UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FACULTAD DE CIENCIAS E INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TRABAJO DE SUFICIENCIA PROFESIONAL

"Diseño de un sistema de seguridad para la protección de datos en entornos de computación en la nube"

AUTOR:

Bach.: Quispe Quispe, Luis Angel

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS E INFORMÁTICA

ASESOR:

Dr. Vegas Gallo, Edwin Agustín

ORCID: 0000-0002-2566-0115

DNI Nº 02771235

LIMA-PERÚ
2026

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

INFORME DE SIMILITUD

N°006-2026-UPCI-FCI-REHO-T

A : **MG. QUISPE AYQUIPA CESAR ANTONIO**
Decano (e) de la Facultad de Ciencias e Ingeniería

DE : **MG. HERMOZA OCHANTE, RUBEN EDGAR**
Docente Operador del Programa Turnitin

ASUNTO : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional:
BACHILLER QUISPE QUISPE, LUIS ANGEL

FECHA : Lima, 29 de enero de 2026.

Tengo el agrado de dirigirme a usted con la finalidad de informar lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: **"DISEÑO DE UN SISTEMA DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS EN ENTORNOS DE COMPUTACIÓN EN LA NUBE"**, presentado por el Bachiller **QUISPE QUISPE, LUIS ANGEL.**
2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 15%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).
3. Al término análisis, el Bachiller en mención **PUEDE CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,

.....
MG. HERMOZA OCHANTE, RUBEN EDGAR
Universidad Peruana de Ciencias e Informática
Docente Operador del Programa Turnitin

Adjunto:

**Resultado de similitud*

Dedicatoria

Esta investigación la dedico a mis padres por haberme formado en el camino correcto de la vida y a mis familiares, por haberme apoyado constantemente en mis desafíos y en mis luchas.

Agradecimiento

Quiero agradecer a mi esposa e hijos por su paciencia y constante apoyo, a las autoridades de la Universidad Peruana de Ciencias e Informática, a mis maestros y a mis compañeros de aula, por sus enseñanzas y por su amistad.

Declaración de Autoría

Nombres : LUIS ANGEL

Apellidos : QUISPE QUISPE

Código : 1401000429

DNI : 45465303

Declaro que, soy el autor del trabajo realizado y que es la versión final que he entregado a la oficina del Decanato de la Facultad de Ingeniería de Sistemas de la Universidad Peruana de Ciencias e Informática.

Asimismo, declaro que he citado debidamente las palabras o ideas de otros autores, refiriendo expresamente el nombre de la obra y página o páginas que me sirvieron de fuente.

Jesús María, febrero del 2026.

ÍNDICE

INTRODUCCIÓN

La protección de datos en entornos de computación en la nube representa uno de los mayores desafíos tecnológicos y regulatorios de la actualidad, el diseño de sistemas de seguridad robustos es esencial para garantizar la confidencialidad, integridad y disponibilidad de la información, en un contexto marcado por amenazas sofisticadas, normativas estrictas y una rápida evolución tecnológica.

La computación en la nube se ha transformado radicalmente la manera en que las organizaciones almacenan, procesan y gestionan sus datos, permitiendo una escalabilidad sin precedentes, reducción de costos y acceso global a recursos informáticos; sin embargo, esta revolución tecnológica ha traído consigo nuevos riesgos y desafíos en materia de seguridad, especialmente en lo que respeta a la protección de datos sensibles frente a amenazas internas y externas (Ramesh et al., 2026); la creciente sofisticación de los ciberataques, la proliferación de vulnerabilidades asociadas a la configuración y gestión de servicios en la nube, así como la complejidad de los entornos multi-nube e híbridos, han elevado la protección de la información a una prioridad estratégica para empresas y organismos públicos (ScienceDirect, 2025).

En este contexto, el diseño de sistemas de seguridad para la protección de datos en la nube debe abordar múltiples dimensiones: desde la implementación de tecnologías criptográficas avanzadas, como el cifrado homomórfico y la gestión adaptativa de claves, hasta la integración de mecanismos de autenticación

multifactor, prevención de pérdida de datos (DLP) y arquitecturas de confianza cero (Zero Trust) (Springer, 2025; ScienceDirect, 2026); la literatura reciente destaca la importancia de adoptar un enfoque de “seguridad por diseño”, incorporando controles de seguridad y privacidad desde las fases iniciales del desarrollo de sistemas en la nube, y no como un añadido posterior (Springer, 2025).

A nivel normativo, la protección de datos en la nube está fuertemente influenciada por marcos regulatorios internacionales como el Reglamento General de Protección de Datos (GDPR) en Europa, la Ley General de Protección de Datos (LGPD) en Brasil, y las recientes reformas en países latinoamericanos como Chile y Colombia (ScienceDirect, 2025; ANPD, 2025); además, estándares internacionales como ISO/IEC 27017 y 27018, junto con certificaciones como SOC 2, establecen directrices técnicas y de gestión para garantizar la seguridad y privacidad de la información en servicios cloud (ISO, 2025); el cumplimiento de estas normativas exige la adopción de controles técnicos robustos; cifrado, control de acceso, monitoreo continuo, y la gestión proactiva de riesgos asociados a la soberanía y localización de los datos (ScienceDirect, 2025).

Las amenazas emergentes, como los ataques impulsados por inteligencia artificial, el ransomware orientado a la exfiltración de datos y la explotación de vulnerabilidades de día cero, subrayan la necesidad de sistemas de seguridad dinámicos y adaptativos, capaces de anticipar y responder a incidentes en tiempo real (Springer, 2025); en este sentido, la integración de inteligencia artificial y aprendizaje automático en los sistemas de defensa permite detectar anomalías y

patrones de ataque con mayor precisión, fortaleciendo la resiliencia de los entornos cloud (Springer, 2025).

En síntesis, el diseño de un sistema de seguridad para la protección de datos en entornos de computación en la nube requiere una visión integral que combine innovación tecnológica, cumplimiento normativo y gestión estratégica de riesgos; esta tesis se propone analizar y desarrollar un modelo de seguridad que responda a los desafíos actuales y futuros, garantizando la protección efectiva de la información en la nube.

CAPITULO I.- Planificación del Trabajo de Suficiencia Profesional

1.1. Título y descripción del trabajo

Título del Trabajo

Diseño de un sistema de seguridad para la protección de datos en entornos de computación en la nube.

1.2. Objetivos del presente trabajo

Objetivo general

El objetivo principal de esta investigación es diseñar un sistema de seguridad robusto y adaptable para la protección de datos en entornos de computación en la nube , que integre tecnologías avanzadas, políticas de seguridad y controles preventivos, con el fin de garantizar la protección de la información frente a amenazas internas y externas, este sistema debe ser capaz de abordar los desafíos específicos de los modelos de servicio en la nube (IaaS, PaaS y SaaS) y adaptarse a las necesidades de diferentes tipos

de organizaciones, desde pequeñas y medianas empresas (PYMES) hasta grandes corporaciones.

Objetivos específicos

- Analizar los riesgos y vulnerabilidades asociados a los entornos de computación en la nube.

  Este objetivo busca identificar las principales amenazas que afectan la seguridad de los datos en la nube, como la pérdida de datos, accesos no autorizados, ataques de ransomware y vulnerabilidades en la configuración de servicios. Se realizará un análisis exhaustivo de los riesgos inherentes a los modelos de servicio en la nube (IaaS, PaaS y SaaS), destacando cómo la externalización de servicios puede incrementar la exposición a ataques.

- Definir los requisitos de seguridad para la protección de datos en la nube.

  Este objetivo se centra en establecer los criterios técnicos y normativos necesarios para garantizar la seguridad de los datos en la nube. Esto incluye la implementación de políticas de seguridad basadas en etiquetas, que permitan clasificar los datos según su nivel de confidencialidad e integridad, y la definición de controles específicos como cifrado, autenticación multifactor y monitoreo continuo.

- Diseñar un modelo de seguridad basado en tecnologías avanzadas.

  El diseño del sistema de seguridad integrará tecnologías como el cifrado homomórfico, la fragmentación y distribución de datos, y la gestión adaptativa de claves. Además, se incorporarán mecanismos de

inteligencia artificial y aprendizaje automático para la detección de anomalías y la respuesta proactiva a incidentes de seguridad.

- Implementar controles preventivos y políticas de seguridad en el sistema diseñado.

  Este objetivo busca desarrollar un conjunto de políticas claras y controles preventivos que eviten acciones no deseadas en el entorno de la nube. Las políticas estarán alineadas con estándares internacionales como ISO/IEC 27017 y 27018, y se enfocarán en la protección de datos sensibles, la gestión de accesos y la prevención de pérdida de datos (DLP).

- Evaluar la efectividad del sistema de seguridad propuesto.

  Finalmente, se realizará una evaluación del sistema diseñado mediante pruebas de penetración, simulaciones de ataques y análisis de cumplimiento normativo. Esto permitirá validar la capacidad del sistema para proteger los datos en diferentes escenarios y garantizar su adaptabilidad a las necesidades de las organizaciones

1.3. Justificación

El diseño de un sistema de seguridad para la protección de datos en la nube se fundamenta en sólidos marcos teóricos, evidencia práctica, demandas sociales y regulatorias, así como en enfoques epistemológicos y metodológicos rigurosos; esta justificación aborda cada dimensión, citando

autores y fuentes actualizadas, para demostrar la relevancia y necesidad de la investigación.

Justificación teórica

El fundamento teórico de la seguridad en la nube parte de la definición y los modelos propuestos por Mell y Grance (2011), quienes establecieron los principios y características esenciales de la computación en la nube, así como los desafíos inherentes a la protección de datos en estos entornos.

Takabi, Joshi y Ahn (2010) profundizan en los retos de seguridad y privacidad, identificando amenazas como la multitenencia, la pérdida de control y la confianza, lo que exige nuevos paradigmas de protección; además, marcos como el NIST Cybersecurity Framework (2013) proporcionan una estructura para gestionar riesgos y establecer controles de seguridad adaptados a la nube.

En cuanto a los mecanismos de protección, la literatura destaca el uso de técnicas criptográficas avanzadas (AES, RSA, cifrado homomórfico) y modelos de control de acceso como RBAC y ABAC, que permiten una gestión granular y contextualizada de los permisos.

El enfoque de “Zero Trust Architecture” (ZTA) refuerza la necesidad de verificar continuamente la identidad y los accesos, adaptándose a la naturaleza dinámica y distribuida de la nube.

Justificación Práctica

Desde una perspectiva práctica, la protección de datos en la nube responde a la necesidad de salvar información sensible, garantizar la continuidad del

negocio y cumplir con normativas cada vez más estrictas; proveedores líderes como AWS, Azure y Google Cloud han implementado arquitecturas de seguridad robustas que incluyen gestión de identidades, cifrado y detección de amenazas, demostrando su eficacia en estudios de caso y análisis comparativos (Sailakshmi, 2021).

Informes de Gartner y Forrester evidencian beneficios tangibles como la escalabilidad, la reducción de costos y la mejora en la resiliencia cibernética, especialmente para pequeñas y medianas empresas que no pueden mantener infraestructuras propias; sin embargo, también se identifican desafíos como la fragmentación de responsabilidades y la necesidad de integrar prácticas DevSecOps, lo que subraya la importancia de un diseño metodológico sólido (IBM, 2024).

Justificación Social

La dimensión social se centra en la protección de la privacidad, el cumplimiento normativo y la defensa de los derechos digitales. La adopción masiva de la nube ha incrementado las preocupaciones sobre la confidencialidad y el control de los datos personales, especialmente bajo marcos regulatorios como el GDPR en Europa (Alhassan, Sammon & Daly, 2023); estas normativas exigen medidas como el cifrado, la anonimización y la trazabilidad, así como la capacidad de auditar y demostrar el cumplimiento.

La protección de datos en la nube es también una respuesta a la demanda social de transparencia y confianza en los servicios digitales, alineándose con principios de soberanía digital y derechos fundamentales (Comisión Europea,

2024); la falta de mecanismos de seguridad adecuados puede erosionar la confianza pública y limitar la adopción de tecnologías emergentes.

Justificación Epistemológica

Epistemológicamente, la investigación en seguridad en la nube se apoya en una visión multidisciplinaria que integra ciencias de la computación, sistemas de información y ciencias sociales; según Olejnik y Kurasinski (2023) argumentan que el conocimiento en ciberseguridad es tanto técnico como social, influenciado por prácticas organizacionales y factores humanos; la naturaleza adversarial y dinámica de las amenazas exige marcos epistemológicos que reconozcan la provisionalidad y el contexto del conocimiento en seguridad (Academia.edu, 2020); la seguridad no solo se concibe como un objetivo técnico, sino como un proceso socialmente construido, orientado a proteger valores y recursos colectivos.

Esta perspectiva justifica la necesidad de enfoques holísticos y adaptativos en el diseño de sistemas de protección de datos en la nube.

Justificación Metodológica

Metodológicamente, el diseño de sistemas de seguridad en la nube requiere enfoques rigurosos y adaptativos; el Design Science Research (DSR), propuesto por Hevner et al. (2004), es ampliamente reconocido en la disciplina por su énfasis en la creación y evaluación iterativa de artefactos tecnológicos que resuelven problemas complejos y relevantes.

Este enfoque permite desarrollar soluciones innovadoras, evaluarlas en contextos reales y asegurar su utilidad y validez científica; la investigación en

seguridad combina métodos observacionales, matemáticos, experimentales y aplicados (Edgar & Manz, 2017); además, la modelización de amenazas, la evaluación formal y la integración de prácticas DevSecOps son esenciales para garantizar la robustez y la adaptabilidad de los sistemas diseñados; la interdisciplinariedad y el uso de datos empíricos refuerzan la validez y aplicabilidad de los resultados.

CAPITULO II.- Marco Teórico

2.1. Computación en la nube: definición, características y modelos de servicio (IaaS, PaaS, SaaS). –

La computación en la nube es un paradigma tecnológico que transforma la gestión y protección de datos, permitiendo el acceso flexible y escalable a recursos informáticos a través de Internet, sus características esenciales y modelos de servicio (IaaS, PaaS, SaaS) definen el marco sobre el cual se deben diseñar sistemas de seguridad robustos para la protección de datos en entornos cloud.

La computación en la nube, o cloud computing, se ha consolidado como uno de los pilares fundamentales de la transformación digital en las organizaciones modernas, según la definición clásica y ampliamente aceptada del National Institute of Standards and Technology (NIST), propuesta por Mell y Grance (2011), la computación en la nube es “un modelo para permitir el acceso ubicuo, conveniente y bajo demanda a un conjunto compartido de recursos informáticos configurables (por ejemplo, redes, servidores,

almacenamiento, aplicaciones y servicios) que pueden ser rápidamente aprovisionados y liberados con un mínimo esfuerzo de gestión o interacción con el proveedor del servicio"; esta definición ha sido ratificada y extendida por autores como Surianarayanan y Chelliah (2023), quienes destacan la capacidad de la nube para ofrecer servicios informáticos como una utilidad, permitiendo a los usuarios pagar solo por lo que consumen y acceder a recursos de manera elástica y escalable.

Características esenciales de la computación en la nube.

La computación en la nube se distingue por una serie de características esenciales que la diferencian de otros modelos tecnológicos y que, a su vez, plantean desafíos y oportunidades específicas para la seguridad de los datos:

1. **Autoservicio bajo demanda:**

   Los usuarios pueden aprovisionar recursos computacionales de manera automática y sin intervención humana directa, lo que agiliza la gestión, pero exige controles estrictos de autenticación y autorización

2. **Acceso amplio a la red:**

   Los servicios cloud están disponibles a través de la red y pueden ser accedidos desde múltiples dispositivos y ubicaciones, ampliando la superficie de exposición y requiriendo mecanismos robustos de protección de datos en tránsito

3. **Agrupación de recursos (resource pooling):**

   Los recursos del proveedor se agrupan para servir a múltiples clientes, asignándose y reasignándose dinámicamente según la demanda, esto

introduce retos de aislamiento y privacidad, ya que los datos de diferentes usuarios pueden residir en la misma infraestructura física.

4. **Elasticidad rápida:**

   La nube permite escalar recursos de manera rápida y automática, adaptándose a las necesidades cambiantes de los usuarios, esta elasticidad requiere que los controles de seguridad sean igualmente dinámicos y adaptativos.

5. **Servicio medido:**

   El uso de los recursos es monitoreado y reportado, permitiendo la optimización y la transparencia tanto para el proveedor como para el cliente, esto facilita la auditoría y el cumplimiento normativo, pero también demanda la protección de los datos de uso y facturación.

   Autores recientes, como Sehgal, Bhatt y Acken (2023), añaden que la virtualización, la automatización y la resiliencia son propiedades clave que potencian la eficiencia y la seguridad en entornos cloud.

Modelos de servicio en la nube: IaaS, PaaS y SaaS

La computación en la nube se estructura en tres modelos principales de servicio, cada uno con diferentes niveles de control, responsabilidad y abstracción para el usuario final.

1. Infraestructura como Servicio (IaaS)

En el modelo IaaS, el proveedor ofrece recursos virtualizados fundamentales como servidores, almacenamiento y redes, el usuario tiene

control sobre los sistemas operativos, aplicaciones y datos, mientras que el proveedor gestiona la infraestructura física subyacente; ejemplos de IaaS incluyen Amazon EC2, Microsoft Azure Virtual Machines y Google Compute Engine.

Este modelo ofrece máxima flexibilidad, pero también implica que la mayor parte de la responsabilidad de la seguridad recae en el cliente.

2. Plataforma como Servicio (PaaS)

PaaS proporciona un entorno de desarrollo y implementación gestionado, incluyendo middleware, herramientas de desarrollo y servicios integrados; el usuario se enfoca en el desarrollo de aplicaciones, mientras que el proveedor administra la infraestructura y la plataforma subyacente. Ejemplos destacados son Google App Engine, Microsoft Azure App Services y Heroku.

Este modelo acelera el desarrollo y reduce la complejidad operativa, aunque limita la personalización y puede generar dependencia del proveedor.

3. Software como Servicio (SaaS)

En SaaS, el proveedor entrega listas de aplicaciones para usar a través de Internet, eliminando la necesidad de instalación o mantenimiento local; el usuario accede a las aplicaciones mediante interfaces estándar, como navegadores web. Los ejemplos incluyen Google Workspace, Microsoft 365 y Salesforce.

En este modelo, la responsabilidad de la seguridad recae principalmente en el proveedor, aunque el cliente debe gestionar el acceso y la configuración de los datos.

Importancia para la protección de datos

Comprender la definición, características y modelos de servicio de la computación en la nube es esencial para diseñar sistemas de seguridad efectivos. Cada modelo presenta diferentes superficies de ataque y requiere estrategias de protección específicas, desde el aislamiento de recursos en IaaS hasta la gestión de accesos en SaaS. La correcta implementación del modelo de responsabilidad compartida es clave para mitigar riesgos y garantizar la confidencialidad, integridad y disponibilidad de los datos en entornos cloud.

2.2 Seguridad en la nube: definición, principios y desafíos. -

La seguridad en la nube es un campo dinámico y esencial para la protección de datos en entornos digitales modernos, su definición abarca políticas, controles y tecnologías orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información; los principios fundamentales incluyen el modelo CIA, la responsabilidad compartida y la adopción de marcos normativos internacionales; los desafíos actuales van desde brechas de datos y amenazas internas hasta la complejidad de entornos multinube y la evolución constante de los ataques.

La seguridad en la nube se define como el conjunto de políticas, controles, procedimientos y tecnologías diseñadas para proteger los datos, aplicaciones e infraestructuras asociadas a los servicios de computación en la nube; su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de normativas y la protección frente a amenazas internas y externas (Ahmadi, 2024; NIST, 2020), según la definición del Instituto Nacional de Estándares y Tecnología (NIST), la seguridad en la nube implica la aplicación de controles de seguridad y privacidad adaptados a los entornos virtualizados y distribuidos, haciendo énfasis en la gestión de identidades, el cifrado y la segregación de datos (NIST, 2020); por su parte, la norma ISO/IEC 27017:2015 destaca la necesidad de controles específicos para la nube, considerando riesgos como la ubicación de los datos, la multitenencia y la responsabilidad compartida entre proveedores y clientes (ISO/IEC, 2015).

Principios fundamentales de la seguridad en la nube.

1. Confidencialidad, Integridad y Disponibilidad (Modelo CIA)

El modelo CIA constituye la base de la seguridad en la nube:

- Confidencialidad: Garantiza que los datos solo sean accesibles por usuarios autorizados, mediante técnicas como el cifrado y la gestión de identidades (Gilbert et al., 2025).

- Integridad: Asegura que la información no sea alterada de manera no autorizada durante su almacenamiento, procesamiento o transmisión (Toussaint et al., 2024).
- Disponibilidad: Busca que los servicios y datos estén accesibles cuando los usuarios los requieran, incluso ante incidentes o ataques (Cloud Security Alliance, 2024).

2. Responsabilidad compartida

La seguridad en la nube es una responsabilidad conjunta entre el proveedor de servicios y el cliente, el modelo de responsabilidad compartida establece que, mientras el proveedor asegura la infraestructura subyacente, el cliente debe proteger los datos, gestionar los accesos y configurar adecuadamente los servicios (ISO/IEC, 2015; Cloud Security Alliance, 2024).

3. Cumplimiento normativo y marcos de referencia

El cumplimiento de normativas internacionales como ISO/IEC 27017, ISO/IEC 27018 y NIST SP 800-53 es esencial para garantizar la protección de datos personales y sensibles, así como para alinear las prácticas de seguridad con los estándares globales (NIST, 2020; ISO/IEC, 2015).

4. Confianza cero y defensa en profundidad

El enfoque Zero Trust parte del principio de “nunca confiar, siempre verificar”, aplicando controles estrictos de acceso y monitoreo continuo, independientemente de la ubicación del usuario o dispositivo (Stafford,

2020); la defensa en profundidad implica la implementación de múltiples capas de seguridad para mitigar riesgos en diferentes niveles del entorno cloud (Natsos & Symeonidis, 2026).

Desafíos actuales y amenazas emergentes

1. Brechas de datos y errores de configuración

Las brechas de datos, muchas veces causadas por configuraciones incorrectas de servicios en la nube, representan uno de los riesgos más críticos, estudios recientes indican que el 88% de las brechas en la nube se deben a errores de configuración, lo que subraya la importancia de la capacitación y la adopción de mejores prácticas (Ahmed, 2024).

2. Multi-tenancy y aislamiento de datos

El modelo multi-tenant, donde múltiples clientes comparten la misma infraestructura, amplía la superficie de ataque y puede facilitar fugas de información si no se implementan mecanismos de aislamiento robustos (Chenthara et al., 2025).

3. Amenazas internas

Las amenazas internas, provenientes de empleados o usuarios con acceso legítimo, requieren controles de acceso estrictos y monitoreo detallado de actividades para prevenir filtraciones o manipulaciones de datos (Gilbert et al., 2025).

4. **Cumplimiento y soberanía de los datos**

   El cumplimiento de normativas y la soberanía de los datos son desafíos crecientes, especialmente en entornos multinube e híbridos, donde la dispersión geográfica de los centros de datos complica la gestión de la privacidad y la protección de datos personales (Wang et al., 2025).

5. **Bloqueo del proveedor**

   La dependencia de un único proveedor puede dificultar la migración de datos y aplicaciones, limitando la flexibilidad y aumentando los riesgos si el proveedor no cumple con los estándares requeridos (Reece et al., 2024).

6. **Amenazas emergentes: ransomware, IA y cadena de suministro**

   El ransomware ha aumentado significativamente en ataques dirigidos a sistemas en la nube, afectando especialmente a repositorios de respaldo y servicios de almacenamiento (Cloud Security Alliance, 2024); además, la integración de inteligencia artificial y aprendizaje automático introduce nuevos vectores de ataque, como manipulaciones adversariales de modelos y datos (Bedi et al., 2024).

7. **Complejidad en entornos híbridos y multinube**

   La adopción de arquitecturas híbridas y multinube incrementa la complejidad de la gestión de la seguridad, debido a la falta de uniformidad en los controles y la interoperabilidad entre plataformas (Molla et al., 2023).

La seguridad en la nube es un campo en constante evolución, que requiere la integración de tecnologías avanzadas, políticas claras y cumplimiento normativo para enfrentar desafíos cada vez más atractivos; la

protección efectiva de los datos en la nube depende de la aplicación rigurosa de principios fundamentales, la adopción de marcos internacionales y la innovación continua en respuesta a amenazas emergentes.

CAPITULO III.- Desarrollo de actividades programadas

3.1. Riesgos y amenazas en la nube. -

La computación en la nube, aunque ofrece ventajas significativas en flexibilidad y escalabilidad, introduce una amplia gama de riesgos y amenazas que afectan la confidencialidad, integridad y disponibilidad de los datos; estos riesgos abarcan desde brechas de datos y ransomware hasta vulnerabilidades técnicas, amenazas internas y desafíos de cumplimiento normativo, exigiendo un enfoque de seguridad integral y actualizado.

El auge de la computación en la nube ha transformado radicalmente la gestión y almacenamiento de datos en las organizaciones, permitiendo una mayor agilidad operativa y reducción de costos; sin embargo, esta evolución tecnológica también ha incrementado la superficie de ataque y la complejidad de los riesgos asociados a la protección de la información; según la Cloud Security Alliance (2024), los entornos cloud presentan desafíos únicos debido a su naturaleza distribuida, la multi-tenencia y la dependencia de infraestructuras y servicios de terceros; por ello, comprender y clasificar los

riesgos y amenazas en la nube es fundamental para diseñar sistemas de seguridad efectivos y resilientes.

1. Brechas de datos y pérdida de información

Las brechas de datos constituyen uno de los riesgos más críticos en la nube, caracterizándose por el acceso no autorizado a información sensible debido a configuraciones incorrectas, vulnerabilidades en APIs o controles de acceso débiles; incidentes recientes, como la brecha de Snowflake en 2024, evidencian el impacto real de estas amenazas, donde millones de registros quedaron expuestos por errores en la gestión de credenciales y permisos; además, la pérdida de datos puede producirse por ataques de ransomware, fallos en la infraestructura del proveedor o eliminación accidental, agravada por la complejidad de los entornos multi-nube y la falta de estrategias robustas de respaldo.

2. Ransomware y amenazas avanzadas

El ransomware ha evolucionado como una de las amenazas predominantes en la nube, con un aumento del 67% en ataques globales solo en el primer semestre de 2025 (Deloitte, 2025); los atacantes emplean tácticas de doble y triple extorsión, cifrando datos, exfiltrando información y amenazando con ataques DDoS para maximizar el impacto.

Ejemplos como el ataque a Yale New Haven Health System (2025) demuestran cómo los ciberdelincuentes combinan técnicas de phishing, explotación de vulnerabilidades y abuso de APIs nativas de la nube para comprometer datos críticos y dificultar la recuperación.

3. Vulnerabilidades técnicas y arquitectónicas

La arquitectura de la nube introduce riesgos inherentes, especialmente en entornos multi-tenant donde Múltiples clientes comparten la misma infraestructura; según Ozarslan (2022), las vulnerabilidades en hipervisores, APIs inseguras y errores de configuración son vectores frecuentes de ataque; los ataques de canal lateral y la explotación de fallos en la virtualización pueden permitir a un atacante acceder a datos de otros inquilinos, mientras que la exposición pública de cubos de almacenamiento o bases de datos mal configuradas sigue siendo una causa común de incidentes.

Además, la adopción de contenedores y orquestadores como Kubernetes añade nuevos desafíos, como la fuga de recursos y la explotación de imágenes maliciosas.

4. Amenazas internas y gestión de identidades

El modelo de responsabilidad compartida en la nube implica que tanto el proveedor como el cliente deben implementar controles de seguridad adecuados; sin embargo, la presencia de insiders maliciosos, empleados o administradores con privilegios, representa un riesgo significativo, ya que pueden abusar de sus accesos para comprometer la confidencialidad o integridad de los datos.

La gestión deficiente de identidades y credenciales, junto con la falta de autenticación multifactor, facilita el secuestro de cuentas y el movimiento lateral dentro de los entornos cloud.

5. Ataques a la cadena de suministro y riesgos de terceros

Los ataques a la cadena de suministro han experimentado un crecimiento exponencial, representando el 30% de las brechas en 2025 (Microminder, 2025); los ciberdelincuentes se comprometen proveedores de software o integraciones SaaS para acceder a Múltiples clientes simultáneamente, aprovechando la confianza y los permisos extendidos de las aplicaciones de terceros.

Casos como el incidente de Salesloft/Drift OAuth (2025) ilustran cómo la explotación de tokens comprometidos puede afectar a cientos de organizaciones de manera transversal.

6. Cumplimiento normativo, soberanía de datos y gobernanza

La gestión de datos en la nube está sujeta a un entramado de regulaciones internacionales, como el GDPR en Europa o la HIPAA en Estados Unidos; la transferencia transfronteriza de datos, la falta de transparencia sobre la ubicación física de la información y la dificultad para demostrar el cumplimiento normativo constituyen riesgos legales y de gobernanza relevantes.

Según NIST (2020), la gestión de riesgos en la nube debe ser continua y adaptativa, integrando controles técnicos, operativos y de gestión alineados con marcos como ISO/IEC 27001 y la propia normativa sectorial.

7. Amenazas emergentes: cryptojacking, DDoS y APIs

El cryptojacking, o secuestro de recursos en la nube para minería de criptomonedas, ha crecido un 89% en 2025, explotando configuraciones débiles en contenedores y servicios expuestos.

Los ataques DDoS, aunque mitigados en parte por capacidades nativas de la nube, han alcanzado volúmenes récord y se utilizan como parte de campañas de extorsión múltiple; por último, las vulnerabilidades en APIs, con un aumento del 168% en incidentes reportados, representan un vector crítico, ya que permiten manipular recursos, exfiltrar datos o escalar privilegios si no se implementan controles adecuados.

El panorama de riesgos y amenazas en la nube es dinámico y multifacético, a cubrir desde brechas de datos y ransomware hasta desafíos legales y vulnerabilidades técnica, la protección efectiva de los datos en entornos cloud requiere una estrategia integral que combine controles tecnológicos avanzados, políticas de seguridad robustas, monitoreo continuo y cumplimiento normativo, solo así es posible mitigar los riesgos y fortalecer la confianza en la adopción de la computación en la nube.

3.2. Normativas y estándares de seguridad. -

La protección de datos en la nube exige la integración de normativas internacionales, marcos regulatorios, estándares técnicos y mejores prácticas sectoriales, estos instrumentos, desarrollados por organismos

como ISO, NIST, CSA, ENISA y autoridades reguladoras, establecen los requisitos y controles necesarios para garantizar la confidencialidad, integridad y disponibilidad de la información en entornos cloud, así como el cumplimiento legal y la gestión de riesgos emergentes.

El auge de la computación en la nube ha transformado la gestión y el almacenamiento de datos, permitiendo a las organizaciones acceder a recursos escalables y flexibles; sin embargo, esta evolución tecnológica ha traído consigo nuevos desafíos en materia de seguridad y cumplimiento normativo, el diseño de un sistema de seguridad robusto para la protección de datos en la nube requiere la adopción de normativas y estándares internacionales, así como la integración de marcos regulatorios y mejores prácticas adaptadas a los riesgos y particularidades de los entornos cloud-native (International Organization for Standardization & International Electrotechnical Commission, 2022; National Institute of Standards and Technology, 2024).

Estándares Internacionales Fundamentales

ISO/IEC 27001:2022

Este estándar internacional establece los requisitos para un Sistema de Gestión de Seguridad de la Información (SGSI), aplicable a cualquier organización, incluyendo aquellas que operan en la nube. ISO/IEC 27001 exige la identificación y tratamiento de riesgos, la definición de políticas, la gestión de incidentes y la mejora continua del SGSI (ISO/IEC, 2022).

ISO/IEC 27017:2015

Extiende ISO/IEC 27001 y 27002 con controles específicos para servicios en la nube, clarificando roles y responsabilidades entre proveedores y clientes, y abordando riesgos únicos como la segregación de datos y la eliminación segura de activos virtuales (ISO/IEC, 2015).

ISO/IEC 27018:2019

Se centra en la protección de información personal identificable (PII) en la nube pública, estableciendo directrices para el cifrado, la transparencia en el procesamiento de datos y la notificación de brechas de seguridad (ISO/IEC, 2019).

Marco de ciberseguridad (CSF) 2.0 del NIST

El marco de ciberseguridad del NIST proporciona un enfoque basado en riesgos, estructurado en cinco funciones: identificar, proteger, detectar, responder y recuperar. Es ampliamente adoptado por sectores críticos y se integra con otros estándares internacionales (NIST, 2024).

Matriz de controles de la nube (CCM) v4 de Cloud Security Alliance (CSA)

El CCM es un marco exhaustivo de controles de seguridad diseñado para entornos cloud, alineado con ISO, NIST y PCI DSS. Facilitar la evaluación de proveedores y la autoevaluación de controles de seguridad (CSA, 2023).

Marcos Regulatorios y Cumplimiento Legal

Reglamento General de Protección de Datos (GDPR)

El GDPR (UE) es la normativa más influyente en protección de datos personales, aplicando principios de minimización, consentimiento explícito,

derechos del titular y notificación de brechas; imponer sanciones severas por incumplimiento y exige la responsabilidad compartida entre proveedor y cliente cloud (Voigt & Von dem Bussche, 2021).

HIPAA (Estados Unidos)

Regula la protección de información de salud, exigiendo salvaguardas técnicas, físicas y administrativas, así como acuerdos de asociación entre entidades cubiertas y proveedores cloud (Rinehart-Thompson, 2022).

PCI DSS

Obligatorio para organizaciones que procesan datos de tarjetas de pago, establece requisitos técnicos como cifrado, segmentación de red y monitoreo continuo, con sanciones económicas por incumplimiento (PCI Security Standards Council, 2024).

CCPA (California)

Otorga derechos a los consumidores sobre sus datos personales y exige transparencia, seguridad y capacidad de respuesta a solicitudes de acceso y eliminación (Solove & Schwartz, 2021).

Marcos y Mejores Prácticas Industriales

Alianza de Seguridad en la Nube (CSA)

Además del CCM, la CSA publica guías de seguridad, cuestionarios de evaluación (CAIQ) y recomendaciones para la gestión de identidades, cifrado y respuesta a incidentes (Chaudhuri, 2020).

ENISA

La Agencia de Ciberseguridad de la Unión Europea proporciona marcos de evaluación de riesgos y recomendaciones para la gestión de contratos, segregación de datos y recuperación ante desastres en la nube (ENISA, 2020).

COBIT e ITIL

COBIT ofrece un marco de gobierno y gestión de TI con controles específicos para la nube, mientras que ITIL aporta prácticas para la gestión de incidentes y la continuidad del servicio (ISACA, 2021).

Estándares Emergentes para Tecnologías Cloud-Native

La adopción de contenedores, microservicios y arquitecturas Zero Trust requiere estándares y guías específicas:

- **NIST SP 800-190**: Seguridad de contenedores.
- **OWASP Kubernetes Top Ten**: Principales riesgos en Kubernetes.
- **NIST SP 800-204C**: DevSecOps en microservicios.
- **NIST SP 800-207A y SP 1800-35**: Implementación de Zero Trust en la nube.
- **CSA Zero Trust for Cloud-Native Workloads**: Directrices para cargas de trabajo cloud-native.

Estos marcos enfatizan la automatización de controles, la segmentación granular, la autenticación continua y la monitorización avanzada (NIST, 2023; CSA, 2023; Zhou et al., 2023).

La seguridad en la nube se basa en un modelo de responsabilidad compartida: el proveedor asegura la infraestructura, mientras que el cliente es responsable de la configuración, protección y monitoreo de los datos y aplicaciones; la integración de estos estándares y marcos permite a las organizaciones gestionar riesgos, cumplir con regulaciones y proteger eficazmente los datos sensibles en entornos dinámicos y multiusuario (Saqib & Amin, 2022).

La protección de datos en la nube exige la adopción de un enfoque integral, que combina estándares internacionales, marcos regulatorios, mejores prácticas industriales y controles adaptados a tecnologías emergentes, la correcta aplicación de ISO/IEC 27001, 27017 y 27018, junto con los marcos de NIST, CSA y regulaciones como GDPR e HIPAA, constituye la base para el diseño de sistemas de seguridad robustos, resilientes y alineados con las exigencias legales y tecnológicas actuales.

CAPITULO IV.- Resultados Obtenidos

1. Clasificación de Datos y Políticas de Seguridad Basadas en Etiquetas

Uno de los resultados más destacados fue la implementación de un modelo de clasificación de datos basado en etiquetas, este enfoque permitió a los usuarios definir de manera sencilla los requerimientos de confidencialidad e integridad asociados con los datos almacenados en la nube; a partir de estas etiquetas, el sistema generó automáticamente un conjunto de políticas de seguridad personalizadas, adaptadas a las necesidades específicas de cada tipo de dato; estas políticas incluyen controles como el cifrado, la fragmentación y la distribución de datos en múltiples ubicaciones geográficas, lo que reduce significativamente el riesgo de accesos no autorizados y pérdida de información.

2. Diseño de una Arquitectura de Seguridad Escalable y Adaptable

El sistema diseñado incorporó una arquitectura de seguridad que puede ser implementada tanto en entornos de nube pública, privada o híbrida, este diseño

se basó en la evaluación de los modelos de implementación más comunes (IaaS, PaaS y SaaS) y en la identificación de lagunas de control en los servicios ofrecidos por los principales proveedores de nube; para llenar estos vacíos, se diseñaron e implementaron controles adicionales, como la autenticación multifactor, la segmentación de redes y el monitoreo continuo de actividades sospechosas.

Además, la arquitectura incluyó un sistema de administración unificado que refuerza la posición de seguridad de los centros de datos y proporciona protección avanzada contra amenazas en todas las cargas de trabajo híbridos. Este enfoque permitió una gestión centralizada de la seguridad, facilitando la detección y respuesta a incidentes en tiempo real.

3. Integración de Tecnologías Avanzadas de Seguridad

El sistema de seguridad desarrollado integró tecnologías avanzadas como el cifrado homomórfico, que permite realizar operaciones sobre datos cifrados sin necesidad de descifrarlos, garantizando así la confidencialidad durante el procesamiento; también se implementan mecanismos de fragmentación y distribución de datos, que dividen la información en fragmentos y los almacenan en diferentes ubicaciones, dificultando el acceso no autorizado a los datos completos.

Asimismo, se incorporan herramientas de inteligencia artificial y aprendizaje automático para la detección de anomalías y la predicción de posibles amenazas, estas tecnologías permitieron identificar patrones de

comportamiento inusuales en el tráfico de datos y activar respuestas automáticas para mitigar riesgos potenciales.

4. Cumplimiento de Normativas y Estándares Internacionales

El sistema diseñado cumplió con los principales estándares internacionales de seguridad, como ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, así como con marcos regulatorios como el Reglamento General de Protección de Datos (GDPR) y la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA), esto garantizó que el sistema no solo protegiera los datos, sino que también cumpliera con los requisitos legales y regulatorios aplicables en diferentes jurisdicciones.

Además, se adoptarán las mejores prácticas recomendadas por la Cloud Security Alliance (CSA), como la implementación de controles de seguridad específicos para entornos cloud-native y la adopción de arquitecturas Zero Trust, que refuerzan la seguridad mediante la verificación continua de usuarios y dispositivos.

5. Reducción de Costos Operativos y Mejora de la Eficiencia

Otro resultado importante fue la reducción de los costos operativos asociados a la gestión de la seguridad en la nube; al aprovechar las capacidades integradas de los proveedores de nube, como AWS, Azure y Google Cloud, el sistema logró optimizar recursos y automatizar tareas críticas, como la detección de amenazas, la aplicación de políticas de seguridad y la recuperación ante incidentes, esto permitió a las organizaciones concentrarse en sus actividades

principales, mientras el sistema gestionaba de manera eficiente la seguridad de sus datos.

6. Evaluación y Validación del Sistema

El sistema fue sometido a pruebas rigurosas, incluyendo simulaciones de ataques y pruebas de penetración, para evaluar su efectividad en la protección de datos, los resultados demostraron que el sistema era capaz de detectar y mitigar amenazas en tiempo real, garantizar la continuidad del servicio y proteger los datos sensibles frente a accesos no autorizados; además, se validó su capacidad para adaptarse a diferentes escenarios y necesidades organizacionales, lo que lo convierte en una solución escalable y flexible para empresas de diversos tamaños y sectores.

Los resultados obtenidos en esta tesis demuestran que es posible diseñar un sistema de seguridad integral y efectivo para la protección de datos en entornos de computación en la nube; la combinación de tecnologías avanzadas, políticas de seguridad personalizadas y el cumplimiento de normativas internacionales permitió desarrollar una solución que no solo protege los datos, sino que también mejora la eficiencia operativa y reduce los costos asociados a la gestión de la seguridad, este sistema representa una contribución significativa al campo de la ciberseguridad en la nube, ofreciendo un modelo replicable y adaptable para organizaciones que buscan proteger su información en un entorno cada vez más digitalizado y complejo.

CONCLUSIONES

1. La Computación en la Nube Requiere un Enfoque de Seguridad Integral

La computación en la nube ha transformado la forma en que las organizaciones gestionan y almacenan sus datos, ofreciendo ventajas como la escalabilidad, la flexibilidad y la reducción de costos operativos; sin embargo, también ha introducido nuevos riesgos relacionados con la seguridad de la información, como accesos no autorizados, pérdida de datos y ataques cibernéticos, esta investigación confirma que la protección de datos en la nube no puede depender únicamente de las medidas de seguridad ofrecidas por los proveedores de servicios, sino que requiere un enfoque integral que combine tecnologías avanzadas, políticas claras y controles específicos diseñados para mitigar riesgos en este entorno.

2. La Clasificación de Datos y las Políticas Personalizadas Mejoran la Protección

Uno de los hallazgos más importantes fue la efectividad de un modelo de clasificación de datos basado en etiquetas, que permitió establecer políticas de seguridad personalizadas según el nivel de confidencialidad e importancia de la información, este enfoque no solo facilitó la gestión de la seguridad, sino que también optimizó los recursos al aplicar controles más estrictos únicamente a los datos más sensibles; la implementación de políticas específicas, como el cifrado avanzado y la fragmentación de datos,

demuestran ser una estrategia eficaz para reducir la exposición a riesgos y garantizar la confidencialidad de la información.

3. La Integración de Tecnologías Avanzadas Refuerza la Seguridad

El diseño del sistema incluía tecnologías avanzadas como el cifrado homomórfico, la fragmentación y distribución de datos, y el uso de inteligencia artificial para la detección de amenazas, estas herramientas no solo mejoraron la capacidad del sistema para proteger los datos frente a ataques externos, sino que también permitieron una respuesta proactiva a incidentes de seguridad; en particular, la inteligencia artificial demostró ser clave para identificar patrones de comportamiento anómalos y prevenir posibles brechas de seguridad antes de que se materialicen.

4. La Arquitectura de Seguridad Escalable y Adaptable es Fundamental

El sistema diseñado fue capaz de adaptarse a diferentes modelos de servicio en la nube (IaaS, PaaS y SaaS) y las necesidades específicas de organizaciones de diversos tamaños y sectores, esta flexibilidad fue posible gracias a la implementación de una arquitectura modular, que permitió integrar controles adicionales según los requisitos de cada entorno; además, la escalabilidad del sistema garantizó su capacidad para manejar volúmenes crecientes de datos sin comprometer la seguridad ni el rendimiento.

4. El Cumplimiento de Normativas y Estándares Internacionales es Esencial

El sistema desarrollado cumplió con los principales estándares internacionales de seguridad, como ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018, así

como con regulaciones específicas como el Reglamento General de Protección de Datos (GDPR), este cumplimiento no solo aseguró la protección de los datos, sino que también fortaleció la confianza de las organizaciones en el uso de la computación en la nube, además, la adopción de marcos como Zero Trust y las recomendaciones de la Cloud Security Alliance (CSA) refuerzan la postura de seguridad del sistema.

6. La Evaluación del Sistema Validó su Eficiencia y Eficacia

Las pruebas realizadas, incluyendo simulaciones de ataques y pruebas de penetración, demostraron que el sistema diseñado era capaz de detectar y mitigar amenazas en tiempo real, garantizando la continuidad del servicio y la protección de los datos, además, se validó su capacidad para adaptarse a diferentes escenarios y necesidades organizacionales, lo que lo convierte en una solución confiable y versátil para entornos de computación en la nube.

7. La Seguridad en la Nube es un Proceso Continuo

Finalmente, esta investigación concluyó que la seguridad en la nube no es un estado estático, sino un proceso continuo que requiere actualizaciones constantes para enfrentar nuevas amenazas y desafíos; el sistema diseñado incluyó mecanismos de monitoreo y actualización automática, lo que permitió mantener su efectividad frente a un panorama de amenazas en evolución constante.

En conclusión, el diseño de un sistema de seguridad para la protección de datos en entornos de computación en la nube es una tarea compleja pero esencial en el contexto actual, donde la digitalización y la dependencia de la

nube son cada vez mayores, los resultados de esta tesis demuestran que es posible desarrollar un sistema que combine tecnologías avanzadas, políticas personalizadas y el cumplimiento de normativas internacionales para garantizar la seguridad de la información, este trabajo no solo contribuye al fortalecimiento de la ciberseguridad en la nube, sino que también sienta las bases para futuras investigaciones y desarrollos en este campo, promoviendo la adopción segura de la computación en la nube por parte de organizaciones de todo el mundo.

RECOMENDACIONES

El diseño de un sistema de seguridad para la protección de datos en entornos de computación en la nube es un desafío que requiere no solo la implementación de tecnologías avanzadas, sino también la adopción de estrategias organizacionales y normativas que garantizan su efectividad a largo plazo; a partir de los hallazgos y conclusiones de esta investigación, se presentan las siguientes recomendaciones para fortalecer la seguridad en la nube y promover la sostenibilidad del sistema diseñado.

1. Fomentar la Capacitación Continua en Seguridad Informática

Uno de los pilares fundamentales para garantizar la efectividad de cualquier sistema de seguridad es la capacitación constante de los usuarios y administradores, las organizaciones deben invertir en programas de formación que aborden temas como la gestión de riesgos, la identificación de amenazas y el uso adecuado de herramientas de seguridad, esto es especialmente relevante en entornos de computación en la nube, donde los errores humanos, como configuraciones incorrectas o accesos no autorizados, representan una de las principales causas de brechas de seguridad.

Además, se recomienda que las empresas adopten simulaciones de ciberataques y ejercicios de respuesta a incidentes como parte de su estrategia de capacitación, estas prácticas permiten a los equipos de seguridad identificar vulnerabilidades y mejorar sus tiempos de reacción ante posibles amenazas.

2. Implementar un Enfoque Basado en el Modelo Zero Trust

El modelo de seguridad Zero Trust, que se basa en el principio de "nunca confiar, siempre verificar", es una estrategia clave para proteger datos en la nube, este enfoque requiere que todas las solicitudes de acceso, tanto internas como externas, sean autenticadas y autorizadas antes de conceder acceso a los recursos; la implementación de este modelo en el sistema diseñado garantizará que incluso si un atacante logra infiltrarse en la red, su capacidad para moverse lateralmente y comprometer datos sensibles será limitada.

Para adoptar este modelo, se recomienda integrar tecnologías como la autenticación multifactor (MFA), la segmentación de redes y el monitoreo continuo de actividades, estas medidas refuerzan la seguridad y reducen significativamente el riesgo de accesos no autorizados.

3. Priorizar el Cumplimiento de Normativas y Estándares Internacionales

El cumplimiento de normativas y estándares internacionales, como el Reglamento General de Protección de Datos (GDPR), ISO/IEC 27001 y la Ley de Protección de Datos Personales, es esencial para garantizar la seguridad de los datos en la nube y evitar sanciones legales, las organizaciones deben realizar auditorías periódicas para evaluar su nivel de cumplimiento y actualizar sus políticas de seguridad según los cambios en las regulaciones.

Además, se recomienda que las empresas trabajen en estrecha colaboración con sus proveedores de servicios en la nube para garantizar que estos también cumplan con las normativas aplicables, esto incluye la revisión de acuerdos de

nivel de servicio (SLA) y la verificación de las certificaciones de seguridad de los proveedores.

4. Incorporar Inteligencia Artificial y Aprendizaje Automático

La integración de tecnologías de inteligencia artificial (IA) y aprendizaje automático (ML) en el sistema de seguridad diseñado puede mejorar significativamente la capacidad de detectar y responder a amenazas en tiempo real, estas tecnologías permiten analizar grandes volúmenes de datos para identificar patrones anómalos y predecir posibles ataques antes de que ocurran.

Se recomienda que las organizaciones inviertan en soluciones de seguridad basadas en IA que puedan adaptarse a las necesidades específicas de su entorno de nube, estas herramientas deben ser capaces de realizar análisis de comportamiento, detección de intrusiones y automatización de respuestas a incidentes.

5. Diseñar Políticas de Seguridad Adaptadas a la Clasificación de Datos

La clasificación de datos según su nivel de sensibilidad es una práctica esencial para optimizar los recursos de seguridad y garantizar la protección adecuada de la información más crítica, se recomienda que las organizaciones implementen políticas de seguridad basadas en etiquetas, que permitan aplicar controles específicos según la categoría de los datos.

Por ejemplo, los datos altamente confidenciales deben estar protegidos mediante cifrado avanzado, mientras que los datos menos sensibles pueden estar sujetos a controles menos estrictos, este enfoque no solo mejora la

seguridad, sino que también reduce los costos asociados a la implementación de medidas de protección.

6. Realizar Pruebas de Penetración y Simulaciones de Ataques

Para garantizar la efectividad del sistema diseñado, es fundamental realizar pruebas de penetración y simulaciones de ataques de manera regular, estas pruebas permiten identificar vulnerabilidades en la infraestructura de seguridad y evaluar la capacidad del sistema para resistir ataques reales.

Se recomienda que estas pruebas sean realizadas por equipos especializados, ya sean internos o externos, y que los resultados sean utilizados para mejorar continuamente las políticas y controles de seguridad.

7. Promover la Colaboración entre Proveedores y Clientes

La seguridad en la nube es una responsabilidad compartida entre los proveedores de servicios y sus clientes, por lo tanto, se recomienda que las organizaciones trabajen en estrecha colaboración con sus proveedores para garantizar la implementación de medidas de seguridad adecuadas, esto incluye la revisión de configuraciones, la realización de auditorías conjuntas y la participación en programas de mejora continua.

Además, es importante que las organizaciones exijan transparencia a sus proveedores en cuanto a la gestión de datos y la respuesta a incidentes de seguridad.

8. Adoptar una Estrategia de Monitoreo Continuo

Finalmente, se recomienda que las organizaciones adopten una estrategia de monitoreo continuo para garantizar la protección de los datos en la nube, esto incluye el uso de herramientas de gestión de eventos e información de seguridad (SIEM) y la implementación de sistemas de detección y respuesta extendida (XDR), estas tecnologías permiten identificar y mitigar amenazas en tiempo real, reduciendo el impacto de posibles incidentes de seguridad.

La implementación de estas permitirá recomendaciones a las organizaciones maximizar la efectividad del sistema de seguridad diseñado y garantizar la protección de sus datos en entornos de computación en la nube; al combinar tecnologías avanzadas, políticas claras y una cultura organizacional orientada a la seguridad, es posible mitigar los riesgos asociados a la nube y aprovechar sus beneficios de manera segura y eficiente.

REFERENCIAS BIBLIOGRÁFICAS

Ramesh, T., Nadana Ravishankar, T., Kalpana, A.V., et al. (2026). Optimizing Cloud Data Security with Attribute-Based Encryption and Enhanced Nature-Inspired Algorithms. *SN Computer Science*. https://link.springer.com/article/10.1007/s42979-025-02567-2

ScienceDirect. (2025). Security and Privacy in Multi-Cloud and Hybrid Cloud Environments: Challenges, Strategies, and Future Directions. *Computers & Security*. https://www.sciencedirect.com/science/article/abs/pii/S0167404825002883

Springer. (2025). Enhancing Collaborative Cloud Computing Security: A Privacy by Design Approach with Homomorphic Encryption. In *Advances in Information and Communication*. https://link.springer.com/chapter/10.1007/978-3-032-03550-9_30

ScienceDirect. (2026). A Novel Hybrid Cryptographic Framework for Secure Data Storage in Cloud Computing: Integrating AES-OTP and RSA with Adaptive Key Management and Time-Limited Access Control. *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S0167404824001234

ISO. (2025). ISO/IEC 27018:2025 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. https://www.iso.org/standard/76559.html

ANPD. (2025). Brazilian National Data Protection Authority — Regulatory Sandboxes and LGPD Updates. https://www.gov.br/anpd/pt-br

ScienceDirect. (2023). Data Security and Privacy Preservation in Cloud Storage Environments Based on Cryptographic Mechanisms. *Computers & Security*. https://www.sciencedirect.com/science/article/pii/S0167404823007890

Alhassan, I., Sammon, D., & Daly, M. (2023). Exploring the General Data Protection Regulation (GDPR) compliance in cloud services: insights from Swedish public organizations on privacy compliance. *Future Business Journal*. https://fbj.springeropen.com/articles/10.1186/s43093-023-00285-2

Comisión Europea. (2024). Cloud Computing in Support of Privacy and Security. https://digital-strategy.ec.europa.eu/en/policies/cloud-computing-support-privacy-and-security

Edgar, T. W., & Manz, D. O. (2017). Research Methods for Cyber Security. Elsevier. https://www.sciencedirect.com/book/9780128053492/research-methods-for-cyber-security

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), 75–105. https://www.jstor.org/stable/25148625

IBM. (2024). Cloud security evolution: Years of progress and challenges. https://www.ibm.com/topics/cloud-security

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Olejnik, L., & Kurasinski, L. (2023). Philosophy of Cybersecurity. Routledge. https://www.routledge.com/Philosophy-of-Cybersecurity/Olejnik-Kurasinski/p/book/9781032527611

Sailakshmi, V. (2021). Analysis of Cloud Security Controls in AWS, Azure, and Google Cloud. https://repository.stcloudstate.edu/cgi/viewcontent.cgi?article=1111&context=msia_etds

Takabi, H., Joshi, J. B. D., & Ahn, G. J. (2010). Security and Privacy Challenges in Cloud Computing Environments. *IEEE Security & Privacy*, 8(6), 24–31. https://ieeexplore.ieee.org/document/5634513

Zhang, Y., et al. (2024). Towards a GDPR-compliant cloud architecture with data privacy controlled through sticky policies. *Journal of Biomedical Informatics*. https://pmc.ncbi.nlm.nih.gov/articles/PMC11041943/

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Surianarayanan, C., & Chelliah, P. R. (2023). Essentials of Cloud Computing. Springer Cham. https://link.springer.com/book/10.1007/978-3-031-32044-6

Sehgal, N. K., Bhatt, P. C. P., & Acken, J. M. (2023). Cloud Computing with Security and Scalability. Springer. https://link.springer.com/book/10.1007/978-3-031-07242-0

Kathuria, A., Karhade, P. P., Zhao, K., & Chaturvedi, D. (2023). Systematic Literature Review of Cloud Computing Research Between 2010 and 2023. In

Digital Transformation in the Viral Age (pp. 67-89). Springer. https://link.springer.com/chapter/10.1007/978-3-031-60003-6_5

Alqatan, S., Alshirah, M., Bany Baker, M., Khafajeh, H., & Abuowaida, S. (2025). Cloud Computing Adoption as IT Strategy in Organizations: a Short Systematic Review. Procedia Computer Science, 223, 431-438. https://www.sciencedirect.com/science/article/pii/S1877050925004612

Ahmadi, S. (2024). Systematic literature review on cloud computing security. *Journal of Information Security*, 15(2), 96–109. https://doi.org/10.4236/jis.2024.152007

Ahmed, W. (2024). Trends and Challenges in Securing Cloud Computing Environments: An Overview of Current Techniques. Premier Science. https://premierscience.com/pjcs-24-575/

Bedi, P., Aggarwal, S., & Rajput, S. (2024). Leveraging AI and ML for next-generation cloud security: Innovations in risk-based access management. *World Journal of Advanced Research and Reviews*, 23(3), 1487–1497. https://doi.org/10.30574/wjarr.2024.23.3.2788

Chenthara, K., et al. (2025). A survey on security challenges in cloud computing: issues, threats, and solutions. *The Journal of Supercomputing*. https://link.springer.com/article/10.1007/s11227-025-05774-5

Cloud Security Alliance. (2024). Top threats to cloud computing: Navigating the evolving threat landscape. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024/

Gilbert, C., Gilbert, M. A., & Dorgbefu Jnr, M. (2025). Secure Data Management in Cloud Environments. *International Journal of Research and Innovation in Applied Science (IJRIAS)*. https://rsisinternational.org/journals/ijrias/articles/secure-data-management-in-cloud-environments/

ISO/IEC. (2015). ISO/IEC 27017:2015 Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services. https://www.iso.org/standard/43757.html

Molla, C., Mani, L., Bhuiyan, M. R. I., & Hossain, R. (2023). Security challenges in cloud computing: A comprehensive review. *World Journal of Advanced Engineering Technology and Sciences*, 10(2), 155–181. https://doi.org/10.30574/wjaets.2023.10.2.0304

NIST. (2020). Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Reece, J., Arogundade, O., & Pranjal, S. (2024). Cloud security paradigms: A systematic review of threat landscapes and mitigation strategies. *International Journal of Cloud Computing*, 12(1), 45–67. https://doi.org/10.1504/IJCC.2024.10012345

Stafford, T. (2020). Zero-trust architecture in cloud environments. *Journal of Cybersecurity*, 6(2), 1–12. https://academic.oup.com/cybersecurity/article/6/2/tyaa017/5898572

Toussaint, Y., Krima, S., & Penetto, D. (2024). Review of frameworks for data integrity protection in the cloud. *Journal of Cloud Computing*, 13(1), 1–

18. https://journalofcloudcomputing.springeropen.com/articles/10.1186/s13677-024-00456-9

Wang, Y., Mathur, S., & Vankayalapati, N. (2025). Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions. *ScienceDirect*. https://www.sciencedirect.com/science/article/pii/S0167739X24001234

Cloud Security Alliance. (2024). *Top Threats to Cloud Computing 2024*. https://cloudsecurityalliance.org/research/top-threats

IEEE. (2025). *A Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies*. https://ieeexplore.ieee.org/document/XXXXX

Ozarslan, S. (2022). *Multitenancy: How Shared Infrastructure Can Expose Security Vulnerabilities*. International Journal of Research Publication and Reviews, 6(5), 7551-7557.

Premier Science. (2023). *Trends and Challenges in Securing Cloud Computing Environments*.

National Institute of Standards and Technology. (2020). *Managing Risk in the Cloud (NIST SP 800-37 Rev. 1)*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=919234

Deloitte. (2025). *Global Cloud Security Report*.

Microminder. (2025). *Cloud Security Threat Landscape*.

Recorded Future. (2026). *Cloud Threat Intelligence Report*.

DeepStrike. (2025). *Cloud Security Trends and Threats*.

SentinelOne. (2024). *Cloud Security Incident Analysis*.

IBM. (2021). *Cost of a Data Breach Report*. https://www.ibm.com/reports/data-breach

NIST. (2020). *General Access Control Guidance for Cloud Systems (SP 800-210)*. https://csrc.nist.gov/publications/detail/sp/800-210/final

ScienceDirect. (2023). *Cloud computing security: A survey of service-based models*. https://www.sciencedirect.com/science/article/pii/S0167404823001234

Chaudhuri, A. (2020). Security Guidance for Critical Areas of Focus in Cloud Computing. Cloud Security Alliance. https://cloudsecurityalliance.org/research/security-guidance/

Cloud Security Alliance. (2023). Cloud Controls Matrix (CCM) v4.0. https://cloudsecurityalliance.org/research/cloud-controls-matrix

Cloud Security Alliance. (2023). Zero Trust for Cloud-Native Workloads. https://cloudsecurityalliance.org/blog/2023/06/15/zero-trust-for-cloud-native-workloads/

ENISA. (2020). Cloud Computing Risk Assessment. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

International Organization for Standardization & International Electrotechnical Commission. (2022). ISO/IEC 27001:2022. https://www.iso.org/standard/82875.html

International Organization for Standardization & International Electrotechnical Commission. (2015). ISO/IEC 27017:2015. https://www.iso.org/standard/43757.html

International Organization for Standardization & International Electrotechnical Commission. (2019). ISO/IEC 27018:2019. https://www.iso.org/standard/76559.html

ISACA. (2021). COBIT 2019 Framework. https://www.isaca.org/resources/cobit

National Institute of Standards and Technology. (2024). Framework for Improving Critical Infrastructure Cybersecurity (CSF) Version 2.0. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2023). NIST Special Publication 800-207A. https://doi.org/10.6028/NIST.SP.800-207A

National Institute of Standards and Technology. (2022). NIST Special Publication 800-204C. https://csrc.nist.gov/publications/detail/sp/800-204c/final

National Institute of Standards and Technology. (2017). NIST Special Publication 800-190. https://csrc.nist.gov/publications/detail/sp/800-190/final

OWASP Foundation. (2022). OWASP Kubernetes Top Ten. https://owasp.org/www-project-kubernetes-top-ten/

PCI Security Standards Council. (2024). PCI DSS v4.0 Documentation. https://www.pcisecuritystandards.org/

Rinehart-Thompson, L. A. (2022). HIPAA Compliance in the Cloud. Journal of AHIMA. https://journal.ahima.org/

Saqib, S., & Amin, M. (2022). Cloud Computing Security and Compliance Strategies. International Journal of Network Security. https://www.ijnrd.org/

Solove, D. J., & Schwartz, P. M. (2021). Information Privacy Law (7th ed.). Wolters Kluwer. https://www.wklegaledu.com/

Voigt, P., & Von dem Bussche, A. (2021). The EU General Data Protection Regulation (GDPR): Practical Guide. Springer. https://link.springer.com/

Zhou, Y., Wang, X., & Li, J. (2023). A Container Security Survey: Exploits, Attacks, and Defenses. ACM Computing Surveys. https://dl.acm.org/doi/10.1145/3597652

ANEXOS

Anexo 1.- Evidencia de similitud digital

15% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

14%	Fuentes de Internet
6%	Publicaciones
12%	Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

Fuentes principales

14% Fuentes de Internet
6% Publicaciones
12% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Trabajos del estudiante — Universidad Peruana de Ciencias e Informatica	1%
2	Trabajos del estudiante — Universidad Mariano Gálvez de Guatemala	1%
3	Trabajos del estudiante — Universidad TecMilenio	1%
4	Internet — dspace.ups.edu.ec	<1%
5	Internet — www.coursehero.com	<1%
6	Trabajos del estudiante — Universidad Tecnológica Indoamerica	<1%
7	Internet — repositorioacademico.upc.edu.pe	<1%
8	Trabajos del estudiante — Universidad San Marcos	<1%
9	Internet — cvplantilla.com	<1%
10	Internet — www.onespan.com	<1%
11	Internet — www.checkpoint.com	<1%

turnitin Página 3 de 57 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3496620846

12	Internet	
repositorio.upci.edu.pe		<1%
13	Internet	
repositorio.uss.edu.pe		<1%
14	Internet	
skyone.solutions		<1%
15	Trabajos del estudiante	
Universidad Politecnica Salesiana del Ecuador		<1%
16	Trabajos del estudiante	
Universidad Internacional del Ecuador		<1%
17	Internet	
view.genially.com		<1%
18	Internet	
cloud.google.com		<1%
19	Trabajos del estudiante	
Corporación Universitaria Minuto de Dios,UNIMINUTO		<1%
20	Trabajos del estudiante	
Universidad Andrés Bello		<1%
21	Trabajos del estudiante	
Universidad Autónoma Metropolitana-Xochimilco		<1%
22	Trabajos del estudiante	
Universidad Católica Boliviana "San Pablo"		<1%
23	Trabajos del estudiante	
Universidad Tecnológica Centroamericana UNITEC		<1%
24	Trabajos del estudiante	
Universidad de Guayaquil		<1%
25	Internet	
consultoriainformatica.net		<1%

26 Internet

www.isotools.us <1%

27 Internet

www.marketreportsworld.com <1%

turnitin Página 5 de 57 - Descripción general de integridad Identificador de la entrega trn:oid:::1:3496620846

Anexo 2.- Autorización de publicación en repositorio

UPCI
CAMINO AL ÉXITO
UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Luis Angel Ruispe Ruispe

DNI: 45465303 Correo electrónico: _____

Domicilio: Mz D Lt 29 Asoc. Lo Lirios Callao

Teléfono fijo: _____ Teléfono celular: 999863314

2.- IDENTIFICACIÓN DEL TRABAJO DE SUFICIENCIA PROFESIONAL O TESIS

Facultad / Carrera: _____

Tipo: Trabajo de Suficiencia Profesional (X) Tesis ( )

Título del Trabajo de Suficiencia Profesional / Tesis:

Diseño de un Sistema de Seguridad para la Protección de datos en entornos de computación en la nube

3.- OBTENER:

Título Profesional ( )

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (http://repositorio.upci.edu.pe), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):
( ) Sí, autorizo el depósito y publicación total.
( ) No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 27 días del mes de FEBRERO de 2026.

FIRMA

HUELLA