



**UNIVERSIDAD TECNOLÓGICA ISRAEL**  
**ESCUELA DE POSGRADOS “ESPOG”**

**MAESTRÍA EN SEGURIDAD INFORMÁTICA**

*Resolución:* RPC-SO-02-No.053-2021

**PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER**

<b>Título del proyecto:</b>
Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017.
<b>Línea de Investigación:</b>
Seguridad Informática
<b>Campo amplio de conocimiento:</b>
Tecnologías de la Información y Comunicación
<b>Autor:</b>
Veloso Canchig Edgar Patricio
<b>Tutor:</b>
Recalde Varela Pablo Marcel

**Quito – Ecuador**

**2022**

## APROBACIÓN DEL TUTOR



Yo, MSc. Pablo Marcel Recalde Varela con C.I: 1711685055 en mi calidad de Tutor del proyecto de investigación titulado: Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017.

Elaborado por: Veloso Canchig Edgar Patricio, de C.I: 1718128604, estudiante de la Maestría: Seguridad Informática, de la **UNIVERSIDAD TECNOLÓGICA ISRAEL**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M.,septiembre del 2022

---

**Firma**

## Tabla de contenidos

APROBACIÓN DEL TUTOR	ii
Tabla de contenidos	iii
Índice de tablas	iv
Índice de figuras	v
INFORMACIÓN GENERAL	1
Contextualización del tema	1
Problema de investigación	2
Objetivo general	2
Objetivos específicos	2
Vinculación con la sociedad y beneficiarios directos:	3
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO	4
1.1. Contextualización general del estado del arte	4
1.2. Proceso investigativo metodológico	5
1.3. Análisis de resultados	6
CAPÍTULO II: PROPUESTA	8
2.1 Fundamentos teóricos aplicados	8
2.2 Descripción de la propuesta	11
2.3 Validación de la propuesta	16
CONCLUSIONES	27
RECOMENDACIONES	28
BIBLIOGRAFÍA	29
ANEXOS	31
Permite que los procesos de seguridad estén equilibrados y a la vez coordinados	
Certificado de confianza y calidad empresarial	37

## Índice de tablas

Tabla 1. Ventajas entre DataCenter y Cloud Computing .....	12
Tabla 2. Desventajas entre DataCenter y Cloud Computing .....	12
Tabla 3. Ventajas de copias de seguridad.....	13
Tabla 4. Desventajas de copias de seguridad.....	14
Tabla 5. Métodos de encriptación entre Cloud Computing y DataCenter Convencional .....	21
Tabla 6. Copias de seguridad en Cloud Computing y DataCenter Convencional .....	22
Tabla 7. Matriz de articulación .....	23
Tabla 8. Comparativa Cloud Computing y DataCenter Convencional. ....	25

## Índice de figuras

Figura 1: Organización Internacional de Normalización .....	8
Figura 2: Firewall .....	10
Figura 3: Estructura de Cloud Computing. ....	15
Figura 4: Estructura de DataCenter.....	15
Figura 5: Firewall rules.....	16
Figura 6: Networking.....	17
Figura 7: Create a firewall rule .....	19
Figura 8: Create a firewall rule llenado.....	20

## INFORMACIÓN GENERAL

### Contextualización del tema

La tecnología es uno de los procesos más usados desde su creación, la misma que se ha enfocado hacia la computación, tomando como referente al Cloud Computing que es una de las tecnologías más populares como servicio, la cual ha causado mucha presión recientemente debido a sus servicios de alta calidad, desde la publicación de la principal fuente de datos de Google en 2003 hasta servicios como AT&T Synaptic Hosting. Es útil porque ha brindado muchos beneficios tanto a las empresas como a las personas, los problemas de seguridad que surgen en la nube hoy en día son un inconveniente importante que se investigará. (Fateme et al, 2022, p. 15).

La utilización del Cloud Computing se vio impulsada con el surgimiento de la pandemia originada por el Covid-19, la misma que obligó a la gran mayoría de empresas y organizaciones a continuar con su trabajo remotamente desde sus hogares casi al cien por ciento, lo que generó que la información o datos que se transportan mediante el internet y la nube se vea más expuestos a la ciberdelincuencia.

Las amenazas a la seguridad aumentan con la creciente demanda de comunicación en la nube, porque no existe propiedad alguna sobre la nube, se compra almacenamiento de un proveedor, el mismo proveedor no garantiza seguridad de la información, lo principal es la protección de datos en la nube (Fursan Thabit, 2022).

Una manera de almacenar información en la actualidad en el ciberespacio, es mediante proveedores de servicios de la nube. Una empresa o institución de cualquier índole puede tener su información en la nube la cual puede estar disponible las veinte y cuatro horas del día y los treientos sesenta y cinco días del año, lo cual es una ventaja que ofrece este servicio, pero a su vez se expone a mayores ataques cibernéticos por lo que, para el resguardo de la información se va a tomar como referencia métodos de seguridad en la nube, los mismos que permiten el aseguramiento, confidencialidad e integridad de datos e información.

Este documento contiene ejemplos de casos reales en el Ecuador, donde se muestra cómo la información de un sistema fue atacada por el ciberterrorismo, para este efecto se aplicará los métodos de seguridad idóneos para cada entorno dependiendo Cloud Computing o DataCenter.

Aplicando estos métodos y mediante su comparación se podrá demostrar que en un sistema empresarial se puede asegurar la información que se encuentra contenida en Cloud

Computing o en un DataCenter, además se busca concientizar al cliente final para que mediante el mismo se puedan prevenir este tipo de eventos.

### **Problema de investigación**

Se ha logrado evidenciar que existe una completa desactualización en los Firewalls lo que ha generado pérdida de información en los DataCenter, lo cual conlleva a una frecuencia constante de ataques cibernéticos que buscan la obtención de información que son de completa confidencialidad, misma que al obtenerla hacen un uso inadecuado de la información.

Hoy por hoy la información sin encriptar en Cloud Computing genera mayor vulnerabilidad al robo de la misma, es por esta razón que surge la necesidad de comparar los métodos de seguridad los cuales sean útiles y amigables para los administradores de Cloud Computing y sus usuarios.

Hoy en día, debido a la expansión de Internet, las aplicaciones informáticas deben contar con mejores softwares o mejores agujeros de seguridad informática porque la multitud de información que se procesa a diario en la Web puede ser interceptada y manipulada por los necesitados. Gente sin escrúpulos se aprovechará de esta inseguridad para delinquir en sus equipos (Zambrano, 2019).

### **Objetivo general**

Realizar una comparación de los métodos de seguridad entre Cloud Computing y DataCenter Convencional mediante las normas ISO 27001 y 27017, para determinar una posible alternativa de seguridad dentro de las mismas.

### **Objetivos específicos**

1. Contextualizar los fundamentos teóricos sobre el Cloud Computing y Datacenter convencional para proteger la información.
2. Establecer el tipo de metodología que ayude a la resolución del problema mediante métodos investigativos.
3. Elaborar mejores prácticas en la empresa Cobis para la seguridad de la información aplicando de forma práctica lo investigado.

### **Vinculación con la sociedad y beneficiarios directos:**

El presente proyecto tiene como propósito comparar los métodos de seguridad para ayudar a los encargados que administran el Cloud Computing y DataCenter Convencional. La Gestión de seguridad informática se basa en la integridad, confidencialidad y disponibilidad por lo cual este proyecto de investigación está enfocado a la seguridad de la información que las empresas manejan haciendo una comparación entre cual sería el mejor servicio que se podría utilizar, los servicios que estamos comparando son el Cloud Computing y los Data Center, utilizando las Normas ISO para así poder aplicar lo investigado en empresas públicas como privadas ya que todas las empresas manejan datos como información y en la actualidad los datos de las personas son los activos que más son atacados por los ciberdelincuentes.

Poniendo en práctica lo investigado se brindara asesorías para que las empresas puedan aplicar las Normas ISO dependiendo con el Servicio que trabajen, y con este aporte se ayuda, a controlar los ataques informáticos ya que dado el desconocimiento de las normas ISO de las empresas se produce el robo de información y por ende el desprestigio de las mismas como ha ocurrido en varios casos que han existido en el país como por ejemplo los ciberataques a bancos y empresas telefónicas entre los más principales.

Teniendo en cuenta los «ODS», esta investigación se centrará en el ODS número 9 ya que “la innovación y el progreso tecnológico son claves para descubrir soluciones duraderas para los desafíos económicos y medioambientales, como el aumento de la eficiencia energética y de recursos” (ETICENTRE, 2019). Ya que contribuye con métodos de seguridad en la infraestructura correspondiente al DataCenter o Cloud Computing, para así poder asegurar que todas las personas tengan acceso a la información de forma confiable, para ello se apoya a que las empresas tengan una optimización en el acceso de la información.

Sin embargo, todavía queda un largo camino por recorrer antes de que el mundo pueda utilizar plenamente este potencial. En particular, las naciones menos desarrolladas deben acelerar el desarrollo de sus sectores y aumentar la inversión en investigación científica si quieren cumplir sus objetivos para 2030.



## CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

### 1.1. Contextualización general del estado del arte

Según Mosquera & Celestino (2017). Dentro de la historia en los años 80, la seguridad de la información ha sido uno de los puntos más prevalecientes que se han aplicado para resguardar toda aquella información que es obtenida bajo el consentimiento de cada una de las fuentes, con el paso del tiempo la protección de los datos ha ido evolucionando con el incremento de nuevas políticas que van reformando las actividades que se encaminan en cada uno de los pasos.

Las Tecnologías de la Información y la Comunicación «TIC» tuvieron efectos que han cambiado la manera en pasado, presente e inclusive cambian la manera en que se ve el futuro. Entonces, por medio de esta indagación, se pretende profundizar en dichos aspectos y aprender más sobre el asunto (seguridad de la información) como un aspecto sustancial de la "tecnología de la información" en la sociedad humana presente, o sea, los "sistemas de información". El tratamiento de la información ya procesada junto con el almacenamiento de datos presente, ha evolucionado con cada generación.

Hablando del Cloud Computing conocido también como computación en la nube, es un término general aplicado a la mayor parte de servicios y procesos que se encuentran almacenados en la nube a través de una red conocida como Internet. Esta tecnología permite el acceso a programas, almacenamiento de información y procesamiento de datos a través de servidores en la nube, tomando en cuenta que este modelo también se le llama cómputo en la nube y no requiere la instalación local de aplicaciones en el ordenador (CITELIA, 2019).

Un centro de datos o centro de procesamiento de datos se necesita para procesar información en una organización. Suele ser un inmueble enorme o una sala con una gigantesca proporción de grupos electrónicos y pcs. generalmente, son creados y mantenidos por enormes organizaciones para entrar a la información primordial para sus operaciones o como espacios para la comercialización o arriendo (Castillo, 2022).

Paralelamente un centro de datos suele ser usado para alojar un sistema de información que consta de elementos de telecomunicaciones, servidores y dispositivos de almacenamiento asociados en un ámbito controlado. El control incluye energía de respaldo, sistema de abastecimiento de energía de respaldo, aire acondicionado, sistema de extinción de incendios y diferentes sistemas de estabilidad, así como además conjuntos como circuito cerrado de televisión, control de ingreso y vigilancia. Es fundamental asegurar que el manejo veinticuatro, siete del dispositivo posibilita una entrada constante a la información de sus consumidores, empleados y proveedores.

En cambio, un DataCenter, es un centro de procesamiento de datos de una o varias empresas, que debe tener una estructura o edificio en el que se permita almacenar y mantener varios dispositivos electrónicos como servidores, ventiladores, conectores y otros recursos necesarios para alojar una red o un sistema informático. (KIONETWORKS, 2022).

“Muchos de los datos que existen en la actualidad son generados desde teléfonos, tabletas, computadoras, electrodomésticos, relojes inteligentes y otros dispositivos conectados a internet y tienen su almacenamiento en DataCenter” (KIONETWORKS, 2022).

Cuando se discute la seguridad de un centro de datos, también es importante discutir las normas ISO 27001. Estos estándares pueden ser implementados en cualquier tipo de organización, ya sea pequeña o grande, privada o pública, con o sin objetivos lucrativos. Además, es posible que una empresa obtenga la certificación. Esto significa que un organismo de certificación independiente confirmará que la implementación de la organización de la ISO 27001 estándar para la seguridad de la información garantizó la estabilidad de la información. (NORMA ISO, 2019)

Es vital tener en cuenta que la norma ISO / IEC 27017 proporciona controles para proveedores y clientes en el mundo virtual. Además, describa las funciones y responsabilidades para ayudar a garantizar que los servicios proporcionados por Internet sean completamente seguros, incluida la información incluida en un sistema de gestión de información certificado. (BSIGROUP, 2022).

## **1.2. Proceso investigativo metodológico**

A continuación, una explicación del proceso de investigación a partir de los siguientes elementos:

### **Investigación Bibliográfica**

Cualquier investigación que requiera la recopilación de datos de fuentes publicadas cae dentro de la definición de investigación bibliográfica. “Estos recursos pueden incluir fuentes más convencionales como libros, revistas, publicaciones periódicas e informes, pero también pueden incluir medios electrónicos como grabaciones de audio, video y películas, así como recursos en línea como sitios web, blogs y datos bibliográficos” (Arteaga, 2020).

Esta investigación ha sido aplicada para la búsqueda de información, con lo cual se logró recopilar toda la información necesaria para sustentar los temas que se están desarrollando en el planteamiento del problema, los datos que se han tomado en cuenta fueron obtenidos de fuentes cuyo origen ha sido verificado, además se cita repositorios

universitarios que han contribuido con información fundamental para la obtención de buenos resultados.

### **La investigación descriptiva**

Hace referencia al diseño de la averiguación, construcción de cuestiones y estudio de datos que se llevarán a cabo sobre el asunto. Se sabe cómo procedimiento de averiguación observacional pues ni una de las cambiantes que son parte del análisis está influenciada. (Taylor & Bogdan, 2012, p. 20)

Se aplicó el uso de la investigación descriptiva para la recolección de los datos más relevantes que ayuden al desarrollo del presente trabajo, mismo que está enmarcado en el análisis frecuente de los datos que se han recolectado por medio de la aplicación de varios instrumentos investigativos, al igual que la aplicación de herramientas completamente necesarias para el análisis de información, se realizó una entrevista aplicada a una población de treinta personas, la herramienta fue un cuestionario en el cual se adjuntó preguntas importantes para el desarrollo de la investigación.

### **1.3. Análisis de resultados**

Para la validación de lo presentado en el proyecto de investigación se realizaron entrevistas a especialistas de la materia sobre la seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 y 27017. Obteniendo los siguientes resultados que se redactan a continuación.

Dentro de las ventajas tenemos que la ISO 27017 proporciona controles para los proveedores y clientes de servicios en la nube, y la ISO 27001 destaca la importancia de la comunicación entre la empresa y el cliente al definir los procesos de gestión.

En cuanto a los protocolos de seguridad informática son reglas o estándares diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información. Son las medidas de seguridad implementadas para evitar que personas no autorizadas accedan, manipulen o destruyan la información como por ejemplo la gestión de IP de acceso limitado, la gestión de IP de acceso libre, la gestión de IP por proxy.

Acerca de los beneficios del Firewall se puede decir que un firewall en la nube es un producto de seguridad que, al igual que un firewall tradicional, filtra el tráfico de red potencialmente dañino. Los cortafuegos basados en la nube forman una barrera virtual alrededor de las plataformas, la infraestructura y las aplicaciones en la nube, al igual que los cortafuegos tradicionales forman una barrera alrededor de la red interna de una empresa. Los cortafuegos en la nube también pueden proteger la infraestructura local.

Se recomendaría el Firewall tanto para el Cloud Computing como para el DataCenter convencional ya que este filtra la información que navega en el internet y la red respectivamente dependiendo de qué servicio vaya a ofrecer

Se toma en cuenta algunos parámetros que se deberían considerar los siguientes: tiempo de respuesta, examinado en cada una de las aplicaciones lanzadas al espacio, rendimiento, que permite analizar cómo se distribuyen los recursos, y fiabilidad, que demuestra la seguridad de los datos que se gestionan.

## CAPÍTULO II: PROPUESTA

Se desarrollará la propuesta del tema de investigación planteado como: Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017.

### 2.1 Fundamentos teóricos aplicados

#### Normas ISO

“Las normas ISO son un conjunto de normas reconocidas internacionalmente creadas para ayudar a las empresas a establecer un nivel de coherencia en la gestión, la prestación de servicios y el desarrollo de productos en la industria.” (Alonso, 2020).

#### Figura 1.

*Organización Internacional de Normalización*



Fuente: Alonso (2020), Se respeta derechos de Autor

#### ISO 27000

Las normas ISO 27000 son un conjunto de estándares a nivel internacional que habla sobre la Seguridad de la Información. “La serie de normas ISO 27000 incluye un conjunto de mejores prácticas para crear, implementar, mantener y mejorar los sistemas de gestión de la seguridad de la información” (INTEDYA, 2019).

#### ISO 27001

Según las normas ISO 27001 describe cómo “La certificación ISO 27001 de gestión de seguridad de la información empresarial es relevante para todo tipo de empresas, independientemente de su tamaño y actividades. Un factor importante en la decisión de implementar un sistema de gestión de seguridad de la información es la cantidad de activos de información necesarios en una organización para lograr sus objetivos” (NORMA ISO, 2019).

## ISO 27017

La más utilizada conjuntamente con la familia de normas ISO 27001, «A diferencia de muchos otros estándares relacionados con la tecnología, ISO/IEC 27017 aclara las funciones y responsabilidades de ambas partes para que el servicio en la nube sea tan seguro como el resto de los datos del sistema de gestión de información de certificados del sistema» (BSIGROUP, 2022).

## Métodos de Seguridad

### Cloud Computing

Según Klusaité (2022) los métodos de seguridad adecuados más conocidos en el cloud computing son:

- **Firewalls:** En la nube son los cortafuegos que ayudan a filtrar conexiones de entrada y salida.
- **Encriptación:** La información que se maneja en la nube debe estar cifrada dependiendo el tipo de cifrado que se maneje por el proveedor.
- **Gestión de la identidad y el acceso (IAM):** La IAM gestiona los accesos a los usuarios dependiendo del rol que posee y esta información la manejan los administradores de la nube.
- **Auditorías de seguridad periódicas:** Se hace un barrido de seguridad en la información contenida en la nube para así estar protegidos de posibles vulnerabilidades que tenga la nube y con esto impedimos que sea atacada por los ciberdelincuentes.
- **Copias de seguridad:** Las copias de seguridad se las realiza para recuperar información en cuanto al tiempo que esta abajo el sistema por ataques a los que está expuesta la información en la nube.

### DataCenter

De acuerdo con (Martínez, 2021), uno de los parámetros iniciales a considerar para mantener seguro un DataCenter tiene que ver con que se deben realizar numerosas visitas y gestiones de la ubicación física del lugar de trabajo, a la luz de posibles inconvenientes naturales y provocados por el hombre, considerando que para un correcto funcionamiento se debe validar toda la infraestructura donde se aloje. En un DataCenter se debe tomar en cuenta los siguientes aspectos:

- Validación de vulnerabilidades.
- Agrupación de equipos y redes según la criticidad.

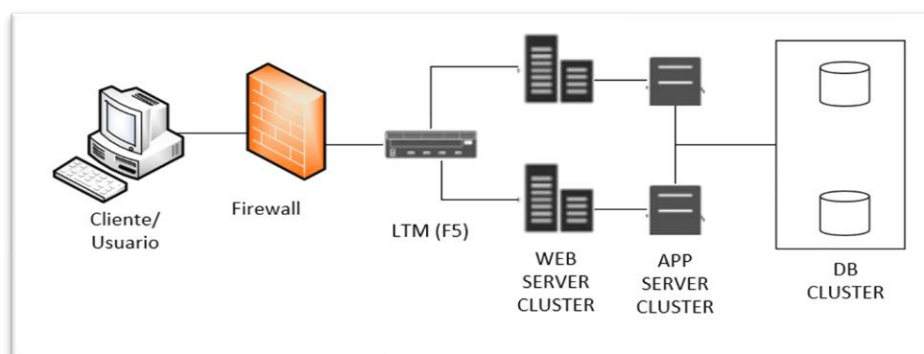
- Firewalls como software y hardware.
- Seguridad para prevenir personas no autorizadas.
- Gestion de acceso.
- Poner mejores controles.
- Gestión privilegiada de acceso
- DLP.
- SIEM.
- Plan de Respuesta y detección de Incidentes.
- Controles de ingreso: validación de ingreso para las tarjetas personales o biométricas.
- Vigilancia los siete días de la semana las veinticuatro horas.
- El personal que se encuentre en seguridad debe estar capacitado para el resguardo de activos.
- Alarmas o videovigilancia.
- Enfriamiento de los servidores para que funcionen de manera óptima y segura para el DataCenter controlando la temperatura constantemente.
- Para finalizar, una medida adicional tenemos la defensa contra incendios protección contra incendios ya que es necesaria para los actores nocivos como el fuego.

## Firewall

Un componente informativo conocido como firewall funciona para evitar que los usuarios no autorizados accedan a una red privada conectada a Internet.” Por ello, el foco de los cortafuegos está en inspeccionar cada mensaje que entra y sale de la red para evitar la aparición de mensajes que no cumplan con ciertos estándares de seguridad y al mismo tiempo permitir un control total sobre las comunicaciones.” (Moes, 2018).

**Figura 2.**

*Firewall*



Fuente: Moes (2018), Se respeta derechos de Autor.

## **Firewall en un Data Center Tradicional**

Un firewall en un Data Center es un software o hardware que utiliza los centros de datos para maximizar la seguridad. “El propósito de un firewall es monitorear el tráfico que ingresa y sale de la red corporativa. En la jerga de la industria, esta red se denomina borde. Para entornos de red fragmentados, los firewalls pueden operar en niveles más bajos para reducir las cargas de trabajo, filtrando las amenazas externas.” (Ramírez, 2022).

## **Firewall en Cloud Computing**

Un firewall en Cloud Computing al igual que un firewall tradicional es un producto de seguridad que “filtra el tráfico de red potencialmente peligroso. A diferencia de los firewalls tradicionales, este firewall está alojado en la nube. Esta forma de firewall en la nube se llama Firewall-as-a-Service.” (Cloudflare, 2020)

## **Encriptación**

Este es un proceso de codificación en el que se cambia el contenido de la información para que sea ilegible, manteniendo la confidencialidad de la información a medida que pasa del remitente al receptor (Fernandez, 2020).

## **Copias de Seguridad**

Se debe entender como una copia de seguridad, a una copia de los datos y archivos originales para evitar la pérdida de parte o totalidad de la información que se mantiene dentro de una entidad (ATICO34, 2018).

## **2.2 Descripción de la propuesta**

En el análisis de los parámetros necesarios para la seguridad de datos se realiza unas tablas comparativas entre ventajas (Tabla 1), desventajas (Tabla 2) entre el Cloud Computing y el DataCenter Convencional, llegando a la conclusión que la más adecuada, puede ser la del Cloud Computing ya que el tráfico de información no tiene que ser canalizado mediante un dispositivo de hardware, de esta manera se evita con mayor eficiencia los ataques cibernéticos y a la vez cuellos de botella en la red.



**Tabla 1.***Ventajas entre DataCenter y Cloud Computing*

<b>Ventajas</b>	
<b>DataCenter</b>	<b>Cloud Computing</b>
<p>Un diseño de firewall confiable y sólido. Toma lo mejor de los firewalls perimetrales y distribuidos para brindar una protección de primer nivel. Un firewall es muy asequible, diagnosticable y escalable.</p> <p>Las reglas se configuran por separado para cada puerto de switch, independientemente del host.</p> <p>Protección de arrendatario obligatoria independientemente del sistema operativo invitado.</p>	<p>Despliegue sencillo sin perder tiempo. Escalable de acuerdo con las necesidades de una organización.</p> <p>La alta disponibilidad garantiza un flujo de servicio continuo y seguro, fuentes de alimentación redundantes y copias de seguridad automáticas.</p> <p>Integre con el control de acceso para proteger las identidades y dar a los usuarios más control sobre las herramientas de filtrado.</p> <p>Se controlan la visibilidad, la configuración, el uso, el registro y más, lo que da como resultado un mejor rendimiento.</p> <p>Si algo sale mal, puede usar instantáneas para restaurar instantáneamente el estado deseado.</p>

Fuente: Pathak(2022)

**Tabla 2.***Desventajas entre DataCenter y Cloud Computing*

<b>Desventajas</b>	
<b>DataCenter</b>	<b>Cloud Computing</b>
<p>Siempre en la mira de los cibercriminales.</p> <p>Vulnerabilidades, malware y cambios no autorizados.</p> <p>Fallas en el acceso o disponibilidad de la información.</p> <p>Deterioro, mal funcionamiento y defectos de los equipos.</p>	<p>La disponibilidad es dependiente del alcance que existe en la infraestructura de la nube.</p> <p>Las funciones avanzadas pueden ralentizar su red.</p> <p>Por lo general, esto tiene en cuenta los casos de uso comunes en los que ciertas vulnerabilidades de software pueden no abordarse de manera efectiva, como las vulnerabilidades de los complementos.</p>

Fuente: Sánchez (2019)

**Tabla 3.**

*Ventajas de copias de seguridad.*

<b>Ventajas</b>	
<b>Cloud Computing</b>	<b>DataCenter</b>
<p>Ahorre tiempo, dinero y recursos. Es más económico utilizar copias de seguridad basadas en la nube que mantener un sistema de copia de seguridad local. Su organización no necesita comprar o mantener hardware y software, ni preocuparse por obtener aprobación para compras de capital. En cambio, paga una tarifa de suscripción, que es un gasto operativo.</p> <p>Protección de datos en caso de siniestro. Huracanes, tornados, inundaciones, etc. En caso de un desastre local, los suministros pueden destruirse en el lugar de trabajo o en las instalaciones. Si bien su oficina y sus sistemas pueden verse comprometidos, sus datos en la nube están aislados de este evento, lo que le permite a su organización volver al trabajo.</p> <p>Se puede acceder a los datos desde cualquier lugar. Siempre que tenga una conexión a Internet, puede acceder a sus datos de respaldo en cualquier momento y en cualquier lugar.</p> <p>Protección contra ataques electrónicos. Si los ciberdelincuentes atacan su sistema local, sus datos estarán seguros. Además de corromper o destruir los datos de producción, los atacantes suelen eliminar o modificar las copias de seguridad locales. Las copias de seguridad externas aisladas en la nube garantizan que los datos estén protegidos.</p>	<p>Recuperación rápida de grandes cantidades. Debido a que las copias de seguridad del centro de datos no dependen de una conexión a Internet, restaurar grandes cantidades de datos desde copias de seguridad locales es mucho más rápido que restaurar desde copias de seguridad en la nube.</p> <p>Usted sabe dónde están sus datos. Si no se aplican las reglas de cumplimiento de datos, su proveedor de nube puede almacenar sus copias de seguridad en diferentes estados o incluso en diferentes países. Con las copias de seguridad de DataCenter, puede comprender dónde están sus datos y controlar directamente el acceso a sus datos..</p>

Fuente: Acronis (2021)

**Tabla 4.***Desventajas de copias de seguridad.*

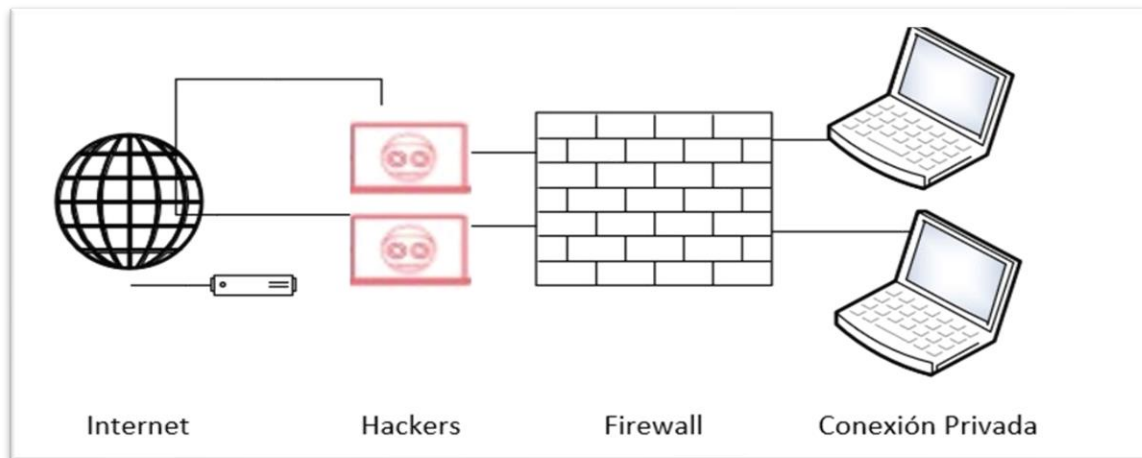
<b>Desventajas</b>	
<b>Cloud Computing</b>	<b>DataCenter</b>
<p>Descargar una copia de seguridad completa lleva tiempo. Según el ancho de banda de Internet y el volumen de datos, puede llevar tiempo, horas o días descargar una copia de seguridad completa desde la nube.</p> <p>Posibilidad de pérdida de datos al final del plazo del contrato. Tenga cuidado y verifique dos veces la política de cancelación de contratos de su proveedor de nube. Si decide cancelar su contrato, asegúrese de poder descargar una copia de seguridad. Después de cancelar su contrato, asegúrese de confirmar cuánto tiempo el proveedor de la nube conservará sus datos.</p> <p>Cambiar de proveedor de servicios en la nube es difícil. Si tiene copias de seguridad con uno de los proveedores de la nube y decide cambiar a otro, la transición puede llevar mucho tiempo. Si bien puede realizar fácilmente una copia de seguridad de su sistema en un nuevo proveedor de la nube, también debe migrar sus copias de seguridad antiguas a la nueva infraestructura de la nube. Existen herramientas que pueden ayudarlo a migrar de una nube a otra, pero solo funcionan mejor si tiene cantidades más pequeñas de datos. Si tiene una copia de seguridad grande de datos de su proveedor de nube original, descargue esos archivos y luego cárguelos en la infraestructura de su nuevo proveedor de nube. Dependiendo de su ancho de banda, la carga y descarga de grandes cantidades de datos puede llevar mucho tiempo.</p>	<p>En caso de un desastre local, no tienes protección. Si las copias de seguridad locales están ubicadas cerca de fuentes de datos, sistemas locales o centros de datos locales, sus datos están en riesgo en caso de desastre. Por lo tanto, se recomienda utilizar siempre una copia de seguridad externa.</p> <p>Si sus sistemas son pirateados, pueden ser alterados. Los ataques cibernéticos de hoy, como el ransomware, no solo afectan sus sistemas y terminales. Su primer paso suele ser eliminar las copias de seguridad locales, lo que impide restaurar el sistema infectado y aumenta sus posibilidades de pagar el rescate requerido.</p> <p>La expansión no es fácil. Si necesita ampliar su sistema de copia de seguridad local, debe invertir en más hardware y software para admitir la mayor cantidad de datos de copia de seguridad.</p>

Fuente: Acronis (2021)

### a. Estructura general

**Figura 3.**

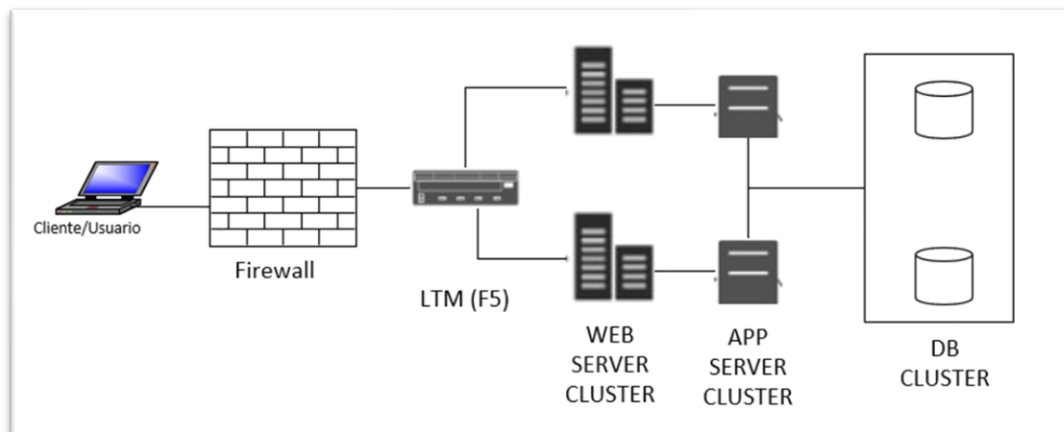
*Estructura de Cloud Computing.*



Fuente: Elaboración propia (2022).

**Figura 4.**

*Estructura de DataCenter*



Fuente: Elaboración propia (2022).

### b. Explicación del aporte

En la Figura (3) se puede observar la estructura del Cloud Computing y en la Figura (4) la estructura de un DataCenter, en el desarrollo de la propuesta se habla de las ventajas y desventajas de las mismas, es por eso que la investigación permitirá un óptimo manejo del firewall aplicando la normas ISO 27001 para el DataCenter y las normas ISO 27017 para el Cloud Computing.

## c. Técnicas

En el desarrollo se implementó técnicas en base a los conceptos ya conocidos y desarrollados por otros trabajos de investigación, de manera que se pueda validar lo propuesto se realizó una entrevista a personas que tienen conocimiento en el tema, para que de esta manera puedan brindar sus opiniones acerca del método de seguridad, mediante firewall para el Cloud Computing y DataCenter, las opiniones brindadas se podrán visualizar en el Anexo 1.

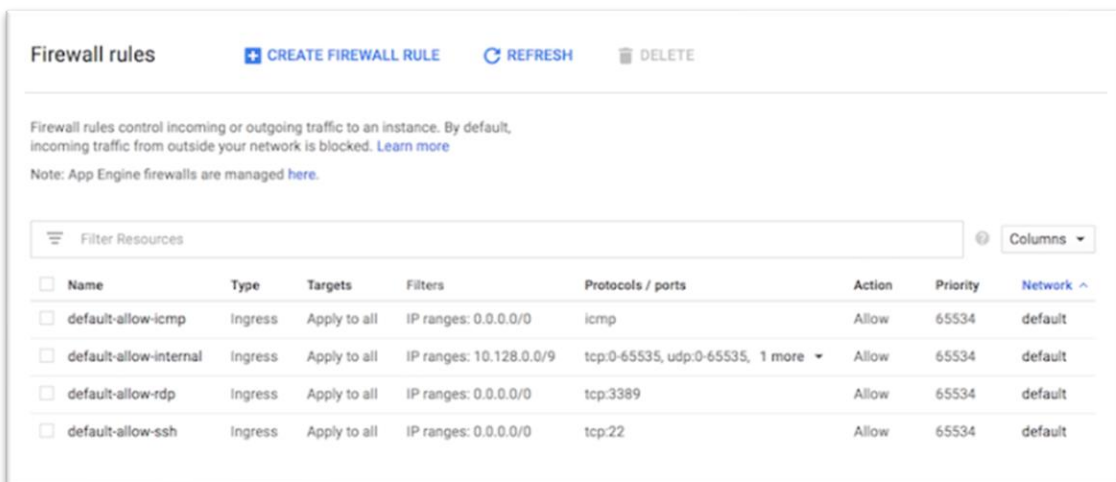
### 2.3 Validación de la propuesta

Para la validación de la propuesta se mostrará los diferentes métodos de seguridad que existen en Cloud Computing y DataCenter Convencional.

#### Configuración Firewall.

Figura 5.

*Firewall rules*



<input type="checkbox"/>	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network
<input type="checkbox"/>	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	icmp	Allow	65534	default
<input type="checkbox"/>	default-allow-internal	Ingress	Apply to all	IP ranges: 10.128.0.0/9	tcp:0-65535, udp:0-65535, 1 more	Allow	65534	default
<input type="checkbox"/>	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:3389	Allow	65534	default
<input type="checkbox"/>	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.0.0/0	tcp:22	Allow	65534	default

Fuente: Google Cloud (2022), Se respeta derechos de Autor

Conceptos de las Reglas de Firewall.

**Default-allow-icmp:** Permitir desde cualquier fuente a toda la red IP. El protocolo ICMP se utiliza principalmente para hacer ping al objetivo.

**Default-allow-internal:** Permitir la conectividad entre instancias en cualquier puerto.

**Default-allow-rdp:** permitir que la sesión RDP se conecte a los servidores de Windows desde cualquier fuente.

**Default-allow-ssh:** Habilite la sesión SSH para conectarse a servidores UNIX desde cualquier fuente.

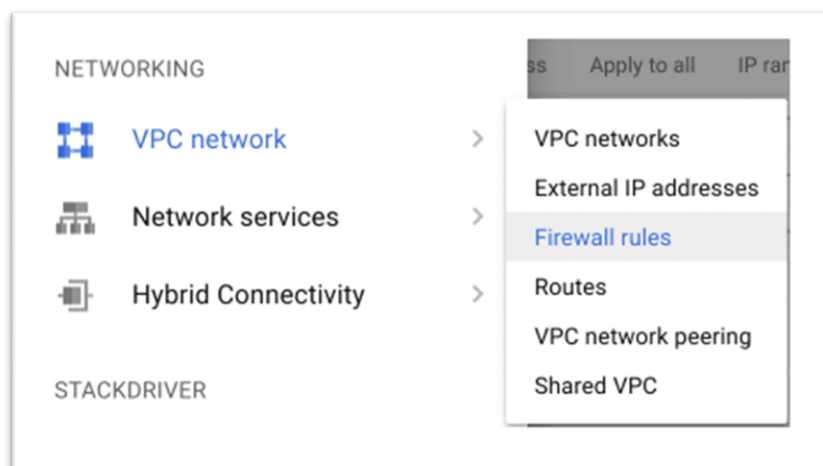
Como puede ver, las reglas predeterminadas para las conexiones básicas le permiten habilitar el comando ping y conectarse al servidor.

El firewall son reglas definidas por software; no necesita aprender o iniciar sesión en dispositivos de hardware de firewall convencionales.

Google Cloud las reglas del cortafuegos tienen estado. Toda la configuración se realiza a través de GCP console o comandos. Por lo tanto, se explica cómo hacerlo usando una consola.

Las reglas de firewall están disponibles en la red de VPC en la sección de redes en el menú del lado izquierdo.

**Figura 6.**  
*Networking*



Fuente: Google Cloud (2022), Se respeta derechos de Autor.

Cuando haga clic en crear una regla de firewall, le preguntará los detalles de conectividad. A continuación, se detalla su correspondiente significado.

**Nombre** - Nombre del firewall (solo en minúsculas y no se permite espacio)

**Descripción** - Opcional pero bueno para ingresar algo significativo, para que recuerde en el futuro

**Red** - Si no ha creado ninguna VPC, verá solo el valor predeterminado y lo dejará como está. Sin embargo, si tiene varias VPC, seleccione la red donde desea aplicar las reglas de firewall.

**Prioridad** - Prioridad de la regla aplicada a la red. El más bajo tiene la prioridad más alta y comienza en 1000. En la mayoría de los casos, desea mantener todos los servicios críticos (HTTP, HTTPS, etc.) con prioridad 1000.

**Dirección del tráfico** - Seleccione el tipo de flujo entre entrada (entrante) y salida (saliente).

**Acción en el partido** - Elige si quiere permitir o denegar.

**Metas** - El objetivo en el que desea aplicar las reglas. Tiene la opción de aplicar las reglas a todas las instancias en la red, solo permitir en etiquetas específicas o cuenta de servicio.

**Filtro de fuente** - Una fuente que se validará para permitir o denegar. Puede filtrar por rangos de IP, subredes, etiquetas de origen y cuentas de servicio.

**Rangos de IP de origen** - Si se selecciona el rango de IP en el filtro de origen, que es el predeterminado, proporcione el rango de IP que se permitirá.

**Filtro de segunda fuente** - Son posibles múltiples validaciones de fuentes.

Ejemplo: puede tener el primer filtro de origen como etiquetas de origen y el segundo filtro como cuenta de servicio. Cualquiera que sea el partido será permitido / denegado.

**Protocolo y puertos** - Puede seleccionar todos los puertos o especificar uno individual (TCP / UDP). Puede tener varios puertos únicos en una sola regla.

**Figura 7.**

*Create a firewall rule*

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

**Name** ⓘ  
lowercase, no spaces

**Description** (Optional)  
[Empty text area]

**Network** ⓘ  
default

**Priority** ⓘ  
Priority can be 0 - 65535 [Check priority of other firewall rules](#)  
1000

**Direction of traffic** ⓘ  
 Ingress  
 Egress

**Action on match** ⓘ  
 Allow  
 Deny

**Targets** ⓘ  
Specified target tags

**Target tags**  
[Empty text area]

**Source filter** ⓘ  
IP ranges

**Source IP ranges** ⓘ  
for example, 0.0.0.0/0, 192.168.2.0/24

**Second source filter** ⓘ  
None

**Protocols and ports** ⓘ  
 Allow all  
 Specified protocols and ports  
semicolon separated, for example, tcp; udp:80; udp:5000-6000

**Create** **Cancel**

Fuente: Google Cloud (2022), Se respeta derechos de Autor

Provea un nombre de regla

Elija un preámbulo en la dirección del tráfico

Elija permitir para la acción del partido

Seleccione todas las instancias en una red en el destino (suponiendo que quiera conectarse a cualquier VM con el puerto 5000)

Seleccione rangos de IP en el filtro de fuente (suponiendo que quiera conectarse desde cualquier fuente)



Para ofrecer rangos de IP de origen  
Seleccione protocolos y puertos especificados  
Haga clic en crear

**Figura 8.**

*Create a firewall rule llenado*

← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name ⓘ  
ssh-custom-port

Description (Optional)  
[Empty text box]

Network ⓘ  
default

Priority ⓘ  
Priority can be 0 - 65535 Check priority of other firewall rules  
1000

Direction of traffic ⓘ  
 Ingress  
 Egress

Action on match ⓘ  
 Allow  
 Deny

Targets ⓘ  
All instances in the network

Source filter ⓘ  
IP ranges

Source IP ranges ⓘ  
0.0.0.0/0

Second source filter ⓘ  
None

Protocols and ports ⓘ  
 Allow all  
 Specified protocols and ports  
tcp:5000

Create Cancel

Fuente: Google Cloud (2022), Se respeta derechos de Autor

## Encriptación

Para la encriptación de datos tanto para el DataCenter y Cloud Computing se tienen diferentes métodos de cifrado la cual se detallará en la (Tabla 5).

**Tabla 5.**

*Métodos de encriptación entre Cloud Computing y DataCenter Convencional*

Método	Encriptación	
	DataCenter Convencional	Cloud Computing
<b>Simétrico</b>	<p>Estándares de cifrado de datos (DES): Es una forma matemática que convierte la información en bloques de 64 bits a claves que se utilizan en 48 bits mediante programas de computador.</p> <p>Triple DES Cifra, descifra y vuelve a cifrar la información para tener mayor Estándar de cifrado avanzado (AES): Es una norma de EEUU que se la utiliza en varios países para cifrar datos de una manera confiable.</p> <p>Twofish es un programa de cifrado de software libre es muy utilizado por su rapidez al cifrar datos.</p>	<p>Debido a que la clave utilizada para realizar la operación es la misma en ambos casos, este es uno de los algoritmos más eficientes y rápidos. Como resultado, se creará una contraseña compleja que será difícil de descifrar, pero que se utilizará tanto para cifrar el archivo como para descifrarlo posteriormente.</p>
<b>Asimétrico</b>	<p>RSA, las siglas que utiliza son las iniciales de sus inventores este programa cifra datos con clave publica y los descifra con claves privadas para tener mejor control de la información en la red.</p> <p>Infraestructura de clave pública (PKI): PKI se utiliza certificados digitales para el cifrado de la información y con esto estamos asegurando la recepción de los datos.</p>	<p>De unas características muy distintas es el cifrado asimétrico, que se desmarca del anterior modelo debido a que se utilizan dos claves distintas en el proceso de encriptación y descifrado. Se utiliza generalmente con envíos de información de menor envergadura, como pueden ser correos electrónicos.</p>
<b>Hibrido</b>		<p>Existe un tercer tipo que es el que saca más partido de cada una de las características naturales de los dos modelos previos, el asimétrico y el simétrico. La idea de este sistema de cifrado híbrido es unir lo mejor de cada lado y que así la fortaleza en la protección sea del</p>

---

doble, lo que deja unas sensaciones muy positivas por garantizar que la conexión siempre será segura.

---

Fuente: García (2018)

### **Copias de Seguridad**

Es un servicio que utiliza una organización para realizar una copia de seguridad de su sistema, aplicaciones y datos en un servidor como se puede visualizar en la Tabla 6.

#### **Tabla 6.**

*Copias de seguridad en Cloud Computing y DataCenter Convencional*

---

<b>Tipos</b>	<b>Cloud Computing</b>	<b>DataCenter Convencional</b>
Totales	Este tipo de copia completa de datos hace una copia de todos los datos. No importa si nada ha cambiado desde la última vez que se realizó la copia.	
Diferenciales	Dado que solo contiene cambios realizados desde la última copia completa, es una copia más segura de lo habitual.	
Incrementales	Todos los archivos se copian completamente por motivos de seguridad, y cualquier dato o alfombra nueva que esté disponible es luego incluido.	

---

Nota: Elaboración propia.

### Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

**Tabla 7.**

*Matriz de articulación*

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
ISO 27001	Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa	La metodología de investigación es bibliográfica, lo que permite conocer la norma ISO 27001.	Fuente bibliográfica	Analiza las características de seguridad que debe poseer según sus normas en un Data Center	
ISO 27017	A diferencia de muchas otras normas relacionadas con la tecnología,	La metodología de investigación fue bibliográfica que	Fuente bibliográfica	Analiza las características de seguridad que debe poseer según sus	

---

ISO/IEC 27017	permitió tener los	normas un Cloud
Aclara las funciones	conceptos sobre la	Computing
y responsabilidades	norma ISO 27017	
de las partes para		
proporcionar		
servicios en la nube		
y otros datos		
contenidos en		
sistemas de gestión		
de información		
aprobados.		

---

**Fuente:** Elaboración propia

**Tabla 8.***Comparativa Cloud Computing y DataCenter Convencional.*

<b>Metodologías</b>	<b>Cloud Computing</b>	<b>DataCenter Convencional</b>
<b>Firewall</b>	X	X
<b>Encriptación</b>	X	X
<b>Gestión de identidad y el acceso (IAM)</b>	X	X
<b>Auditorías de seguridad periódicas</b>	-	X
<b>Copias de seguridad</b>	X	X
<b>Segmentación de redes y equipos críticos</b>	-	X
<b>IPS Sistema de Prevención de Intrusos</b>	-	X
<b>Adecuación de Permisos</b>	X	X
<b>Vigilancia 24/7</b>	X	X
<b>Climatización de los Servidores</b>	-	X
<b>Protección contra incendios</b>	-	X
<b>Plan de Detección y respuestas a incidentes</b>	X	X

Fuente: Elaboración propia (2022).

La tabla que precede (Tabla 8), muestra la comparativa de Cloud Computing y DataCenter Convencional, dejando a cada empresa la decisión de su uso acorde a su realidad, teniendo en cuenta las diferentes metodologías como el firewall, encriptación, gestión de identidad y el acceso, copias de seguridad, IPS, adecuación de permisos, vigilancia veinte y cuatro horas y siete días, plan de detección y respuestas a incidentes estos se muestran optimizados, mostrando una similitud en cuanto al funcionamiento tanto para el Cloud Computing y DataCenter Convencional.

Las Auditorias de seguridad periódicas dentro del Cloud Computing se encarga de realizar la empresa a la que se contrató el servicio, en cambio en el DataCenter las auditorias tienen que realizar las personas que están a cargo del servidor, la segmentación de redes y equipos críticos no es muy necesario dentro del Cloud Computing ya que como es un servicio por internet se puede conectar desde cualquier dispositivo, al contrario en el DataCenter se debe segmentar las redes y configurar puertos para evitar que cualquier persona pueda acceder a la información, la Climatización y Protección contra Incendios el Cloud Computing no tiene disponible ya que el servidor se encuentra en la nube, mientras que el DataCenter debe tener protocolos contra incendios ya que los servidores son físicos y deben mantener temperaturas bajas para evitar el sobrecalentamiento.

## CONCLUSIONES

Se elaboró la búsqueda de información para la comparación de métodos de seguridad entre data center y Cloud Computing, en la que se pudo evidenciar los beneficios que cada uno de ellos ofrece.

Se ha logrado contextualizar todos los fundamentos teóricos que se han encontrado de acuerdo al manejo de información que existe en el Cloud Computing y el Data Center.

Se aplicó la utilización de metodologías de investigación entre ellas la bibliográfica y la descriptiva donde se usó de herramienta un banco de preguntas para el cuestionario aplicado a los usuarios que estaban relacionados de forma directa con la empresa Cobis.

Se realizó una tabla comparativa donde se muestra los diferentes métodos seguridad como el firewall evidenciando de esta manera que su funcionamiento es similar en el manejo en el Cloud Computing y el DataCenter.

La metodología de seguridad que existe dentro de Cloud Computing y DataCenter Convencional se aplica de formas distintas de acuerdo a la gestión de datos, debido a que el uno se maneja de forma virtual y el otro necesariamente físico.

Es importante que se adecúe cada tipo de seguridades dependiendo de la necesidad de cada empresa tanto si lo maneja de manera física (DataCenter Convencional) o virtual (Cloud Computing).

Se concluye que la investigación promueve a la innovación de las empresas ya que se aplicó normas que rigen la seguridad y el acceso a la información de parte de toda la población de una forma segura.

En la presente investigación se menciona sobre la aplicación de las normas ISO 27001 para el DataCenter Convencional y 27017 para Cloud Computing, manifestando que son necesarias para el resguardo de la información, en estas se mencionan varios métodos de seguridad como el firewall, encriptación y copias de seguridad, llegando a la conclusión mediante la tabla comparativa que el firewall es una mejor opción de seguridad para el Cloud Computing y el DataCenter Convencional se vería beneficiado con el uso de copias de seguridad, pero dejando a cada empresa la decisión de su uso acorde a su realidad.



## **RECOMENDACIONES**

Se recomienda analizar los métodos de seguridad que se han investigado para la conservación de los datos adecuados en Cloud Computing y DataCenter.

Es recomendable mantener constante revisión teórica acerca de las nuevas actualizaciones que pueden salir con respecto al Data Center y Cloud Computing

Se recomienda utilizar métodos investigativos para el desarrollo de cualquier trabajo de titulación debido a que sus herramientas brindarán la facilidad en la obtención de resultados favorables para la investigación.

Se recomienda revisar todo el trabajo realizado y continuar con mejoras que puedan asegurar la información que se mantiene dentro de la empresa Cobis.

Es recomendable que las seguridades que se apliquen siempre vayan conforme a las necesidades que se van ir adecuando a los servicios que brindan a sus clientes.

Es recomendable que se revise el cuadro comparativo que se realizó respecto a cada método de protección de acuerdo a su almacenador de datos para generar una anticipación ante posibles desastres ya sean por ataques cibernéticos o incendio físico del almacenador.

## BIBLIOGRAFÍA


- Acronis. (22 de Febrero de 2021). *Acronis*. Obtenido de Acronis: <https://www.acronis.com/es-es/blog/posts/cloud-vs-local-backup/>
- Alonso, C. (5 de Marzo de 2020). *globalsuitesolutions*. Obtenido de globalsuitesolutions: <https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.>
- ATICO34. (5 de Octubre de 2018). *Hosting pedia*. Obtenido de Hosting pedia: <https://hostingpedia.net/copias-de-seguridad.html>
- BSIGROUP. (4 de Junio de 2022). *bsigroup*. Obtenido de bsigroup: <https://www.bsigroup.com/es-ES/ISO27017-controles-seguridad-servicios-cloud/>
- Castillo, G. (30 de Junio de 2022). *Innovación digital 360*. Obtenido de Innovación digital 360: <https://www.innovaciondigital360.com/big-data/que-son-y-como-funcionan-los-data-center/>
- CITELIA. (9 de Diciembre de 2019). *citelia*. Obtenido de Citelio conéctate con nosotros: <https://citelia.es/blog/que-es-cloud-computing-y-como-funciona/>
- Cloudflare. (27 de Marzo de 2020). *cloudflare*. Obtenido de cloudflare: <https://www.cloudflare.com/es-es/learning/cloud/what-is-a-cloud-firewall/>
- ETICENTRE. (30 de Agosto de 2019). *ETICENTRE*. Obtenido de ETICENTRE: <https://www.eticentre.org/objetivos-desarrollo-sostenible/industria-innovacion-e-infraestructuras/>
- Fatemeh Khoda Parast, C. S. (2022). *Cloud computing security: A survey of service-based models*,. Obtenido de <https://www.sciencedirect.com/science/article/pii/S0167404821003977>
- Fernandez, Y. (6 de Marzo de 2020). *Ayuda le proteccion datos*. Obtenido de Ayuda le proteccion datos: <https://ayudaleyprotecciondatos.es/2022/02/11/enciptacion-datos/#:~:text=La%20enciptaci%C3%B3n%20de%20datos%20es%20un%20proces%20de,la%20informaci%C3%B3n%20mientras%20viaja%20del%20emisor%20al%20receptor.>
- Fursan Thabit, O. C.-G. (2022). *A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing*. Obtenido de International Journal of Intelligent Networks: <https://www.sciencedirect.com/science/article/pii/S2666603022000033>
- García, R. (15 de Julio de 2018). *Media Cloud*. Obtenido de Media Cloud: <https://blog.mdcloud.es/tipos-de-enciptacion-en-cloud-computing/>
- INTEDYA. (1 de Septiembre de 2019). *INTEDYA*. Obtenido de INTEDYA INTERNATIONAL DYNAMIC ADVISORS: <https://www.intedya.com/internacional/757/noticia-iso-27000-y-el-conjuntode-estandares-de-seguridad-de-la-informacion.html>
- KIONETWORKS. (14 de Junio de 2022). *KIONETWORKS*. Obtenido de KIONETWORKS: <https://www.kionetworks.com/blog/data-center/qu%C3%A9-es-un-data-center>
- Klusaité, L. (7 de Abril de 2022). *NordVPN*. Obtenido de NordVPN: <https://nordvpn.com/es/blog/seguridad-cloud-computing/>

- Martínez, E. (21 de Abril de 2021). *Seguridad en América*. Obtenido de Seguridad en América: <https://www.seguridadenamerica.com.mx/noticias/articulos/27438/soluciones-de-seguridad-en-data-centers>
- Moes, T. (25 de Marzo de 2018). *SoftwareLab*. Obtenido de SoftwareLab ORG: <https://softwarelab.org/es/que-es-un-firewall/>
- NORMA ISO. (25 de Junio de 2019). *normaiso27001*. Obtenido de normaiso27001: <https://advisera.com/27001academy/es/que-es-iso-27001/>
- Pathak, A. (7 de Abril de 2022). *geekflare*. Obtenido de geekflare: <https://geekflare.com/es/hardware-vs-software-cloud-firewall/>
- Ramírez, A. (1 de Junio de 2022). *Community*. Obtenido de FS Community: <https://community.fs.com/blog/what-is-a-data-center-firewall.html>
- Sánchez, F. (17 de Febrero de 2019). *Smartekh*. Obtenido de Smartekh: <https://blog.smartekh.com/4-de-las-principales-problematicas-y-riesgos-en-los-data-center>
- Zambrano, G. A. (2019). DIAGNÓSTICO DE LAS VULNERABILIDADES INFORMÁTICAS EN. (*Tesis de Ingeniería*). Universidad Tecnológica Israel, Quito.

**ANEXOS**

**ANEXO 1**

**FORMATO DE ENTREVISTA**

	<p><b>UNIVERSIDAD TECNOLÓGICA ISRAEL</b></p> <p>Maestría en Seguridad Informática</p>
---	---

El objetivo del presente instrumento es conocer la importancia sobre Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

Fecha: \_\_\_\_\_

**1. Datos Personales**

<b>Nombre:</b>		Ingeniería		PhD
<b>Título:</b>		Especialización		Otro

**2. Banco de Preguntas**

- ¿Cuáles son las ventajas de las Normas ISO 27001 y 27017?
- ¿Cuáles son los protocolos de seguridad para la configuración del Firewall?
- ¿Cuáles son los beneficios de utilizar el Firewall en un DataCenter y Cloud Computing?
- ¿Por qué se recomendaría el uso del Firewall en un DataCenter y en Cloud Computing?
- ¿Según su experiencia cuales sería los parámetros para la configuración del Firewall en un DataCenter y Cloud Computing?

**GRACIAS POR SU COLABORACIÓN**

**Firma y Sello**

\_\_\_\_\_  
Ci: \_\_\_\_\_  
Nombre: \_\_\_\_\_

## Entrevista

	<b>UNIVERSIDAD TECNOLÓGICA ISRAEL</b> Maestría en Seguridad Informática
---	--

El objetivo del presente instrumento es conocer la importancia sobre Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

**Fecha:** 11/08/2022

### 1. Datos Personales

<b>Nombre:</b> Alex Asimbaya	X	Ingeniería		PhD
<b>Título:</b> Ing. En informática y sistemas computacionales		Especialización		Otro

### 2. Banco de Preguntas

#### • ¿Cuáles son las ventajas de las Normas ISO 27001 y 27017?

##### **Ventajas de implementar la norma ISO 27001**

- Permite que los procesos de seguridad estén equilibrados y a la vez coordinados entre sí.
- Permite crear metodologías que contribuyan a la mitigación de los riesgos y a incrementar el nivel de seguridad en la información que se tiene.
- Si se materializa un riesgo, posibilita que este no cause grandes pérdidas y que se cuente con un plan de acción para actuar de manera eficaz.
- Favorece el cumplimiento de los requerimientos legales exigidos por los entes de control.
- Genera valor agregado para la compañía, pues aún no son muchas las empresas que cuenten con la certificación de seguridad en la información.
- Permite reducir costos gracias a la eficiencia que se emplea.
- Genera confianza entre todas las personas de la organización, sean clientes, proveedores o empleados.

- Posibilita la activación de alertas en caso de que se llegue a presentar alguna actividad sospechosa.
- Permite hacerles seguimiento a los controles de seguridad.
- Ayuda a planificar y darle seguimiento a los procesos.
- Contribuye a la imagen corporativa (reputación).

### **Ventajas de implementar la norma ISO 27017**

- Se genera un aumento en la confianza que la organización proporciona a los clientes del servicio.
- Proporciona mayor seguridad y protección de datos.
- Es una **ventaja** competitiva dentro del mercado.
- **¿Cuáles son los protocolos de seguridad para la configuración del Firewall?**
  - Denegar el tráfico de forma implícita (por defecto)
  - Optimizar las reglas creadas y ordenarlas
  - El listado de reglas lo más corto posible
  - Revisar que las reglas siguen vigentes en la red
  - Documentar todas las reglas en el campo «descripción»
  - Loggear el tráfico solamente que necesitemos
  - Mirar detenidamente los registros de cierto tráfico
- **¿Cuáles son los beneficios de utilizar el Firewall en un DataCenter y Cloud Computing?**

### **DataCenter**

- Un buen firewall bien configurado y administrado evita que los hackers entren y roben información valiosa.
- Se puede decir que es un policía, ya que va identificando cada paquete de información antes de que les permita el acceso.
- Cabe mencionar que permite definir una “barrera” manteniendo a un lado a los usuarios sin autorización, ayuda en la prevención de los ataques hacia la red privada desde otras redes externas.
- Maneja control de la seguridad de la red y los equipos individuales cuando se produce cualquier actividad sospechosa, también permite llevar control en el uso de Internet bloqueando o desbloqueando material inapropiado o apropiado.
- El hecho de que la empresa no esté conectada a Internet, permite que los directores no se preocupen por establecer políticas de seguridad para la red interna, sin embargo, es un gran error ya que si establecen por lo menos una

política podrán administrar el acceso de los empleados a sitios específicos de la red y proteger la información sensible.

### **Cloud Computing**

- Plataforma integrada con automatización del ciclo de vida para el cloud.
  - Agilidad, escalabilidad y gran capacidad de respuesta a la hora de prestar los servicios de TI.
  - Alta eficiencia, rendimiento mejorado y optimización de la capacidad, con escalabilidad entre entornos.
  - Seguridad integrada en todos los niveles de la infraestructura y las operaciones.
  - Rápida transformación en una plataforma común para las cloud requeridas (públicas y privadas).
- **¿Por qué se recomendaría el uso del Firewall en un DataCenter y en Cloud Computing?**

### **Data Center**

- El firewall supervisa todo el tráfico de red y tiene permisos para identificar y bloquear el tráfico no deseado.
- El hecho de que hoy en día la mayoría de equipos estén conectados a Internet facilita a los atacantes un sinnúmero de víctimas potenciales.
- Los atacantes sondean otros equipos conectados a Internet para determinar si son vulnerables a varias clases de ataques.
- Cuando detectan una víctima propicia, pueden franquear sus sistemas de seguridad e infiltrarse en ese equipo.
- Llegados a este punto, el atacante puede obligar al equipo a efectuar prácticamente cualquier tarea que quiera.
- Los atacantes suelen intentar apropiarse de información personal para cometer fraudes financieros.
- Toda esta actividad tiene lugar en segundo plano, sin que el usuario sea consciente de lo que sucede.

### **Cloud Computing**

- Reducción de costes
- Mayor accesibilidad y movilidad
- Más seguridad
- Capacidad de almacenamiento ilimitada

- Escalabilidad
- Respeto al medio ambiente
- Actualizaciones automáticas
- Optimizar el uso de recursos
- Igualdad
- Colaboración y comunicación del personal
- **¿Según su experiencia cuales sería los parámetros para la configuración del Firewall en un DataCenter y Cloud Computing?**

### **DataCenter**

- La dirección de la conexión: Las reglas de entrada se aplican a las conexiones entrantes de los orígenes especificados a los objetivos de Google Cloud, y las reglas de salida se aplican a las conexiones que se dirigen a destinos especificados desde los objetivos
- Una prioridad numérica, que determina si se aplica la regla. Solo se aplica la regla con la prioridad más alta (número de prioridad más bajo), cuyos otros componentes coinciden con el tráfico. Se ignoran las reglas en conflicto con prioridades más bajas
- Una acción en caso de coincidencia, ya sea allow o deny, que determina si la regla permite o bloquea las conexiones.
- El estado de aplicación de la regla de firewall: Puedes habilitar e inhabilitar reglas de firewall sin tener que borrarlas.
- Un objetivo, que define las instancias (incluidos los clústeres de GKE y las instancias del entorno flexible de App Engine) a las que se aplica la regla
- Un filtro de origen para las reglas de entrada o un filtro de destino para las reglas de salida.
- El protocolo (como TCP, UDP o ICMP) y el puerto de destino
- Una opción booleana de registros que registra las conexiones que hacen que la regla coincida con Cloud Logging.

### **Cloud Computing**

- Regla de permiso de salida IPv4 implícita.
- Regla de denegación de entrada IPv4 implícita
- Regla de permiso de salida IPv6 implícita.
- Regla de denegación de entrada IPv6 implícita.
- Tráfico bloqueado y limitado



- Tráfico que siempre está permitido
- Reglas de firewall y balanceadores de cargas de paso
- Reglas de firewall y balanceadores de cargas de prox
- Reglas de firewall y Cloud VPN
- Reglas de firewall y GKE

**GRACIAS POR SU COLABORACIÓN**


**Firma y Sello**



---

**Ci:** 723175764  
**Nombre:** Alex Asimbaya

## Entrevista 2

 Universidad Israel	<b>UNIVERSIDAD TECNOLÓGICA ISRAEL</b>  Maestría en Seguridad Informática
--	--

El objetivo del presente instrumento es conocer la importancia sobre Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

**Fecha:** 11 de agosto de 2022

### Datos Personales

<b>Nombre:</b> Geovany Erazo	<input checked="" type="checkbox"/>	Ingeniería	<input type="checkbox"/>	PhD
<b>Título:</b> Ingeniero en Electrónica y Telecomunicaciones	<input type="checkbox"/>	Especialización	<input type="checkbox"/>	Otro

### 1. Banco de Preguntas

- **¿Cuáles son las ventajas de las Normas ISO 27001 y 27017?**

Permite que los procesos de seguridad estén equilibrados y a la vez coordinados Certificado de confianza y calidad empresarial

- **¿Cuáles son los protocolos de seguridad para la configuración del Firewall?**

Los firewalls son una herramienta fundamental para proteger adecuadamente toda la red de intrusiones externas. Los firewalls permitirán controlar el tráfico desde y hacia un destino, incorporando diferentes reglas. Si el paquete recibido o enviado cumple con una regla configurada, se ejecutará una de las tres acciones típicas de los cortafuegos: permitir el paquete (ACCEPT), denegar el paquete y eliminarlo (DROP), lanzar mensaje de rechazo (reject)

Dependiendo del sistema operativo y del firewall, es posible que tengamos diferentes políticas del firewall en diferentes interfaces.

Todos los firewalls, en función de una determinada regla, van a permitir registrar el tráfico de red permitido o denegado en el firewall (dirección IP de origen y destino, puerto de origen y destino, y hora), de esta manera, podremos ver los intentos de acceso, tráfico permitido o denegado y más.

- **¿Cuáles son los beneficios de utilizar el Firewall en un DataCenter y Cloud Computing?**

Con un servicio de firewall podrás controlar quienes tienen acceso a esta información clasificada y denegar cualquier otro permiso a fuentes externas, asegurando así la información clasificada de tu negocio y clientes.

Con un servicio de firewall puedes segmentar el acceso a internet e incluso ser más específico y controlar de punto a punto qué acceso tienen tus empleados, clientes y grupos de trabajo, estableciendo directrices y reglas sobre la navegación dentro de tu Red.

Con esto podrás gestionar y denegar ciertas Webs por sus dominios, centralizando más tu Red empresarial, por ejemplo: puedes prohibir el acceso a "Facebook.com" para tus empleados y así no tengan distracciones en horas de trabajo.

- **¿Por qué se recomendaría el uso del Firewall en un DataCenter y en Cloud Computing?**

La información es tan importante para lograr los objetivos en las organizaciones, que es considerada el activo más importante. Por eso, es objeto de diversas amenazas, como el robo, la falsificación, el fraude, la divulgación y la destrucción, entre muchas otras.

Un firewall funciona como una serie de capas que componen una estrategia de defensa en sentido de profundidad; también es como un sistema de filtros que identifica y categoriza cada elemento del flujo de datos para impedir el acceso de los no deseados. Por lo que el sistema analiza todo el tráfico de la red en lugar de responder ante un ataque ya iniciado.

La función básica del firewall en la seguridad de la red es controlar el tráfico que pasa entre dos redes y bloquear todo lo que no esté explícitamente permitido.

De esta manera los firewalls previenen muchos ataques. También impiden el acceso remoto a estaciones de trabajo y servidores empresariales, al aislar una red y el internet en general, como un muro de contención.

- **¿Según su experiencia cuales sería los parámetros para la configuración del Firewall en un DataCenter y Cloud Computing?**

Podemos pensar que registrar todo el tráfico de red es buena idea, pero no lo es.

Es recomendable solamente registrar el tráfico que realmente interesa para tareas de debug o para comprobar si están atacando.


Si registramos una gran cantidad de tráfico, tendremos muchísimo ruido, en estos registros, es decir, registros que no servirán, y tendremos que empezar a filtrar ingentes cantidades de logs para llegar al que de verdad interesa. Por ejemplo, equipos con Windows o Mac envían y reciben continuamente información desde Internet, resuelven cientos de veces varios dominios y mucho más, por tanto, asegúrate si realmente quieres loggear este tráfico de navegación web. Además, si utilizas en tu red protocolos de enrutamiento dinámico como RIP o OSPF, y tienes entre medias el firewall, recibirás continuamente tráfico de estos protocolos, lo mismo si tienes HSRP o VRRP para la redundancia de los routers.

**GRACIAS POR SU COLABORACIÓN**



Georany Erazo

### Entrevista 3

	<b>UNIVERSIDAD TECNOLÓGICA ISRAEL</b> Maestría en Seguridad Informática
---	--

El objetivo del presente instrumento es conocer la importancia sobre Comparación de Métodos de Seguridad entre Cloud Computing y DataCenter Convencionales utilizando normas ISO 27001 Y 27017. La información aquí registrada es de carácter confidencial y será utilizada exclusivamente con los fines anteriormente mencionados.

Fecha: 11/08/2022

#### 1. Datos Personales

<b>Nombre:</b> Roberto Ortega	X	Ingeniería		PhD
<b>Título:</b> Ingeniero en Sistemas •		Especialización		Otro

#### 2. Banco de Preguntas

- **¿Cuáles son las ventajas de las Normas ISO 27001 y 27017**

La norma ISO 27017 proporciona controles para proveedores y clientes de servicios en la nube y La norma ISO 27001 expone la importancia de la comunicación entre una empresa y sus clientes a la hora de definir ciertos procesos de gestión de seguridad.

- **¿Cuáles son los protocolos de seguridad para la configuración del Firewall?**

Los protocolos de seguridad informática son las reglas o normas diseñadas para garantizar la confidencialidad, la integridad y la disponibilidad de la información. Son las medidas de seguridad implementadas para evitar que personas no autorizadas puedan acceder a la información, manipularla o destruirla.

- **¿Cuáles son los beneficios de utilizar el Firewall en un DataCenter y Cloud Computing?**

Un firewall en la nube es un producto de seguridad que, al igual que un firewall tradicional, filtra el tráfico de red potencialmente malicioso

- **¿Por qué se recomendaría el uso del Firewall en un DataCenter y en Cloud Computing?**

Los firewalls basados en la nube forman una barrera virtual alrededor de las plataformas, la infraestructura y las aplicaciones en la nube, de la misma manera que los firewalls tradicionales forman una barrera alrededor de la red interna de una organización. Los firewalls en la nube también pueden proteger la infraestructura local.

- **¿Según su experiencia cuales sería los parámetros para la configuración del Firewall en un DataCenter y Cloud Computing?**

Algunos parámetros se deberían considerar los siguientes como: el tiempo de respuesta, analizado en cada una de las aplicaciones desplegadas en la nube, el rendimiento, que permite analizar los recursos están bien distribuidos y la fiabilidad, que demuestra que tan confiables son los datos que están siendo manejados

### **GRACIAS POR SU COLABORACIÓN**

#### **Firma y Sello**



**Ci:** 1712285079

**Nombre:** Roberto Ortega