Modelo de Políticas, Estrategias y Controles que Permita Minimizar los Riesgos para la Seguridad de la Información en la Nube Híbrida Existente en las Organizaciones

Darío Soto Duran, Fabio Alberto Vargas Agudelo y Antonio Toro Moncada.
Facultad de Ingeniería
Institución Universitaria Tecnológico de Antioquia
Medellin, Colombia

Abstract

Due to the great growth of Organizations that migrate their services to a cloud environment, neglecting the security of the information and the risks that this represents for the companies, a model for the security of the information in the hybrid clouds is proposed. To this end, in the first chapter a general description was made of the types of clouds and the services that different service providers offer through them, Likewise, the analysis of the risks for the security of the information described by some of the most relevant entities at world-wide level like it is it The Cloud Security Alliance (CSA), The European Union Agency for Cybersecurity (ENISA), Gartner company dedicated to the investigation and the consultancy of technologies of the information and The National Institute of Standards and technology (NIST) for its initials in English.

In the second chapter, different information security models were analyzed in which the different areas such as organizational, financial and public sector were addressed and from which the most relevant aspects and best practices were extracted, which facilitated the basic concepts of the model and helped to shape its structure.

The third chapter contains the development of the model which consists of a diagram of it and is divided into 4 implementation phases in which the risks for the security of information in the hybrid clouds are determined, and a strategy is designed that accompanied by the implementation of policies and the establishment of controls will help to minimize or mitigate these risks.

Finally, chapter 4 presents the validation of the model with the endorsement by a group of experts in different areas, as well as the respective analysis with the contributions of each of the respondents. The conclusions on the evaluation results are established.

Palabras Clave

Nube Híbrida, Modelo, Seguridad de la Información, Riesgos, Políticas, Controles, Estrategias, Información y Tecnología.

1. Introducción

Las organizaciones en su deseo de ser cada vez más competitivas y rentables están implantando nuevos modelos de computación, entre los que se encuentra como opción la nube, dado que: representa una iniciativa viable al permitir contar con recursos como Infraestructura, aplicaciones y servicios que operan bajo demanda y son fácilmente configurables con un bajo costo y un aprovisionamiento rápido [1]. Así mismo, según el informe *Innovation Insights 2* de 2015, ISACA revela que la computación en la nube como una de las principales tendencias que impulsan la estrategia comercial se ubicó en el tercer lugar entre las 10 tecnologías emergentes más importantes y con mayor probabilidad de ofrecer un valor comercial significativo por encima del costo, (…). Este mismo informe describe a la nube como un modelo de prestación de servicios informáticos que proporcionan acceso bajo demanda a servicios tecnológicos en los que se incluyen aplicaciones, almacenamiento e infraestructura, en comparación con los servicios de las TI de origen tradicional, este modelo ofrece un despliegue rápido con poca participación de Tecnología de la información y una mínima

inversión de capital y sin la necesidad de una estructura de apoyo significativa [2].

2. Antecedentes

En esta sección se mencionarán algunos trabajos de investigación que demuestra un estado del arte de las temáticas relevantes en el presente estudio, los cuales se relacionan con el tema abordado, y que toman como referentes fuentes de amplio interés por parte de la comunidad científica por esclarecer y entender el fenómeno de los aspectos mencionados e inmersos en la investigación.

En primer lugar, se presenta el trabajo realizado por Primorad (2015), titulado *Seguridad en la Computación en la Nube*, siendo su propósito el facilitar una visión general de las principales amenazas, riesgos y aspectos a considerar en la seguridad en la Computación en la Nube. De allí que se presentan las principales amenazas a la seguridad según la Cloud Security Alliance (CSA), los riesgos a evaluar antes de contratar un proveedor en la nube, mencionados por la consultora Gartner y se describen las cuestiones de seguridad y privacidad, consideradas por el Instituto Nacional de Normas y Tecnología (NIST: National Institute of Standards and Technology), que pueden tener impacto a largo plazo en una infraestructura en nube pública [3].

Por otra parte, se encuentra el estudio realizado por Santiago & Sánchez (2017) titulado *Riesgos de Ciberseguridad en las Empresas*, siendo su objetivo abordar los principales riesgos para la seguridad de la información y enfatizar el impacto al que se encuentran expuestas las empresas actualmente cuando los activos de información se ven comprometidos. Por otro lado, se presenta un análisis de las principales amenazas, los riesgos y los efectos negativos que trae consigo la carencia de un sistema de monitoreo que dejarían vulnerables a las organizaciones ante potenciales ataques a la confidencialidad, la integridad y la disponibilidad de los activos de la información que actualmente son gestionados por estas [4].

Se encuentra el trabajo de investigación realizado por Arcila (2019), intitulada *Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información*, siendo su objetivo Plantear recomendaciones de seguridad para los servicios de computación en la nube, dado que en la actualidad las empresas invierten para migrar su información y asegurar a través de aplicaciones, plataformas, entre otros, a la computación en la nube; lo que les brinda la oportunidad de disminuir los costos de mantenimiento de infraestructura propia. Sin embrago las empresas deben implantar controles de seguridad acudiendo a diferentes referentes como lo son las buenas prácticas, estándares y modelos para brindar un mayor nivel de aseguramiento [5].

Por último, se abordarán algunos temas tratados en el trabajo realizado por Cano (2020) titulado *Seguridad y Ciberseguridad 2009-2019*, cuyo objetivo fue revisar los aprendizajes durante el 2009-2019 y las enseñanzas que dejan los eventos adversos de los últimos 365 días de ese período. Las interrogantes planteadas en la investigación señalan: ¿Qué hemos aprendido en esta década? ¿Cuáles son los retos a 2030? El autor realiza una retrospectiva acerca de la seguridad en la última década y cómo esta evolución ha cambiado considerablemente la forma de enfrentar las amenazas y mitigar los riesgos para la seguridad de la información en las organizaciones. De igual forma, esta investigación muestra cómo algunos factores presentes en la nube híbrida, entre los que se encuentran el cómputo en la nube y los dispositivos móviles, y que enmarcan aquellos retos a ser considerados en la nueva década cada vez que los dispositivos interactúan con los activos de información de las

organizaciones que estén digital y tecnológicamente adaptadas [6].

3. Metodología

El apartado metodológico es fundamental para de toda investigación; puesto que, forma cada uno de los componentes para alcanzar los objetivos planeados; por tanto, da a conocer el enfoque metodológico, así como el tipo de investigación y los instrumentos que van a emplearse para obtener datos; además, de los procedimientos para procesar los resultados [7].

Enfoque metodológico.

El presente estudio fue desarrollado bajo el enfoque metodológico mixto que puede concebirse como un conjunto de procesos sistemáticos, empíricos y críticos dentro de la investigación, en esta se toman en cuenta los datos tanto cualitativo como cuantitativo y se integran en un solo estudio para obtener una visión global del fenómeno, se pueden aplicar métodos de tal forma que uno de los dos anteceda al otro o de forma paralela, pero conservando sus estructuras originales [8].

Tipo de investigación.

Se llevó a cabo la investigación aplicada que tal y como lo señala Lozada (2014) Busca la generación de conocimiento con aplicación directa a los problemas de la sociedad o el sector productivo. Esta se basa fundamentalmente en los hallazgos tecnológicos de la investigación básica, ocupándose del proceso de enlace entre la teoría y el producto [9]. En el caso de la presente investigación se propone un modelo que accederá a la aplicación práctica de estrategias y controles que permitan minimizar los riesgos para la seguridad de la información en la nube híbrida existente en las organizaciones.

Técnica para la recolección de la información.

La técnica que permitió la recolección de la información fue el *análisis documental*, el cual se llevó a cabo forma sistémica analizando la información sobre las principales organizaciones de relevancia mundial en el ámbito de la seguridad de la información y la tecnología como lo son: The Cloud Security Alliance (CSA), The European Union Agency for Cybersecurity (ENISA), Gartner y The National Institute of Standards and technology (NIST).

La población.

Tal y como la define Arias (2012) la población es un conjunto finito o infinito de elementos con características comunes para los cuales serán extensivas las conclusiones de la investigación. Esta queda delimitada por el problema y por los objetivos del estudio [10].

En el caso de la presente investigación la población se encuentra constituida por aquellas empresas que puedan adoptar el presente Modelo de Políticas, estrategias y controles que permita minimizar los riesgos para la seguridad de la información en la nube híbrida existente en las organizaciones.

Validación del modelo a juicio de expertos

El juicio de expertos sobre el modelo permitió reconocer si realmente este es aplicable como medio para minimizar los riesgos para la seguridad de la información en la nube híbrida existente en las organizaciones. Fue elaborado por el autor de la investigación y lo validaron tres expertos en el área de seguridad de la información: Julián Grisales, Freddy Gutiérrez y Juan Esteban Puerta, señalando la pertinencia de las preguntas para con el estudio del tema y para con la pretensión de la información que se necesitaba recabar.

El método utilizado para efectos del juicio de experto fue el método Delphi; empleando para ello el cuestionario, cuyas

respuestas fueron expresadas mediante un grado de adecuación que soporta la opinión de los expertos a través de la escala tipo Likert.

4. Resultados

Componentes del modelo de seguridad de la información en la nube híbrida.

Los diferentes componentes descritos en el modelo son el resultado del análisis investigativo realizado a modelos implantados para diferentes ámbitos tecnológicos y organizacionales tanto del sector público, el privado y el financiero, en los cuales se enfatiza en los aspectos más relevantes para la seguridad de la información, algunos de estos enfocados hacia los centros de datos privados al interior de las Organizaciones y otros transferidos para que sean los proveedores de servicios en la nube los que los implanten, dejando de lado el gran porcentaje las empresas que optan por tener sus sistemas de información en ambientes híbridos.

El modelo propuesto, contiene los diferentes momentos que, de acuerdo con las normas internacionales, se deberían tener en cuenta para garantizar la seguridad de la información. Estos momentos se encuentran plasmados en cuatro fases, cada una de estas fases se convierte en el componente primordial de un ciclo constante que abarca las principales tipologías de riesgo como son el Tecnológico, Financiero, Legal y Organizacional que normalmente se dan en el ámbito de la seguridad informática a nivel Empresarial.

Planteamiento del modelo.

Esta sección tiene como objetivo presentar el modelo propuesto, el cual busca facilitar la identificación de riesgos para la seguridad de la información en las nubes hibridas, la implementación de estrategias que faciliten el tratamiento de estos seguido de un diseño de políticas de seguridad de la información y finalmente el establecimiento de controles que permitan mitigar y contener la materialización de los riesgos descritos en el modelo y que pueden afectar la seguridad de la información de las nubes hibridas en las organizaciones.

En la Figura 1, se pueden observar las cuatro fases que abarca el modelo propuesto, las cuales, se encuentran organizadas en un ciclo continuo que va desde la determinación hasta la mitigación o control del riesgo siguiendo una secuencia de fases en la cual se incluyen estrategias políticas y controles que dependen entre sí y que permitirán el logro de este objetivo.

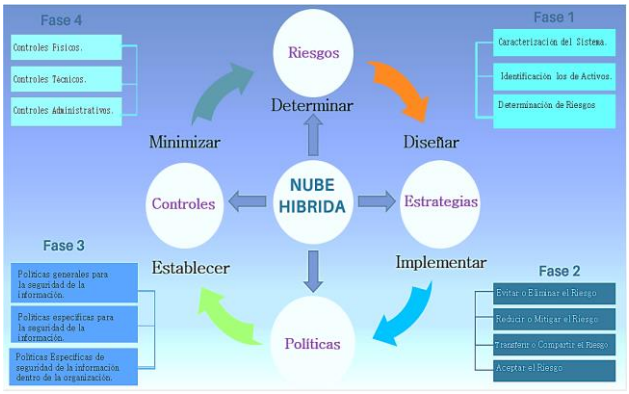

Figura 1. Modelo propuesto

Fuente: Elaboración propia.

Fase 1: Determinación de riesgos.

El objetivo principal de esta fase es determinar los principales riesgos a los cuales se encuentran expuestas las nubes híbridas en las Organizaciones, para lograrlo se definen 3 actividades con las cuales se obtendrá la información necesaria para dar paso a la fase 2 del modelo; ellas son:

a) Realizar una caracterización de los sistemas de información.

Debido a que cada entidad cuenta con unas características particulares que la hacen única bien sea por la infraestructura con la que opera, los servicios alojados en ella o bien las particularidades propias de su nube hibrida, se

debe realizar una descripción completa de esta y se debe determinar entre otros aspectos: la ubicación física de los centros de datos privados y de nube, el personal con acceso a las diferentes tecnologías, documentos y procedimientos existentes, etc.

b) Identificación de los activos de información existentes en la organización.

En esta actividad se debe realizar un completo inventario de todos y cada uno de los activos de información existentes en la organización incluyendo los que se encuentran alojados en las diferentes nubes, se debe asignar un valor a cada activo identificado que de acuerdo con el nivel de criticidad de los atributos de (Disponibilidad, Integridad y Confidencialidad) del activo debe ir entre (1-5) y el cual representara la importancia del activo dentro de la organización.

c) Determinación de los riesgos.

En un análisis de los riesgos para la seguridad de la información en las nubes hibridas y en general para cualquier sistema informático es imperante determinar cuáles son las vulnerabilidades y las amenazas a las cuales se encuentran expuestos los activos de la información, ya que dependiendo de la probabilidad de ocurrencia de estas es que se determinara que tan nocivo y que tanto impacto tendrá este para los sistemas de información, los resultados de este análisis proveerán la información necesaria para la toma de decisiones acerca de las prioridades del que, de qué y cómo proteger dichos activos.

Fase 2: Diseño de estrategias.

Después del análisis de riesgos realizado en la fase 1 se obtiene la información necesaria para diseñar las estrategias que permitan establecer una hoja de ruta acerca de las acciones que la organización tomará para mitigar o reducir el riesgo de su nube híbrida, estas estrategias deben quedar plasmadas en documentos y procedimientos en el cual se definan y prioricen aspectos tan relevantes como los resultados de la evaluación Inicial acerca del estado de la seguridad de la información. La planificación de las actividades encaminadas a la ejecución del modelo, la Implementación y el monitoreo de este con las cuales se podrá llevar una trazabilidad de la eficiencia de este.

En esta fase, se adoptarán las estrategias pertinentes que actuaran como plan de respuesta para el tratamiento de los riesgos, estas se dividen en 4 Estrategias así:

a) Evitar o eliminar: Esta Estrategia permite la implementación de acciones y los mecanismos necesarios que le garanticen a la organización que los escenarios y los factores que posibilitan la generación del riesgo se eliminen completamente reduciendo al máximo la probabilidad de ocurrencia y su alto impacto para la empresa.

b) Reducir o mitigar: Esta estrategia de respuesta al riesgo nos da la posibilidad de reducir el impacto negativo a la organización y debe ser implantada si definitivamente el riesgo no se logra eliminar completamente, para ello se pueden implantar mecanismos de control físicos y lógicos que ayuden en su mitigación.

c) Transferir o compartir: Dentro del diseño de las estrategias para la implementación del modelo es importante contemplar el transferir o compartir el riesgo con terceros bien sea por qué la organización no cuenta con las herramientas necesarias para hacer frente al riesgo para lo cual se pueden entre otras adquirir pólizas de seguro, sin embargo es importante establecer un monitoreo constante del cumplimiento de los proveedores frente a los planes de respuesta a riesgos igualmente se pueden contemplar, la realización de auditorías, establecimiento de indicadores de eficacia y evaluación constante de resultados entre otros.

d) Aceptar el riesgo: Esta estrategia entra en ejecución cuando se han agotado todos los mecanismos y los recursos para tratar de eliminar el riesgo o en casos cuando definitivamente la organización no puede hacer

nada frente a estos como por ejemplo desastres naturales, en este punto las organizaciones deciden aceptarlo y convivir con el dado su baja probabilidad de ocurrencia.

Fase 3: Implementación de políticas.

Después de haber determinado los riesgos para la seguridad de la información en las nubes híbridas inherentes a cada organización en la fase uno del modelo y acorde con las estrategias diseñadas en la fase dos las cuales deben estar alineadas con el desarrollo de las fases tres y cuatro, ya que, como estrategia principal del modelo se encuentran la implementación de políticas, estas establecerán las guías para el comportamiento personal y profesional que tanto el personal interno como externo deben conservar sobre la información que se obtenga, se genere o se procese al interior de la entidad.

En este sentido, el modelo contempla la implementación de las políticas descritas en la siguiente tabla:

Código Política	Descripción de la Política
P-1	Políticas de continuidad de las operaciones del negocio y recuperación ante desastres.
P-2	Política para la gestión de los activos de la información.
P-3	Políticas sobre las reglas de comportamiento del personal de la organización y proveedores.
P-4	Políticas de adquisición, desarrollo de Software y mantenimiento de sistemas informáticos.
P-5	Políticas para la gestión de proveedores.
P-6	Políticas de gestión de comunicaciones y operaciones.
P-7	Política de cumplimiento.
P-8	Política para el tratamiento de datos personales
P-9	Políticas de gestión de riesgos.
P-10	Políticas para la gestión de incidentes de seguridad.

Tabla 1. Descripción de políticas.

Fuente: Elaboración propia.

Fase 4: Establecer controles

Como parte final del modelo y para garantizar el éxito de este se deben establecer los controles que ayuden a reducir o a mitigar los riesgos hallados en la fase 1, para algunos de los cuales se podrán definir controles automatizables.

En esta fase del modelo, además de establecer los controles, contempla la medición de los mismos con el objetivo de comprobar su eficacia, medir la disminución del impacto sufrido por los activos de la información comprometidos y recalcular los valores tanto del impacto como del riesgo residual a los que se encuentran expuestos una vez son establecidos los controles y los valores obtenidos ayudaran a identificar cuáles deben ser las acciones que se deben tomar y dónde aplicarlas a fin de seguir trabajando en su disminución.

En este sentido, se debe tener en cuenta que la seguridad en la nube híbrida se comporta de manera similar que la seguridad informática en general. De esta manera, el modelo propone un total de 22 controles que servirán como marco para el modelo propuesto y de los cuales se realiza una descripción en la siguiente tabla.

Código Control	Descripción del Control
C-1	Implementación de estándares de seguridad sobre la plataforma tecnológica.
C-2	Especificación y cumplimiento de cláusulas legales.
C-3	Implementación de API seguras para el control de acceso.
C-4	Ejecución permanente de pruebas de vulnerabilidades a la plataforma tecnológica.
C-5	Control al cumplimiento de regulaciones nacionales o internacionales por parte del proveedor de servicios en la nube.
C-6	Planes para la recuperación de desastres por parte del proveedor de servicios en la nube y la organización.
C-7	Implementación de herramientas perimetrales de seguridad como firewall y detectores de intrusos entre otros.
C-8	Implementación de un plan de respuesta a incidentes por parte del proveedor de servicios en la nube en los cuales se deben incluir los ANS.

C-9	Implementación de una herramienta de centralización de LOGS.
C-10	Generación de ANS para controlar la instalación de parches de seguridad y la debida corrección de vulnerabilidades.
C-11	Control para la administración de los usuarios
C-12	Vigilancia y monitoreo de los aspectos políticos y económicos del país donde residen los datos con un previo aseguramiento de su ubicación.
C-13	Control sobre el aislamiento de los datos por medio de la segmentación de redes debido a que la infraestructura tecnológica del proveedor de servicio es compartida con varios clientes.
C-14	Control para asegurar que el proveedor de servicios en la nube garantice que los datos en reposo estarán cifrados.
C-15	Realización de Auditorías regulares al proveedor de servicios en la nube sobre la administración de los usuarios a su cargo
C-16	Controlar el almacenamiento de copias de respaldo, definiendo las medidas de seguridad exigidas por los organismos de control y auditoria
C-17	Control para garantizar que se realice la adecuada destrucción de la clave de cifrado de los datos en reposo por parte del proveedor de servicios en la nube cuando el dueño de la información así lo requiera o cuando la relación contractual entre ambos se dé por terminada.
C-18	Control sobre la seguridad física de los centros de datos
C-19	Definición y revisión periódica de las políticas para la seguridad de la información tanto para los proveedores de servicios en la nube como para la organización
C-20	Control para el acceso de a los sistemas informáticos para usuarios en ambientes de teletrabajo.
C-21	Control sobre los procedimientos necesarios para el cambio de un proveedor de servicios en la nube.
C-22	Establecer alertas para configuraciones de nubes riesgosas.

Tabla 2. Descripción de controles.

Fuente: Elaboración propia.

Finalmente, el modelo propone la utilización de la siguiente tabla como base para la determinación de los riesgos para la seguridad de la información en la nube hibrida y se proponen las políticas y los controles idóneos para su eliminación o mitigación.

Cód. Riesgo	Tipo de Riesgo	Des del Riesgo	Cód. Política	Cód. Control
R-1	Legal Financiero Tecnológico Organizacional	Dependencia de un proveedor.	P-3 P-5 P-7 P-8	C-2 C-5 C-12 C-19 C-21 C-22
R-2	Legal Organizacional	Legislaciones extranjeras.	P-5, P-7 P-8	C-2 C-5 C-12
R-3	Tecnológico	Uso, visibilidad y acceso limitado en la nube.	P-1 P-2 P-4 P-5 P-9 P-10	C-1 C-4 C-7 C-8 C-9 C-10 C-11 C-13 C-14 C-15 C-16 C-17 C-18 C-19
R-4	Organizacional	Viabilidad a largo plazo.	P-1 P-2 P-4 P-6 P-7 P-9 P-10	C-2 C-5 C-6 C-8 C-12 C-13 C-14 C-16 C-17 C-18 C-19 C-21 C-22
R-5	Legal Financiero Tecnológico Organizacional	Ataques a la Infraestructura de la nube hibrida.	P-1 P-2 P-3 P-4 P-6 P-7 P-9 P-10	C-1 C-3 C-4 C-6 C-7 C-8 C-9 C-10 C-11 C-13 C-14 C-15 C-16 C-17 C-18 C-19 C-20 C-22
R-6	Financiero Tecnológico	Perdida de la disponibilidad por aspectos como ataques de código malicioso, desastres naturales, etc.	P-1 P-2 P-4 P-9 P-10	C-1 C-3 C-4 C-6 C-7 C-8 C-9 C-10 C-11 C-13 C-14 C-16 C-17 C-18 C-19 C-20
R-7	Legal Financiero Organizacional	Exposición accidental de información confidencial.	P-2 P-3 P-5 P-6 P-7 P-8 P-10	C-1 C-2 C-3 C-6 C-8 C-9 C-11 C-13 C-14 C-15 C-16 C-17 C-18 C-19 C-20
R-8	Tecnológico Organizacional	Inadecuado manejo de incidentes.	P-5 P-7 P-9 P-10	C-1 C-2 C-6 C-8 C-9 C-15 C-19
R-9	Tecnológico	Uso y abuso nefasto de la nube.	P-2 P-3 P-5 P-6 P-7 P-10	C-1 C-2 C-4 C-5 C-6 C-8 C-9 C-11 C-12 C-13 C-15 C-16 C-18 C-19 C-20 C-21 C-22
R-10	Tecnológico Organizac	Planes de controles débiles,	P-5 P-7 P-9 P-10	C-1 C-2 C-6 C-8 C-15 C-19 C-21

	ional	Gestión inadecuada de riesgos.		
R-11	Legal Financiero Tecnológico Organizacional	Amenazas internas	P-2 P-3 P-5 P-7 P-9 P-10	C-1 C-2 C-3 C-4 C-5 C-6 C-7 C-8 C-9 C-10 C-11 C-13 C-14 C-15 C-16 C-17 C-18 C-19 C-20
R-12	Tecnológico	Falta de una estrategia de arquitectura y seguridad en la nube hibrida.	P-2 P-4 P-5 P-7 P-9 P-10	C-1 C-8 C13 C-16 C-18 C-19 C-20
R-13	Tecnológico Organizacional	Configuración incorrecta y control de cambios inadecuado.	P-2 P-3 P-4 P-5 P-6 P-7 P-9 P-10	C-1 C-4 C-6 C-8 C-9 C-10 C-13 C-14 C-16 C-19
R-14	Legal Tecnológico	Aislamiento y localización de los datos	P-2 P-5 P-7 P-8 P-9 P-10	C-1 C-2 C-5 C-12 C-13 C-14 C-16 C-17 C-22
R-15	Financiero Tecnológico	Ataques de Ingeniería Social.	P- P-3 P-4 P-5 P-7 P-8 P-9 P-10	C-1 C-3 C-4 C-6 C-7 C-8 C-9 C-10 C-11 C-13 C-14 C15 C-16 C-19 C-20
R-16	Tecnológico	Seguridad de Software	P-2 P-4 P-5 P-7 P-8, P-9 P-10	C-1 C-3 C-4 C-7 C-8 C-9 C-10 C-13 C-16 C-19 C-22
R-17	Tecnológico	Insuficiencia en credenciales de acceso, identidad y gestión de claves.	P-2 P-3 P-4 P-5 P-6 P-7 P-8 P-9 P-10	C-1 C-3 C-4 C-7 C-9 C-11 C15 C-16 C-18 C-20

Tabla 3. Descripción del riesgo, políticas y controles aplicables para mitigarlo.

Fuente: Elaboración propia.

5. Evaluación del Modelo a Juicio de Expertos

Para Lograr el objetivo número cuatro se utilizó la metodología de evaluación de expertos, para ello, se recogieron las impresiones de un grupo de personas expertas en áreas del conocimiento afines a la seguridad de la información, el grupo de expertos recibió el modelo para que lo analizaran y evaluaran, dicha evaluación se aplicó a seis preguntas relacionadas con aspectos puntuales del modelo, sus bondades y las ventajas que traería a las organizaciones que en un momento determinado decidieran implantarlo. La metodología de evaluación fue diseñada de acuerdo con el estándar de la escala likert. Sobre la base de los resultados de las evaluaciones se realizó un análisis y se sacaron las conclusiones descritas en la parte final del documento.

6. Discusión

Dentro de las similitudes más relevantes es que tanto en la nube privada como en la pública se utiliza la virtualización como plataforma para los servicios alojados en ellas, si bien no son lo mismo, es importante resaltar que la virtualización es la infraestructura que sustenta la computación en la nube privada de las organizaciones, mientras que la computación en la nube pública se enfoca en la prestación de servicios compartidos a través de entornos virtualizados.

De acuerdo con las definiciones anteriores, se puede concluir que la nube híbrida es la combinación de lo mejor de ambos mundos, donde los recursos se organizan como un entorno de infraestructura integrada, en la cual las aplicaciones y cargas de trabajo pueden compartir los recursos en función de las políticas y técnicas organizacionales en torno a la seguridad, el rendimiento, la escalabilidad, el costo y la eficacia, a fin de utilizarlos como una estrategia para aplicaciones no críticas alojadas en la nube pública y en privada para las aplicaciones más críticas o simplemente para acomodar picos ocasionales en el tráfico de la red.

la nube híbrida es una combinación de los modelos de nube pública y privada de tal forma que, la combinación de estas características proporcione por un lado y de forma privada la mayoría de los elementos que componen la infraestructura; y por otro lado herramientas de desarrollo, aplicativos y servicios de una manera compartida [11].

De igual forma, teniendo en cuenta la posición definida por el NIST "La nube Híbrida, es una composición de dos o más nubes distintas (privadas, comunitarias o públicas) que siguen siendo entidades únicas, pero que coexisten por tener tecnología estandarizada y patentada que permite compartir datos o aplicaciones entre las mismas" [12].

7. Conclusiones

Con respecto al análisis de los riesgos de seguridad de la información existente en las organizaciones que implanten nube híbrida, se debe señalar que las organizaciones si bien tienen sus propias características hay aspectos importantes que pueden ayudar a garantizar la seguridad de la información en un entorno de nube híbrida como lo son los riesgos determinados en este y como en un ciclo continuo se definen y establecen las estrategias, las políticas y los controles que ayudarán a mitigarlo, eliminarlo o en un caso dado aceptarlo.

En relación con la Comparación de los modelos existentes a fin de extraer las mejores prácticas implantadas en estos, hay coincidencia en que su clave principal para minimizar los riesgos para la seguridad de la información en las organizaciones se encuentra en el análisis, diseño y la implementación de una arquitectura en la cual todos sus componentes se encuentren alineados con los requerimientos de seguridad necesarios para garantizar la seguridad de la información.

Con respecto a la Definición del modelo que integre políticas, estrategias y controles de seguridad que ayuden a minimizar los riesgos existentes para la seguridad de la información en la nube híbrida, se propusieron cuatro fases. La Fase 1: Determinación de riesgos, cuyo objetivo principal fue determinar los principales riesgos a los cuales se encuentran expuestas las nubes híbridas en las organizaciones, definidas en tres actividades:

1. Realización de la caracterización de la información existente en la organización
2. Identificación de los activos y
3. Determinación de los riesgos.

Fase 2: Diseño de Estrategias que permitan establecer una hoja de ruta acerca de las acciones que la organización tomará para mitigar o reducir el riesgo de su nube híbrida, estas estrategias deben quedar plasmadas en documentos y procedimientos en el cual se definan y prioricen aspectos tan relevantes como los resultados de la evaluación Inicial acerca del estado de la seguridad de la información.

Fase 3: Implantación de políticas que establecerán las guías para el comportamiento personal y profesional que tanto el personal interno como externo deben conservar sobre la información que se obtenga, se genere o se procese al interior de la entidad. Se tomará como referencia el marco COBIT 5 (ISACA, 2012) en cuyas políticas destacan: a) las generales de seguridad de la información, b) las específicas de seguridad de la información, c) las específicas de seguridad de la información dentro de la organización.

Fase 4: Establecer Controles: se deben establecer para ayudar a reducir o a mitigar los riesgos hallados en la fase 1, para algunos de los cuales se podrán definir controles automatizables, para proceder con el tratamiento de los riesgos hallados y de acuerdo con lo establecido en el estándar de la ISO 27001 se deben adoptar cuatro posibles acciones entre las cuales se encuentran: reducirlos, aceptarlos, evitarlos o, finalmente

transferirlos, y entre los Controles cuentan los físicos, los técnicos y los administrativos [13].

Finalmente, para la Validación del modelo con un caso de estudio en un contexto empresarial y que fue realizada por tres expertos en el área de la seguridad de la información en los que, aunque con enfoques distintos, todos concordaron sobre su pertinencia y señalando que el modelo abarca aspectos sumamente importantes y con enormes beneficios para las organizaciones que en un momento dado pudiesen implantarlo.

8. Agradecimientos

Un agradecimiento muy especial al Tecnológico de Antioquia, a sus docentes y en general a toda la familia de esta amada institución en la cual he realizado todo mi proceso formativo y profesional como Tecnólogo, Ingeniero, Especialista y que ahora con la finalización de la Maestría puedo ver como los frutos de tanto esfuerzo se ven reflejados en mi crecimiento profesional.

A mis asesores de tesis Darío Enrique Soto Duran, decano de la facultad de Ingeniería, y Fabio Alberto Vargas Agudelo, director de Investigación codirector; ambos con sus valiosos aportes y extraordinarios conocimientos enriquecieron paso a paso el desarrollo de esta investigación, mil gracias por toda su disposición.

9. Referencias

[1] Ariza, W. D. (2015). Computación en la nube y su seguridad. Obtenido de Wdda - articulo SIA - UPILOTO - Seguridad en la nube. Obtenido de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2785/00002645.pdf?sequence=1

[2] ISACA. (2015). TOP DIGITAL TECHNOLOGY TRENDS THAT AFFECT STRATEGY. Obtenido de Innovation Insights: https://vdocuments.net/innovation-insights-insights-2-published-uly-2015-we-consider-the-following-trends.html

[3] Primorad, C. R. (2015). Seguridad en la Computación en la Nube. Obtenido de http://exa.unne.edu.ar/informatica/SO/carlos_primorac_monografia_seguridad_en_la_computacio_en_la_nube_preeliminar.pdf

[4] Santiago, E. J. & Sánchez Allende, J. (2017). Riesgos de ciberseguridad en las empresas. Revista de Ciencia, tecnología y medio ambiente, XV, 1-33.

[5] Arcila Bonfate, J. L. (2019). Recomendaciones de seguridad para los servicios de computación en la nube, a partir de los estándares y modelos de seguridad de la información. (Trabajo de grado). Obtenido de https://repository.ucatolica.edu.co/bitstream/10983/23388/1/RECOMENDACIONES%20DE%20SEGURIDAD%20PARA%20LOS%20SERVICIOS%20DE%20COMPUTACION%20EN%20LA%20NUBE.pdf

[6] Cano M., J. J. (2020). Seguridad y ciberseguridad 2009-2019. Seguridad y ciberseguridad: ¿Qué hemos aprendido en esta década? ¿Cuáles con los retos a 2030?, VaRZN, 81-94. Obtenido de: https://www.researchgate.net/publication/342048759_Seguridad_y_ciberseguridad_2009-2019_Lecciones_aprendidas_y_retos_pendientes

[7] Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2012). Metodología de la investigación. (6ta ed.). Distrito Federal, México: Interamericana Editores, S.A.

[8] Hernández-Sampieri, R., & Mendoza, C. P. (2018). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta. Ciudad de México: McGraw-Hill Interamericana Editores.

[9] LOZADA, José. Investigación Aplicada: Definición, Propiedad Intelectual e Industria. CienciAmérica, [S.l.], v. 3, n. 1, p. 47-50, dic. 2014. ISSN 1390-9592. Disponible en: http://cienciamerica.uti.edu.ec/openjournal/index.php/uti/article/view/30

[10] Arias, F. G. (2012). El Proyecto de Investigación. Introducción a la metodología científica. (6ta ed.). Caracas, Venezuela: Episteme, C.A.

[11] Martin, E. (12 de 2014). TICBeat. Obtenido de ¿Qué es ‘cloud computing’? Definición y concepto para neófitos: https://www.ticbeat.com/cloud/que-es-cloud-computing-definicion-concepto-para-neofitos/

[12] Grance, P. M. (09 de 2011). The NIST Definition of Cloud. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[13] ISO. (2013). Una Explicación Sencilla de los Principales Aspectos de la Norma ISO 27001. Obtenido de https://normaiso27001.es/