Arquitecturas *multicloud* desde una perspectiva de seguridad

Marcos Calderón Badilla
Escuela de Ingeniería, ULACIT
San José, Costa Rica
mcalderonb772@ulacit.ed.cr

Gabriela Gómez López
Escuela de Ingeniería, ULACIT
San José, Costa Rica
mgomezl087@ulacit.ed.cr

César Vargas Zumbado
Escuela de Ingeniería, ULACIT
San José, Costa Rica
cvargasz959@ulacit.ed.cr

Julio Córdoba Retana,
Escuela de Ingeniería, ULACIT,
San José, Costa Rica
jcordobar022@ulacit.ed.cr

Resumen*—La preferencia de las tecnologías multicloud por parte de las empresas que buscan una infraestructura que les permita la administración y utilización de los sistemas de una mejor manera ha aumentado en los últimos años, pues este tipo de arquitecturas les ofrece muchos beneficios como la disponibilidad de servicios, seguridad en las plataformas, ahorro en costos de equipos para los centros de datos y un gran nivel de escalabilidad que jamás hubieran tenido con sus propios equipos. Además, también destacan otros factores de estas tecnologías, por ejemplo la seguridad, acuerdos de niveles de servicio, conocimiento de las plataformas y monitoreo constante de estas, así como actualizaciones en conjunto por parte del cliente y de la empresa que ofrece el servicio en la nube. En cuanto a los riesgos de implementar este tipo de tecnologías, estos son completamente subsanables si se tiene un control adecuado. Adicionalmente, se mencionan varias empresas líderes a nivel mundial en tecnologías multicloud.

***Palabras clave*—arquitectura, multicloud, seguridad en la nube, ciberseguridad, computación en la nube**

Abstract*— The preference of multicloud technologies by companies searching for an infrastructure that allows the administration and use of systems in a better way has increased in recent years, offering benefits to the companies that want to migrate to this kind of architecture such as the availability of services, security in platforms, savings in equipment costs for the data centers and a great level of scalability that they would never achieve using their own equipment. In addition to this, important factors to consider regarding migration to this type of technology are also highlighted, such as security, service level agreements, knowledge of the platforms and continuous monitoring, also updates of the cloud platform and the client are important. It also talks about the risks involved implementing this kind of technology, which, although it is true, there are risks, but they are completely rectifiable if you make an adequate control. Additionally, several leading companies worldwide in multicloud technologies are mentioned.

***Keywords*—architecture, multicloud, cloud security, cybersecurity, cloud computing**

I. Introducción

El auge de las tecnologías en la nube ha llevado a las empresas a utilizar este tipo de arquitectura y contratar los servicios de computación de diferentes proveedores. La presente investigación pretende esclarecer las incógnitas relacionadas con los riesgos y amenazas con los que podría contar el negocio y la información de una empresa que ha decidido adoptar estas plataformas. WMware, una compañía dedicada a este negocio a nivel mundial, define las tecnologías *multicloud* o multinube como un modelo de computación en el que una organización utiliza una combinación de nubes públicas o privadas, y se cuenta con más de un proveedor de servicios [1]. Microsoft define las nubes públicas como el lugar en donde recursos en la nube (como los servidores y el almacenamiento) son propiedad de un proveedor de servicios en la nube, que los administra y los ofrece a través de internet. Por su parte, la nube privada está compuesta por recursos informáticos que utiliza exclusivamente una empresa u organización. También se describen otro tipo de nubes, como las híbridas, en la cuales se combinan nubes privadas, públicas y entornos locales [2].

Como cualquier sistema informático, los entornos en la nube cuentan con vulnerabilidades que los hacen propensos a recibir ataques. Debido a esto, la seguridad se considera un tema imprescindible, ya que, al existir muchos tipos de arquitecturas y proveedores que compiten en el mercado, se debe determinar cuáles son las medidas óptimas que se deben seguir cuando se contratan este tipo de servicios, los cuales de no ser gestionados adecuadamente podrían significar grandes pérdidas económicas y la filtración de información confidencial que podría incluso dañar la reputación de la empresa. También, la administración de este tipo de plataformas se vuelve más compleja, pues ya no es un solo servicio o plataforma el que estaría alojado, sino múltiples servicios, y se requieren esfuerzos adicionales para asegurar un manejo adecuado.

Es de gran importancia determinar las acciones que toman las empresas en materia de ciberseguridad para proteger los sistemas con los que ya cuentan, especialmente si se utiliza la nube. El servicio contratado por medio de un proveedor posiblemente ofrece un nivel de seguridad asociado, definido en el contrato; sin embargo, complementario a esto, la empresa puede optar por otras funcionalidades u otros sistemas externos para brindar una protección adicional en sus aplicaciones, datos y portales hospedados en estos entornos en la nube.

Adicionalmente, estas plataformas cuentan con capacidades que podrían ser de gran beneficio para la compañía, como la disponibilidad de los servicios al encontrarse replicados en dos

o más plataformas y en diferentes localidades, incluso en distintos países, con lo cual se protegen los recursos de la empresa ante cualquier inconveniente. Por este motivo, es importante realizar un análisis previo que permita determinar todas estas características, asegurar un manejo adecuado y una utilización óptima de todas las cualidades de estas tecnologías.

Por estos motivos, es indispensable definir una estrategia para el manejo de la seguridad en las plataformas que se van a utilizar. Esta debe demostrar los términos de disponibilidad, integridad y confidencialidad, tomando en cuenta las herramientas disponibles y las prácticas recomendadas, ya que no se requiere el mismo esfuerzo para proteger una página web en la que se ingresan y consultan datos de la empresa, a una solución más robusta como lo es la nube.

Como parte de la investigación, se busca determinar si es conveniente para las empresas la implementación de plataformas *multicloud* desde un punto de vista de ciberseguridad; si han demostrado ser más seguras que las *single cloud*, en la cual todos los servicios son ofrecidos por el mismo proveedor [3]; y las implicaciones que conlleva la utilización de entornos bajo diferentes proveedores, con respecto al nivel de complejidad en cuanto al manejo y administración, y si ofrece una mejor gestión de riesgos en comparación con ambientes locales administrados por el personal de la empresa.

II. Metodología

Esta investigación emplea un método cualitativo, con un diseño de tipo investigación-acción, el cual busca determinar si la migración hacia plataformas *multicloud* por parte de las empresas es un movimiento y estrategia acertada; y, a su vez, si los niveles de seguridad que ofrece este tipo de infraestructura se adecúan para salvaguardar los datos de las empresas que serán migrados, almacenados y procesados por este tipo de tecnologías. También, se requiere conocer los riesgos o beneficios que ofrecen este tipo de entornos en la nube, así como la comparación entre distintas soluciones, como las *single cloud* y las nubes híbridas y de esta manera determinar si *multicloud* es realmente confiable a nivel de seguridad, en comparación con otras arquitecturas.

La investigación inicia con la revisión de bibliografía disponible, artículos de investigación realizados por otras empresas en los que se haga una comparación entre las plataformas y los servicios que ofrecen diferentes proveedores en el mercado a nivel global, entre ellas WMware, Amazon, Google y Microsoft. Como instrumento de recolección de datos se realizó la lectura e investigación de artículos relacionados con seguridad en las tecnologías *multicloud*; implementaciones y aplicaciones en la nube; beneficios y experiencias en la migración hacia este tipo de plataformas; así como los datos capturados, evaluaciones y encuestas realizadas por empresas dedicadas a los servicios en la nube.

Se realizó un análisis de la información recopilada, y se determinó cuál se encuentra relacionada con el tema de estudio y que sea de interés para la investigación, además de respaldar las hipótesis ya existentes.

Finalmente, después de efectuar el análisis de los datos, se procedió a plantear las recomendaciones basadas en la información recolectada en la investigación.

III. Marco teórico

Es importante iniciar este artículo brindando la definición de lo que será la base del análisis: la nube, sus servicios, modelos y arquitecturas. CloudFlare [4] describe la nube como el conjunto de servidores a los cuales se accede a través de internet, y que están ubicados en centros de datos por todo el mundo. Asimismo, existen diversos modelos de servicio de computación en la nube que proveen distintos niveles y características conforme a las necesidades de negocio de las empresas. Entre ellos existen el Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS), los cuales son definidos por la empresa Red Hat de la siguiente manera: SaaS es un servicio en el cual el proveedor ofrece los servicios de una aplicación accedida a través de la web y se encarga de la administración de todos los recursos. En el caso de PaaS, el proveedor se encarga del soporte y administración de la plataforma y pone a disposición de los usuarios el manejo de las aplicaciones. Finalmente, en el IaaS, el proveedor se encarga de proveer la infraestructura necesaria, pero es el usuario el encargado de las aplicaciones y sistemas operativos [5]. Además, existen diferentes tipos de implementaciones en la nube, de las que las más habituales son la nube privada, la nube pública, la nube híbrida y la multinube.

Estos tipos de implementaciones se encuentran dentro de ambientes o arquitecturas de una sola nube o multinube. En el primer tipo se ubican las nubes privadas y públicas, las cuales constan de componentes y servicios contratados en servidores exclusivos en el caso de la nube privada, y compartidos para la pública. Por otra parte, las nubes híbridas y la multinube implican el uso de varias nubes —ya sean privadas o públicas— contratadas a proveedores externos [20].

Ahora bien, la transición hacia un modelo de nube es un proceso complejo, especialmente si la empresa o el usuario no cuenta con experiencia previa en dichas plataformas. Requiere de la migración de los sistemas e información de un ambiente local al almacenamiento en la nube e implica dejar el manejo de los recursos e infraestructura en manos de personas externas, por lo cual no debe tomarse a la ligera y se debe hacer la pregunta de si es factible adoptar un modelo de una sola nube o multinube, lo cual determinará los requisitos para realizar la migración.

Los ambientes de una sola nube son descritos como la contratación de un solo proveedor para el despliegue de todas las aplicaciones o servicios que la organización decide migrar a

la nube. A menudo, las organizaciones hacen uso de estos ambientes *single cloud* para un servicio o aplicación, tales como el correo electrónico; el sistema de planificación de recursos empresariales, conocidos como ERP, utilizados para el manejo de las actividades del negocio como recursos humanos; y el CRM, por las siglas en inglés de Customer Relationship Management [6], la cual es una aplicación que permite centralizar las interacciones entre una empresa y sus clientes o similares [7]. Usualmente, estas contrataciones de un solo proveedor la realizan organizaciones pequeñas o con poco conocimiento técnico, que desean obtener los beneficios de la nube sin necesidad de invertir mucho tiempo o dinero.

Asimismo, también se describen a los ambientes multinube, como el agregar más nubes a la ecuación, quizás dos o más proveedores de IaaS, PaaS o demás implementaciones, de manera que las empresas cuenten con distintas soluciones adecuadas según los diferentes tipos de proyectos y necesidades que posean [20].

De acuerdo con los datos obtenidos del Cloud Security Report 2021 —informe publicado por Fortinet y que es el resultado de una encuesta realizada en abril del año 2021 a 572 profesionales de la ciberseguridad de todo el mundo— un 71 % de las empresas encuestadas utilizan un enfoque multinube o híbrido [8], y de ese total, un 67 % hace uso de dos o más proveedores de servicios en la nube, lo cual evidencia que este tipo de ambientes multinube es preferido por las empresas debido a la necesidad de alcanzar requerimientos específicos sin necesariamente estar conectados entre sí.

CloudFlare [9] brinda ciertas ventajas y desventajas con respecto a la estrategia multinube. Entre las ventajas menciona la fiabilidad y redundancia, las cuales les facilitan a las empresas la descentralización y dependencia a una sola nube, dado que si una falla, las demás funcionalidades alojadas en otras nubes aún estarán disponibles para los usuarios y, a la vez, como estrategia de recuperación puede utilizar una nube pública como respaldo y copia de seguridad de las demás nubes. Seguidamente, habla sobre la reducción de dependencia de los proveedores, ya que si se utiliza una estrategia de múltiples nubes, los sistemas y el almacenamiento se distribuyen entre varios proveedores. Por último, destaca el ahorro potencial de costos, al no depender de un solo proveedor, pues la empresa tiene la libertad de elegir los servicios más económicos del proveedor que sea más conveniente y hacer uso de los beneficios que ofrecen a los clientes, como desactivar servicios cuando no se están utilizando o el pago solamente por la cantidad de transacciones realizadas.

Como bien se sabe, las plataformas *multicloud* ofrecen aspectos favorables como la disponibilidad, ya que la plataforma puede estar en dos lugares distintos y si uno falla el otro puede iniciar su funcionamiento, pero también hay muchos riesgos o amenazas que se deben tomar en cuenta con este tipo de ambientes.

Con respecto a las desventajas, se mencionan algunas asociadas con estas arquitecturas [9], entre las que destaca la complejidad de la gestión que implica interactuar con varios proveedores diferentes, cada uno con procesos y tecnologías distintas. A la vez, se menciona el problema de latencia aumentada, vinculada con la comunicación de los servicios entre múltiples nubes originados por distribuciones geográficas, centros de datos o la frecuencia de interacción. También existe un crecimiento de la superficie de ataque, lo que puede provocar que existan más vulnerabilidades en sistemas con componentes integrados y distribuidos entre los proveedores. Además, se menciona sobre la dificultad al equilibrar las cargas en diferentes nubes, en especial si los centros de datos se encuentran muy alejados entre sí.

Si bien es cierto que existe una tendencia hacia la elección de estos ambientes, Linthicum [10] menciona tres aspectos que se deben tomar en cuenta sobre las arquitecturas multinube: el primero se relaciona con la necesidad inherente en temas de seguridad y gobernanza, dada la complejidad y distribución que caracteriza el *multicloud*. Segundo, estos ambientes pueden generar problemas de resiliencia, considerando el gran número de partes en movimiento; y, por último, menciona que estas implementaciones tienen valor solo si se seleccionan los proveedores correctos que satisfagan los requerimientos funcionales y no funcionales de la organización y el negocio.

Por lo cual, con respecto a la privacidad y seguridad en estos ambientes, se debe entender que es una responsabilidad compartida entre la empresa y los proveedores, por lo tanto, entre mayor sea el número de proveedores, mayor será la complejidad para manejar la seguridad. Por esto existen diversas prácticas, plataformas y herramientas que permiten analizar cómo y dónde están los datos almacenados, y a su vez prevenir fugas de información y detectar vulnerabilidades, de manera que las empresas se encuentren seguras y en regla en cuanto al cumplimiento con las regulaciones.

La organización necesita unificar la administración y monitoreo de los sistemas de tecnologías de información, estandarizando políticas y procesos, así como compartiendo herramientas con múltiples proveedores. Este diseño se vuelve un desafío al querer implementar aplicaciones nativas en la nube, y que estas suban el nivel de seguridad y funcionen adecuadamente en entornos *cloud*, garantizando la migración y la interoperabilidad de las distintas plataformas.

Otro riesgo son los controles de seguridad, que entre un servicio en la nube y otro pueden variar, por lo que la seguridad es responsabilidad compartida entre la empresa y los proveedores de servicios *cloud*. El proveedor es responsable de administrar la seguridad de su plataforma y el cliente es responsable de implementar los controles adecuados con el fin

de asegurar los datos, para lo cual no se debe discriminar entre los modelos de servicio de computación que contrate la empresa, como el PaaS o el IaaS mencionados anteriormente.

Para el 2025, Gartner [11] predice que el 99 % de los fallos de seguridad serán por culpa del cliente; las herramientas nativas de *cloud* están disponibles, pero las brechas de seguridad serán por mala configuración o falta de esta. En el 2020, el Ponemon Group-IBM [11] reveló que una de las principales causas de las brechas de seguridad eran las nubes mal configuradas, ya que en un estudio de esta empresa se indica que la mayoría de las empresas que trasladan sus servicios a plataformas *multicloud* no siguen las controles necesarios y buenas prácticas relacionadas con la seguridad y, a su vez, cuando se identifican errores, estos no son corregidos de manera oportuna y proactiva.

La administración de múltiples plataformas *cloud* es otro riesgo, ya que se vuelve difícil el manejo de cuentas de los distintos ambientes, cada una con diferentes configuraciones de seguridad y múltiples aplicaciones con usuarios que las administran. Además, no todos conllevan los mismos criterios de seguridad o pueden existir variaciones en las configuraciones, lo que podría provocar que se pierda el control sobre el manejo de esta y se presenten problemas o vulnerabilidades. Por lo tanto, tal como menciona Bekker [17], para la revista Computer World, la nube ha venido a ofrecer muchos beneficios, pero al mismo tiempo también añade mucha complejidad por tantas tareas y consideraciones que se deben tomar en cuenta.

La idea no es limitar el uso de plataformas *multicloud*, sino más bien evaluar las distintas plataformas con sus niveles de seguridad, y siempre tener un manejo adecuado de las configuraciones de seguridad y un correcto seguimiento de los cambios en las configuraciones que brindan estas plataformas en seguridad, a fin de aprovechar al máximo estos tipos de servicios, pues brindan muchas ventajas.

En cuanto a las herramientas y prácticas, las plataformas multinube proveen mayor flexibilidad; les permiten a las organizaciones administrar los costos, ya que al haber tantos proveedores se puede elegir la mejor opción; ahorrar costos; y, al contar con plataformas en diferentes nubes, se evita el bloqueo y dependencia de un solo proveedor.

Se pueden mencionar varias prácticas o consideraciones que se tienen que tomar a la hora de implementar plataformas *multicloud*. De acuerdo con DataCenter Dynamics [18], las mejores prácticas se centran en las configuraciones, políticas de seguridad adecuadas, automatización, monitoreo e integración de soluciones de seguridad. Para ello, Aquasec [19] recomienda la búsqueda de alguna herramienta de autenticación que soporte los diferentes modelos de autenticación utilizados por los proveedores en la nube, para centralizar cuentas de usuario, permisos y roles en una sola plataforma de administración.

Otra medida es aplicar las actualizaciones de seguridad en los sistemas y velar por que cada plataforma cuente con ellas, debido a que el manejo de estas se realiza distinto en los diferentes ambientes, por lo que como cliente también se debe verificar el debido manejo de los sistemas y así evitar algún riesgo o vulnerabilidad de seguridad por la falta de alguna actualización.

Por otra parte, se debe realizar un fortalecimiento de las plataformas, como por ejemplo cerrar puertos de conexión poco seguros o puertos que no se van a utilizar, removiendo software innecesario; subir la seguridad de aplicaciones e interfaces web; y además, seguir el principio de brindar los permisos necesarios solamente a los usuarios de los servicios (*least privilege*), dado que al tener menor cantidad de permisos se reduce el riesgo.

También, es recomendable adquirir alguna herramienta de seguimiento y monitoreo que funcione en varias plataformas *multicloud*, que permita tener una visibilidad de las plataformas en todo momento, para poder detectar, investigar y responder a algún ataque cibernético en el menor tiempo posible.

Implementar el almacenamiento *multicloud* es otra práctica muy recomendable; se busca así clasificar y almacenar los datos sensibles en ambientes que sean clasificados como más seguros, planeando una distribución geográfica (que los datos se almacenen fuera de la empresa y en varios lugares) e implementando soluciones de DLP (*data loss prevention*) que puedan identificar información filtrada o pérdida de datos.

Una de las mejores prácticas es velar por la seguridad de las plataformas *multicloud* por medio de la implementación de políticas o niveles de seguridad iguales para todas las plataformas; además de buscar siempre herramientas de administración y monitoreo que sean multiplataforma, para centralizar estas labores y evitar el acceso a cada ambiente de manera frecuente, a fin de mejorar el control de estas.

Tanto las plataformas *single cloud* como las *multicloud* son vulnerables a los ataques cibernéticos y cada una tiene sus fortalezas y debilidades. Si se realiza una comparación entre los dos tipos de plataformas, ambas ofrecen beneficios y también pueden contener riesgos.

Muchas empresas migran sus servicios a una sola nube, como por ejemplo Amazon Web Services (AWS), Microsoft Azure o Google Cloud (GCP). Si se analizan las diferentes opciones, las *single cloud* cuentan con varias limitaciones, por ejemplo: tiempos de caída, porque al tenerse todas las aplicaciones o servicios con un solo proveedor y si este sufre algún problema y la plataforma se cae, también se caen los servicios de la empresa y se debe esperar hasta que el proveedor

reestablezca su infraestructura para continuar con los servicios; con las *multicloud* no ocurre esto, ya que, al tener los sistemas en otras nubes replicados, si un proveedor tiene problemas con su infraestructura, inmediatamente se redirige el tráfico al otro servicio sin que hayan caída de los sistemas por largo tiempo. Otro inconveniente en las plataformas *single cloud* es que dependiendo de la infraestructura se puede tener un control y flexibilidad limitado a las capacidades de la plataforma y de la empresa, esto ha llevado a muchas empresas a optar por servicios *multicloud*, en los cuales al contratar varias plataformas unas ofrecen otros servicios con los que otras no cuentan, ayudando a flexibilizar el diseño y control de los servicios.

De acuerdo con la investigación realizada en el año 2020 por Flexera [12] —empresa encargada de proveer a sus clientes soluciones SaaS, que les permitan acelerar los negocios e incrementar los servicios—, un 83 % de las personas encuestadas (entre ellas usuarios y expertos en el mercado de nubes públicas y privadas) consideran que la seguridad se ha convertido en un reto para las compañías que utilizan plataformas *multicloud*. Además, se incluyen datos que evidencian como el mercado está liderado por dos compañías principales que brindan los servicios en la nube. En la encuesta realizada, un 76 % de los entrevistados afirmaron que actualmente utilizan Amazon Web Services (AWS) y un 12 % se encontraba en un periodo de pruebas. Microsoft Azure es utilizado en un 69 % y un 18 % de los usuarios se encontraban en una fase de pruebas; por su parte, Google Cloud Platform solamente cuenta con un 34 % y un 26 % en el área de pruebas.

Por lo tanto, es de gran importancia conocer cómo garantizan estas empresas a los clientes que sus datos y sistemas se encuentran seguros. Amazon cuenta con una estrategia robusta de seguridad, y ofrece a los clientes una plataforma segura y eficiente con capacidad de cumplir con requerimientos de seguridad tales como localización de datos, protección y confidencialidad [13]; también pone a disposición de los clientes, expertos en el área, encargados de brindar altos estándares de seguridad de datos y privacidad. La estrategia se basa en cuatro pilares sobre los cuales esta compañía ofrece una implementación con la seguridad óptima, entre ellos se mencionan: evitar problemas relacionados con la seguridad, por medio de una definición de permisos que garantice la protección de la infraestructura; detectar actividad sospechosa o no autorizada, mediante servicios de monitoreo con que disponen los clientes; respuesta rápida y recuperación ante incidentes; y la automatización de acciones y tareas que permitan solucionar problema de forma rápida para evitar el impacto a los servicios brindados.

Por otra parte, Microsoft ha desarrollado diferentes soluciones para el manejo de la seguridad en los ambientes en la nube y que se encuentran a disposición de los clientes [14], entre ellas se encuentra Azure Security Center, la cual se encarga de centralizar la administración de la seguridad y proveer una herramienta para el manejo de medidas y protección contra amenazas. Cuenta con capacidades claves para la prevención y respuesta ante cualquier eventualidad, como lo son la definición de políticas basadas en los requerimientos de seguridad de los clientes y en las recomendaciones por parte de los expertos en el área; también ofrecen servicios de monitoreo, recolección y análisis, si se presenta alguna eventualidad; así como el uso de inteligencia artificial para una analítica más avanzada de posibles ataques y soluciones. Finalmente, provee a los usuarios un sistema de alertas que emite notificaciones a los interesados, lo que facilita una reacción temprana y la prevención de problemas de mayor escala.

A su vez, esta empresa ha desarrollado otra herramienta con el fin de velar por la seguridad de los clientes: Azure Defender, que proporciona alertas de seguridad y protección contra amenazas [14]. Se integra con Azure Security Center para un manejo más avanzado de la seguridad en plataformas en la nube e híbridas. Este sistema cuenta con sistemas mejorados para la detección y respuesta ante cualquier eventualidad, ofrece medidas de seguridad que permiten limitar el acceso a los entornos de una forma controlada, maneja listas de acceso específicas para las aplicaciones y el monitoreo en tiempo real de los eventos relacionados a la plataforma en la nube.

En un comunicado emitido por Microsoft en enero del 2021 [16], la empresa dio a conocer la expansión de los servicios que ya provee Azure Security Center, al incluir la cobertura de las capacidades a plataformas y recursos en la nube manejados por empresas externas como Google Cloud Platform y Amazon Web Services, ofreciendo un soporte *multicloud*, con el fin de mejorar la seguridad entre estas plataformas. Estos nuevos servicios permiten la comunicación entre las diferentes cuentas, para obtener los datos relacionados a la seguridad manejados por cada empresa externa y analizados por Azure. Dentro de las características, también ofrece una centralización en la configuración y provisionamiento de políticas y accesos, así como el manejo de vulnerabilidades.

Existen otras herramientas de Microsoft que colaboran con la seguridad en diferentes ámbitos. Cloud App Security establece seguridad de acceso a la nube, proporciona visibilidad, control sobre el desplazamiento de datos y un análisis para identificar y combatir amenazas en todos los servicios en la nube. Por último, está GitHub Advanced Security, que busca y analiza posibles vulnerabilidades de seguridad y errores en el código de las aplicaciones.

Google, por su parte, también ofrece servicios para la administración y monitoreo de la seguridad de su plataforma en la nube. Google Cloud Platform contiene funcionalidades para la detección y análisis de ataques; protege tecnologías en la

nube o locales; realiza recuperación ante errores; y protege aplicaciones y servicios en la nube, locales o híbridos. Sin embargo, es notable que sus funcionalidades son limitadas, si se compara con empresas como Amazon y Microsoft.

Cuando se adopta este tipo de plataformas, el proveedor o proveedores elegidos por la empresa deben proporcionar los controles necesarios para brindar la seguridad requerida y velar por la protección de los datos y sistemas de los clientes. Estas prácticas son establecidas en el contrato y se definen medidas y penalidades en caso de que se presente algún inconveniente o fuga de información. No obstante, esto no podría ser suficiente para solventar todos los problemas que podrían ocurrir, por esta razón Grande, en el artículo "The Challenges Managing Multi-Cloud Environments" [15], establece que la seguridad debe considerarse una responsabilidad compartida, ya que además de que el proveedor debe ofrecer seguridad a nivel de plataforma, es el cliente o la empresa como tal, el principal encargado de implementar los controles necesarios para el manejo adecuado de la información y activos de la compañía, así como establecer herramientas de monitoreo y alerta.

IV. Análisis y Resultados

Posterior a la conclusión de las tareas de investigación, se procedió con el análisis de la información y el desarrollo de las ideas obtenidas del conocimiento adquirido sobre el tema, así como de las mejoras que estas arquitecturas *multicloud* han aportado a una empresa estadounidense incluida en el estudio.

Tal como se mencionó anteriormente, la selección, utilización y configuración adecuadas de herramientas de monitoreo, control y prevención pueden ser de gran ayuda para una mejor gestión de las arquitecturas multinube o con múltiples proveedores. Además, la creación de una buena estrategia de seguridad, el desarrollo de procesos de gobernanza y la alineación entre las diferentes áreas de la empresa deben ser contempladas desde el inicio de la migración hacia arquitecturas en la nube; así como también aspectos importantes de replicación de información o páginas de las empresas, para evitar que estas o sus servicios fallen por la caída de una de estas plataformas, todo lo cual está relacionado directamente con el nivel de seguridad o los niveles de servicio que ofrece la plataforma y las medidas de seguridad según los lineamientos que requiera la empresa para sus sitios.

Entre las empresas que pueden servir de ejemplo de una implementación exitosa de este tipo de arquitecturas se puede mencionar a Equifax, empresa norteamericana con su centro de negocios ubicado en Atlanta, que brinda servicios financieros a nivel mundial y que en el año 2017 fue víctima de un ciberataque considerado dentro de los 10 con mayor impacto a nivel mundial.

Debido a este incidente de seguridad y al gran impacto económico y reputacional [21], la empresa decidió dar un giro extremo e impulsar la migración hacia la nube ese mismo año, de manera que aquellas vulnerabilidades descubiertas en la infraestructura y servicios en sitio pudiesen ser resueltas con la implementación de una arquitectura en la nube, pues es mucho más económico contratar un servicio con distintos sitios en la nube, con altos niveles de seguridad y con SLA (*service level agreement*) de un 99 % y no tener que invertir tiempo y dinero en plataformas de seguridad locales para su centro de datos. Por lo tanto, la empresa contrató tres grandes proveedores de servicios *multicloud*: Amazon Web Services, Google Cloud y Microsoft Azure Cloud, con el objetivo de buscar solución a sus problemas y al mismo tiempo recuperar la confianza de sus clientes, quienes incluso optaron por rescindir los servicios de la empresa e irse con la competencia directa.

Así fue como una empresa tan grande inició esta transformación, incorporando dentro de su estrategia de seguridad mejorada, un planteamiento nuevo, en el cual su principal arma es la implementación de una arquitectura multinube, donde cada proveedor brinda soluciones adecuadas a las necesidades operativas y no operativas, que con el transcurrir de los años y hasta la fecha siguen evolucionando y adaptándose a nuevos retos en materia de seguridad. Al contratarse este tipo de servicio, este tiene que ir evolucionando para proteger a sus clientes de las nuevas amenazas que puedan surgir, por ejemplo, aplicando parches de seguridad o solucionando vulnerabilidades en las plataformas con actualizaciones. La empresa contratante de los servicios, por su parte, siempre tiene que estar pendiente de este tipo de acciones, para mantener siempre un sitio seguro donde almacenar sus páginas web y datos.

Una de las actividades llevadas a cabo por la empresa fue la creación de un órgano centralizado encargado de la gobernanza y cumplimiento de las políticas de seguridad en la nube, el cual, al contar con representación de varios departamentos —como los de seguridad de aplicaciones, cumplimiento, legal, protección de activos y desarrolladores— fue el encargado de establecer el conjunto de políticas base que es utilizado para el monitoreo activo de sus activos en la nube desde las perspectivas de seguridad, privacidad, confidencialidad y disponibilidad, incluidas dentro de la estrategia de seguridad de la información corporativa.

Asimismo, existe un conjunto de políticas base para cada uno de los proveedores contratados, de manera que ciertas revisiones son compartidas entre ellos, mientras que otras fueron desarrolladas específicamente para cada ambiente y proveedor. El objetivo es tener una visión holística sobre el inventario completo y a su vez observar en tiempo real, a través de herramientas de automatización, visualización y reporteo, el nivel de cumplimiento y el detalle de aquellas fallas que deben ser remediadas según su criticidad, determinada por el impacto y probabilidad de ocurrencia, según la metodología de riesgos

empresarial, diseñada tomando en cuenta diferentes marcos de trabajo y estándares internacionales de seguridad.

Luego de unos años de haber iniciado la migración y transformación hacia la arquitectura multinube, Equifax podría reconocer que gran parte de su crecimiento y la recuperación de su reputación es debido a la nueva estrategia implementada, la cual es soportada por nuevos procesos, herramientas, recurso humano y constante capacitación. Esto pudo haber sido diferente de haber elegido una *single cloud* o un solo proveedor, tomando en cuenta los riesgos y beneficios previamente descritos en este artículo; o incluso comparado con su antigua implementación "en sitio", la cual a pesar de las medidas de seguridad existentes, fue víctima de ataques por cibercriminales.

A su vez, la empresa es consciente de que a diario surgen nuevas amenazas al negocio, en especial relacionadas con riesgos en las arquitecturas en la nube, por lo cual sus esfuerzos son constantes para garantizar que su activo más valioso —la información— se mantenga seguro, y que a su vez no se vean afectadas la disponibilidad, integridad y confidencialidad de sus datos, procurando siempre evitar una tragedia como la del año 2017.

Incluso, reconocen que la gestión de múltiples proveedores y su orquestación ha resultado ser bastante complicada y requiere de mucho esfuerzo, por lo cual consideran la idea de migrar ciertos servicios alojados en un proveedor hacia otro de los existentes, para solucionar problemas de rendimiento y seguridad. Buscan así evitar abrir brechas que puedan ser vulneradas por el simple hecho de una inadecuada gestión y sincronización entre las plataformas de cada ambiente de cada proveedor y sus conexiones, por lo cual continúan aprendiendo día a día, y construyendo su estrategia de seguridad con el conocimiento adquirido y evidenciado por los constantes esfuerzos para asegurar su infraestructura con cada uno de los proveedores contratados.

Otros datos importantes que se recopilaron con esta investigación es que muchos de los servicios que ofrecen las plataformas *multicloud* pueden ser dinámicos, fácilmente escalables y con precios que varían según el consumo y las configuraciones que necesiten los clientes. Esto demuestra que estos servicios se adaptan de manera personalizada para cada cliente, según sus requerimientos en el momento y pudiendo después realizar cambios de configuración según las necesidades que vayan surgiendo y a un costo mucho menor que si se tuvieran que adquirir equipos nuevos en el centro de datos para solventar las nuevas necesidades.

Como parte de la información que se recopiló durante la investigación sobre los servicios *multicloud* se mencionan tres modelos de servicios principales utilizados que traen consigo diferentes riesgos y amenazas a la seguridad de la empresa, los cuales son:

Infraestructura como Servicio, con sus siglas en inglés IaaS (Infrastructure as a Service): es el modelo más simple de los tres; se basa en la contratación de la infraestructura en la nube y está orientado a administradores de tecnología de información que pueden gestionar máquinas virtuales, servidores y almacenamiento. En este caso, a la empresa se le da el recurso informático —por ejemplo, un servidor virtual— para que lo administre y suba sus servicios dentro de este, y los administradores de tecnología de información siguen gestionando los servidores, incluyendo las configuraciones de seguridad necesarias así como sus actualizaciones.

El segundo modelo de servicio es Plataforma como Servicio, con las siglas en inglés PaaS (Plataform as a Service): en este modelo, el cliente no controla la infraestructura donde se almacenan las aplicaciones. Este modelo es orientado para servicios web, herramientas de desarrollo y bases de datos. En este modelo, el cliente solo puede gestionar las aplicaciones que tiene almacenadas en la nube, no así la infraestructura en la que se encuentran hospedadas las aplicaciones.

El tercer modelo es Software como Servicio, con las siglas en inglés SaaS (Software as a Service): en este caso, el cliente no gestiona ningún servicio en la plataforma, solo lo utiliza, ya sea instalando un cliente liviano, un navegador web o una interfaz de programa. Un ejemplo de esto son los servicios de correo electrónico en la nube.

V. Conclusiones y Recomendaciones

Como resultado de esta investigación, así como de la información y datos obtenidos, se concluye que la migración de los servicios de las empresas a ambientes o plataformas *multicloud* ha demostrado ofrecer mayor seguridad y gestión de los riesgos que los servicios en sitio o los *single cloud*, ya que al tener los servicios en varias plataformas, estas brindan niveles de seguridad superiores y que se ajustan al nivel de seguridad que desee la empresa, sin tener que recurrir a la contratación de servicios o plataformas de ciberseguridad adicionales. Por otra parte, estas plataformas también ofrecen niveles de SLA altos, sin tener que preocuparse las empresas por la caída de un servicio por mucho tiempo, ya que estas plataformas tienen que velar por que el servicio solo tenga fallas mínimas.

Con este estudio se logró comprender que las empresas migran a ambientes *multicloud* por la variedad de servicios y los altos niveles de seguridad, disponibilidad y la confianza que ofrecen no solo para la empresa, sino para los mismos clientes de esta, que saben que los servicios que se les están ofreciendo no van a fallar.

Una medida que se tiene que tomar en cuenta siempre en estos ambientes *multicloud* es el monitoreo constante que deben tener las empresas de sus servicios en la nube, ya que si bien es cierto que las plataformas tienen sus propios servicios de monitoreo, también es importante que la empresa que contrate estos servicios cuente con herramientas de monitoreo y control centralizadas y administradas por personal capacitado, puesto que este es un punto que puede afectar la seguridad de sus servicios en la nube. De no tenerse un seguimiento continuo, cuando la empresa que brinda el servicio avise a la empresa que lo contrató sobre alguna eventualidad, puede ser muy tarde para remediar la afectación de la plataforma.

Un tema muy importante en la implementación de los servicios *multicloud* son los beneficios que trae a las empresas, de los que se pueden detallar dos principales: 1) Reducción de costos, ya que no es necesario que la empresa tenga su centro de datos, ni tampoco que tenga que invertir en infraestructura tecnológica que a los pocos años va a ser obsoleta y ofrecer poca capacidad para los servicios nuevos que vayan surgiendo con el pasar de los años. 2) Aumento muy considerable en la seguridad, pues se pueden combinar diferentes plataformas en distintos sitios del mundo, por lo que si llegara a suceder algo, los datos o servicios estarían seguros en otro lugar, sin que afecte los servicios de la empresa. Esto ofrece más flexibilidad que si se brindara este servicio en solo una plataforma, y se logra un mayor crecimiento y autonomía, pues si se necesita un servicio nuevo o que por algún requerimiento un servidor requiera mayor capacidad de almacenamiento, solo se pasa el requerimiento a la empresa y esta agrega el espacio solicitado sin tener la empresa que adquirir hardware para realizar este cambio, y que además el cambio se haga de forma transparente y no genere ningún impacto para la misma empresa ni para sus clientes.

En cuanto a los riesgos, se puede decir que estos tienen que ver con la estrategia de implementación de las plataformas *multicloud* que quiera utilizar la empresa, pues tiene que ser una transición viable y segura, porque en esta migración no puede comprometer las aplicaciones, sino más bien buscar una plataforma que se ajuste a los modelos *multicloud* que espera la empresa. Al pensar en este tipo de migraciones se tiene que ser consciente de que se tiene que capacitar el personal para que pueda asumir el rol de monitoreo y seguimiento de las nuevas plataformas; y tratar de reducir la complejidad de gestión de estas plataformas, ya que como bien se sabe cada una de estas plataformas tienen niveles de seguridad distintos y tan complejos como se quieran contratar, eso sí asegurando la interoperabilidad de las plataformas, pues aunque sean distintas, tiene que haber una comunicación transparente entre cada una de ellas.

Según el estudio que se realizó, las arquitecturas *multicloud* sí han demostrado ser más seguras que las arquitecturas *single cloud*, pues al tener varios lugares donde esté alojada la información, siempre se va a contar con disponibilidad e integridad de los datos, indistintamente del lugar en el que se encuentren. También brindan confidencialidad por parte de las empresas que se contratan para el alojamiento de estos servicios, ya que con la contratación de estos servicios *multicloud*, las empresas tienen que evaluar cuáles son los servicios que brinden mayores niveles de seguridad y confianza para la empresa, cumpliendo con las necesidades del negocio de la empresa que los contrata. Además de esto, se debe entender que es una responsabilidad compartida entre la empresa y los proveedores, por lo tanto, entre mayor sea el número de proveedores, mayor será la complejidad para manejar la seguridad.

Por otra parte, se habla de que muchos de los ataques cibernéticos registrados ocurren en este tipo de ambientes *multicloud*, pero los ataques ocurren en todas las plataformas, indistintamente de si son *multicloud, single cloud* o centros de datos propios de las empresas; el detalle está en que la información de ataques en estas plataformas *multicloud* sí se registra y funciona como parte de las estadísticas para las empresas, a fin de que puedan mejorar sus servicios de seguridad y confianza a nivel de mercado. En cambio, con las otras plataformas, muchas veces no es conveniente publicar estos datos, pues puede verse afectada la imagen de la empresa no solo a nivel de seguridad, sino también de confianza de los clientes. En otras palabras, no significa que ataquen más los ambientes *multicloud*, sino que los datos de ataques cibernéticos de este tipo de plataformas son más fáciles de obtener y publicar, ya que les sirven de referencia a otras empresas que brindan estos servicios, y son datos estadísticos que dan a las compañías que quieren contratar sus servicios.

Se recomienda como estrategia para la migración a plataformas *multicloud*, que la empresa tenga un equipo encargado de valorar las políticas de seguridad y acuerdos a nivel de servicio (SLA), evaluar las necesidades de las plataformas que se tienen actualmente en el centro de datos y comparar los servicios *multicloud*, para determinar cuál es el que se ajusta mejor a las aplicaciones que se requiere migrar. Este equipo también debe tener un control de acceso y perfiles de administración definidos y monitoreados, así como evaluar la confidencialidad que brinda la empresa en el manejo de sus datos privados o sensibles, siempre manteniendo un monitoreo centralizado y activo de todas las plataformas que contrate la empresa.

VI. Trabajos Futuros

Tomando en cuenta los resultados y el conocimiento obtenidos de esta investigación, se insta a las empresas a incursionar en el mundo de las arquitecturas *multicloud* y al mismo tiempo transmitir sus experiencias a través de la realización y publicación de un artículo donde muestre el proceso de migración y las medidas tomadas en aspectos de

seguridad para sus arquitecturas, con el fin de complementar las bases teóricas y resultados de este artículo.

Adicionalmente, se propone la extensión de la investigación y el análisis de un caso de éxito de la implementación de arquitecturas *multicloud,* en las cuales se hayan contratado otros proveedores distintos a los analizados en este artículo, de manera que se puedan comparar las experiencias y conocimientos, para afianzar la idea de que dichas arquitecturas, independientemente del proveedor, demuestran ser seguras e incluso mejores que las *single cloud* o aquellas en sitio.

A su vez, con el objetivo de analizar el tema desde una perspectiva distinta, se propone investigar y desarrollar un caso de estudio exponiendo el ejemplo de un fracaso de estas implementaciones, donde se muestren los retos vividos, prácticas y tareas llevadas a cabo en ese momento en materia de seguridad, y al mismo tiempo mostrando las experiencias tanto positivas como negativas, para así recopilar aquellas lecciones aprendidas que sirvan como enseñanza para otras empresas o personas interesadas en futuras implementaciones de estas arquitecturas en la nube.

REFERENCIAS

[1] WMware, "Multi-Cloud". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.vmware.com/topics/glossary/content/multi-cloud

[2] Microsoft Azure, "Diferencias entre una nube pública, una nube privada y una nube híbrida". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://azure.microsoft.com/es-es/overview/what-are-private-public-hybrid-clouds/#overview

[3] IBM, "Multicloud". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.ibm.com/cloud/learn/multicloud

[4] CloudFlare, "What is the cloud |Cloud definition". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.cloudflare.com/es-es/learning/cloud/what-is-the-cloud/

[5] Red Hat, "Types of cloud computing". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.redhat.com/en/topics/cloud-computing/public-cloud-vs-private-cloud-and-hybrid-cloud

[6] Oracle, "What is ERP?". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.oracle.com/erp/what-is-erp/

[7] Oracle, "What is CRM?". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.oracle.com/cx/what-is-crm/

[8] Fortinet, "Cloud Security Report". (2021). Accedido el 20 de agosto de 2021. Disponible en: https://www.fortinet.com/content/dam/fortinet/assets/-reports/ar-cybersecurity-cloud-security.pdf

[9] CloudFlare, "What is multi-cloud? |Multi-cloud definition". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.cloudflare.com/es-es/learning/cloud/what-is-multicloud/

[10] Linthicum, D. "Why you should care about multicloud". (2013). Accedido el 19 de agosto de 2021. Disponible en: https://www.infoworld.com/article/2611544/why-you-should-care-about-multicloud.html

[11] Network Computing, "Mitigating the Risks of Multi-Cloud Environments". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.networkcomputing.com/cloud-infrastructure/mitigating-risks-multi-cloud-environments

[12] Flexera, "Releases 2020 State of the Cloud Report". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.flexera.com/about-us/press-center/flexera-releases-2020-state-of-the-cloud-report.html

[13] Cloud Security, "Amazon Web Services (AWS)". (2021. Accedido el 19 de agosto de 2021. Disponible en: https://aws.amazon.com/security/

[14] Azure Security Center | Microsoft Azure. (2021). Accedido el 19 de agosto de 2021. Disponible en: https://azure.microsoft.com/en-us/services/security-center/

[15] Arsys, "Retos de la seguridad en entornos Multicloud". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.arsys.es/blog/soluciones/infraestructura/retos-de-seguridad-en-entornos-multicloud/

[16] Protecting multi-cloud environments with Azure Security Center | Microsoft Security Blog. (2021). Disponible en: https://www.microsoft.com/security/blog/2021/01/27/protecting-multi-cloud-environments-with-azure-security-center/

[17] Computerworld, "Construir una seguridad MultiCloud más fuerte: tres elementos clave". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://cso.computerworld.es/tendencias/construir-una-seguridad-multicloud-mas-fuerte-tres-elementos-clave

[18] Datacenterdynamics, "Las 5 mejores prácticas para una Multicloud segura". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.datacenterdynamics.com/es/noticias/las-5-mejores-pr%C3%A1cticas-para-una-multicloud-segura

[19] Aquasec, "Multi-cloud Security". (2021). Accedido el 19 de agosto de 2021. Disponible en: https://www.aquasec.com/cloud-native-academy/cspm/multi-cloud-security/

[20] Stratoscale, "Cloud or Clouds? How and Why to Choose a Single or Multicloud Approach". (2017). Accedido el 19 de agosto de 2021. Disponible en: https://www.stratoscale.com/blog/it-leadership/cloud-clouds-choose-single-multi-cloud-approach/

[21] CSOOnline, "Equifax data breach FAQ: What happened, who was affected, what was the impact?". (2020). Accedido el 19 de agosto de 2021. Disponible en: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html