https://doi.org/10.69639/arandu.v13i1.2011

Análisis comparativo de seguridad y gestión de archivos en herramientas Cloud: Google Drive vs. Microsoft OneDrive vs. Dropbox

Comparative analysis of security and file management in cloud tools: Google Drive vs. Microsoft OneDrive vs. Dropbox

Ángel Mauricio Ramón Noblecilla
aramon@utmachala.edu.ec
https://orcid.org/0000-0003-4310-8321
Universidad Técnica de Machala
Machala – Ecuador

Amanda Carolina Herrera Peña
carolinaherrerapena0@gmail.com
https://orcid.org/0009-0001-9601-2908
Universidad Técnica de Machala
Milagro-Ecuador

Jazmín Alejandra Durán Capa
jazzduran1@gmail.com
https://orcid.org/0009-0008-2559-6767
Universidad Técnica de Machala
Quito – Ecuador

Kevin David Cruz Pazmiño
tics@teclemas.edu.ec
https://orcid.org/0000-0002-5637-957X
Instituto Superior Tecnológico LEMAS
Guayaquil -Ecuador

Alejandro Mauricio Salinas Castro
alexsan58@hotmail.com
https://orcid.org/0009-0006-9863-9209
Universidad Técnica de Machala
Guayaquil -Ecuador

Artículo recibido: 18 enero 2026-Aceptado para publicación: 20 febrero 2026
Conflictos de intereses: Ninguno que declarar.

RESUMEN

En la actualidad, donde todo el mundo guarda sus archivos en la nube, de forma independiente si son personales, corporativos, triviales o de gran importancia, es necesario identificar qué plataforma protege mejor dichos documentos, Google Drive, Microsoft OneDrive o Dropbox. El presente artículo analiza comparativamente la seguridad y la gestión documental en las plataformas mencionadas y que son ampliamente utilizadas en contextos organizacionales. El objetivo es evaluar su robustez en cifrado, autenticación, controles de acceso, auditoría, gobierno de datos y cumplimiento normativo, identificando fortalezas, debilidades y escenarios de uso más

adecuados. En la parte metodológica, Se emplea un enfoque mixto, combinando revisión documental sistemática de fuentes oficiales y académicas con pruebas funcionales estandarizadas en cuentas empresariales, utilizando matrices de análisis, listas de chequeo y guías de observación. Los resultados muestran que OneDrive alcanza la mayor madurez en autenticación, auditoría y gobierno de la información cuando se integra con Microsoft 365, Google Drive ofrece un nivel de seguridad robusto y una colaboración especialmente eficiente en el ecosistema Workspace y Dropbox destaca por su simplicidad, rapidez de configuración y adecuación para PYMES y equipos distribuidos. Se concluye que la elección de la plataforma debe basarse en el perfil organizacional, el ecosistema tecnológico existente y las exigencias regulatorias. Se proponen futuras investigaciones con estudios de caso reales y la inclusión de otros proveedores y funciones basadas en inteligencia artificial.

Palabras clave: Gestión de archivos, herramientas Cloud, almacenamiento en la nube, seguridad de la información

ABSTRACT

Today, everyone stores their files in the cloud, regardless of whether they are personal, corporate, trivial, or critical. It's essential to identify which platform best protects these documents: Google Drive, Microsoft OneDrive, or Dropbox. This article comparatively analyzes the security and document management of these platforms, which are widely used in organizational contexts. The objective is to evaluate their robustness in encryption, authentication, access controls, auditing, data governance, and regulatory compliance, identifying strengths, weaknesses, and the most suitable use cases. In the methodological section, a mixed-methods approach is employed, combining a systematic review of official and academic sources with standardized functional testing on business accounts, using analysis matrices, checklists, and observation guides. The results show that OneDrive achieves the highest maturity in authentication, auditing, and information governance when integrated with Microsoft 365, Google Drive offers a robust level of security and particularly efficient collaboration within the Workspace ecosystem, and Dropbox stands out for its simplicity, speed of setup, and suitability for SMEs and distributed teams. It is concluded that the choice of platform should be based on the organizational profile, the existing technological ecosystem, and regulatory requirements. Future research is proposed, including real-world case studies and the inclusion of other providers and AI-based features

Keywords: File management, cloud tools, cloud storage, information security

INTRODUCCIÓN

La adopción masiva de servicios de almacenamiento en la nube ha transformado profundamente la forma en que organizaciones y usuarios gestionan, comparten y resguardan su información digital (Ortiz et al., 2024). Entre las soluciones más extendidas a escala global destacan Google Drive, Microsoft OneDrive y Dropbox, plataformas que se han consolidado como componentes críticos de la infraestructura tecnológica en empresas, instituciones educativas y administraciones públicas. Para Fargana (2023) Estas herramientas no solo ofrecen capacidad de almacenamiento y sincronización entre dispositivos, sino que integran funciones avanzadas de colaboración en tiempo real, control de versiones y acceso remoto, configurándose como piezas esenciales en entornos de teletrabajo, trabajo híbrido y transformación digital.

El problema central que aborda este estudio radica en la falta de análisis comparativos sistemáticos y rigurosos que integren simultáneamente los aspectos de seguridad y de gestión de archivos en estas tres plataformas de referencia. La literatura existente suele centrarse en evaluaciones parciales, revisando características de una única herramienta o atendiendo solo a dimensiones específicas, como el cifrado o el cumplimiento regulatorio, sin considerar la experiencia de gestión de archivos, el gobierno de la información ni el impacto operativo en las organizaciones (Alshayeji & Abed, 2022).

Esta fragmentación dificulta la toma de decisiones informadas por parte de responsables de TI, gestores de seguridad y directivos que deben seleccionar, configurar o migrar entre servicios Cloud en función de requisitos de confidencialidad, integridad, disponibilidad y cumplimiento legal (Rezqallah y otros, 2023).

La relevancia del estudio se fundamenta en la creciente dependencia de servicios Cloud para almacenar información sensible, incluyendo datos personales, propiedad intelectual y documentación estratégica. En un contexto marcado por marcos regulatorios cada vez más estrictos y por un aumento sostenido de incidentes de ciberseguridad, disponer de un análisis comparativo detallado de Google Drive, Microsoft OneDrive y Dropbox adquiere un valor estratégico (Shameer et al., 2023). Este trabajo aspira a proporcionar evidencia sólida que oriente decisiones de adopción y configuración, contribuyendo a reducir riesgos, optimizar la gestión de archivos y fortalecer la gobernanza de la información en organizaciones de distintos tamaños y sectores.

El trabajo se sostiene en un marco teórico interdisciplinario que integra aportes de la seguridad de la información, la gobernanza de datos en la nube y los modelos contemporáneos de gestión de riesgos tecnológicos (Navin & Rekha, 2023). En el ámbito de la seguridad, se retoman los principios del modelo de zero trust, según el cual ningún usuario, dispositivo o solicitud debe ser considerado confiable por defecto y el acceso a los recursos se concede únicamente tras verificación explícita, aplicación del mínimo privilegio y monitoreo continuo.

Dichos trabajos, se articulan con los fundamentos de la protección de datos en entornos Cloud, donde el cifrado en tránsito y en reposo, el control de acceso granular, la autenticación multifactor y la segmentación lógica de recursos se consideran variables clave para mitigar amenazas y limitar el movimiento lateral de atacantes (ThiBac & Hieu, 2022). Desde la perspectiva de la gobernanza de la información, se adopta el enfoque de marcos de gobierno en la nube que enfatizan la clasificación de datos, las políticas de gestión de información, el cumplimiento normativo y la evaluación continua de riesgos.

En consecuencia, las categorías de análisis centrales del estudio incluyen: mecanismos de cifrado, modelos de autenticación y gestión de identidades, controles de acceso y auditoría, capacidades de clasificación y retención de información y grado de alineación con marcos de gobernanza y cumplimiento (Soveizi et al., 2023). Estas categorías permiten operacionalizar constructos como confidencialidad, integridad, disponibilidad y trazabilidad en el contexto específico de Google Drive, Microsoft OneDrive y Dropbox.

En cuanto a los antecedentes comparativos, Negrete et al. (2025) manifiesta que los estudios técnicos que examinan diferencias de seguridad y funcionalidad entre plataformas de almacenamiento en la nube, se centran en aspectos como la presencia de cifrado de extremo a extremo, la robustez de la autenticación y las certificaciones de cumplimiento alcanzadas por cada proveedor. Mientras que, Khaddage & Haraty (2024) afirma que la clasificación y comparación de vulnerabilidades de estas soluciones, tiene como propósito proponer mejoras y guías de buenas prácticas para su adopción segura.

De igual forma, Mosquera et al. (2018) trabajó en la elaboración de marcos de gobernanza específicos para entornos gubernamentales o corporativos, resaltando la importancia de políticas claras de selección de proveedores, gestión de riesgos, continuidad del negocio y control de costos en la nube. Sin embargo, estos antecedentes tienden a abordar de forma separada la dimensión estrictamente técnica de la seguridad o la dimensión organizacional de la gobernanza y rara vez integran de manera sistemática ambas perspectivas en un análisis comparativo focalizado en Google Drive, Microsoft OneDrive y Dropbox (De Souza et al., 2018).

El aporte de este trabajo radica precisamente en articular ese vacío, ofreciendo una evaluación comparativa que combina criterios de seguridad técnica con criterios de gestión y gobernanza de la información y que traduce estos hallazgos en implicaciones prácticas para distintos perfiles organizacionales. De este modo, se contribuye a enriquecer la literatura existente con un marco analítico más integral y orientado a la toma de decisiones estratégicas sobre la adopción y configuración de herramientas Cloud de almacenamiento y colaboración

La presente investigación se sitúa en un contexto de acelerada transformación digital, en el que las organizaciones dependen crecientemente de infraestructuras basadas en la nube para sostener sus procesos operativos e inclusive de gestión del conocimiento. que requieren acceso remoto, simultáneo y seguro a documentos y recursos críticos. En este escenario, plataformas

como Google Drive, Microsoft OneDrive y Dropbox se han convertido en herramientas omnipresentes tanto en el ámbito corporativo como en instituciones educativas, organizaciones del sector público y pequeñas y medianas empresas, configurando un ecosistema sociotécnico en el que las fronteras entre lo local y lo remoto y entre lo personal y lo corporativo, se difuminan (Negrete et al., 2025).

En este contexto, la investigación plantea como El objetivo general del estudio es analizar comparativamente los mecanismos de seguridad, las funcionalidades de gestión de archivos y las implicaciones de gobierno de la información de las tres herramientas. Como objetivos específicos, se propone: a) describir y contrastar los modelos de cifrado, autenticación, control de acceso y auditoría de cada plataforma, b) evaluar las capacidades de gestión de archivos, colaboración y control de versiones, y c) identificar escenarios de uso y perfiles de organización para los cuales cada solución resulta más adecuada en términos de seguridad y eficiencia operativa

MATERIALES Y MÉTODOS

La investigación adopta un enfoque mixto, combinando componentes cuantitativos y cualitativos con el propósito de obtener una comprensión integral de las capacidades de seguridad y gestión de archivos de Google Drive, Microsoft OneDrive y Dropbox en contextos organizacionales. El estudio se clasifica como descriptivo–comparativo y explicativo. Para Hernández & Mendoza (2018) estos tipos metodológicos buscan, describir las funcionalidades y características relevantes de cada plataforma. Por otro lado, analizar cómo estas diferencias pueden influir en el nivel de riesgo y en la gobernanza de la información en las organizaciones. El diseño es no experimental, observacional y de corte transversal, para Arias & Covino (2021) se justifica dicha elección al centrarse en el análisis de las herramientas y de su documentación en un momento específico del tiempo, sin manipulación de variables ni intervención sobre el objeto de estudio

El objeto de estudio está conformado por servicios de almacenamiento y colaboración en la nube de uso extendido a nivel empresarial, delimitándose intencionalmente a tres casos paradigmáticos: Google Drive, Microsoft OneDrive y Dropbox. La selección corresponde a un muestreo teórico intencional, basado en criterios de amplia adopción en distintos sectores y disponibilidad de documentación técnica y de seguridad. No se incluyen otros proveedores como el caso de Box o iCloud, para mantener la profundidad analítica en estos tres referentes y asegurar comparabilidad en términos de funcionalidades empresariales.

En cuanto a las técnicas de recolección o producción de datos, el componente cualitativo se sustenta en una revisión documental sistemática de fuentes primarias, como documentación oficial de seguridad, guías de cumplimiento y manuales administrativos. De igual forma, las fuentes secundarias como los artículos académicos, informes técnicos y estudios comparativos previos.

Para ello se utiliza una matriz de análisis de documentos y una ficha de extracción de datos, soluciones creadas para abordar un problema específico, que permiten registrar de forma estructurada información relativa a cifrado, autenticación, controles de acceso, auditoría, gobierno de datos y cumplimiento normativo. El componente cuantitativo se concreta en la construcción de un sistema de puntuación y escalas de valoración de 0 a 5 aplicadas a cada categoría de análisis, a partir de la evidencia recogida, lo que posibilita comparar numéricamente la robustez de las plataformas en cada dimensión.

Adicionalmente, se realizan pruebas funcionales estandarizadas en entornos de prueba como el caso de cuentas empresariales o de características equivalentes para observar y registrar pasos, opciones de configuración, registros de actividad y experiencias de uso, utilizando como instrumentos listos de chequeo y guías de observación estructurada.

Las consideraciones éticas del estudio se centran en el uso exclusivo de información pública, es decir fuente abierta y en entornos de prueba controlados, sin acceso ni tratamiento de datos personales reales ni información sensible de organizaciones específicas. Se garantiza la transparencia metodológica mediante la descripción explícita de criterios de evaluación y procedimientos, de modo que el estudio pueda ser replicado por otros investigadores.

Como criterios de inclusión se consideran plataformas con alcance global, orientación a uso organizacional, funcionalidad de colaboración y documentación de seguridad detallada, como criterios de exclusión, se dejan fuera servicios de almacenamiento puramente personales o de nicho y herramientas sin documentación suficiente. Entre las limitaciones se reconoce la dependencia de la información proporcionada por los proveedores, el carácter estático del análisis frente a la rápida evolución de las plataformas y la ausencia de datos empíricos provenientes de incidentes reales en organizaciones específicas. Estos elementos permiten valorar el rigor y la coherencia del diseño, así como la replicabilidad de los procedimientos seguidos.

RESULTADOS Y DISCUSIÓN

Los resultados que se presentan a continuación, se muestran en el mismo orden que se detalló en la metodología. En este caso, primero se exponen los hallazgos de la revisión documental, que se organizan a partir de la matriz de análisis y la ficha de extracción, de modo que cada dimensión (cifrado, autenticación, controles de acceso, auditoría, gobierno de datos y cumplimiento) queda claramente caracterizada en las tres plataformas. A continuación, se presentan los hallazgos cualitativos de manera ordenada y didáctica.

Cifrado

La información recopilada muestra que las tres herramientas implementan cifrado en tránsito y en reposo como estándar básico de protección. Se identifican, sin embargo, matices en la forma en que gestionan las claves y en la oferta de cifrado de extremo a extremo o cifrado del lado del cliente

En este caso, OneDrive sobresale por su integración con Microsoft 365, que facilita una gestión centralizada de claves y políticas. Google Drive ofrece buenas capacidades nativas, aunque depende más de la correcta configuración administrativa. Dropbox resulta muy potente cuando se combina con cifrado del lado del cliente o E2E, por lo que puede ser la opción más fuerte en entornos que despliegan herramientas adicionales

Tabla 1

Arquitectura de cifrado y gestión de claves en servicios de almacenamiento en la nube

Aspecto	Google Drive	Microsoft OneDrive	Dropbox
Cifrado en tránsito	Protocolo TLS para comunicaciones cliente–servidor y entre centros de datos	TLS/HTTPS para acceso web y sincronización de clientes	SSL/TLS para comunicaciones y sincronización
Cifrado en reposo	Cifrado a nivel de disco/objeto con algoritmos de grado industrial	Cifrado de datos almacenados con algoritmos de grado industrial	Cifrado de archivos almacenados con algoritmos de grado industrial
Gestión de claves	Claves gestionadas por el proveedor, opciones de cifrado del lado del cliente en entornos avanzados	Claves gestionadas por el proveedor, integración con servicios corporativos de gestión de claves	Claves gestionadas por el proveedor, posibilidad de integrar soluciones de cifrado adicional
Cifrado extremo a extremo (E2E)	No nativo para todos los contenidos, depende de soluciones complementarias	Limitado a escenarios específicos mediante herramientas adicionales	Ofrece escenarios E2E o cifrado del lado del cliente en planes avanzados

Autenticación y gestión de identidades

La matriz evidenció que las tres plataformas han incorporado mecanismos de autenticación reforzada, con especial énfasis en la autenticación multifactor. También se constató la importancia de la integración con sistemas de identidad corporativos.

OneDrive es la alternativa más completa cuando la organización usa Azure AD, gracias a políticas avanzadas de acceso condicional y control por riesgo. Google Drive brinda MFA sólida e integración eficiente con Google Workspace, suficiente para muchas empresas e instituciones educativas. Dropbox ofrece MFA y SSO con proveedores externos, adecuado para PYMES y equipos distribuidos, aunque con menor profundidad nativa que los ecosistemas de Google y Microsoft.

Tabla 2

Controles de acceso basados en identidades digitales en plataformas Cloud

Aspecto	Google Drive	Microsoft OneDrive	Dropbox
Autenticación multifactor (MFA)	Disponible e integrada con la cuenta de Google	Disponible e integrada con Azure AD y Microsoft 365	Disponible en cuentas profesionales y empresariales
Integración con directorios de identidad	Integración con Google Workspace (usuarios, grupos, unidades organizativas)	Integración fuerte con Azure AD, directorio local y otras soluciones de identidad	Integración con proveedores externos de identidad (SSO, SAML, etc.)
Políticas de autenticación	Políticas centralizadas desde la consola de administración	Políticas avanzadas (condicionales, por riesgo, ubicación, dispositivo)	Políticas disponibles según plan, con énfasis en verificación en dos pasos y SSO

Controles de acceso y compartición

La revisión de manuales y guías administrativas permitió detallar el nivel de granularidad de los permisos y las opciones de compartición interna y externa. En todos los casos se observan mecanismos robustos, aunque con énfasis y usabilidad diferentes.

Tabla 3

Modelos de autorización y políticas de compartición de recursos digitales

Aspecto	Google Drive	Microsoft OneDrive	Dropbox
Granularidad de permisos	Permisos a nivel de archivo y carpeta (lector, comentarista, editor), restricciones por dominio	Permisos a nivel de archivo y carpeta, alineados con grupos y políticas de Microsoft 365	Permisos a nivel de archivo y carpeta, control sobre edición, visualización y descarga
Compartición externa	Enlaces restringidos, por dominio o públicos, opciones para desactivar descarga o impresión	Enlaces con diferentes niveles de acceso, expiración y protección con contraseña en ciertos planes	Enlaces compartidos con contraseña y fecha de caducidad en planes de negocio
Revocación de acceso	Posibilidad de revocar enlaces y accesos individuales desde la consola de administración	Revocación de enlaces y accesos gestionada desde el centro de administración de Microsoft 365	Revocación de enlaces y de accesos específicos desde el panel de administración

En control de acceso y compartición, OneDrive y Google Drive proporcionan alta granularidad de permisos y fuerte integración con estructuras organizativas. OneDrive se integra

con SharePoint y políticas globales de Microsoft 365, lo que refuerza el gobierno centralizado. Google Drive permite reglas finas por dominio y unidad organizativa, muy útiles en entornos educativos. Dropbox privilegia la simplicidad: es muy fácil de usar, pero con menos sofisticación en gobierno centralizado.

Auditoría y registro de actividad

La ficha de extracción permitió sistematizar la información sobre los registros que genera cada servicio y las herramientas disponibles para su consulta. Todas las plataformas ofrecen algún nivel de auditoría, con diferencias en profundidad y en herramientas analíticas asociadas.

Tabla 4

Sistemas de registro de eventos y soporte de actividad en servicios de nube

Aspecto	Google Drive	Microsoft OneDrive	Dropbox
Tipo de eventos registrados	Accesos, modificaciones, comparticiones, descargas, cambios de permisos	Accesos, modificaciones, comparticiones, actividades sospechosas, integración con registros de Microsoft 365	Accesos, modificaciones, comparticiones, dispositivos conectados
Herramientas de consulta	Consola de administración y paneles de seguridad de Google Workspace	Centro de cumplimiento y auditoría de Microsoft 365	Panel de administración de Dropbox Business, con informes descargables
Exportación y análisis	Exportación de registros para análisis externo (SIEM u otras herramientas)	Amplias opciones de exportación e integración con soluciones de seguridad y cumplimiento	Exportación limitada según plan, integración posible con herramientas externas

OneDrive destaca en auditoría al integrarse con el centro de cumplimiento de Microsoft 365 y herramientas de seguridad avanzadas. Mientras que, Google Drive ofrece registros detallados y exportables suficientes para monitoreo y análisis forense básico. Dropbox dispone de paneles e informes adecuados para seguimiento general, pero con menor profundidad e integración nativa, por lo que se ajusta mejor a necesidades de empresas PYMES que a entornos altamente regulados

Gobierno de datos y políticas de retención

Los documentos de referencia y guías de cumplimiento destacan la importancia de las políticas de retención, clasificación y borrado seguro como parte de la gobernanza de datos. La revisión mostró que las funciones más avanzadas suelen estar ligadas a planes empresariales y a la integración con suites más amplias.

Tabla 5

Gestión del ciclo de vida documental y soporte al gobierno de datos corporativos

Aspecto	Google Drive	Microsoft OneDrive	Dropbox
Políticas de retención	Configurables desde las herramientas de gobierno de Google Workspace	Integradas en las políticas de retención y archivado de Microsoft 365	Políticas de retención disponibles en planes de negocio, con opciones de recuperación
Clasificación de información	Integrable con herramientas de clasificación y etiquetas de seguridad	Soporte para etiquetas de confidencialidad y clasificación dentro del ecosistema Microsoft	Opciones de clasificación más básicas, la clasificación avanzada depende de integraciones
Borrado y recuperación	Papelera con plazos de recuperación y opciones de restauración a nivel de unidad organizativa	Papelera, versiones anteriores y restauración del sitio o de bibliotecas completas	Historial de versiones y recuperación dentro de ventanas de tiempo definidas por el plan

OneDrive lidera el gobierno de datos gracias a Microsoft Purview y políticas de retención, archivado y clasificaciones muy completas. Google Drive ofrece políticas de retención y administración centralizada suficientes para organizaciones que requieren un gobierno robusto sin demasiada complejidad. Dropbox se centra más en continuidad operativa, versiones y restauración, por lo que es adecuado para la gestión cotidiana, pero menos para esquemas de gobernanza estrictos.

Cumplimiento normativo

La revisión de whitepapers o documentos generados en pdf que explica de forma pormenorizada y guías de cumplimiento permitió identificar los marcos normativos y certificaciones con los que cada proveedor declara alinearse. Aunque esta dimensión no sustituye una auditoría independiente, muestra el esfuerzo de cada plataforma por dar soporte a entornos regulados.

Con esta estructura, los resultados de la revisión documental quedan organizados de modo que el lector puede identificar rápidamente cómo se comporta cada plataforma en cada dimensión. Si quieres, en la siguiente parte podemos profundizar en el análisis interpretativo (discusión parcial) o pasar a los resultados de las pruebas funcionales que definiste en tu metodología.

Tabla 6

Soporte a normativas de protección de datos y estándares internacionales de seguridad

Aspecto	Google Drive	Microsoft OneDrive	Dropbox
Certificaciones habituales	ISO/IEC (seguridad), estándares de centros de datos y cumplimiento de marcos de privacidad	Varias certificaciones ISO, SOC y cumplimiento para sectores regulados	Certificaciones de seguridad y cumplimiento adaptadas a clientes empresariales
Soporte a protección de datos	Herramientas para ayudar al cumplimiento de normativas de protección de datos	Herramientas amplias para cumplimiento de protección de datos y marcos sectoriales	Herramientas y documentación para apoyar el cumplimiento de protección de datos
Documentación de cumplimiento	Whitepapers y guías específicas de cumplimiento y privacidad	Documentación extensa integrada en el portal de cumplimiento de Microsoft	Guías de seguridad, cumplimiento y prácticas recomendadas

OneDrive suele presentar el conjunto más amplio de certificaciones y recursos para cumplir normativas sectoriales complejas. Google Drive también dispone de certificaciones y guías sólidas para protección de datos y privacidad, siendo muy competitivo en organizaciones que ya utilizan su infraestructura. Dropbox ofrece certificaciones y documentación adecuadas para muchas empresas, pero con un enfoque algo menos integral, por lo que suele requerir apoyo en políticas internas y soluciones adicionales.

Por otro lado, se presentan los resultados cuantitativos del sistema de puntuación de 0 a 5 aplicado a las categorías de análisis. Las puntuaciones se basan en la evidencia documentada sobre mecanismos de seguridad, gobierno de datos y cumplimiento en cada plataforma, Para facilitar la lectura, primero se muestra la tabla resumen y luego se interpreta cada dimensión.

Tabla 7

Puntuaciones globales (0–5) por dimensión de análisis

Dimensión de análisis	Google Drive	Microsoft OneDrive	Dropbox
1. Cifrado y protección de datos	4	4	4
2. Autenticación y gestión de identidades	4	5	3
3. Controles de acceso y políticas de compartición	4	5	3
4. Auditoría, trazabilidad y monitoreo	4	5	3
5. Gobierno de datos, retención y ciclo de vida de archivos	4	5	3
6. Cumplimiento normativo y certificaciones	4	5	4
Promedio global aproximado	**4**	**4,8**	**3,3**

Cifrado y protección de datos

Las tres plataformas alcanzan una puntuación de 4 en cifrado, porque todas ofrecen cifrado de datos en tránsito mediante SSL/TLS y cifrado en reposo con algoritmos de nivel industrial equivalentes a AES-256, considerados mejores prácticas en la industria. Ninguna de las tres proporciona de forma nativa cifrado de extremo a extremo para todos los contenidos con modelo de "conocimiento cero", esto impide otorgar la máxima puntuación de 5, que se reserva para escenarios donde el proveedor no tiene acceso posible al contenido cifrado. No obstante, las tres permiten complementar la protección con cifrado del lado del cliente u otras herramientas, lo que las sitúa en un nivel robusto, pero no "máximo" desde la perspectiva de seguridad criptográfica avanzada.

Autenticación y gestión de identidades

En autenticación e identidad, OneDrive alcanza la puntuación máxima (5) debido a su integración profunda con Azure Active Directory, que permite políticas de acceso condicional, evaluación de riesgo, segmentación por dispositivo, ubicación y tipo de aplicación, además de MFA generalizada. Google Drive obtiene 4, al ofrecer MFA sólida e integración consistente con Google Workspace, suficientes para la mayoría de organizaciones, pero con un nivel de sofisticación algo menor en políticas condicionales avanzadas. Dropbox se sitúa en 3 ya que incorpora MFA y SSO mediante terceros, pero su gestión de identidades y políticas de acceso avanzadas suele depender de integraciones externas y de la capacidad de las empresas para complementar el servicio.

Controles de acceso y políticas de compartición

En controles de acceso y compartición, OneDrive obtiene 5, porque combina permisos muy granulares con la integración de SharePoint y de políticas de Microsoft 365, permitiendo a los administradores definir reglas consistentes a nivel de toda la organización. Google Drive logra 4, al ofrecer permisos detallados por archivo y carpeta, restricción por dominio y controles avanzados sobre enlaces, aunque con menos alineación formal con un marco de gobierno corporativo tan amplio como el de Microsoft. Dropbox recibe 3, al priorizar controles simples y fáciles de usar (enlaces con contraseña, caducidad, permisos básicos), que son suficientes para muchas PYMES, pero menos adecuados para políticas complejas de segmentación y compartición en grandes entornos.

Auditoría, trazabilidad y monitoreo

En auditoría y monitoreo, OneDrive vuelve a alcanzar 5 gracias a su integración con el centro de cumplimiento de Microsoft 365 y sus capacidades de búsqueda de registros, correlación de eventos e integración con soluciones SIEM y herramientas de seguridad corporativas. Google Drive recibe 4, porque ofrece registros detallados de accesos, cambios y comparticiones, además de opciones de exportación que permiten análisis externo, pero con menos amplitud de herramientas nativas para análisis avanzado. Microsoft Dropbox obtiene 3, al contar con paneles

e informes suficientes para monitoreo general y auditorías básicas, pero con menor profundidad, grado de integración y automatización en comparación con OneDrive y, en parte, con Google Drive.

Gobierno de datos, retención y ciclo de vida

En gobierno de datos y retención, OneDrive se sitúa de nuevo en 5, apoyado en las políticas de retención, archivado, eDiscovery y etiquetas de confidencialidad de Microsoft 365 y Purview, que permiten administrar de forma integral el ciclo de vida documental y el riesgo asociado a la información. Google Drive se valora con 4, ya que dispone de políticas de retención, herramientas de administración centralizada y opciones de clasificación integradas en Google Workspace, lo que constituye un gobierno robusto, pero algo menos amplio que el de Microsoft en escenarios altamente regulados. Dropbox alcanza 3, al ofrecer versiones, recuperación y políticas de retención orientadas a continuidad operativa, pero sin un marco tan completo de gobernanza normativa.

Cumplimiento normativo y certificaciones

En cumplimiento y certificaciones, OneDrive obtiene 5 debido a su extenso portafolio de certificaciones como el caso de ISO, SOC, FedRAMP y a la integración con el portal de cumplimiento de Microsoft, que provee guías, plantillas y herramientas para diversos marcos regulatorios. Google Drive recibe 4, con un conjunto sólido de certificaciones de seguridad y privacidad, además de documentación específica para apoyar el cumplimiento de normativas de protección de datos y estándares internacionales, suficiente para muchas organizaciones públicas y privadas. Dropbox también se valora con 4 en esta dimensión, ya que mantiene certificaciones relevantes y ofrece documentación orientada a clientes empresariales, aunque con una cobertura menos “ecosistémica” que la de Microsoft.

Síntesis interpretativa

Al promediar las puntuaciones, OneDrive alcanza un valor global aproximado de 4,8, lo que refleja una madurez muy alta en seguridad, gobierno de datos y cumplimiento, especialmente cuando se utiliza integrado al ecosistema Microsoft 365. Google Drive se sitúa en torno a 4,0, mostrando un perfil robusto y equilibrado, particularmente apropiado para organizaciones que ya operan en Google Workspace y requieren buen nivel de seguridad sin tanta complejidad de configuración. Dropbox obtiene alrededor de 3,3, lo que lo posiciona como una solución aceptable a robusta para PYMES y equipos distribuidos, muy fuerte cuando se complementa con buenas políticas internas y herramientas adicionales, pero menos orientada, de forma nativa, a entornos de cumplimiento extremadamente exigentes.

DISCUSIÓN

La discusión de resultados muestra que, aunque las tres plataformas analizadas ofrecen un nivel de seguridad y gestión de archivos adecuado para contextos organizacionales, existen diferencias claras en el grado de madurez y en el perfil de uso al que parecen dirigirse. En términos

globales, OneDrive presenta la configuración más completa en seguridad, gobernanza y cumplimiento cuando se utiliza integrado al ecosistema Microsoft 365, mientras que Google Drive se posiciona como una opción robusta y equilibrada y Dropbox como una alternativa muy usable y suficiente para PYMES y equipos distribuidos.

Para Mossebo et al. (2026)en su análisis técnicos y comparativos señalan que OneDrive tiende a situarse en una posición ventajosa en organizaciones que ya utilizan Microsoft 365, precisamente porque puede aprovechar Azure Active Directory, políticas de acceso condicional y herramientas de cumplimiento centralizadas. Esta superioridad relativa en autenticación, auditoría y gobierno formal coincide con las puntuaciones más altas obtenidas en el presente estudio en las dimensiones de gestión de identidades, controles de acceso avanzados y trazabilidad. En contraste, Al Lelah et al. (2023) centró su estudio en la facilidad de uso y en la experiencia del usuario final resaltan con frecuencia la simplicidad de Dropbox para tareas de compartición y sincronización, especialmente en equipos pequeños o sin un departamento de TI altamente especializado. Esto es coherente con los resultados del presente estudio donde Dropbox obtiene la puntuación más alta en rapidez y claridad de configuración de permisos y enlaces.

Desde la perspectiva del cifrado, Mosquera et al. (2018)diversas fuentes coinciden en que Google Drive, OneDrive y Dropbox comparten un núcleo común: cifrado en tránsito mediante TLS/HTTPS y cifrado en reposo con algoritmos de grado industrial como AES-256. El análisis cuantitativo otorga la misma puntuación (4/5) a las tres plataformas en esta dimensión, lo que refleja esa convergencia en las prácticas mínimas esperadas de seguridad en la nube. No obstante, algunos autores critican la ausencia de cifrado extremo a extremo generalizado y señalan que, para alcanzar un nivel de “cero conocimientos”, es necesario integrar soluciones de cifrado del lado del cliente u otras herramientas adicionales (Khaddage & Haraty, 2024).

En cuanto al gobierno de datos y al cumplimiento normativo, trabajos sobre gobernanza en la nube De Souza et al. (2018)que el valor añadido de una plataforma no depende solo de las funciones técnicas, sino de la capacidad para integrarse en marcos formales de gestión de riesgos, calidad de datos y cumplimiento. En este sentido, los resultados de este estudio, que sitúan a OneDrive por encima de Google Drive y Dropbox en políticas de retención, eDiscovery y soporte a estándares múltiples, se corresponden con la forma en que la literatura describe el ecosistema Microsoft como fuertemente orientado a organizaciones reguladas y sector público. Google Drive se reconoce como una solución muy difundida en educación y empresas digitales, con herramientas de gobierno suficientes para muchos escenarios, mientras que Dropbox suele ser presentado como una opción sólida pero más dependiente de políticas internas y herramientas externas para alcanzar el mismo nivel de formalización.

Las diferencias encontradas también pueden explicarse por el enfoque de diseño de cada proveedor. Microsoft prioriza la integración de OneDrive en un entramado más amplio de servicios empresariales como identidad, seguridad, cumplimiento, analítica, lo que favorece

puntuaciones altas en dimensiones relacionadas con gobierno y auditoría. Google. Por su parte Jaskula et al. (2022), enfatiza la colaboración ágil en el ecosistema Workspace, por eso, sus puntuaciones son altas, pero algo menos extremas en cumplimiento formal, aunque muy competitivas en facilidad de colaboración y administración. Dropbox, nacido como servicio de sincronización centrado en el usuario, ha ido incorporando capacidades empresariales, pero mantiene un fuerte sesgo hacia la simplicidad y la experiencia de uso.

Por otro lado, la gestión de archivos en herramientas Cloud a nivel institucional debe priorizar estabilidad, acceso flexible y recuperación rápida de materiales, fortaleciendo así la resiliencia de los usuarios. Tal como lo afirma Salinas et al. (2025) quien infiere que para sostener la continuidad pedagógica en contextos educativos se debe favorecer entornos donde preparar, resguardar y compartir recursos educativos sea de mayor provecho para la comunidad estudiantil.

los resultados de este estudio son en gran medida consistentes con la literatura confirman que, OneDrive es especialmente ventajoso en organizaciones integradas en Microsoft 365, que Google Drive ofrece un equilibrio robusto entre seguridad y colaboración y que Dropbox destaca en usabilidad y simplicidad operativa. Las diferencias detectadas en puntuaciones concretas se deben, sobre todo, a que aquí se ha adoptado un enfoque explícitamente orientado a gobierno de la información y cumplimiento, mientras que muchos trabajos previos han puesto el foco en comparaciones de precio, capacidad o experiencia de usuario final

CONCLUSIONES

La investigación concluye que las tres herramientas analizadas, Google Drive, Microsoft OneDrive y Dropbox, ofrecen un nivel de seguridad y gestión de archivos adecuado para contextos organizacionales, pero con perfiles claramente diferenciados. En conjunto, los resultados cuantitativos y funcionales muestran que OneDrive presenta la mayor madurez en seguridad, gobierno de datos y cumplimiento normativo, especialmente cuando se integra plenamente con el ecosistema Microsoft 365. Google Drive se configura como una solución robusta y equilibrada, particularmente ventajosa para organizaciones que trabajan en Google Workspace y priorizan la colaboración ágil. Dropbox, por su parte, destaca por su simplicidad de uso, rapidez de sincronización y claridad en la gestión de permisos, cualidades que lo hacen muy atractivo para pequeñas y medianas empresas y equipos distribuidos que no requieren un andamiaje tan complejo de gobernanza.

Estas conclusiones dialogan con trabajos que señalan la ventaja de OneDrive en entornos corporativos y gubernamentales donde la integración con Azure Active Directory, políticas de acceso condicional y portales de cumplimiento resulta decisiva para satisfacer exigencias regulatorias y de auditoría interna. De forma similar, diversos análisis técnicos destacan que Google Drive ofrece un equilibrio notable entre seguridad, capacidad de colaboración y relación coste–beneficio, lo que coincide con las puntuaciones medias–altas obtenidas en este estudio en

la mayoría de dimensiones. En cuanto a Dropbox, la literatura y comparativas recientes resaltan su superioridad en sincronización y experiencia de uso, sobre todo en la gestión cotidiana de archivos pesados, aspecto que aquí se refleja en sus buenos resultados en pruebas funcionales de compartición y restauración, aunque no lidere en gobierno formal de la información.

Entre las principales limitaciones del estudio se encuentra la dependencia de documentación pública y pruebas en entornos de demo o cuentas empresariales controladas, sin acceso a métricas internas de incidentes ni a configuraciones reales de organizaciones específicas. Esto implica que algunos aspectos, como la respuesta ante incidentes complejos o la eficacia real de las políticas en contextos de alta presión, no pueden ser evaluados directamente. Además, el análisis se centra en un conjunto de dimensiones definidas, dejando fuera factores como rendimiento bajo distintas cargas, experiencia de usuario final en distintos perfiles profesionales o costos totales de propiedad, que también influyen en la elección de una plataforma.

A partir de estos hallazgos, se abren varias líneas futuras de investigación. Una prioridad sería incorporar estudios de caso en organizaciones reales de distintos sectores como educación, salud, sector público, entre otros. Para observar cómo las capacidades descritas se traducen en prácticas concretas de seguridad y gobernanza y qué configuraciones son más efectivas en la práctica. Otra línea relevante consiste en ampliar el análisis a otros proveedores como Box, pCloud o soluciones con cifrado de conocimiento cero, de modo que se pueda comparar el modelo clásico de nube gestionada por el proveedor con alternativas centradas en privacidad extrema.

Asimismo, sería pertinente explorar el impacto de las nuevas funciones basadas en inteligencia artificial, que ya se están integrando en estos servicios, sobre la seguridad como detección de amenazas, clasificación automática de datos, recomendaciones de compartición y sobre los riesgos emergentes, como el tratamiento masivo de metadatos y contenido para entrenamiento de modelos. Finalmente, futuras investigaciones podrían profundizar en la percepción y comportamiento de los usuarios frente a las opciones de seguridad disponibles, analizando hasta qué punto la usabilidad de los controles influye en que las políticas de seguridad se apliquen efectivamente en el día a día de las organizaciones

REFERENCIAS

Al lelah, T., Theodorakopoulos, G., Reinecke, P., Javed, A., & Anthi. (2023). Abuse of Cloud-Based and Public Legitimate Services as Command-and-Control (C&C) Infrastructure Literature Review. *Journal of Cybersecurity and Privacy, 3*(3), 558-590. https://doi.org/10.3390/jcp3030027

Alshayeji, M. H., & Abed, S. (2022). Enhanced video-on-demand security in cloud computing against insider and outsider threats. *InderScience, 17*(1), 48-55. https://doi.org/https://doi.org/10.1504/IJSN.2022.122550

Arias, G. J., & Covino, G. M. (2021). *Diseño y metodología de la investigación.* Enfoques Consulting Eirl. https://doi.org/ISBN: 978-612-48444-2-3

De Souza, S. I., Alburqueque, P., Giritana, G. F., & MOURA NICKEL, E. A. (2018). Avaliação comparativa de drives de armazenamento na nuvem: Usabilidade e learnability do Dropbox, Google Drive e OneDrive. *Human Factors in Design,, 5*(10), 48-61. https://doi.org/https://doi.org/10.5965/2316796305102016048

Fargana, A. (2023). Cyber resilience and cyber security issues of intelligent cloud computing systems. *Published by Elsevier* , 1-16. https://doi.org/https://doi.org/10.1016/j.rico.2023.100268

Hernández, R., & Mendoza, C. P. (2018). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta.* Mc Graw Hill. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/SampieriLasRutas.pdf

Jaskula, K., Papadonikolaki, E., & Dimitrios, R. (2022). Proceedings of the 2022 European Conference on Computing. *information management along the entire lifecycle of a built asset.* University College London, United Kingdom. https://doi.org/10.35490/EC3.2022.168

Khaddage, N., & Haraty, R. A. (2024). Comparative Analysis of Security Approaches in Cloud Databases. *Included in the following conference series: International Conference on Mathematical Modelling, Applied Analysis and Computation*, (pp. 29-41). https://link.springer.com/chapter/10.1007/978-3-031-90914-6_2

Mosquera, R. X., Chilán, R. M., & Rodríguez, X. E. (2018). Análisis de la información en la nube y su impacto en la seguridad y confiabilidad en las PyMES. *Revista Científica Ciencia y Tecnología, 18*(17), 141-155. https://doi.org/DOI:10.47189/rcct.v18i17.160

Mossebo, T. S., Moyou, M. L., Kalachi, H. T., Ekodeck, S. G., Ndoundam, R., & Tchana, A. (2026). Contextual Cloud Steganography(CCS): Breaking the Capacity-Security Trade-Off. *Journals & Magazines*, 1-8. https://doi.org/10.1109/TCC.2026.3663281

Navin, P., & Rekha, C. (2023). Block chain based IAS protocol to enhance security and privacy in cloud computing. *Measurement: Sensors, 28*, 1-6. https://doi.org/https://doi.org/10.1016/j.measen.2023.100813

Negrete, R. M., Elizondo, N. A., Muñoz, M., & Güemes, C. D. (2025). COMPARATIVE ANALYSIS OF CLOUD COMPUTING ADOPTION FOR AN E-COMMERCE PLATFORM IN THE MANUFACTURING INDUSTRY: A SYSTEM-DYNAMICS APPROACH USING AWS. *Rev. Fac. ing., 34*(72), 2-18. https://doi.org/https://doi.org/10.19053/01211129.v34.n72.2025.19063

Ortiz, E., Villacorta, C., & Mendoza, A. (2024). Seguridad de la Información en la Nube Una revisión sistemática. *Revista Científica Ciencias Ingenieriles, 4*(1), 69–78. https://doi.org/https://doi.org/10.54943/ricci.v4i1.383

Rezqallah, M. A., Muhamad, S. A., & Dahlin, Z. B. (2023). Indonesian Journal of Electrical Engineering and Computer Science (IJEECS). *Muhamad , 30*(3), 1707-1712. https://doi.org/ http://doi.org/10.11591/ijeecs.v30.i3.pp1707-1712

Salinas, C. A., Castillo Jiménez, A., & Elías Piguave, M. (2025). Resiliencia Docente en Tiempos de Crisis Energética en una Institución Pública de Guayaquil,Ecuador. *Revista Veritas De Difusão Científica, 6*(1), 261-276. https://doi.org/https://doi.org/10.61616/rvdc.v6i1.408

Shameer, M. a., Nanthini e b, N. B., & Ashok, K. M. (2023). A new lightweight data security system for data security in the cloud computing. *Measurement: Sensors, 29*, 1-7. https://doi.org/https://doi.org/10.1016/j.measen.2023.100856

Soveizi, N., Turkmen, F., & Dimka, K. (2023). Security and privacy concerns in cloud-based scientific and business workflows: A systematic review. *Future Generation Computer Systems, 148*, 184-197. https://doi.org/https://doi.org/10.1016/j.future.2023.05.015

ThiBac, D., & Hieu, M. N. (2022). Design of network security storage system based on under cloud computing technology. *Computers and Electrical Engineering, 103*. https://doi.org/https://doi.org/10.1016/j.compeleceng.2022.108334