para mantener la continuidad, seguridad y control de

la infraestructura tecnológica, de tal forma que el cliente, confíe, ejecute y utilice los servicios contratados con el tercero. En este escenario, los referentes de seguridad y control propios de tecnologías de información, adquieren una relevancia marcada, dado que se está entregando en un tercero la información propia de la empresa, que inicialmente pareciera volverse más vulnerable y abierta, pero que, con un adecuado balance de riesgos, habrá que analizar y decidir si dichos riesgos se asumen, se transfieren o se mitigan.

Riesgos de seguridad de la información en la nube

Bien argumenta Paul W. Homer “cuando se tiene una perspectiva orientada a los datos, implica mirar el sistema completo por la estructura subyacente que sugiere la información, lo que genera una reducción significativa de la complejidad del sistema a diseñar, mostrando una colección de detalles tangibles, que son determinantes para la construcción y ejecución de soluciones más elaboradas”.

Si lo anterior es correcto, acercarnos a los riesgos de la computación en la nube, implica tener una mirada sistémica, como la requerida por aquellos que hacen los cambios.

Para ello, tomaremos como referencia el documento publicado por la Cloud Security Alliance - CSA, denominado Security Guidance for Critical Areas of Focus in Cloud Computing, disponible al público.

En dicho documento se establecen una serie de características y variables a tener en cuenta cuando se trata de aplicar una estrategia de computación en la nube, de tal manera que le permita a los analistas de riesgos revisar cada uno de ellos y evaluar en el contexto de cada organización lo pertinente para decidirse o no con una estrategia de computación en la nube.

El proveedor de los servicios tiene una alta responsabilidad para mantener la continuidad, seguridad y control de la infraestructura tecnológica.

Se establece quince (15) dominios de acción para considerar los aspectos de seguridad de la computación en la nube:

- Marco arquitectónico de la computación en la nube
- Gobierno y administración de riesgos empresariales
- Consideraciones legales
- Descubrimiento electrónico (Electronic Discovery)
- Cumplimiento y auditoría
- Administración del ciclo de vida de la información
- Portabilidad e interoperabilidad
- Seguridad tradicional, continuidad de negocio y recuperación ante desastres • Operaciones de centros de cómputo
- Respuesta a incidentes, notificación y remediación
- Seguridad en aplicaciones
- Cifrado y administración de llaves
- Administración de la identidad y el acceso
- Almacenamiento
- Virtualización

A continuación, una breve explicación del alcance de cada una de las categorías establecidas en el documento de la CSA.

Marco arquitectónico de la computación en la nube

Es este domino se establecen las definiciones propias de la computación en la nube, que define este paradigma de servicios computacionales como una colección distribuida de servicios, aplicaciones, información e infraestructura compuesta de múltiples recursos de tecnología de información como redes, información, servidores y recursos de almacenamiento, los cuales son orquestados, aprovisionados, implementados y

configurados utilizando un modelo de demanda, basado en la localización de los recursos y las tasas de consumo de éstos.

Gobierno y administración de riesgos empresariales

Dado que en el contexto de la computación en la nube la participación de un tercero es factor fundamental de la estrategia, la gestión de riesgos requerida para este caso requiere un análisis cuidadoso de la debida diligencia del proveedor, los acuerdos de nivel de servicio que se requieren, las consideraciones legales de propiedad de los datos, la jurisdicción aplicable, los aspectos de continuidad de negocio, resolución de conflictos, entre otros temas que ofrezcan a la organización que esté pensando en esta opción valorar con claridad los riesgos claves de esta opción.

Consideraciones legales

En este aspecto las organizaciones deben estar atentas para revisar entre otros aspectos las obligaciones de cumplimiento regulatorio propias de la organización (como de otros países) y cómo esta son asumidas por el proveedor de servicios en la nube, analizar las implicaciones de la localización de los datos, los elementos de protección de la privacidad de los datos de clientes y empleados de la empresa, los usos secundarios de la información almacenada en la infraestructura del proveedor, el manejo de las brechas de seguridad que se presenten, el aseguramiento de los planes de continuidad de negocio, la respuesta a los posibles litigios donde se solicite información corporativa disponible en la nube, los elementos del monitoreo de los servicios contratados en la nube y los elementos concretos de terminación del contrato con el proveedor.

Descubrimiento electrónico

Este elemento llama la atención de mantener unas buenas prácticas de seguridad de la

información por parte del proveedor de servicios, de tal forma que la evidencia informática o electrónica materializada en los registros de la operación de la empresa sea auténtica y confiable como evidencia. Esto implica que el cliente deberá asegurar en los acuerdos de nivel de servicio, la custodia y control de la información de la empresa alineada con los estándares de autenticidad y confiabilidad requeridos por su cliente y propios del contexto legal de su empresa y país.

Cumplimiento y auditoría

Si bien no es evidente asegurar aspectos de cumplimiento y revisión por parte de terceros en la nube, ciertamente es posible adelantar un programa de evaluación que mantenga un monitoreo y revisión de las consideraciones de seguridad y control requeridas frente a las buenas prácticas y el marco normativo vigente.

Administración del ciclo de vida de la información

Adicional a los pasos naturales del ciclo de vida de la información: creación, clasificación, transporte, almacenamiento, recuperación y disposición, en la estrategia de computación en la nube se deben considerar aspectos como:

- El nivel de controles lógicos y físicos que deben estar diseñados en el sitio de almacenamiento
- La validación de la integridad de los datos que soportan la información
- La identificación y control de acceso de la persona a los datos
- Los términos del servicio relacionados con el control y revelación de información sensible
- Los requisitos de privacidad
- Los elementos de recuperación y respaldo
- Los tiempos de retención de lo datos y su destrucción posterior
- La respuesta a solicitudes de información por parte de terceros autorizados

- El tránsito o transmisión de información entre países
- La validez y continuidad del proveedor de servicios en la nube.

Portabilidad e interoperabilidad

Esta variable nos habla sobre la calidad del proveedor de servicios en la nube, de la capacidad de manejo de sus recursos computacionales y la migración interna de ambientes o nubes que este tenga configuradas al interior de su arquitectura de tecnologías de información. Así mismo, nos exige revisar los temas de recuperación ante desastres y capacidad de restauración del servicio de acuerdo con los niveles de servicio previstos.

Seguridad tradicional, continuidad de negocio y recuperación ante desastres

El reto en esta sección es identificar las interdependencias de la infraestructura que conforma la nube, cómo se integra y soporta ésta de manera dinámica y de acuerdo con la demanda. Aún cuando los servicios en la nube requieren de elementos de seguridad tradicional y el cumplimiento de sus fundamentos (confidencialidad, integridad, disponibilidad, no repudio, autenticación, autorización y auditabilidad), los conceptos de continuidad de negocio y recuperación ante desastres son requerimientos fundamentales de la protección de los servicios.

Las organizaciones deben estar atentas para revisar entre otros aspectos las obligaciones de cumplimiento regulatorio propias de la organización (como de otros países) y cómo esta son asumida por el proveedor de servicios en la nube.

Operaciones de centros de cómputo

Los clientes de proveedores en la nube, deben con frecuencia validar el nivel de maestría de éste en el soporte de sus servicios. Esto es someterlo a evaluaciones periódicas de la gestión

del servicio prestado, la presencia de ambientes pilotos de pruebas para soportar cambios y nuevos productos, validación de la segregación de funciones y ambientes para cada uno de los clientes del proveedor, el nivel de la administración de parches de la infraestructura, así como el nivel de las evaluaciones efectuadas por terceros a la gestión de sus servicios.

Los conceptos de continuidad de negocio y recuperación ante desastres son requerimientos fundamentales de la protección de los servicios.

Respuesta a incidentes, notificación y remediación

Este aspecto exige de los proveedores de la nube la responsabilidad de la identificación y notificación del incidente, con la opción preferente de remediación de un acceso no autorizado a los datos generados por una aplicación. En este sentido, el análisis del incidente puede adquirir un significado y acciones diferentes dependiendo de los requerimientos de ubicación del usuario de la aplicación. Por lo tanto, la atención de incidentes, si bien podrá seguir lo establecido por los discursos metodológicos existentes al respecto, deberá tener en cuenta el contexto del país donde se materializa o se ubica el usuario.

Seguridad en aplicaciones

En este punto decisiones como dónde deben ser desarrolladas o ejecutadas las aplicaciones son las que se deben tomar, dado el modelo de entrega de las mismas en una plataforma particular. Adicionalmente, se debe dar respuesta a preguntas como:

- ¿Qué controles deben tener las aplicaciones tanto dentro de su diseño, como en la nube?
- ¿Qué tanto debe cambiar el modelo de desarrollo de software para acomodarse a la computación en la nube?

Cifrado y administración de llaves

En el concepto de computación en la nube no es clara la definición de perímetro de seguridad, dado que los componentes y sus localizaciones varían según la demanda. En este contexto y de acuerdo con lo establecido por la CSA, la única vía para asegurar los recursos de computación son un cifrado fuerte y una administración escalable de llaves.
Si bien los autores hablan del cifrado como la única vía para el aseguramiento en la nube, esta decisión implica elementos de gestión y control propios de la infraestructura que deben ser manejados y administrados por los clientes, los cuales son los que mantienen el control sobre sus datos en la infraestructura de la nube. En este escenario, los diseños y aplicación de los servicios deben estar articulados con esta directriz de confidencialidad de la información.

Administración de la identidad y el acceso

Esta variable de análisis nos invita a revisar los temas de la identidad de los usuarios en el consumo de los servicios de una infraestructura. Si bien, a la fecha no existe un ambiente maduro que evidencie la preparación de las organizaciones para la administración de la identidad, se hace necesario revisar en el contexto de los proveedores en la nube, el grado de madurez de esta estrategia, de cara a una futura implementación de la misma, como parte interesada y participante de la identidad de los usuarios en ella.

Almacenamiento

En este segmento del documento las preguntas que el cliente de los servicios en la nube se hace son:

- ¿Cómo el proveedor asegura que sus datos sean confiables y estén disponibles de acuerdo con sus necesidades de negocio?
- ¿Está usted y sus clientes confiados en la promesa de que toda su información privada y confidencial permanece como tal y debidamente protegida?

- ¿Están sus datos almacenados de manera confiable y debidamente segregados de otros residentes en la misma granja de almacenamiento?

Virtualización

Este componente es uno de las variables fundamentales al considerar la estrategia de computación en la nube. Dentro del conjunto de riesgos a revisar en este aspecto se encuentran:

- Nuevas tecnologías, que mantienen antiguas vulnerabilidades y el surgimiento de nuevas. Esto implica que, a mayor complejidad de la configuración del entorno de operación, menores y poco homogéneos aspectos de seguridad y control
- Pérdida de la seguridad por defecto, es decir, que, al cambiar un entorno previamente configurado, se requiere una nueva configuración de las condiciones de seguridad tanto en el hardware como en el software utilizado.
- Mezcla de retos alrededor de la integridad, que implica la mixtura de datos y niveles de confidencialidad. El tratamiento de la reconfiguración de entornos, implica un manejo de información que puede no ser la más adecuada.
- Aspectos de jurisdicción, regulatorios y de control, tema que ha sido tratado en otros apartes del documento de la CSA.
- Nuevos retos administrativos que impactan la seguridad, esto es, la configuración de las máquinas y sus recursos, requiere un nivel de seguridad y control adicional al propio de las aplicaciones que se ejecutarán en ellas. La seguridad de la virtualización en sí misma, es una característica necesaria dentro de la administración de ambientes computacionales en esta condición.

Balanceando la funcionalidad y los requisitos de seguridad y control en la nube

Si bien cuando se desarrollaron los marcos normativos y buenas prácticas que gobiernan las infraestructuras de TI, éstas fueron diseñadas sin considerar los ambientes virtualizados y las consideraciones de un mundo computacional sin perímetros de seguridad conocidos (como ocurre en la nube), se hace necesario revisar en el contexto de este cambio de paradigma computacional, cómo ser parte de este cambio y ajustar lo requerido para sacar el mayor provecho de éste y al mismo tiempo incrementar la confiabilidad en la utilización de esta estrategia.

La única vía para asegurar los recursos de computación son un cifrado fuerte y una administración escalable de llaves.

En la revisión de literatura se encuentran una serie de buenas prácticas en la gestión de tecnologías de información que han sido consideradas para enfrentar el reto del aseguramiento de la nube.
Entre las prácticas y estándares identificados se tienen:

- Statment of Auditing Standard - SAS 70 (http://www.sas70.com/index2. htm)
- Webtrust (http://www.webtrust.org/) y SysTrust (http://www. sas70.com/systrust.html)
- Service Capability & Performance (http:// www.servicestrategies.com/solutions/scp-standards/)
- El ISO 27001 (http://www.iso27000.es/iso27000. html)
- Cobit (http://www.isaca. org/cobit)
- Los fundamentos de ITIL (http://www.itil-officialsite.com/ home/home.asp)
- Las consideraciones del marco de control de Basilea II (http://www.bis.org/publ/bcbsca. htm), entre otros.

En cada uno de estos marcos de buena práctica, los proveedores deben asumir retos de protección de los activos de información de los clientes, que articulen los números de

eficiencia y efectividad en la entrega del servicio, con los niveles confiabilidad esperados por el cliente tanto en rendimiento de la plataforma, efectividad de los servicios invocados, así como en las condiciones de acceso y monitoreo de la plataforma en sus estrategias de administración.

Balancear la funcionalidad y las necesidades de seguridad y control en la computación en la nube, implica planear y analizar la demanda esperada de los servicios, enfrentar y atender los tráficos de información inesperados, los balances de cargas tanto en almacenamiento como en ancho de banda, así como valorar la capacidad de la nube para atender estas características.

En este contexto, desde el diseño de la nube, se hace necesario seguir algunas prácticas de seguridad y control, que se hagan parte de los procedimientos de redimensionamiento de la infraestructura y que están atadas al modelo de demanda que se tenga previsto.

Lo anterior parece una labor altamente demandante y efectivamente lo es, pero no por ello debemos abandonar nuestros esfuerzos para abordar la complejidad propia de este nuevo paradigma. El reto consiste en reconocer las alternativas que ofrece la computación en la nube, los riesgos que vamos a transferir, asumir y mitigar, para que conscientes de nuestro análisis podamos ver integrados en un balance el valor de la estrategia tecnológica y las cifras de la inversión realizada.

No hay duda que la computación en la nube es una tendencia formal que adquiere día a día mayores practicantes y que promete rediseñar el concepto de servicios computacionales en el mediano y largo plazo. Es probable que en el futuro, con el riesgo de equivocarnos, los centros de procesamiento de datos (anteriormente denominados centros de cómputo) sean extensiones de los centros de servicios compartidos de las organizaciones, lugares donde se articulan las estrategias de tecnología de información con los procesos de negocio.

Conclusión

Así las cosas, es natural que las organizaciones simplifiquen los esquemas de gestión de tecnologías de información, considerando éstos como plataformas de apoyo para apalancar la innovación y generación de valor para las empresas que si bien no están en el negocio de las TI, si quieren encontrar en ellas una manera de brindar una experiencia única para sus clientes, donde la nube es el universo de recursos disponibles y su interfase liviana y conocida, como lo es el navegador web (por ahora), es la llave para repensar la organización con TI.

En este contexto, el reto de los modelos, buenas prácticas y estrategias de seguridad y control, no es ubicar las restricciones necesarias para mitigar o limitar las fallas propias de la operación de la nube, sino reconocer las relaciones y puntos de integración entre sus componentes que permitan simultáneamente compartir y aprender de la dinámica de la nube, y así aceptar el cambio continuo y natural de un concepto tecnológico que entiende el control y la seguridad como esa propiedad emergente propia del diseño de la interacción de cada uno de sus componentes tecnológicos, procedimentales y humanos, en el tejido estratégico de las iniciativas empresariales para generar valor con el cliente, que ahora vive en la nube.

Referencias bibliográficas

- IONOS. (2018). Seguridad en la nube: utiliza sus servicios evitando riesgos. Sitio de donde se obtuvo la información: https://www.ionos.es/digitalguide/servidores/seguridad/seguridad-en-la-nube-desafios-y-soluciones/

- Tecnogital. Guia de controles y Aseguramiento de la calidad en la nube. Sitio de donde se obtuvo la información: http://www.tdtechnodigital.com/index.php/36-seguridad-informatica1/604-cobit-5-guia-de-controles-y-aseguramiento-en-la-nube

- http://acistente.acis.org.co/typo43/fileadmin/Revista_112/uno.pdf

- AWS. (2020). Marco de Buena Arquitectura. Sitio de donde se obtuvo la información: https://wa.aws.amazon.com/wat.introduction.wa-intro.es.html

- CloudComputingTecnlogies. (2020). MODERNIZACIÓN DE APLICACIONES Y PLATAFORMAS PARA EL TELETRABAJO CON AMAZON AWS, KUBERNETES, DATA ANALYTICS Y CLOUD COMPUTING Sitio de donde se obtuvo la información: https://cloudcomputingtechnologies.com/es/

- JL Goyes Lara. (2020). Sitio de donde se obtuvo la información: http://repositorio.uasb.edu.ec/bitstream/10644/7468/1/T3265-MAE-Goyes-Estudio.pdf

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica