

# CONESCAPANHONDURAS2025paper56.pdf

 Institute of Electrical and Electronics Engineers (IEEE)

---

## Document Details

### Submission ID

trn:oid:::14348:477758472

### Submission Date

Jul 31, 2025, 11:27 PM CST

### Download Date

Aug 12, 2025, 2:38 PM CST

### File Name

CONESCAPANHONDURAS2025paper56.pdf

### File Size

231.2 KB

6 Pages




4,943 Words

28,332 Characters

# 19% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

## Top Sources

- 18%  Internet sources
- 13%  Publications
- 0%  Submitted works (Student Papers)

## Integrity Flags




### 0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

## Top Sources

- 18%  Internet sources
- 13%  Publications
- 0%  Submitted works (Student Papers)

## Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Internet	
	datatracker.ietf.org	2%
2	Internet	
	buleria.unileon.es	2%
3	Internet	
	www.coursehero.com	1%
4	Internet	
	arxiv.org	1%
5	Internet	
	ri.ues.edu.sv	<1%
6	Internet	
	www.mdpi.com	<1%
7	Internet	
	www.jatit.org	<1%
8	Publication	
	Jumei Zhang, Zhenhua Liu, Dongdong Yao. "Lattice-based puncturable blind sign...	<1%
9	Internet	
	joiv.org	<1%
10	Publication	
	"Applied Cryptography and Network Security", Springer Science and Business Me...	<1%
11	Internet	
	fastercapital.com	<1%

12	Internet	eprints.qut.edu.au	<1%
13	Publication	Tsuyoshi TAKAGI. "Recent Developments in Post-Quantum Cryptography", IEICE T...	<1%
14	Publication	Esmot Ara Tuli, Jae-Min Lee, Dong-Seong Kim. "Integration of Quantum Technolo...	<1%
15	Internet	jisem-journal.com	<1%
16	Internet	upcommons.upc.edu	<1%
17	Publication	Mestas Yucra, Edwin Edgar. "Modelo basado en Deep Learning para predecir el in...	<1%
18	Internet	pure.tue.nl	<1%
19	Internet	www.researchgate.net	<1%
20	Internet	dspace.ups.edu.ec	<1%
21	Internet	digitalid.certisur.com	<1%
22	Internet	hal.upmc.fr	<1%
23	Internet	www.nist.gov	<1%
24	Internet	www.cyber.gc.ca	<1%
25	Internet	benchmarks.ul.com	<1%

26	Internet	diposit.ub.edu	<1%
27	Internet	dsl.sk	<1%
28	Internet	files.bbystatic.com	<1%
29	Internet	oai.repec.org	<1%
30	Internet	patents.google.com	<1%
31	Internet	www.cenaim.espol.edu.ec	<1%
32	Internet	www.dacya.ucm.es	<1%
33	Internet	www.newtech.co.cr	<1%
34	Internet	www.sbu.ac.ir	<1%
35	Internet	www.wicc2019.unsj.edu.ar	<1%
36	Internet	aircconline.com	<1%
37	Internet	inis.iaea.org	<1%
38	Internet	investigaciones.uniatlantico.edu.co	<1%
39	Internet	moam.info	<1%

40	Internet	news.backbox.org	<1%
41	Internet	uvadoc.uva.es	<1%
42	Internet	www.trabajosdistinguidos.com	<1%
43	Internet	www.cacic2016.unsl.edu.ar	<1%
44	Publication	Perez, Esteban Jove. "Advanced Anomaly Detection Algorithms Based on Virtual S...	<1%

# Comparación y Agrupamiento de Algoritmos Post-Cuánticos de Firma Digital para Aplicaciones Móviles, IoT y Servidores

1 <sup>st</sup> Given Name Surname	2 <sup>nd</sup> Given Name Surname	3 <sup>rd</sup> Given Name Surname
dept. name of organization (of Aff.)	dept. name of organization (of Aff.)	dept. name of organization (of Aff.)
name of organization (of Aff.)	name of organization (of Aff.)	name of organization (of Aff.)
City, Country	City, Country	City, Country
email address or ORCID	email address or ORCID	email address or ORCID

**Resumen**—La aparición de la computación cuántica representa un reto considerable para la criptografía convencional, dado que numerosos sistemas de firma digital existentes podrían tornarse vulnerables ante ataques cuánticos. En este trabajo aplicamos un enfoque de agrupamiento no supervisado para analizar algoritmos de firma digital post-cuánticos, utilizando métricas de rendimiento obtenidas con distintos tamaños de mensaje. Para ello, se emplearon técnicas de reducción de dimensionalidad mediante Análisis de Componentes Principales (PCA) y el algoritmo DBSCAN, que permite identificar agrupaciones sin requerir una cantidad previa de grupos. La calidad de los agrupamientos fue evaluada mediante los índices Silhouette, Davies-Bouldin y Calinski-Harabasz. Los resultados permitieron asociar algoritmos con escenarios específicos: SLH-DSA fast para dispositivos móviles, SLH-DSA small para IoT, y ML-DSA y Falcon para servidores. Esta clasificación puede orientar la selección de algoritmos según las capacidades y restricciones del entorno de implementación.

**Palabras clave**— Algoritmos post-cuánticos, clustering, computación cuántica, criptografía de clave pública, DBSCAN, firma digital

## I. INTRODUCCIÓN

La criptografía de clave pública es fundamental para garantizar la seguridad de las comunicaciones digitales a nivel global. Su aplicación es clave en servicios como la telefonía móvil, el comercio electrónico, las redes sociales y la computación en la nube. En un entorno interconectado, donde se transmite información sensible entre individuos, empresas y gobiernos, la robustez criptográfica se vuelve crítica para preservar la confidencialidad e integridad de los datos.

La computación cuántica, que utiliza propiedades como la superposición y el entrelazamiento de cúbits, representa una amenaza para los criptosistemas de clave pública actuales, como RSA y ECDSA, que dependen de problemas complejos como la factorización y el logaritmo discreto [1], [2]. En 1994, Peter Shor demostró que las computadoras cuánticas pueden resolver estos problemas eficientemente, comprometiendo la seguridad de dichos sistemas [3].

Ante esta situación, el NIST y otros actores han promovido la criptografía post-cuántica (PQC), buscando algoritmos resistentes a ataques cuánticos [4]. En 2022, el NIST seleccionó para estandarización tres algoritmos de firma digital:

ML-DSA, SLH-DSA y Falcon, este último próximo a ser estandarizado como FIPS 206 [5], [6].

Dado el interés creciente en su adopción, diversos estudios han evaluado el rendimiento de estos algoritmos en entornos reales. En [7] se implementó un entorno experimental basado en Python y contenedores Docker para analizar la eficiencia de los algoritmos de firma digital post-cuánticos estandarizados por el NIST. La evaluación se centró en tres métricas fundamentales: el tamaño de la firma, así como los tamaños de las claves pública y privada. Por otra parte, en [8] se propone un marco de evaluación más integral, en el cual se analizan varios esquemas criptográficos, evaluándolos en una amplia gama de entornos computacionales desde sistemas embebidos hasta infraestructuras en la nube. De manera similar, en [4] se presenta un marco de evaluación empírica para algoritmos post-cuánticos, evaluando en diferentes dispositivos y sobrecarga en protocolo como TLS 1.3. En [9], se comparó la idoneidad de los esquemas de firma Falcon y Dilithium para aplicaciones de IoT, centrándose en el rendimiento de la verificación y el coste de transmisión. Además, en [10] implementaron una aplicación de correos electrónicos en Android que integra diversos esquemas de firma digital.

Aunque diversas investigaciones han tratado los principios matemáticos y las características de seguridad de los algoritmos post-cuánticos (PQC), las evaluaciones de rendimiento en entornos reales siguen siendo limitadas. Esto crea brechas en el entendimiento de su funcionamiento en dispositivos IoT, móviles o servidores. Adicionalmente, pocas investigaciones exploran las distintas variantes y configuraciones de estos algoritmos, lo que restringe la comprensión de su rendimiento en distintos contextos. También son escasos los estudios que clasifican algoritmos de firma digital post-cuánticos según las restricciones específicas de cada dispositivo, como capacidad de procesamiento, consumo energético o memoria disponible.

En este trabajo ofrecemos una evaluación detallada de los algoritmos de firma digital post-cuánticos ML-DSA, Falcon y SLH-DSA, incluyendo sus variantes. Para ello, aplicamos métodos de evaluación comparativa (benchmarking) para analizar su desempeño en tres contextos: servidores,

dispositivos IoT y móviles. Además, incorporamos técnicas de aprendizaje automático no supervisado, utilizando el algoritmo DBSCAN para identificar patrones de rendimiento y realizar una agrupación significativa de los algoritmos. La calidad de estos agrupamientos se evaluó mediante tres métricas ampliamente utilizadas: *Silhouette Score*, *Davies-Bouldin Index* y *Calinski-Harabasz Score*. Finalmente, presentamos una clasificación de algoritmos apropiados para cada tipo de dispositivo, considerando sus características técnicas y limitaciones operativas.

## II. METODOLOGÍA

Nuestra metodología emplea un enfoque cuantitativo y experimental, basado en la evaluación del rendimiento de algoritmos de firma digital post-cuánticos propuestos por el NIST, con el fin de analizar su viabilidad en distintos entornos informáticos. Para ello, se realizaron pruebas controladas que permitieron medir su comportamiento bajo condiciones específicas de hardware y software. Durante estas pruebas se consideró el nivel de seguridad definido por el NIST, con el objetivo de asegurar la comparabilidad entre algoritmos del mismo nivel criptográfico, aunque dicho nivel no se incluyó como variable en el análisis de agrupamiento.

El estudio se centró en tres contextos: dispositivos móviles, entornos IoT con recursos limitados y plataformas servidor. En cada uno se evaluó el desempeño utilizando métricas benchmark estandarizadas.

Los resultados se organizaron en un conjunto de datos para análisis exploratorio y agrupamiento, identificando patrones y clústeres según desempeño y eficacia. Esto permitió proponer recomendaciones fundamentadas sobre los algoritmos más adecuados para cada tipo de dispositivo, considerando seguridad y eficiencia computacional.

### A. Selección y descripción de los algoritmos

En este estudio se analizaron tres algoritmos de firma digital post-cuánticos: ML-DSA, Falcon y SLH-DSA, junto con sus variantes, sumando un total de 19 esquemas evaluados. Estos algoritmos están diseñados para resistir futuros ataques que puedan ser llevados a cabo mediante computadoras cuánticas, las cuales representan una amenaza significativa para la seguridad de los esquemas criptográficos tradicionales [11].

Los algoritmos ML-DSA y SLH-DSA fueron estandarizados en 2024 [12], mientras que FALCON está a la espera de ser estandarizado [6]. Estos esquemas se basan en problemas matemáticos que, hasta el momento, son vistos como computacionalmente inviables incluso para las tecnologías cuánticas más sofisticadas, lo que asegura un elevado grado de seguridad para salvar las comunicaciones digitales y sistemas críticos de terceros no autorizados.

A continuación, se describen en detalle los algoritmos seleccionados y las principales características de sus variantes.

**ML-DSA:** originalmente conocido como CRYSTALS-Dilithium, fue renombrado oficialmente como ML-DSA (*Module Lattice-based Digital Signature Algorithm*) tras su estandarización por el NIST en el estándar FIPS 204 (2024)

[5]. Su seguridad se fundamenta en dos problemas difíciles sobre retículos modulados: Module-LWE y Module-SIS.

El problema *Module-LWE* consiste en recuperar el secreto  $s$  a partir de la matriz pública  $A$ , el vector resultante  $t$ , y un pequeño error  $e$ , lo cual es computacionalmente difícil.

$$t = A \cdot s + e$$

El problema *Module-SIS* requiere encontrar un vector corto  $z \neq 0$  que satisfaga la congruencia, siendo también intratable incluso frente a adversarios con capacidades cuánticas.

$$A \cdot z = 0 \pmod{q}, \quad \text{con } \|z\| \text{ pequeña}$$

El esquema cuenta con tres variantes ML-DSA-44, ML-DSA-65 y ML-DSA-87— que corresponden a niveles de seguridad aproximados de 128, 192 y 256 bits, respectivamente. Esta variedad permite su adaptación a diferentes contextos según los requerimientos de seguridad y rendimiento [5].

**Falcon:** aun está a la espera de ser estandarizado como FN-DSA (*Fast Fourier NTRU Lattice-Based Digital Signature Algorithm*). Está diseñado para ofrecer firmas digitales compactas y rápidas, basadas en problemas matemáticos difíciles como las redes NTRU. Utiliza la técnica de muestreo gaussiano junto con transformadas rápidas de Fourier discretas para lograr eficiencia y seguridad post-cuántica [6].

Las versiones estándar de Falcon incluyen variantes denominadas *padded*, específicamente Falcon-512 y Falcon-1024, que añaden relleno para mejorar propiedades de seguridad frente a ciertos ataques, manteniendo tamaños de firma y rendimiento adecuados para aplicaciones prácticas.

Los esquemas basados en NTRU utilizan una clase específica de redes con simetría adicional. Las bases de estas redes se representan, en el caso más general, mediante una matriz de dimensión  $n \times n$ . La principal ventaja de NTRU y otros esquemas basados en redes radica en su rendimiento: con niveles de seguridad equivalentes, estos esquemas suelen ser de 10 a 100 veces más rápidos que la criptografía de clave pública convencional [13].

**SLH-DSA:** originalmente conocido como SPHINCS+, fue renombrado como SLH-DSA (*Stateless Hash-Based Digital Signature Algorithm*) tras su estandarización por el NIST en el estándar FIPS 205 (2024) [14]. Se trata de un esquema de firma digital basado en funciones hash, caracterizado por no requerir el mantenimiento de estado entre firmas, lo que elimina riesgos asociados a errores en la gestión de claves.

SLH-DSA combina dos componentes fundamentales: el esquema de firma de pocas veces *FORS* (Forest of Random Subsets), que firma los mensajes directamente, y un esquema de árbol de Merkle extendido conocido como *XMSS hypertree*, utilizado para autenticar múltiples firmas de FORS. Esta estructura en capas garantiza tanto seguridad como eficiencia.

El proceso de firma puede expresarse como:

$$\sigma = \text{Sign}_{\text{FORS}}(m) \parallel \text{Sign}_{\text{XMSS}}(\text{PK}_{\text{FORS}})$$

donde  $m$  es el mensaje,  $\sigma$  la firma resultante, y  $\text{PK}_{\text{FORS}}$  la clave pública intermedia.



Tabla I: Especificaciones técnicas de los dispositivos utilizados en los tres escenarios de simulación

Especificación	Servidor	IoT	Dispositivo móvil
Procesador	AMD Ryzen 5 8400F 6-Core 4.20 GHz	Quad-core ARM Cortex-A53 a 1.2 GHz	Octa-core 2.0 GHz
Memoria RAM	32.0 GB	1 GB LPDDR2	4 GB
Sistema operativo	SO de 64 bits, procesador x64	Raspberry Pi OS	Android 13
Arquitectura	x64	ARM (Cortex-A53)	ARM 64 bits

La verificación es válida si se cumple:

$$\text{Verify}_{\text{XMSS}}(\text{PK}_{\text{FORS}}, \sigma) = \text{PK}$$

El estándar incluye 12 variantes que combinan distintas funciones hash (SHA-2 y SHAKE), lo que da lugar a diferentes tamaños de clave, firmas y niveles de seguridad (128, 192 y 256 bits), permitiendo así adaptar su implementación a diversos escenarios de uso.

### B. Escenarios de prueba

Para la evaluación de los algoritmos post-cuánticos de firma digital, se definieron tres escenarios experimentales representativos: servidores, dispositivos del Internet de las Cosas (IoT) y dispositivos móviles. En cada escenario fue seleccionado un dispositivo representativo, incluyendo las especificaciones técnicas del hardware y software empleado, con el objetivo de garantizar la reproducibilidad en escenarios reales y la validez comparativa de los resultados obtenidos.

En la tabla I se presentan las especificaciones técnicas de los dispositivos utilizados en la evaluación de cada entorno de prueba.

**Servidores:** Este escenario representa una infraestructura típica de centro de datos o entorno en la nube, donde los recursos computacionales son abundantes y se prioriza la potencia de procesamiento.

**Dispositivos del Internet de las Cosas (IoT):** Este escenario representa una red de objetos físicos conectados a Internet mediante software, sensores y otras tecnologías. Para simular este entorno, se utilizó una Raspberry Pi 3 como dispositivo IoT, con el objetivo de evaluar el comportamiento de los algoritmos post-cuánticos en entornos con recursos computacionales limitados.

**Dispositivos móviles:** Este escenario representa un dispositivo portátil comúnmente usado por usuarios finales para tareas como comunicación, navegación y ejecución de aplicaciones. Para evaluar el comportamiento de los algoritmos, se empleó un teléfono inteligente con especificaciones estándar y un emulador de terminal Android (Termux), que permite ejecutar un entorno Linux en móviles.

### C. Evaluación de rendimiento (Benchmark)

Una prueba de rendimiento o comparativa (benchmark) es una técnica utilizada para medir el rendimiento de un sistema o de uno de sus componentes. Consiste en la ejecución de un programa informático, o conjunto de programas, en una máquina específica con el objetivo de estimar el comportamiento de un elemento concreto y comparar los resultados entre diferentes plataformas o configuraciones similares.

En este estudio, se realizaron pruebas benchmark sobre un sistema operativo Linux para evaluar el desempeño de los algoritmos seleccionados. Se utilizaron 17 tamaños distintos de mensajes, que varían desde 500 bytes hasta 1 MB, con el objetivo de analizar el comportamiento de los algoritmos frente a diferentes volúmenes de datos. Cada algoritmo fue evaluado en 961 ejecuciones. Para ello, se empleó el lenguaje de programación C y dos bibliotecas criptográficas especializadas: PQClean, una colección de implementaciones “limpias” de algoritmos poscuánticos [15], y liboqs, una biblioteca de código abierto en C que ofrece algoritmos resistentes a la computación cuántica, con integraciones prototipo en protocolos y aplicaciones reales [16].

A partir de estas pruebas se recopilaron las siguientes características y métricas:

- **Nombre del algoritmo:** denominación específica del esquema de firma digital evaluado.
- **Nivel de seguridad NIST:** clasificación entre 1 y 5, donde el nivel 5 representa el grado más alto de seguridad según las directrices del NIST.
- **Seguridad en bits:** estimación de la fortaleza criptográfica del algoritmo frente a ataques clásicos y cuánticos.
- **Tamaño de la clave pública (bytes):** cantidad de memoria que ocupa la clave pública del algoritmo.
- **Tamaño de la clave secreta (bytes):** tamaño en bytes de la clave privada utilizada para firmar.
- **Tamaño de la firma (bytes):** longitud de la firma generada por el algoritmo.
- **Uso máximo de memoria residente (RSS):** máximo tamaño del conjunto residente durante la ejecución de cada operación criptográfica.
- **Tiempo de generación de claves:** duración necesaria para generar el par de claves pública y privada.
- **Tiempo de firma:** tiempo requerido para firmar un mensaje.
- **Tiempo de verificación:** tiempo que tarda el algoritmo en verificar la validez de una firma.
- **Tiempo de CPU en modo usuario:** tiempo de CPU consumido específicamente por el proceso del usuario durante la ejecución.

### D. Agrupamiento de algoritmos

El clustering es una técnica de aprendizaje automático que busca agrupar datos en subconjuntos o clústeres de modo que los elementos dentro de cada grupo presenten características similares.

Entre los algoritmos de agrupamiento, destaca DBSCAN (Density-Based Spatial Clustering of Applications with Noise), un método basado en densidad, que a diferencia de algoritmos

como K-Means, no requiere especificar previamente el número de clústeres ( $k$ ), lo que lo hace especialmente útil cuando se desconoce la estructura subyacente de los datos. En su lugar, utiliza dos parámetros fundamentales:  $\varepsilon$  (epsilon), el radio de la vecindad alrededor de un punto  $x$  (es decir, la distancia máxima permitida para que otro punto sea considerado vecino), y  $MinPts$  (puntos mínimos), el número mínimo de puntos (incluyendo el propio  $x$ ) que deben estar dentro de la  $\varepsilon$ -vecindad para que el punto  $x$  sea considerado un *punto central* y, por tanto, pueda formar parte de un clúster [17].

Se eligió el algoritmo DBSCAN debido a su capacidad para identificar clústeres de forma arbitraria y detectar puntos atípicos (outliers). Esto es especialmente útil en el contexto en el que los datos pueden tener distribuciones o ruido que no están definidos uniformemente. DBSCAN aumenta la flexibilidad para trabajar con estructuras complejas y densidades variables [17], condiciones que se presentan frecuentemente en los escenarios evaluados durante la experimentación con algoritmos criptográficos. Además, se implementó la técnica de Análisis de Componentes Principales (PCA) con el propósito de reducir la dimensión del conjunto de datos, conservando aquellos componentes que explicaban el 95% de la varianza total, lo que nos permitió simplificar el conjunto de características manteniendo la estructura esencial de la información.

#### E. Métricas de evaluación del agrupamiento

Los indicadores de evaluación se emplean para medir la calidad y precisión de los modelos de aprendizaje automático. En este estudio, se utilizaron tres métricas internas con el fin de validar los resultados obtenidos durante el proceso de agrupamiento: el coeficiente de silueta, el índice de Davies–Bouldin y el índice de Calinski–Harabasz. Estas métricas permitieron comparar las agrupaciones generadas y seleccionar aquellas que ofrecían una mejor estructura interna y una mayor separación entre los clústeres.

**Coeficiente de silueta:** esta métrica evalúa qué tan bien se encuentra un punto dentro de su clúster en comparación con otros clústeres. El coeficiente que resulta se encuentra en el rango de  $[-1, 1]$ . Un valor cercano a  $+1$  indica que el punto está bien agrupado dentro de su clúster. Un valor cercano a 0 sugiere que el punto se encuentra en el límite entre dos clústeres. Finalmente, un valor cercano a  $-1$  implica que el punto podría haber sido asignado al clúster incorrecto [18].

**Índice de Davies–Bouldin:** esta métrica mide la similitud promedio entre cada clúster y el clúster más similar a él, considerando tanto la dispersión interna como la distancia entre clústeres. En términos generales, cuanto más compactos estén los clústeres y más separados estén entre sí, mejor será la puntuación. Una puntuación más baja indica una mejor calidad de agrupamiento.

**Índice de Calinski–Harabasz:** este índice evalúa la calidad del agrupamiento midiendo la relación entre la dispersión entre clústeres y la dispersión dentro de los clústeres. En este caso, una puntuación más alta indica una mejor separación entre los clústeres y, por tanto, una mayor calidad del agrupamiento.

### III. RESULTADOS

En este trabajo evaluamos el rendimiento de distintos algoritmos de firma digital post-cuánticos en tres entornos computacionales: dispositivo móvil, IoT y servidor. Para cada escenario, se aplicó el algoritmo de agrupamiento DBSCAN sobre los datos obtenidos, con el fin de identificar patrones de comportamiento y formar clústeres representativos en función de diversas métricas de desempeño.

La Tabla II presenta los valores promedio de cada clúster (CL) por escenario, considerando ocho indicadores clave: tamaño de la clave pública en bytes (PK), tamaño de la clave privada en bytes (SK), tamaño de la firma en bytes (SG), tiempo (ms) de generación de clave (KG), tiempo (ms) de firma (ST), tiempo (ms) de verificación (VT), tiempo de CPU en ms y consumo de memoria (RSS).

Tabla II: Métricas promedio por cluster y tipo de dispositivo

Móvil								
CL	PK	SK	SG	KG	ST	VT	CPU	RSS
1	1605.1	2052	2066.9	40	9.7	1.3	127	7000.9
2	48	96	34202.7	8.6	186	18.6	7.64	7818.7
3	48	96	17957.3	285	2.76	3.8	10.7	7822.9

IoT								
CL	PK	SK	SG	KG	ST	VT	CPU	RSS
1	1605	2652	2066.9	53.5	4.62	2.83	167	5973.1
2	48	96	34202.7	28.6	616	26.2	29970	6608.2
3	48	96	17957.3	967	9160	11.5	40100	6631.9

Servidor								
CL	PK	SK	SG	KG	ST	VT	CPU	RSS
C1	1605.14	2652	2066.86	4.9	0.42	0.30	16.15	5861.8
C2	48	96	34202.67	0.69	14.4	0.86	577	7774.9
C3	44	88	15432	17.58	159.3	0.40	505.3	7774.1
C4	48	96	16224	36.38	329	0.67	1285	7859.2
C5	64	128	29792	23.66	282.4	0.77	1655.9	7853.2

Para facilitar la interpretación visual de los resultados de agrupamiento, se aplicó un Análisis de Componentes Principales (PCA) a los conjuntos de datos de cada entorno. La Figura 1 muestra la proyección bidimensional de los clústeres generados por DBSCAN sobre los dos primeros componentes principales (PC1 y PC2), que capturan la mayor parte de la varianza de los datos. Cada gráfico representa uno de los escenarios evaluados (móvil, IoT y servidor) y permite observar la separación entre clústeres, así como su distribución relativa. Esta visualización es útil para validar la coherencia de los agrupamientos obtenidos.

La Tabla III resume los valores obtenidos de las métricas de evaluación de agrupamiento en los tres escenarios analizados.

Tabla III: Métricas de calidad de agrupamiento por entorno de evaluación

Métrica	Móvil	IoT	Servidor
Silueta	0.514	0.500	0.550
Índice de Davies–Bouldin	0.841	0.899	0.602
Índice de Calinski–Harabasz	329.26	318.34	372.97

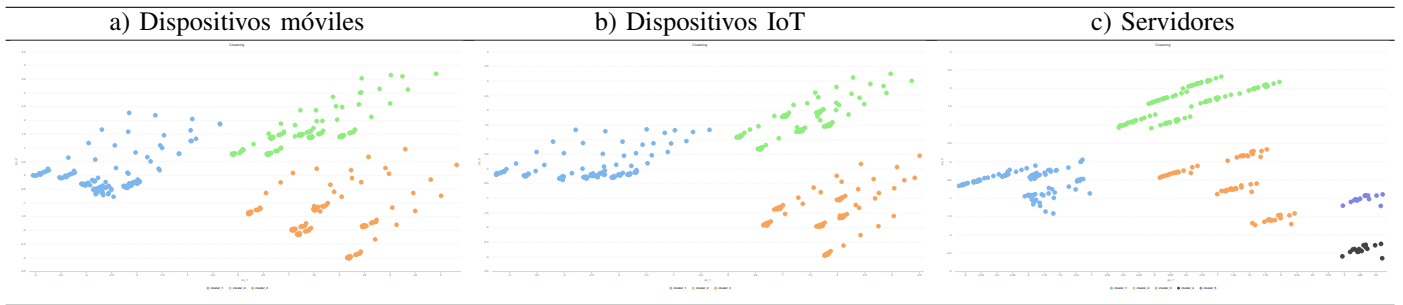


Fig. 1: Proyección PCA de clústeres generados por DBSCAN en los tres entornos: móvil, IoT y servidor.

#### A. Dispositivos móviles

Se aplicó DBSCAN con  $\varepsilon = 1.7$  y  $MinPoints = 5$ , obteniéndose tres clústeres. Su distribución, proyectada sobre los dos primeros componentes principales por PCA, se muestra en la Figura 1a. La Tabla IV muestra la distribución de los algoritmos de firma digital post-cuánticos agrupados por DBSCAN en el entorno móvil. Cada clúster agrupa variantes con comportamientos de rendimiento similares, lo que permite identificar patrones de eficiencia y posibles agrupaciones equivalentes en este tipo de dispositivos.

Tabla IV: Algoritmos asignados a cada clúster en el escenario de dispositivos móviles

Clúster	Algoritmos
1	ML-DSA 2, ML-DSA 3, ML-DSA 5, Falcon 1024, Falcon 512, Falcon PAD 1024, Falcon PAD 512
2	SLH-DSA 128f SHA2, SLH-DSA 192f SHA2, SLH-DSA 256f SHA2, SLH-DSA 128f SHAKE, SLH-DSA 192f SHAKE, SLH-DSA 256f SHAKE
3	SLH-DSA 128s SHA2, SLH-DSA 192s SHA2, SLH-DSA 256s SHA2, SLH-DSA 128s SHAKE, SLH-DSA 192s SHAKE, SLH-DSA 256s SHAKE

La calidad del agrupamiento se evaluó mediante tres métricas, cuyos resultados se muestran en la Tabla III. El Coeficiente de Silueta (0.514) sugiere una buena separación entre clústeres. El Índice de Davies–Bouldin (0.841) indica clústeres razonablemente compactos y separados, mientras que el alto valor del Índice de Calinski–Harabasz (329.26) refleja una estructura bien definida.

#### B. Dispositivos IoT

En el escenario IoT, se aplicó DBSCAN con  $\varepsilon = 1.9$  y  $MinPoints = 5$ , identificando tres clústeres con patrones de rendimiento diferenciados (Figura 1a). La distribución de algoritmos en cada grupo se muestra en la Tabla V. Las métricas de agrupamiento, detalladas en la Tabla III, confirman una buena separación y cohesión entre clústeres.

#### C. Plataforma servidores

Para este último escenario se emplearon valores de  $\varepsilon = 1.2$  y  $MinPoints = 5$ . En contraste con los otros escenarios, este conglomerado derivó en cinco agrupaciones, tal como se muestra en la Figura 1c. La Tabla VI muestra la asignación

Tabla V: Algoritmos agrupados por clúster en el escenario IoT

Clúster	Algoritmos
1	ML-DSA 2, ML-DSA 3, ML-DSA 5, Falcon 1024, Falcon 512, Falcon PAD 1024, Falcon PAD 512
2	SLH-DSA 128f SHA2, SLH-DSA 192f SHA2, SLH-DSA 256f SHA2, SLH-DSA 128f SHAKE, SLH-DSA 192f SHAKE, SLH-DSA 256f SHAKE
3	SLH-DSA 128s SHA2, SLH-DSA 192s SHA2, SLH-DSA 256s SHA2, SLH-DSA 128s SHAKE, SLH-DSA 192s SHAKE, SLH-DSA 256s SHAKE

de algoritmos a cada grupo. Los clústeres 1 y 2 agrupan algoritmos con patrones de rendimiento consistentes y eficientes, mientras que los grupos 3, 4 y 5 contienen configuraciones con características más particulares.

En especial, los clústeres 4 y 5 están conformados por un único algoritmo cada uno, debido a su comportamiento significativamente distinto. Estas variantes presentan mayor consumo de memoria y tiempos de firma más altos, lo que provoca su aislamiento en el espacio de características. DBSCAN los identifica como regiones densamente separadas, lo que justifica su clasificación independiente. Las métricas de calidad (ver Tabla III) respaldan esta segmentación: el coeficiente de silueta (0.55) refleja una separación clara entre grupos, el índice de Davies–Bouldin (0.602) indica buena compacidad y el valor de Calinski–Harabasz (372.97) evidencia una estructura bien definida del agrupamiento.

Tabla VI: Algoritmos agrupados por clúster en servidores

Clúster	Algoritmos
1	ML-DSA 2, ML-DSA 3, ML-DSA 5, Falcon 1024, Falcon 512, Falcon PAD 1024, Falcon PAD 512
2	SLH-DSA 128f SHA2, SLH-DSA 192f SHA2, SLH-DSA 256f SHA2, SLH-DSA 128f SHAKE, SLH-DSA 192f SHAKE, SLH-DSA 256f SHAKE
3	SLH-DSA 128s SHA2, SLH-DSA 192s SHA2, SLH-DSA 256s SHA2
4	SLH-DSA 128s SHAKE, SLH-DSA 192s SHAKE
5	SLH-DSA 256s SHAKE

## IV. DISCUSIÓN

El agrupamiento realizado mediante DBSCAN permitió identificar patrones de rendimiento que vinculan ciertos algoritmos con escenarios tecnológicos específicos. Aunque el



nivel de seguridad NIST no se incluyó como variable en el modelo, se controló previamente para asegurar equivalencia criptográfica entre los esquemas evaluados. Los resultados permiten formular recomendaciones fundamentadas para la selección de algoritmos en función del tipo de dispositivo.

En el contexto de dispositivos móviles, se recomienda el grupo correspondiente al cluster 2, compuesto por variantes SLH-DSA fast. Estos algoritmos ofrecen un rendimiento más equilibrado frente a sus contrapartes small, ya que combinan una ejecución más rápida con un tamaño de clave razonable, resultando adecuados en entornos con recursos limitados. Además, su diseño sin estado aporta ventajas en seguridad, al evitar vulnerabilidades asociadas a la gestión de claves.

Para entornos IoT, caracterizados por severas restricciones de memoria y procesamiento, el grupo del cluster 3 compuesto por variantes SLH-DSA small resulta el más adecuado. Estos algoritmos destacan por sus claves y firmas de tamaño reducido, lo cual facilita su implementación en microcontroladores y sistemas embebidos. Aunque su ejecución es más lenta, este aspecto no suele ser crítico en aplicaciones IoT, donde las operaciones criptográficas son poco frecuentes.

Para servidores, el cluster 1 ofrece una alternativa robusta, integrando algoritmos como ML-DSA y Falcon que equilibran velocidad y seguridad post-cuántica. Aunque sus demandas computacionales son elevadas, su uso se justifica en infraestructuras críticas y aplicaciones que requieren firmar o verificar grandes volúmenes de datos, donde el rendimiento es prioritario sobre la eficiencia de recursos.

En conjunto, los agrupamientos obtenidos permiten establecer perfiles de uso claros para cada familia de algoritmos post-cuánticos, alineados con las capacidades y restricciones de distintos entornos tecnológicos. Esta clasificación orientada al contexto facilita decisiones de implementación más informadas y robustas frente al desafío que plantea la transición hacia criptografía resistente a la computación cuántica.

## V. CONCLUSIONES

Este análisis permitió clasificar algoritmos post-cuánticos de firma digital basándose en métricas benchmark mediante DBSCAN. Así, se identificaron grupos de algoritmos con características comunes que permiten recomendar soluciones adaptadas a dispositivos móviles, IoT y servidores.

Para dispositivos móviles, se destacó el cluster 2, compuesto por variantes SLH-DSA fast, que presentan un buen equilibrio entre tamaño de clave/firma y tiempo de ejecución. Estos algoritmos ofrecen un rendimiento ágil y un uso moderado de recursos, lo que los hace apropiados para aplicaciones móviles. En el caso de los dispositivos IoT, el cluster 3, dominado por variantes SLH-DSA small, fue el más adecuado debido a los tamaños reducidos de clave y firma, priorizando la eficiencia energética y el bajo uso de memoria, aspectos clave en sistemas embebidos y sensores. Finalmente, para entornos con mayor capacidad como los servidores, el cluster 1 integrado por ML-DSA en sus tres versiones y Falcon en sus variantes 512, 1024 y padded fue el más favorable. Estos algoritmos se caracterizan por su alto rendimiento criptográfico y eficiencia

en operaciones de firma y verificación, siendo adecuados para servicios de gran escala como aplicaciones en la nube o infraestructuras críticas.

En conjunto, esta clasificación basada en clusters permite guiar de forma efectiva la selección de algoritmos post-cuánticos según el entorno, promoviendo implementaciones más seguras, eficientes y sostenibles.

## REFERENCIAS

- [1] R. Rietsche, C. Dremel, S. Bosch, L. Steinacker, M. Meckel, and J.-M. Leimeister, "Quantum computing," *Electronic Markets*, vol. 32, no. 4, pp. 2525–2536, 2022.
- [2] U. Musa, M. Adebisi, O. Aroba, and A. Adebisi, "Rsa and elliptic curve encryption system:," *International Journal of Information Security and Privacy*, vol. 18, pp. 1–27, 03 2024.
- [3] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "Report on post-quantum cryptography," *NIST Interagency/Internal Report (NISTIR)*, vol. 8105, April 2016, national Institute of Standards and Technology, U.S. Department of Commerce.
- [4] M. Abbasi, F. Cardoso, P. Váz, and J. Silva, "A practical performance benchmark of post-quantum cryptography across heterogeneous computing environments," *Cryptography*, vol. 9, no. 2, 2025.
- [5] N. I. of Standards and Technology, "Federal Information Processing Standards Publication 204: ML-DSA – Module Lattice-Based Digital Signature Algorithm," U.S. Department of Commerce, Tech. Rep. FIPS PUB 204, 2024, available free of charge from NIST.
- [6] —, "Submission requirements and evaluation criteria for the fast-fourier ntru lattice-based digital signature algorithm (fn-dsa)," U.S. Department of Commerce, NIST, Tech. Rep. NIST IR 8547, 2024.
- [7] D. Dziechciarz and M. Niemiec, "Efficiency analysis of nist-standardized post-quantum cryptographic algorithms for digital signatures in various environments," *Electronics*, vol. 14, no. 1, p. 70, dec 2025.
- [8] P. Pote and R. Bansode, "Performance evaluation of post-quantum cryptography: A comprehensive framework for experimental analysis," *Journal of Information Systems Engineering and Management*, vol. 10, no. 9s, pp. 548–556, Feb. 2025.
- [9] L. Beckwith, D. T. Nguyen, and K. Gaj, "Hardware accelerators for digital signature algorithms dilithium and falcon," *IEEE Design & Test*, vol. 41, no. 5, pp. 27–35, 2023, aceleradores de hardware para algoritmos de firma digital en entornos IoT.
- [10] R. Mandev and E. B. Kavun, "Performance comparison of post-quantum signature algorithms through an android email application plug-in," in *Proceedings of the IEEE International Conference on Omni-layer Intelligent Systems (COINS)*. IEEE, 2023.
- [11] C. Balamurugan, K. Singh, G. Ganesan, and M. Rajarajan, "Post-quantum and code-based cryptography—some prospective research directions," *Cryptography*, vol. 5, no. 4, 2021.
- [12] National Institute of Standards and Technology (NIST), "Nist releases first 3 finalized post-quantum encryption standards," <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>, Aug. 2024, Último acceso: 26jun2025.
- [13] V. Clupek, L. Malina, and V. Zeman, "Secure digital archiving in post-quantum era," in *2015 38th International Conference on Telecommunications and Signal Processing (TSP)*, 2015, pp. 622–626.
- [14] N. I. of Standards and Technology, "Stateless hash-based digital signature standard," U.S. Department of Commerce, Tech. Rep. FIPS 205, August 2024.
- [15] M. J. Kannwischer, P. Schwabe, D. Stebila, and T. Wiggers, "Improving software quality in cryptography standardization projects," *Cryptology ePrint Archive*, Paper 2022/337, 2022.
- [16] D. Stebila and M. Mosca, "Post-quantum key exchange for the internet and the open quantum safe project," in *Selected Areas in Cryptography (SAC) 2016*, ser. Lecture Notes in Computer Science, R. Avanzi and H. Heys, Eds., vol. 10532. Springer, Oct. 2017, pp. 1–24.
- [17] N. Ohadi, A. Kamandi, M. Shabankhah, S. M. Fatemi, S. M. Hosseini, and A. Mahmoudi, "Sw-dbscan: A grid-based dbscan algorithm for large datasets," in *2020 6th International Conference on Web Research (ICWR)*, 2020, pp. 139–145.
- [18] K. R. Shahapure and C. Nicholas, "Cluster quality analysis using silhouette score," in *2020 IEEE 7th International Conference on Data Science and Advanced Analytics (DSAA)*, 2020, pp. 747–748.