innova SCIENCE JOURNAL ISSN:3091-1680

OM EDITORIAL

Artículo Científico

Seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos

Security and privacy in the storage of data in distributed information systems

Pinargote Bravo, Víctor Joel [1]*.

[1] Escuela Superior Politécnica Agropecuaria de Manabí Manuel Félix López; Ecuador, Calceta; https://orcid.org/0000-0003-0599-1651; vpinargote@espam.edu.ec

[1] Autor Correspondencia

https://doi.org/10.63618/omd/isj/v3/n1/5

Cita: Pinargote Bravo, V. J. (2025). Seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos. *Innova Science Journal*, 3(1), 59-74. https://doi.org/10.63618/omd/isj/v3/n1/5

Recibido: 29/10/2024
Aceptado: 30/12/2024
Publicado: 31/01/2025

Resumen: La seguridad y privacidad en los sistemas de información distribuidos representan un desafío creciente debido a la descentralización de datos y el incremento de ciberataques. Este estudio analiza las amenazas, estrategias de mitigación y desafíos futuros en la protección de datos distribuidos. Mediante una revisión sistemática de literatura, se identificaron riesgos como el ransomware, el phishing y ataques DDoS, así como vulnerabilidades en la interoperabilidad y la nube híbrida. Entre las estrategias de mitigación destacan el cifrado de datos, la autenticación multifactor y el monitoreo basado en inteligencia artificial. Se reconoce que la falta de regulaciones homogéneas a nivel global dificulta la implementación de políticas de seguridad unificadas, mientras que la adopción de tecnologías emergentes, como blockchain y computación cuántica, ofrece soluciones prometedoras. Sin embargo, la falta de concienciación y formación en ciberseguridad sigue siendo un obstáculo significativo. Se concluye que la protección de los datos en sistemas distribuidos requiere un enfoque integral que combine normativas adecuadas, innovación tecnológica y capacitación continua para fortalecer la resiliencia de las infraestructuras digitales.

Palabras clave: seguridad de datos; ciberseguridad; sistemas distribuidos; computación en la nube; privacidad digital.

Abstract: Security and privacy in distributed information systems represent a growing challenge due to data decentralization and increasing cyber-attacks. This study analyzes the threats, mitigation strategies, and future challenges in protecting distributed data. Through a systematic literature review, risks such as ransomware, phishing and DDoS attacks, as well as vulnerabilities in interoperability and hybrid cloud were identified. Mitigation strategies include data encryption, multi-factor authentication and artificial intelligence-based monitoring. It is recognized that the lack of globally homogeneous regulations hinders the implementation of unified security policies, while the adoption of emerging technologies, such as blockchain and quantum computing, offers promising solutions. However, the lack of cybersecurity awareness and training remains a significant obstacle. It is concluded that data protection in distributed systems requires a comprehensive approach combining appropriate regulations, technological innovation and continuous training to strengthen the resilience of digital infrastructures.

Keywords: data security; cybersecurity; distributed systems; cloud computing; digital privacy.

1. Introducción

La seguridad y privacidad en el almacenamiento de datos dentro de sistemas de información distribuidos representa un desafío creciente en la era digital. El desarrollo y la expansión de tecnologías como la computación en la nube y los entornos híbridos han facilitado el acceso y la gestión de grandes volúmenes de datos, pero también han incrementado las vulnerabilidades asociadas a la confidencialidad, integridad y disponibilidad de la información (Gil et al., 2023). A medida que las organizaciones y empresas migran hacia infraestructuras distribuidas, surgen riesgos asociados a ataques cibernéticos, brechas de seguridad y accesos no autorizados, lo que plantea la necesidad de implementar estrategias efectivas para mitigar estas amenazas.

El problema central radica en que, si bien los sistemas de información distribuidos ofrecen ventajas en términos de escalabilidad y accesibilidad, también presentan riesgos significativos en cuanto a la protección de datos. Uno de los principales desafíos es la gestión segura del almacenamiento y transmisión de información en entornos con múltiples nodos interconectados, donde cada punto de acceso podría representar una vulnerabilidad potencial (Velásquez Acevedo, 2022). Además, la interoperabilidad de servicios en la nube híbrida conlleva la exposición de datos sensibles a diversas normativas y estándares de seguridad, lo que dificulta su protección homogénea (Asencios Mory & Pacherres Paredes, 2023). En este sentido, la falta de mecanismos robustos de encriptación y autenticación puede facilitar la filtración de datos críticos, afectando la privacidad y la confianza de los usuarios.

Los factores que contribuyen a este problema incluyen, en primer lugar, la creciente sofisticación de los ciberataques, que pueden comprometer la seguridad de los sistemas mediante técnicas como la inyección de código malicioso, el phishing y los ataques de denegación de servicio (Gil et al., 2023). En segundo lugar, la heterogeneidad de las plataformas y protocolos empleados en los sistemas distribuidos dificulta la aplicación de políticas de seguridad uniformes. Asimismo, la falta de regulación y cumplimiento de estándares internacionales en el tratamiento de datos personales es un aspecto crítico que afecta la privacidad de los usuarios. Un caso particular es el almacenamiento de información en la nube, donde las brechas de seguridad pueden derivar en la exposición de datos médicos o financieros altamente sensibles, como lo evidencian Urquijo Morales et al. (2023) en su estudio sobre la seguridad de la historia clínica electrónica en entornos distribuidos.

Desde una perspectiva práctica, la justificación de este estudio radica en la necesidad de fortalecer los mecanismos de seguridad en los sistemas de información distribuidos para garantizar la protección de datos frente a amenazas emergentes. La importancia de abordar esta problemática se fundamenta en la creciente digitalización de procesos en sectores clave como la salud, la banca y el comercio electrónico, donde la confiabilidad en la gestión de información es esencial para el desarrollo tecnológico y la protección de los derechos de los usuarios. Además, la viabilidad de este análisis se respalda en la disponibilidad de estudios previos y marcos teóricos que permiten evaluar metodologías y estrategias efectivas para mejorar la seguridad y privacidad en entornos distribuidos (Velásquez Acevedo, 2022). La revisión de literatura permitirá identificar enfoques innovadores y mejores prácticas adoptadas en la industria para enfrentar los desafíos actuales en este ámbito.

El objetivo principal de esta investigación es analizar los principales riesgos, metodologías y estrategias de seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos. Para ello, se realizará una revisión sistemática de la literatura reciente con el fin de identificar las mejores prácticas y tecnologías emergentes que pueden contribuir a la mitigación de vulnerabilidades en estos entornos. A través de este análisis, se pretende proporcionar un marco conceptual sólido que sirva como referencia para futuras investigaciones y desarrollos en el campo de la ciberseguridad aplicada a sistemas distribuidos.

La seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos es un tema de relevancia creciente en la era digital. Las amenazas y desafíos asociados requieren un enfoque integral que combine estrategias de seguridad avanzadas con regulaciones adecuadas y políticas de gestión de riesgos efectivas. La presente investigación busca aportar conocimiento sobre las mejores prácticas y enfoques tecnológicos disponibles para garantizar la protección de datos en estos entornos, contribuyendo al desarrollo de soluciones más seguras y confiables en la gestión de la información distribuida.

2. Materiales y Métodos

La presente investigación adopta un enfoque exploratorio basado en un estudio documental, con el propósito de analizar la seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos. Este tipo de estudio permite identificar, recopilar y analizar información relevante proveniente de fuentes científicas actualizadas, garantizando una visión integral de los riesgos, metodologías y estrategias utilizadas en la protección de datos en entornos distribuidos.

Para la recolección de información, se realizó una revisión sistemática de la literatura, considerando artículos científicos, tesis y documentos técnicos publicados en repositorios académicos y bases de datos indexadas. Se emplearon criterios de selección que incluyeron la pertinencia del contenido, el año de publicación y la rigurosidad metodológica de las fuentes, priorizando estudios recientes con enfoques relevantes para el tema de investigación. Se descartaron aquellos documentos que carecieran de fundamentación teórica sólida o que no cumplieran con criterios de calidad académica.

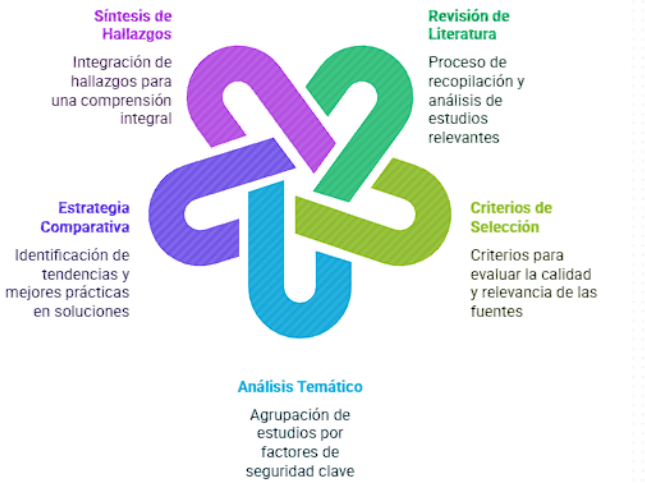
El análisis de la información se realizó mediante una clasificación temática, agrupando los estudios según los principales factores que afectan la seguridad y privacidad en los sistemas distribuidos, como amenazas cibernéticas, vulnerabilidades en la gestión de datos y estrategias de protección. Se utilizó una estrategia comparativa para identificar similitudes y diferencias en las soluciones propuestas por diversos autores, con el fin de determinar tendencias y mejores prácticas en el ámbito de la ciberseguridad aplicada a entornos distribuidos.

El proceso de síntesis y sistematización de la información permitió estructurar los hallazgos en función de los objetivos de la investigación. Se buscó no solo describir las problemáticas existentes, sino también establecer relaciones entre diferentes enfoques teóricos y prácticos en la protección de datos. A partir del análisis de la literatura, se generaron conclusiones fundamentadas que contribuyen a la comprensión de los

desafíos actuales y posibles soluciones en el almacenamiento seguro de información en sistemas distribuidos. A continuación, en la figura 1 se representará de manera grafica la metodología:

Figura 1

Metodología para el Análisis de Seguridad en Sistemas de Información Distribuidos



Nota: El diagrama representa los pasos clave en la revisión de literatura, desde la selección y análisis de estudios hasta la síntesis de hallazgos para una comprensión integral (Autores, 2024).

La validez del estudio se sustenta en la utilización de fuentes confiables y en la rigurosidad del análisis documental. Al tratarse de una investigación de carácter exploratorio, los resultados obtenidos no pretenden ser definitivos, sino servir como una base teórica para futuras investigaciones que profundicen en la implementación de soluciones específicas para la protección de datos en sistemas de información distribuidos.

3. Resultados

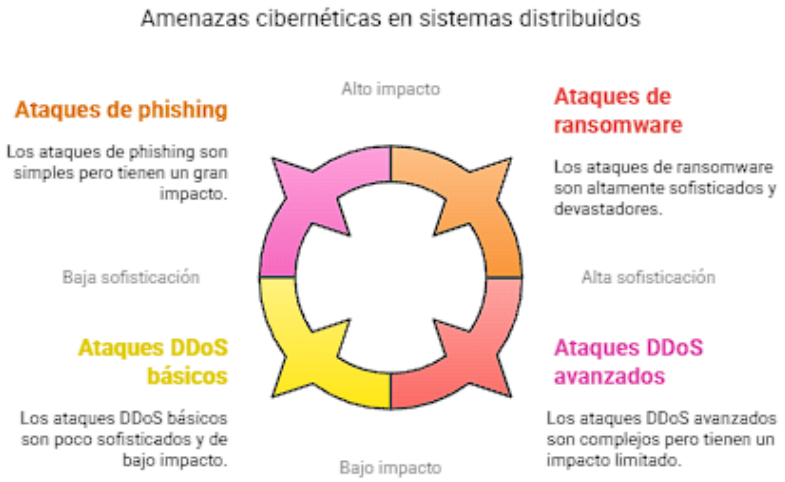
3.1. Principales amenazas a la seguridad y privacidad en sistemas de información distribuidos

Ataques cibernéticos dirigidos

Los sistemas de información distribuidos han transformado la gestión y almacenamiento de datos en diversos sectores, permitiendo mayor accesibilidad, escalabilidad y eficiencia en el procesamiento de información. Sin embargo, esta evolución tecnológica ha traído consigo múltiples desafíos en materia de seguridad y privacidad, ya que la descentralización de los datos y su distribución en múltiples nodos interconectados generan nuevas vulnerabilidades que pueden ser explotadas por actores malintencionados. Entre las amenazas más críticas que afectan a estos sistemas se encuentran los ataques cibernéticos dirigidos, las vulnerabilidades en la interoperabilidad y los riesgos asociados a la nube híbrida.

Figura 2

Principales amenazas cibernéticas en sistemas de información distribuidos



Nota: La figura 2 presenta una clasificación de amenazas cibernéticas en sistemas distribuidos (Autores, 2024).

Uno de los principales riesgos en los sistemas de información distribuidos es el incremento de los ataques cibernéticos dirigidos, que buscan comprometer la integridad, confidencialidad y disponibilidad de los datos almacenados en múltiples servidores interconectados. En la actualidad, los atacantes han desarrollado estrategias cada vez más sofisticadas para vulnerar la seguridad de estos sistemas, destacándose entre ellas el *ransomware*, el *phishing* y los ataques de denegación de servicio distribuido (DDoS).

El *ransomware* representa una amenaza significativa debido a su capacidad para cifrar datos sensibles y exigir un rescate económico a cambio de su liberación. Este tipo de ataque no solo afecta la disponibilidad de la información, sino que también puede comprometer su integridad si los atacantes deciden modificar o eliminar archivos antes de restaurarlos. En sistemas distribuidos, donde la información se encuentra replicada en múltiples servidores, un ataque de este tipo puede propagarse rápidamente, afectando nodos interconectados y generando una interrupción masiva de los servicios (Troncoso Reigada & González Rivas, 2021).

El *phishing*, por otro lado, se ha convertido en una de las tácticas más utilizadas para obtener credenciales de acceso a plataformas distribuidas. A través de correos electrónicos fraudulentos o sitios web falsificados, los atacantes engañan a los usuarios para que revelen información confidencial, facilitando accesos no autorizados a bases de datos y recursos críticos. En un entorno distribuido, donde diferentes usuarios acceden a la información desde múltiples ubicaciones y dispositivos, este tipo de ataque representa un riesgo elevado, ya que una sola brecha de seguridad puede comprometer toda la infraestructura (Rosa Rodríguez, 2021).

Los ataques DDoS son otra amenaza relevante en la seguridad de sistemas distribuidos. Estos ataques buscan sobrecargar los servidores con un volumen masivo de solicitudes falsas, afectando su capacidad de respuesta y provocando interrupciones en los servicios. En entornos donde los datos deben estar disponibles en tiempo real, como en plataformas financieras o sanitarias, un ataque DDoS puede causar daños significativos,

afectando la operatividad y la confianza en la infraestructura tecnológica (Troncoso Reigada & González Rivas, 2021).

Vulnerabilidades en la interoperabilidad

Otro aspecto crítico en la seguridad de los sistemas distribuidos es la falta de estandarización en la gestión de datos entre diferentes plataformas, lo que genera importantes vulnerabilidades en la interoperabilidad. La interconexión de múltiples sistemas con arquitecturas y protocolos de seguridad diversos puede abrir brechas que faciliten el acceso no autorizado a la información, ya sea por errores en la configuración de permisos o por incompatibilidades en los mecanismos de cifrado.

Uno de los principales problemas derivados de la interoperabilidad es la exposición de datos personales sin el consentimiento explícito de los usuarios. En el ámbito educativo, por ejemplo, se ha observado que muchas aplicaciones digitales no cuentan con medidas de seguridad adecuadas para proteger la privacidad de los estudiantes y docentes, permitiendo filtraciones de información sin cumplir con normativas de protección de datos (Rosa Rodríguez, 2021). Este problema se agrava en sistemas distribuidos donde múltiples entidades comparten información en tiempo real, dificultando la implementación de una estrategia unificada de seguridad.

La interoperabilidad entre distintos sistemas suele depender de terceros proveedores de tecnología, lo que introduce un nuevo nivel de riesgo. Si las plataformas utilizadas no implementan políticas de seguridad homogéneas, los datos pueden ser vulnerables a accesos indebidos o manipulaciones no autorizadas. Esta falta de coordinación en la gestión de datos distribuidos puede generar inconsistencias en la información almacenada, afectando su integridad y fiabilidad (Troncoso Reigada & González Rivas, 2021).

Riesgos asociados a la nube híbrida

El uso de entornos de nube híbrida ha permitido a las organizaciones optimizar sus procesos de almacenamiento y procesamiento de datos combinando infraestructuras locales con servicios en la nube. Sin embargo, este modelo introduce desafíos significativos en términos de seguridad y privacidad, ya que la información puede estar distribuida en múltiples jurisdicciones con diferentes regulaciones y estándares de protección de datos.

Uno de los principales riesgos de la nube híbrida es la dificultad de aplicar medidas de seguridad unificadas en entornos heterogéneos. Mientras que los sistemas locales suelen contar con controles estrictos de acceso y políticas de protección bien definidas, los servicios en la nube pueden operar bajo normativas distintas, lo que puede generar inconsistencias en la protección de los datos almacenados. Además, la dependencia de proveedores externos implica que la responsabilidad de la seguridad de la información no siempre es clara, lo que puede dar lugar a vulnerabilidades explotables por atacantes (Quintero Acevedo, 2023).

Otro problema crítico en la nube híbrida es el acceso no autorizado a la información por parte de empleados internos o administradores de los servicios en la nube. En muchos casos, las organizaciones confían en terceros para la gestión de su infraestructura tecnológica, lo que significa que estos proveedores tienen acceso a datos sensibles sin

mecanismos adecuados de auditoría y control. Si no se implementan políticas estrictas de gestión de identidad y autenticación, existe el riesgo de que la información sea accedida o manipulada indebidamente (Quintero Acevedo, 2023).

La privacidad de los datos en la nube híbrida puede verse comprometida por la transferencia de información entre diferentes entornos. Si los datos no están cifrados correctamente durante su tránsito, pueden ser interceptados por actores malintencionados, lo que representa una amenaza significativa para la confidencialidad de la información. La falta de una estrategia integral de protección en la nube híbrida puede exponer a las organizaciones a brechas de seguridad y posibles sanciones por incumplimiento de normativas de protección de datos (Quintero Acevedo, 2023).

Las amenazas a la seguridad y privacidad en los sistemas de información distribuidos son cada vez más complejas debido a la evolución de las técnicas de ataque y la creciente interconectividad de plataformas tecnológicas. La sofisticación de los ataques cibernéticos dirigidos, la falta de estandarización en la interoperabilidad y los desafíos en la gestión de la nube híbrida representan riesgos significativos que requieren medidas de protección avanzadas. Para mitigar estos peligros, es fundamental implementar estrategias de seguridad robustas, como el cifrado de datos, la autenticación multifactor y la auditoría continua de accesos, garantizando así la integridad y confidencialidad de la información en entornos distribuidos.

3.2. Estrategias de protección y mitigación de riesgos

Ante las crecientes amenazas que enfrentan los sistemas de información distribuidos, es fundamental implementar estrategias de protección y mitigación de riesgos que garanticen la seguridad y privacidad de los datos. La sofisticación de los ataques cibernéticos y las vulnerabilidades asociadas a la interoperabilidad exigen el uso de tecnologías avanzadas para prevenir accesos no autorizados, detectar actividades sospechosas y proteger la integridad de la información. Dentro de las principales estrategias se encuentran la criptografía y cifrado de datos, la autenticación y control de acceso, y el monitoreo con inteligencia artificial para la detección de intrusos.

Criptografía y cifrado de datos

El cifrado de datos es una de las técnicas más efectivas para garantizar la confidencialidad y evitar el acceso indebido a la información almacenada en sistemas distribuidos. Consiste en la conversión de los datos en un formato ilegible sin la clave de desencriptación correspondiente, protegiéndolos contra accesos no autorizados. En entornos distribuidos y de computación en la nube, la criptografía es esencial para mitigar riesgos relacionados con la interceptación de datos en tránsito y el almacenamiento en servidores remotos (Abbas et al., 2021).

Los algoritmos de cifrado más utilizados incluyen AES (Advanced Encryption Standard) y RSA (Rivest-Shamir-Adleman), los cuales ofrecen altos niveles de seguridad en la protección de información sensible. Sin embargo, la implementación de estas tecnologías debe ir acompañada de una gestión adecuada de claves criptográficas, ya que una administración deficiente podría comprometer la efectividad del cifrado. En este sentido, Abbas et al. (2021) destacan la importancia de utilizar mecanismos de gestión segura de claves, como el almacenamiento distribuido y la rotación periódica, para minimizar el riesgo de exposición de datos cifrados.

Además, el concepto de "data provenance" ha cobrado relevancia en la seguridad de la nube, ya que permite rastrear el origen y las modificaciones realizadas sobre los datos cifrados. Este enfoque facilita auditorías de seguridad y la identificación de accesos sospechosos en sistemas distribuidos, mejorando así la capacidad de respuesta ante incidentes (Abiodun et al., 2022).

Autenticación y control de acceso

El control de acceso y la autenticación robusta son medidas fundamentales para proteger los sistemas de información distribuidos contra accesos indebidos. La autenticación multifactor (MFA) ha demostrado ser una estrategia efectiva para reforzar la seguridad, combinando múltiples factores de verificación, como contraseñas, biometría y códigos de un solo uso. Esta metodología reduce significativamente la probabilidad de que actores malintencionados obtengan acceso a los sistemas, incluso si logran vulnerar una credencial individual (Abiodun et al., 2022).

Otro aspecto relevante en el control de acceso es la gestión de identidades, que permite restringir permisos y definir roles específicos para cada usuario dentro del sistema. El uso de modelos de acceso basado en roles (RBAC) y acceso basado en atributos (ABAC) permite establecer restricciones dinámicas según el contexto y nivel de riesgo de cada sesión de usuario. De acuerdo con Robalino-Latorre et al. (2023), la integración de modelos de control de acceso con técnicas de inteligencia artificial puede mejorar la detección de patrones anómalos en la autenticación, alertando sobre intentos de acceso no autorizados y posibles ataques internos.

El acceso a la información en entornos distribuidos debe estar regulado mediante protocolos de seguridad como OAuth y SAML, que garantizan la autenticación federada y la transmisión segura de credenciales entre plataformas. La implementación de estos protocolos permite que diferentes sistemas interconectados puedan compartir información de autenticación sin exponer las credenciales originales del usuario, reduciendo así el riesgo de robo de identidad y accesos indebidos (Abiodun et al., 2022).

Monitoreo y detección de intrusos

El monitoreo continuo y la detección de intrusos son estrategias esenciales para identificar comportamientos sospechosos y prevenir ataques en tiempo real. La inteligencia artificial (IA) y el aprendizaje automático han revolucionado los sistemas de seguridad, permitiendo la identificación automática de patrones anómalos en el tráfico de red y el acceso a datos sensibles (Erazo-Luzuriaga et al., 2023).

El uso de IA en la ciberseguridad se basa en algoritmos capaces de analizar grandes volúmenes de datos para detectar actividades inusuales que podrían indicar un intento de intrusión o una posible vulnerabilidad en el sistema. Tecnologías como el *deep learning* han mejorado la precisión de estos sistemas, permitiendo una respuesta proactiva ante amenazas emergentes. Según Erazo-Luzuriaga et al. (2023), la optimización de programas informáticos mediante inteligencia artificial ha permitido mejorar la detección temprana de ataques cibernéticos, reduciendo la tasa de falsos positivos y aumentando la eficacia de los sistemas de monitoreo.

Otra técnica relevante es el análisis de registros (*log analysis*), que permite rastrear eventos dentro de los sistemas y detectar intentos de acceso no autorizados. La

combinación de IA con herramientas de análisis de registros facilita la correlación de eventos sospechosos y la generación de alertas en tiempo real, lo que contribuye a una respuesta rápida ante incidentes de seguridad (Montalván-Vélez et al., 2024).

La implementación de sistemas de detección y prevención de intrusos (IDPS) basados en IA permite el bloqueo automático de accesos no autorizados y ataques en curso, fortaleciendo la resiliencia de los sistemas distribuidos. Estos sistemas pueden integrarse con herramientas de *Security Information and Event Management* (SIEM) para centralizar la gestión de alertas de seguridad y facilitar la toma de decisiones basada en datos (Montalván-Vélez et al., 2024).

Las estrategias de protección y mitigación de riesgos en sistemas de información distribuidos deben basarse en un enfoque integral que combine cifrado avanzado, autenticación robusta y monitoreo continuo con inteligencia artificial. La criptografía garantiza la confidencialidad de los datos, mientras que el control de acceso impide accesos no autorizados y el monitoreo inteligente permite la detección temprana de amenazas. La implementación de estas medidas es crucial para fortalecer la seguridad de los sistemas distribuidos y reducir el impacto de los ataques cibernéticos en la privacidad y disponibilidad de la información.

3.3. Desafíos y perspectivas futuras en la seguridad de datos distribuidos

El crecimiento exponencial de los sistemas de información distribuidos ha traído consigo nuevos desafíos en materia de seguridad y privacidad de los datos. La descentralización de la información y la dependencia de infraestructuras externas, como la computación en la nube, han incrementado la necesidad de regulaciones más estrictas, tecnologías innovadoras y formación continua en ciberseguridad. Para garantizar la protección de la información en estos entornos, es esencial abordar tres aspectos fundamentales: el cumplimiento normativo y la regulación, la adopción de innovaciones tecnológicas y la capacitación de los usuarios en estrategias de protección.

Cumplimiento normativo y regulación

Uno de los principales retos en la seguridad de datos distribuidos es la falta de una regulación homogénea a nivel internacional. Las diferencias en las normativas de protección de datos entre países complican la implementación de políticas de seguridad unificadas, lo que puede derivar en brechas de cumplimiento y exposición de información sensible. En este sentido, los marcos regulatorios desarrollados por instituciones como el National Institute of Standards and Technology (NIST, 2011) establecen principios clave para garantizar la seguridad jurídica en la gestión de datos en la nube, promoviendo el uso de buenas prácticas en cifrado, control de accesos y auditorías de seguridad.

La adopción de regulaciones específicas para la protección de datos en entornos digitales también se ha vuelto una prioridad en sectores como la educación y el comercio electrónico. Benites Medina et al. (2024) destacan que las instituciones de educación superior enfrentan desafíos en la protección de los datos de sus estudiantes, particularmente en plataformas de marketing digital que recopilan información personal sin mecanismos adecuados de anonimización. Este problema es aún más grave en sistemas distribuidos, donde los datos pueden almacenarse en múltiples servidores ubicados en distintas jurisdicciones con regulaciones variables.

Omaza (2020) resalta la importancia de implementar arquitecturas de seguridad en la nube que cumplan con los estándares internacionales y regulaciones locales, permitiendo a las organizaciones gestionar adecuadamente la privacidad de la información. Sin embargo, muchas empresas aún no han adoptado medidas efectivas para cumplir con estas normativas, lo que deja sus sistemas vulnerables a ataques y sanciones legales. La falta de capacitación en el ámbito normativo también representa un obstáculo significativo, ya que muchos administradores desconocen las obligaciones legales en materia de protección de datos.

Innovaciones tecnológicas en ciberseguridad

El desarrollo de nuevas tecnologías ha abierto oportunidades para fortalecer la seguridad de los datos en sistemas distribuidos. Soluciones basadas en blockchain, redes neuronales artificiales y computación cuántica están revolucionando la ciberseguridad, ofreciendo enfoques innovadores para mitigar amenazas emergentes.

La tecnología blockchain ha demostrado ser una herramienta eficaz para garantizar la integridad y trazabilidad de los datos en entornos distribuidos. García-Peña (2023) señala que su aplicación en la seguridad digital permite descentralizar la gestión de la información y evitar modificaciones no autorizadas en bases de datos, lo que reduce significativamente el riesgo de manipulación fraudulenta. Este enfoque es particularmente útil en sistemas financieros y gubernamentales, donde la inmutabilidad de los registros es esencial para garantizar la transparencia y confiabilidad de la información.

Las redes neuronales artificiales y la inteligencia artificial han mejorado la detección de amenazas cibernéticas mediante el análisis en tiempo real de patrones sospechosos en grandes volúmenes de datos. Sánchez-Caguana et al. (2024) destacan que la implementación de inteligencia artificial en sistemas contables ha permitido mejorar la precisión y eficiencia en la detección de irregularidades, lo que sugiere un alto potencial para su aplicación en la ciberseguridad de infraestructuras distribuidas.

La computación cuántica plantea tanto oportunidades como desafíos en el ámbito de la seguridad. Telo (2023) menciona que las tecnologías emergentes en ciudades inteligentes están adoptando enfoques cuánticos para reforzar la seguridad de los datos, pero también advierte que los sistemas criptográficos actuales podrían quedar obsoletos ante la capacidad de procesamiento de los ordenadores cuánticos. Esto obliga a las organizaciones a prepararse para una transición hacia algoritmos de cifrado post-cuánticos que sean resistentes a ataques de gran escala.

Otro enfoque tecnológico en la ciberseguridad es el análisis de datos forenses en la nube. Abiodun et al. (2022) enfatizan la importancia de la trazabilidad y la recolección de pruebas digitales en entornos distribuidos, lo que facilita la investigación de incidentes de seguridad y la identificación de vulnerabilidades explotadas por los atacantes. Esta metodología es clave para mejorar la capacidad de respuesta ante incidentes y reforzar las estrategias de protección en infraestructuras críticas.

Concienciación y formación en seguridad

A pesar de los avances tecnológicos, el factor humano sigue siendo uno de los eslabones más débiles en la seguridad de los datos distribuidos. La falta de

concienciación sobre ciberseguridad y la ausencia de formación especializada en protección de datos aumentan la probabilidad de que errores humanos comprometan la integridad de los sistemas.

Del Pino et al. (2023) subrayan que la educación en ciberseguridad es esencial para reducir los riesgos asociados al uso inadecuado de tecnologías digitales. En el ámbito educativo, los docentes y estudiantes deben ser instruidos en prácticas seguras, como la gestión adecuada de contraseñas y el reconocimiento de ataques de *phishing*. Este enfoque también es aplicable a sectores empresariales, donde la falta de capacitación en ciberseguridad facilita la explotación de vulnerabilidades por parte de atacantes.

Erazo-Luzuriaga (2024) enfatiza que la integración de las TIC en entornos laborales y educativos debe ir acompañada de programas de formación en seguridad digital. Sin esta capacitación, los usuarios pueden convertirse en el punto de acceso más vulnerable para los ciberdelincuentes, exponiendo datos críticos a riesgos de filtración o manipulación indebida.

Sivan & Zukarnain (2021) advierten que los sistemas de salud basados en la nube requieren una formación constante en privacidad y seguridad, ya que los datos médicos son altamente sensibles y pueden ser objeto de ataques dirigidos. La implementación de programas de formación específicos para profesionales de la salud y administradores de sistemas permitiría reducir el riesgo de incidentes y mejorar la gestión de la información médica.

La expansión del uso de aplicaciones móviles en la gestión de datos distribuidos plantea nuevos retos en términos de formación en ciberseguridad. García-Peña (2023) destaca que la proliferación de aplicaciones móviles en el ámbito ecuatoriano ha incrementado la exposición de datos personales, lo que resalta la importancia de educar a los usuarios sobre la configuración de privacidad y la adopción de buenas prácticas en seguridad digital.

Los desafíos en la seguridad de datos distribuidos exigen un enfoque integral que combine cumplimiento normativo, innovación tecnológica y formación continua en ciberseguridad. La adopción de estándares internacionales permite establecer bases sólidas para la protección de la información, mientras que tecnologías emergentes como blockchain, inteligencia artificial y computación cuántica ofrecen nuevas soluciones para mitigar riesgos. Sin embargo, ninguna estrategia será completamente efectiva sin una adecuada concienciación y formación de los usuarios, quienes juegan un papel clave en la prevención de incidentes de seguridad. A medida que los sistemas distribuidos continúan expandiéndose, será fundamental fortalecer la colaboración entre reguladores, investigadores y profesionales de la seguridad para garantizar un entorno digital más seguro y resiliente.

4. Discusión

La seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos constituye un desafío crucial en la era digital. La creciente interconexión de infraestructuras tecnológicas y la expansión del uso de la computación en la nube han intensificado las vulnerabilidades a las que están expuestos estos entornos. En este

contexto, la literatura revisada resalta tres ejes fundamentales que impactan la seguridad de estos sistemas: la proliferación de amenazas cibernéticas, la evolución de estrategias de mitigación de riesgos y los desafíos futuros en la protección de la información distribuida.

Uno de los aspectos más críticos analizados es la sofisticación de los ataques cibernéticos dirigidos, entre los que destacan el *ransomware*, el *phishing* y los ataques de denegación de servicio distribuido (DDoS). Según Troncoso Reigada y González Rivas (2021), el *ransomware* ha evolucionado en los últimos años hasta convertirse en una de las amenazas más devastadoras para organizaciones con infraestructuras distribuidas, debido a su capacidad para cifrar información crítica y exigir rescates financieros. De igual manera, el *phishing* sigue siendo un vector de ataque predominante, aprovechando la ingeniería social para obtener credenciales de acceso a sistemas vulnerables (Rosa Rodríguez, 2021). Estos métodos se han potenciado con el auge del acceso remoto y la descentralización del almacenamiento de datos, lo que facilita la explotación de fallos humanos y técnicos en la administración de credenciales y en los protocolos de autenticación.

En este mismo orden de ideas, la interoperabilidad entre plataformas de diferentes proveedores introduce desafíos adicionales en la seguridad de los datos distribuidos. Como señala Quintero Acevedo (2023), la falta de estandarización en la gestión de datos y la diversidad de protocolos de seguridad dificultan la aplicación de medidas homogéneas de protección, lo que incrementa la exposición a accesos no autorizados y filtraciones de información. Esta problemática se ve agravada en entornos de nube híbrida, donde la combinación de infraestructuras locales y servicios en la nube complica la implementación de políticas de seguridad integradas. En este sentido, Velásquez Acevedo (2022) destaca la necesidad de modelos de gobernanza de datos que permitan establecer controles estrictos sobre la información almacenada en sistemas distribuidos, garantizando su confidencialidad y disponibilidad sin comprometer la interoperabilidad.

Ante este panorama, diversas estrategias han sido propuestas para mitigar los riesgos asociados a la seguridad en sistemas de información distribuidos. Entre ellas, el cifrado de datos juega un papel fundamental, pues su implementación adecuada permite resguardar la información frente a accesos no autorizados. Abbas et al. (2021) destacan que el uso de algoritmos criptográficos robustos, como AES y RSA, ha demostrado ser una solución eficaz para la protección de datos en tránsito y en reposo, aunque advierten que su correcta implementación depende de una adecuada gestión de claves criptográficas. Además, Abiodun et al. (2022) subrayan la importancia de la trazabilidad de los datos a través de la tecnología *data provenance*, la cual facilita auditorías de seguridad y la detección de accesos indebidos en entornos distribuidos.

Otro elemento clave en la mitigación de riesgos es el control de acceso y la autenticación multifactor, dado que los ataques a credenciales siguen representando una amenaza recurrente en estos sistemas. Según Robalino-Latorre et al. (2023), los modelos de acceso basado en roles (RBAC) y en atributos (ABAC) han permitido mejorar la seguridad en entornos distribuidos al restringir permisos y establecer controles dinámicos según el nivel de riesgo. Paralelamente, el uso de herramientas de monitoreo y detección de intrusos basadas en inteligencia artificial ha demostrado ser una estrategia efectiva para la identificación de actividades sospechosas y la prevención de ataques en tiempo real (Erazo-Luzuriaga et al., 2023).

A pesar de estos avances, persisten importantes desafíos y perspectivas futuras en la seguridad de datos distribuidos, especialmente en lo que respecta al cumplimiento normativo y la adopción de nuevas tecnologías. La ausencia de regulaciones homogéneas a nivel global dificulta la implementación de políticas de protección consistentes, lo que deja expuestas a muchas organizaciones a riesgos legales y operativos (Benites Medina et al., 2024). En este sentido, el *National Institute of Standards and Technology* (NIST, 2011) ha desarrollado marcos regulatorios que establecen principios clave para la protección de datos en la nube, aunque su adopción aún es limitada en algunos sectores.

La innovación tecnológica sigue siendo un factor determinante en la evolución de la ciberseguridad en entornos distribuidos. García-Peña (2023) señala que la tecnología *blockchain* ha emergido como una alternativa prometedora para garantizar la inmutabilidad de los registros en sistemas de información distribuidos, reduciendo los riesgos de manipulación de datos. Por su parte, Sánchez-Caguana et al. (2024) resaltan el potencial de la inteligencia artificial y las redes neuronales en la detección temprana de amenazas, lo que podría revolucionar la capacidad de respuesta ante incidentes de seguridad. Sin embargo, Telo (2023) advierte que la computación cuántica plantea un desafío significativo para los sistemas criptográficos actuales, dado que su capacidad de procesamiento podría vulnerar los algoritmos de cifrado convencionales en un futuro cercano, obligando a la adopción de nuevas estrategias de protección post-cuántica.

La concienciación y formación en seguridad informática sigue siendo una asignatura pendiente en la gestión de datos distribuidos. Del Pino et al. (2023) enfatizan que la falta de capacitación sobre buenas prácticas de ciberseguridad es una de las principales causas de incidentes de seguridad, lo que pone de manifiesto la necesidad de programas de formación continua para usuarios y administradores de sistemas. En este mismo sentido, Sivan y Zukarnain (2021) sostienen que en sectores como la salud, donde la información almacenada es altamente sensible, la capacitación del personal es crucial para minimizar riesgos y fortalecer la protección de los datos.

5. Conclusiones

La seguridad y privacidad en el almacenamiento de datos en sistemas de información distribuidos es un desafío crítico en la actualidad, donde el crecimiento de la digitalización y la interconectividad ha incrementado la exposición a amenazas cibernéticas. La descentralización de la información y el uso de infraestructuras en la nube han permitido una mayor eficiencia en la gestión de datos, pero también han generado vulnerabilidades que deben abordarse con estrategias de protección avanzadas. La necesidad de garantizar la confidencialidad, integridad y disponibilidad de la información en estos entornos requiere la adopción de enfoques multidisciplinarios que combinen regulaciones adecuadas, innovaciones tecnológicas y capacitación continua en ciberseguridad.

Las amenazas cibernéticas que afectan a los sistemas distribuidos han evolucionado en términos de sofisticación y capacidad de impacto. Ataques como el *ransomware*, el *phishing* y las denegaciones de servicio distribuido (DDoS) representan riesgos constantes para la operatividad de estos sistemas, comprometiendo tanto la información

almacenada como la estabilidad de las infraestructuras tecnológicas. La facilidad con la que los atacantes pueden explotar vulnerabilidades en la gestión de accesos y en la interoperabilidad de plataformas demuestra que la seguridad debe ser una prioridad en el diseño e implementación de sistemas distribuidos. La falta de estandarización en la seguridad de datos entre diferentes plataformas y proveedores también se presenta como un problema relevante, ya que dificulta la aplicación de políticas homogéneas de protección y genera riesgos de accesos no autorizados a información sensible.

Para mitigar estos riesgos, se han desarrollado diversas estrategias que buscan reforzar la seguridad en los sistemas distribuidos. El uso de técnicas de cifrado avanzadas es una de las principales soluciones, pues garantiza que los datos sean inaccesibles para actores no autorizados incluso en caso de una brecha de seguridad. La implementación de modelos de autenticación multifactor y de control de acceso basado en roles ha demostrado ser eficaz para restringir el acceso a la información únicamente a usuarios autorizados. Además, el monitoreo y la detección de intrusos mediante inteligencia artificial han permitido mejorar la capacidad de respuesta ante incidentes de seguridad, identificando patrones de comportamiento sospechosos y previniendo ataques antes de que causen daños significativos. Sin embargo, la efectividad de estas estrategias depende de su correcta implementación y de la actualización constante de las medidas de protección en función de las amenazas emergentes.

Uno de los mayores retos que enfrenta la seguridad en sistemas distribuidos es la falta de una regulación global uniforme que establezca estándares claros sobre la protección de datos. La diversidad de normativas en diferentes países genera incertidumbre en la gestión de la seguridad y dificulta la adopción de prácticas homogéneas entre organizaciones que operan en múltiples jurisdicciones. La implementación de marcos regulatorios específicos para la protección de datos en la nube y en sistemas distribuidos resulta fundamental para garantizar la seguridad jurídica y evitar brechas normativas que puedan ser explotadas por atacantes. Además, la regulación debe evolucionar a la par de las innovaciones tecnológicas, asegurando que las nuevas herramientas de seguridad sean compatibles con las exigencias legales y que las organizaciones puedan adaptarse a los cambios en el panorama digital sin comprometer la protección de la información.

El avance de la tecnología ha abierto nuevas oportunidades para reforzar la seguridad de los datos en entornos distribuidos. Soluciones emergentes como la tecnología *blockchain*, la inteligencia artificial aplicada a la ciberseguridad y la computación cuántica han comenzado a transformar la manera en que se protegen los datos y se previenen ataques. La descentralización y la inmutabilidad de *blockchain* han demostrado ser herramientas útiles para garantizar la integridad de la información, mientras que la inteligencia artificial ha permitido mejorar la detección y respuesta ante amenazas en tiempo real. No obstante, el desarrollo de la computación cuántica plantea un desafío adicional, ya que su capacidad para resolver problemas complejos en tiempos reducidos podría poner en riesgo los sistemas criptográficos actuales, haciendo necesaria la transición hacia nuevos modelos de cifrado post-cuántico.

Además de la implementación de tecnologías avanzadas, la concienciación y formación en ciberseguridad sigue siendo un factor determinante en la protección de los datos en sistemas distribuidos. El error humano sigue siendo una de las principales causas de incidentes de seguridad, ya sea por una gestión inadecuada de credenciales, la falta de

actualización de software o la apertura involuntaria de puertas de acceso a atacantes mediante prácticas inseguras. La educación en ciberseguridad debe ser una prioridad tanto en el ámbito empresarial como en el académico, fomentando la adopción de buenas prácticas que minimicen los riesgos asociados a la administración de datos en entornos distribuidos. La capacitación constante y la promoción de una cultura de seguridad digital permitirán fortalecer la resiliencia de los sistemas y reducir la vulnerabilidad frente a ataques.

En síntesis, la protección de los datos en sistemas de información distribuidos es un reto que requiere un enfoque integral y dinámico. La combinación de estrategias de cifrado, control de acceso, monitoreo con inteligencia artificial y cumplimiento normativo resulta esencial para garantizar la seguridad de la información en estos entornos. Sin embargo, la rápida evolución de las amenazas cibernéticas exige una actualización constante de los mecanismos de defensa, así como la adopción de tecnologías innovadoras que permitan anticiparse a los riesgos emergentes. La cooperación entre reguladores, desarrolladores tecnológicos, organizaciones y usuarios será clave para la construcción de un ecosistema digital más seguro y confiable en el futuro.

Referencias Bibliográficas

Abbas, H., Jaaz, Z., Al Barazanchi, I., & Abdulshaheed, H. (2021). Survey on Enhanced Security Control measures in Cloud Computing systems. Journal of Physics: Conference Series, 1878, 012004. https://doi.org/10.1088/1742-6596/1878/1/012004

Abiodun, O., Alawida, M., Omolara, A & Alabdulatif, A. (2022). Data provenance for cloud forensic investigations, security, challenges, solutions and future perspectives: A survey, Journal of King Saud University - Computer and Information Sciences, (Vol 34, Pag 10217-10245). https://doi.org/10.1016/j.jksuci.2022.10.018

Asencios Mory, A. J., & Pacherres Paredes, M. A. (2023). Análisis comparativo de Odoo en un servidor de la nube vs un servidor local en relación a la privacidad y seguridad de los datos en una empresa tecnológica. https://hdl.handle.net/20.500.12692/131439

Benites Medina, R. M., Erazo Álvarez, J. C., & Narváez Zurita, C. I. (2024). Protección de datos de estudiantes en Marketing Digital: un desafío para las Instituciones de Educación Superior. *Conrado*, *20*(98), 124-131. http://scielo.sld.cu/scielo.php?pid=S1990-86442024000300124&script=sci_arttext

del Pino, M. S., Permisán, C. G., & Oliva, M. F. R. (2023). Formación del profesorado sobre control, seguridad y privacidad en internet. *Revista de ciencias sociales*, *29*(1), 47-64. https://dialnet.unirioja.es/servlet/articulo?codigo=8822426

Erazo-Luzuriaga, A. F. (2024). Integración de las TICs en el aula: Un análisis de su impacto en el rendimiento académico. *Revista Científica Zambos, 3*(1), 56-72. https://doi.org/10.69484/rcz/v3/n1/12

Erazo-Luzuriaga, A. F., Ramos-Secaira, F. M., Galarza-Sánchez, P. C., & Boné-Andrade, M. F. (2023). La inteligencia artificial aplicada a la optimización de programas informáticos. *Journal of Economic and Social Science Research*, *3*(1), 48–63. https://doi.org/10.55813/gaea/jessr/v3/n1/61

García-Peña, V. R. (2023). Desarrollo y Uso de Aplicaciones Móviles en el Contexto Ecuatoriano. *Revista Científica Zambos*, *2*(3), 1-15. https://doi.org/10.69484/rcz/v2/n3/46

Gil, A. J. L., Dionicio, P. O. G., & De Los Santos, A. C. M. (2023). Principales medidas de seguridad para la protección de información y datos en la nube: una revisión sistemática. *INGENIERÍA INVESTIGA*, *5*. https://doi.org/10.47796/ing.v5i0.796

Montalván-Vélez, C. L., Mogrovejo-Zambrano, J. N., Romero-Vitte, I. J., & Pinargote-Carrera, M. L. D. C. (2024). Introducción a la Inteligencia Artificial: Conceptos Básicos y Aplicaciones Cotidianas . *Journal of Economic and Social Science Research*, *4*(1), 173–183. https://doi.org/10.55813/gaea/jessr/v4/n1/93

National Institute of Standards and Technology. (2011). Cloud Computing [Special Publication 800-145]. https://doi.org/10.6028/NIST.SP.800-145

Omaza, K. (2020). Arquitectura de Seguridad en la nube: Revisión de la Implementación en AWS(Trabajo de fin de grado,Universidad politécnica de madrid). https://oa.upm.es/58279/1/TFG_KIYOSHI_JOSE_OMAZA_SALDANA.pdf

Quintero Acevedo, N. (2023). Seguridad y privacidad en la Nube, fortalezas y vulnerabilidades: Recomendaciones para tener en cuenta con los proveedores de servicios de la nube. http://hdl.handle.net/1992/66531

Robalino-Latorre, M. C., Ramirez-Klinger, W. N., Guadalupe-Copa, R. C., & Cuello-García, S. A. (2023). Aplicación del Método Montecarlo en flujo de potencias a través del Software Octave. *Journal of Economic and Social Science Research*, *3*(1), 31–47. https://doi.org/10.55813/gaea/jessr/v3/n1/60

Rosa Rodríguez, P. I. D. L. (2021). Aplicaciones educativas digitales y la falta de seguridad de los datos personales de sus usuarios. *RIDE. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *12*(23). https://doi.org/10.23913/ride.v12i23.980

Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. *Journal of Economic and Social Science Research*, *4*(3), 1–12. https://doi.org/10.55813/gaea/jessr/v4/n3/117

Sivan, R. & Zukarnain, Z. (2021). Security and Privacy in Cloud-Based E-Health System.Symmetry,13,5. https://doi.org/10.3390/sym13050742

Telo, J. (2023). Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing, 6(1), 31–45. https://research.tensorgate.org/index.php/IJIAC/article/view/18

Troncoso Reigada, A., & González Rivas, J. J. (2021). *Comentario al Reglamento general de protección de datos ya la Ley orgánica de protección de datos personales y garantía de los derechos digitales*. Thomson Reuters Aranzadi. https://produccioncientifica.uca.es/documentos/60a5b3ab12012f5be2d27ac0

Urquijo Morales, Y., Orellana García, A., & Vega Izaguirre, L. (2023). Seguridad de los datos: El desafío de la historia clínica en la nube. https://repositorio.uci.cu/handle/123456789/10693

Velásquez Acevedo, E. (2022). Metodología de evaluación para preservar la seguridad y privacidad de la información en la interoperabilidad de nubes híbridas, tomando como modelo de prueba un entorno virtual experimental. https://repositorio.itm.edu.co/handle/20.500.12622/5786