Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Xander: un ensamble cuántico-clásico para la detección de intrusiones avanzadas en redes modernas

Oscar Javier Peñaloza Araque
https://orcid.org/0009-0000-5482-9891
Universidad Internacional de La Rioja, Logroño, España
oscarjavier.penaloza063@comunidadunir.net

Fecha de recepción: 7 de junio de 2026
Fecha de aceptación: 30 de junio de 2026
Fecha de publicación: 31 de julio de 2026

DOI: https://doi.org/10.59722/riic.v3i2.1233

Cómo citar: Peñaloza Araque, O. J. (2026). Xander: un ensamble cuántico-clásico para la detección de intrusiones avanzadas en redes modernas. *Revista Iberoamericana de Innovación Científica JA TUAIDA, 3*(2), 4–36. https://doi.org/10.59722/riic.v3i2.1233

RESUMEN

La creciente complejidad de las amenazas cibernéticas exige sistemas de detección de intrusiones capaces de procesar tráfico de red dinámico y de alta dimensión. Aunque los métodos clásicos de aprendizaje automático han logrado un gran rendimiento en este ámbito, siguen enfrentándose a limitaciones relacionadas con la escalabilidad, la adaptabilidad y la robustez frente a los patrones de ataque en constante evolución. El aprendizaje automático cuántico se ha revelado como una alternativa prometedora; sin embargo, los procesadores cuánticos actuales imponen limitaciones prácticas relacionadas con el ruido, la disponibilidad limitada de qubits, la decoherencia y la profundidad de los circuitos. Este artículo presenta a Xander, una arquitectura híbrida en ensamble cuántico-clásico para la detección de intrusiones en redes bajo las restricciones de la era NISQ. El marco propuesto integra modelos cuánticos, entre los que se incluyen componentes de máquinas de vectores de soporte cuánticos, clasificadores cuánticos variacionales y redes neuronales convolucionales cuánticas, con modelos clásicos como Random Forest, XGBoost y perceptrones multicapa. Estos modelos se combinan mediante un mecanismo optimizado de votación suave ponderada y se complementan con una estrategia de respaldo dinámica diseñada para reducir el impacto de los resultados cuánticos inestables. Los experimentos se llevaron a cabo utilizando subconjuntos reducidos y preprocesados de los conjuntos de datos CIC-IDS-2017 y CIC-IDS-2018, aplicando el análisis de componentes principales para permitir la codificación de características compatibles con la cuántica. El marco se evaluó mediante simulación clásica, simulación cuántica y ejecución en hardware cuántico real. Los resultados muestran que el enfoque híbrido alcanza un alto rendimiento de clasificación y mantiene un comportamiento estable bajo el ruido inducido por el hardware, alcanzando un rendimiento competitivo. Los hallazgos sugieren que los modelos híbridos constituyen una vía práctica para integrar la computación cuántica en aplicaciones de ciberseguridad sin requerir una ventaja cuántica a corto plazo.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Palabras clave:
aprendizaje automático cuántico, ciberseguridad, modelos híbridos, NISQ, sistemas de detección de intrusiones.

Xander: A Quantum-Classical Hybrid Ensemble for Advanced Network Intrusion Detection

ABSTRACT

The increasing complexity of cyber threats calls for intrusion detection systems capable of processing dynamic, high-dimensional network traffic. Although classical machine learning methods have achieved strong performance in this field, they continue to face limitations in scalability, adaptability, and robustness against constantly evolving attack patterns. Quantum machine learning has emerged as a promising alternative; however, current quantum processors impose practical constraints related to noise, limited qubit availability, decoherence, and circuit depth. This article introduces Xander, a hybrid quantum–classical ensemble architecture for network intrusion detection under the constraints of the noisy intermediate-scale quantum (NISQ) era. The proposed framework integrates quantum models, including quantum support vector machine components, variational quantum classifiers, and quantum convolutional neural networks, with classical models such as Random Forest, XGBoost, and multilayer perceptrons. These models are combined through an optimized weighted soft-voting mechanism and supplemented by a dynamic fallback strategy designed to mitigate the impact of unstable quantum outputs. Experiments were conducted using reduced and preprocessed subsets of the CIC-IDS2017 and CSE-CIC-IDS2018 datasets. Principal component analysis was applied to enable quantum-compatible feature encoding. The framework was evaluated through classical simulation, quantum simulation, and execution on real quantum hardware. The results show that the hybrid approach achieves high classification performance and remains stable under hardware-induced noise while delivering competitive results. The findings suggest that hybrid models provide a practical pathway for integrating quantum computing into cybersecurity applications without requiring a near-term quantum advantage.

Keywords:
quantum machine learning; cybersecurity; hybrid models; noisy intermediate-scale quantum; intrusion detection systems.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Xander: um ensemble quântico-clássico para a detecção avançada de intrusões em redes modernas

RESUMO

A crescente complexidade das ameaças cibernéticas exige sistemas de detecção de intrusões capazes de processar tráfego de rede dinâmico e de alta dimensionalidade. Embora os métodos clássicos de aprendizado de máquina tenham alcançado elevado desempenho nesse domínio, eles ainda enfrentam limitações relacionadas à escalabilidade, à adaptabilidade e à robustez diante de padrões de ataque em constante evolução. O aprendizado de máquina quântico tem se mostrado uma alternativa promissora; contudo, os processadores quânticos atuais impõem restrições práticas relacionadas ao ruído, à disponibilidade limitada de qubits, à decoerência e à profundidade dos circuitos. Este artigo apresenta o Xander, uma arquitetura híbrida de ensemble quântico-clássico para a detecção de intrusões em redes, desenvolvida sob as restrições da era quântica de escala intermediária e ruidosa (NISQ). O framework proposto integra modelos quânticos, incluindo componentes de máquinas de vetores de suporte quânticas, classificadores quânticos variacionais e redes neurais convolucionais quânticas, a modelos clássicos, como Random Forest, XGBoost e perceptrons multicamadas. Esses modelos são combinados por meio de um mecanismo otimizado de votação suave ponderada e complementados por uma estratégia dinâmica de contingência, desenvolvida para reduzir o impacto de resultados quânticos instáveis. Os experimentos foram conduzidos com subconjuntos reduzidos e pré-processados dos conjuntos de dados CIC-IDS-2017 e CIC-IDS-2018. Aplicou-se a análise de componentes principais para viabilizar uma codificação de atributos compatível com sistemas quânticos. O framework foi avaliado por meio de simulação clássica, simulação quântica e execução em hardware quântico real. Os resultados demonstram que a abordagem híbrida alcança elevado desempenho de classificação e mantém um comportamento estável sob o ruído induzido pelo hardware, apresentando resultados competitivos. Os achados indicam que os modelos híbridos constituem uma alternativa prática para integrar a computação quântica a aplicações de cibersegurança, sem exigir a obtenção de vantagem quântica no curto prazo.

Palavras-chave:
aprendizado de máquina quântico; cibersegurança; modelos híbridos; computação quântica de escala intermediária e ruidosa; sistemas de detecção de intrusões.

Introducción

Los sistemas para observar y detectar intrusos en la red IDS, constituyen elementos fundamentales en las infraestructuras actuales de ciberseguridad, permitiendo encontrar actividades anómalas en el tráfico de red. Debido a la complejidad de las redes y a la sofisticación de los ataques cibernéticos, los sistemas tradicionales basados en firmas no son suficientes y ha habido un cambio hacia los enfoques del aprendizaje automático.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Recientemente, este campo demuestra un gran potencial utilizando conceptos como superposición y entrelazamiento mejorando la representación informática. Sin embargo, las limitaciones actuales, de la era cuántica ruidosa, impiden que los modelos cuánticos superen técnicas convencionales en momentos concretos de ciberseguridad.

Con el fin de lograr esta detección, en redes empresariales y sistemas modernos distribuidos, son fundamentales los IDS, que permiten identificar anomalías en el tráfico de red. Antes, estos sistemas enfocaban patrones conocidos usando métodos de aprendizaje automático comunes, que funcionaban bien en situaciones con tráfico predecible (Almseidin et al., 2018; Sarker, 2021).

No obstante, investigaciones recientes muestran que estos enfoques son insuficientes con tráfico encriptado, anómalo, nuevas vulnerabilidades, y entorno cambiante (Khan et al., 2019; Musa et al., 2020; Rawat et al., 2022; Alotaibi & Rassam, 2023). Se observa precisión baja y alertas falsas en redes 5G e Internet de las Cosas (Pinto et al., 2023; Sharafaldin et al., 2018). Ahora, hay enfoques hacia redes 6G, donde la cantidad de dispositivos y velocidad de respuesta casi instantánea superan la estabilidad metodológica actual (Sharafaldin et al., 2018). Mientras tanto, se exploran combinaciones de técnicas cuánticas y clásicas, pero todavía estamos lejos de poder usarlas en la práctica (Alluhaibi, 2024; Fan et al., 2024; Shen et al., 2024).

Para superar estos inconvenientes, la ciencia ha avanzado hacia el uso de estructuras de aprendizaje profundo. Se han propuesto esquemas que emplean redes neuronales, LSTM y GRU para una mejor obtención de atributos temporales en flujos de red complicados (Odeh & Abu Taleb, 2023; Rehman et al., 2025). Asimismo, se han aplicado métodos generativos como MAD-GAN y otras versiones de GAN para expandir las colecciones de datos de adiestramiento y hallar irregularidades multivariadas en secuencias temporales de alta dimensión (Li et al., 2019; Ajdani, 2025; Kalyan et al., 2025). También se están revisando sistemas de conjunto y modelos mixtos de aprendizaje profundo para lidiar con la variedad de problemas de seguridad en IoT y en la nube (Danso et al., 2022; Maseer et al., 2023; Nazim et al., 2025; Premalatha, 2025). Últimamente, ha aparecido una corriente hacia estructuras que integran ensamblajes, las cuales juntan modelos cuánticos y clásicos mediante sistemas de votación y ajuste dinámico (Abreu et al., 2024; Nazim et al., 2025; Premalatha, 2025). No obstante, los esquemas de aprendizaje profundo habituales aún se

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

topan con elevados gastos de cálculo y obstáculos de escalabilidad, en especial al examinar grupos enormes como CIC-IDS-2017 o IoT-23 (Akif et al., 2025; Ganapathi & Shanmugapriya, 2019; Noor et al., 2025).

En este escenario, el aprendizaje automático cuántico surge como una solución novedosa. Hacer uso del espacio de Hilbert con mapeos de características cuánticas permite distinguir mejores categorías complejas de datos (Havlíček et al., 2019; Orazi et al., 2024). La cuántica actual, afectada por el ruido, es investigada con un enfoque de algoritmos híbridos, los cuales son integrados por componentes cuántico-clásicos (Cerezo et al., 2021; Metawei et al., 2020; Solar et al., 2024), entre ellos; QSVM y VQC. Quienes demuestran ser bastante eficientes en clasificación de dos o más categorías de datos (Camargo et al., 2024; Abdulrazzaq Altarraji & Mokdad, 2024; Farhi & Neven, 2018).

Es así como las combinaciones QSVM con optimizadores en evolución implementados recién, junto con arquitecturas QCNN y QNN, alcanzan precisiones sobre el 98% referenciadas en (Dong et al., 2022; Elsedimy et al., 2024; Kadry et al., 2023; Kalinin & Krundyshev, 2023; Nicesio et al., 2023). Estas pruebas suelen ser realizadas con datasets estándar como; NSL-KDD, UNSW-NB15 y CIC-MalMem 2022 (Gong et al., 2022; Kim & Madhavi, 2024; Talukder et al., 2023). La literatura enmarca la precisión en metodologías reproducibles aún, cuando la ventaja cuántica pura está en avances exploratorios, los sistemas híbridos computados inspirados en la cuántica, representan el camino de facto para los IDS de próxima generación (Fan et al., 2024; Shen et al., 2024). La evolución de los modelos tradicionales hacia los híbridos automatizados sigue siendo un área de estudio, soporte para garantizar la solidez y estabilidad de las infraestructuras digitales globales (Noor et al., 2018; Khan et al., 2024; Hozouri et al., 2025).

Problema de investigación

Los sistemas tradicionales de detección de intrusos presentan problemas para adaptarse ante ataques que están en constante cambio. Por su parte, los modelos cuánticos actuales, debido a las limitaciones de la era NISQ, no pueden superar de manera eficiente a los métodos tradicionales debido al ruido, la pérdida de coherencia y la escasez de qubits. Por tal razón, es importante investigar arquitecturas que combinen ambos enfoques para conseguir una mayor estabilidad y un rendimiento confiable en situaciones reales de ciberseguridad.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Objetivo general

Diseñar y evaluar una arquitectura híbrida cuántico-clásica, para la detección de intrusiones en redes modernas, capaz de integrar modelos de ambos dominios y superar las limitaciones de los enfoques puramente clásicos o cuánticos bajo la era NISQ.

Objetivos específicos

1. Implementar modelos cuánticos (QSVM, VQC, QCNN) y clásicos (RF, XGBoost, MLP) sobre datasets estándar de IDS.
2. Integrar dichos modelos mediante un mecanismo de votación ponderada suave con ajuste dinámico de pesos.
3. Evaluar el desempeño del ensamble híbrido en simulación clásica, simulación cuántica y hardware cuántico real.
4. Validar estadísticamente los resultados mediante pruebas de hipótesis, intervalos de confianza y tamaños de efecto.

Hipótesis

El ensamble híbrido Xander indica un desempeño más robusto y confiable que los modelos cuánticos individuales, manteniendo métricas comparables con los mejores modelos clásicos, gracias a la integración de representaciones cuánticas y la estabilidad de los algoritmos clásicos bajo las limitaciones NISQ.

Contribución científica

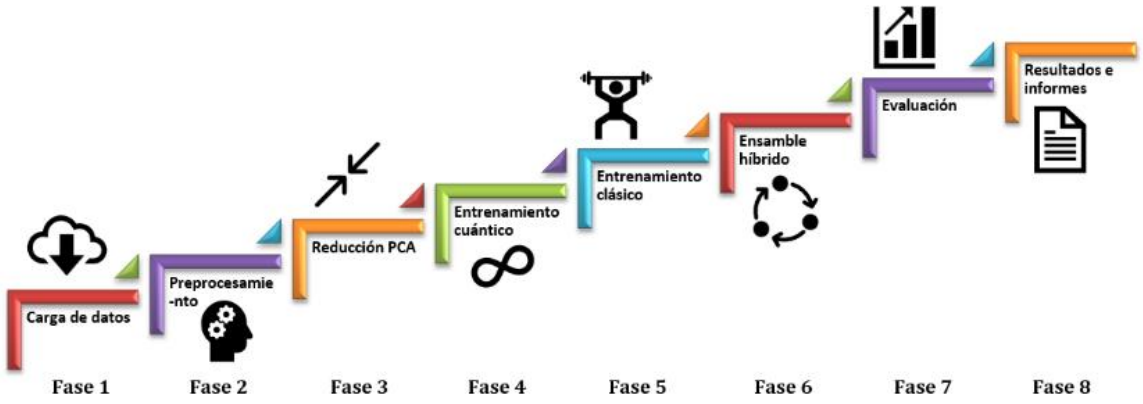
Xander aporta un marco reproducible y práctico para la integración híbrida cuántico-clásica en ciberseguridad, demostrando que la ventaja cuántica no es indispensable a corto plazo. Su principal aporte radica en la estabilidad intermodelo, la reducción de la varianza de error y la validación experimental en entornos reales de hardware cuántico.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Metodología

La Figura 1 presenta las ocho fases que integran el proceso de ejecución del algoritmo Xander, desde la carga y el preprocesamiento de los datos hasta la evaluación y generación de los resultados.

Figura 1
Fases de ejecución del algoritmo Xander



Esta metodología detalla un estudio experimental, realizado a través de procesadores los cuales buscan comparar un sistema híbrido cuántico-clásico para detectar intrusiones, teniendo en cuenta las consideraciones acerca de las limitantes del NISQ.

Conjunto de datos

CIC-IDS-2017 y CIC-IDS-2018, esta data contiene tráfico de red que simula situaciones reales, donde se observan tanto comportamientos normales y malicioso, abarcan ataques como; denegación de servicio distribuida (DDoS), escaneo de puertos y ataques de fuerza bruta (Sharafaldin et al., 2018).

Preprocesamiento de datos

El preprocesamiento de la data se lleva a cabo, para garantizar la compatibilidad cuántico-clásica de los modelos. Por tanto, se aplicaron los siguientes pasos:

- Limpieza de datos y eliminación de valores faltantes o inconsistentes.
- Codificación de etiquetas para las variables categóricas.
- Escalado de características mediante StandardScaler.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Configuración experimental

Para poder repetir el experimento, se fijaron las condiciones de esta forma:

- Semilla aleatoria: 42 (para garantizar reproducibilidad).
- División de datos: 70 % de entrenamiento, 15 % de validación, 15 % de prueba
- Validación cruzada: validación cruzada de 5 pliegues sobre los datos de entrenamiento
- Número de muestras: 2.500 estratificadas (balance entre representatividad y coste computacional).
- Reducción dimensional (PCA): 6 componentes principales.
- Entorno de software: Python 3.x con Scikit-learn, Qiskit IBM Quantum Runtime.
- Ejecución cuántica: simulador Aer local, simulador IBM Quantum, procesador real ibm_kingston.

Submuestreo y tamaños muestrales

Dataset = 20.000 registros

Submuestreo estratificado = 2.500 muestras para;

- Reducir el coste computacional en simuladores cuánticos (*Aer, IBM Simulador*).
- Ajustar la dimensionalidad al número de qubits disponibles (*6 qubits → PCA con 6 componentes principales).*
- Evitar decoherencia y tiempos excesivos en (*ibm_kingston*).

Impacto de los tamaños muestrales

- 20.000 registros (dataset completo); Usado para entrenamiento de clasificadores clásicos (RF, XGB, MLP). Resultados estables y métricas cercanas al 98-99% de accuracy.
- 2.500 registros (submuestreo); Usado en pipelines cuánticos (QSVM, VQC, QCNN). Accuracy cerca al 97.8%
- 200 registros en hardware real con una caída al 76%.
- 500 registros obtenidos mediante validación cruzada estratificada; Sobre las observaciones obtenidas en dicho conjunto se calcularon las métricas de

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

desempeño y se aplicaron las pruebas estadísticas (Shapiro-Wilk, Levene, t-test, ANOVA). Para evaluar la consistencia del desempeño de los modelos.

Arquitectura del modelo e hiperparámetros

- Modelos clásicos:
  - Bosque aleatorio (RF); *500 árboles, profundidad máxima = None, criterio = Gini.*
  - Refuerzo de gradientes extremos (XGBoost); *learning rate = 0.1, max_depth = 6, n_estimators = 300, subsample = 0.8.*
  - Perceptrón multicapa (MLP); *3 capas ocultas (128–64–32), activación ReLU, optimizador Adam, learning rate = 0.001, batch size = 64, épocas = 50.*
- Modelos cuánticos:
  - Máquina de vectores de soporte cuántica (QSVM); *kernel cuántico con aproximación Nyström (m=50), ZZFeatureMap con reps=1, regularización C=1.0.*
  - Clasificador cuántico variacional (VQC); *6 qubits, ansatz con capas de RY y CX, optimizador COBYLA, learning rate adaptativo.*
  - Red neuronal convolucional cuántica (QCNN); *6 qubits, bloques convolucionales con entrelazamiento lineal, profundidad limitada para reducir ruido, optimizador SPSA.*

Parámetros de ejecución cuántica

- Número de qubits: 6, (sweet spot para balancear expresividad y ruido).
- Shots: 1024 por circuito.
- Batch size: 900 circuitos por lote.
- Anchors Nyström: 50 puntos de referencia seleccionados aleatoriamente.
- Tiempo de ejecución en simulador Aer: ~25 minutos por experimento.
- Circuitos con profundidad mínima, entrelazamiento lineal, segmentación en lotes pequeños para evitar decoherencia y límites de tiempo.

Pseudocódigo del algoritmo Xander

Entrada: Dataset CIC-IDS-2017 / CIC-IDS-2018

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Parámetros: *N_QUBITS, N_SAMPLES, N_ANCHORS, BATCH_SIZE, SHOTS*

1. Preprocesamiento de datos
   1.1. Cargar dataset
   1.2. Limpiar valores faltantes/inconsistentes
   1.3. Codificar etiquetas categóricas
   1.4. Escalar características (StandardScaler)
   1.5. Reducir dimensionalidad con *PCA* → *N_QUBITS* componentes
2. División de datos
   2.1. Estratificar y dividir en entrenamiento, validación y prueba
   2.2. Seleccionar puntos de anclaje Nyström (m)
3. Construcción de circuitos cuánticos
   3.1. Para cada par(x_t, x_a);
      3.1.1. Inyectar datos $U(x_t)$ qubits
      3.1.2. Aplicar entrelazamiento (CX)
      3.1.3. Inyectar datos inversos $U^{\dagger}(x_a)$
      3.1.4. Medir registro clásico

   Fin para

4. Ejecución en backend
   4.1. Si *USE_REAL_QPU* = 1;
      4.1.1. Transpilar circuitos → backend IBM Quantum
      4.1.2. Ejecutar en lotes de tamaño *BATCH_SIZE*
      4.1.3. Recuperar probabilidades de colapso $|0 \ldots 0\rangle$

   Si no;

      Ejecutar en simulador local *Aer/StatevectorSampler*

5. Reconstrucción de matrices kernel
   5.1. Construir $K_t rainyK_t est$ con probabilidades Nyström
   5.2. Guardar matrices para reproducibilidad
6. Entrenamiento de modelos
   6.1. Modelos clásicos: *RF, XGBoost, MLP*

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

6.2. Modelos cuánticos: QSVM, VQC, QCNN

6.3. Ajustar hiperparámetros mediante validación cruzada

7. Ensamble híbrido

7.1. Calcular predicciones $p_k(y|x)d$ de cada modelo

7.2. Combinar mediante votación ponderada:

$$\hat{p}\,(y=1|x) = \sum_{k=1}^{M} w_k \,.p_k\,(y=1|x)$$

7.3. Ajustar pesos dinámicamente según confianza c_k

8. Regla de decisión

$$Si\ \ \hat{p}\,(y=1|x)\ \geq ;$$

$$y_{pred} = 1$$

En otro caso:

$$y_{pred} = 0$$

9. Evaluación

9.1. Calcular métricas: *Accuracy, Precision, Recall, F1, ROC-AUC*

9.2. Aplicar pruebas estadísticas: *Shapiro-Wilk, Levene, t-test pareado, ANOVA*

9.3. Reportar intervalos de confianza y tamaños de efecto

Salida:

- Rendimiento del ensamble híbrido Xander
- Comparación con modelos clásicos y cuánticos individuales

Formulación matemática

Componentes matemáticos del modelo; variables, parámetros y restricciones empleadas durante el entrenamiento y la inferencia.

- Kernel cuántico con aproximación Nyström

Sea

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

el conjunto de entrenamiento, donde:

$\boldsymbol{N}$ → representa el número total de muestras utilizadas para el entrenamiento.

$\boldsymbol{x_i} \in \mathbb{R}^{\boldsymbol{d}}$ → corresponde al vector de características de la muestra $\boldsymbol{i}$.

$\boldsymbol{d}$ → representa el número de características después del proceso de reducción de dimensionalidad mediante PCA.

$\boldsymbol{y_i} \in \{\boldsymbol{0}, \boldsymbol{1}\}$ → corresponde a la etiqueta de clasificación, donde **0** representa tráfico benigno y **1** tráfico malicioso.

Con el propósito de reducir el costo computacional asociado al cálculo del kernel cuántico completo, se emplea la aproximación de Nyström.

Para cada par $(Muestra = x_t,\ Anclaje = x_a)$ se define el kernel cuántico como;

$$K(x_t, x_a) = \Pr\left(|0 \dots 0\rangle \mid U(x_t)\, U^{\dagger}(x_a) \right)$$

donde;

$\boldsymbol{x_t}$ = Muestra;

$\boldsymbol{x_a}$ = Anclaje;

$\boldsymbol{U(\cdot)}$ → representa el circuito de codificación o feature map cuántico;

$\boldsymbol{U^{\dagger}}$ → denota el operador adjunto del circuito;

$\mathbf{Pr}(|\mathbf{0} \dots \mathbf{0}\rangle)$ → corresponde a la probabilidad de medir el estado base después de aplicar el circuito cuántico;

$\boldsymbol{K(x_t, x_a)} \in [\boldsymbol{0}, \boldsymbol{1}]$ → representa la similitud cuántica entre ambas muestras.

A partir de esta definición, las matrices aproximadas del kernel se construyen como;

donde:

K_{train} → corresponde al número de muestras de entrenamiento;

K_{test} → representa el número de muestras de evaluación;

m → es el número de anclajes Nyström.

- Clasificador cuántico (QSVM)

Una vez reconstruido el espacio de características mediante el kernel aproximado, el

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

clasificador QSVM determina la frontera de decisión mediante

donde:

$\boldsymbol{\alpha_i}$ → representa los multiplicadores de Lagrange obtenidos durante el proceso de entrenamiento;

$\boldsymbol{y_i}$ → corresponde a la etiqueta asociada a la muestra de entrenamiento;

$\boldsymbol{K(x, y_i)}$ → representa el kernel cuántico evaluado entre la muestra de entrada y la muestra de entrenamiento;

$\boldsymbol{b}$ → corresponde al término de sesgo del hiperplano de separación;

$\boldsymbol{f(x)}$ → determina la clase predicha por el modelo.

- Función objetivo del entrenamiento

Durante el proceso de entrenamiento, cada clasificador optimiza una función de pérdida específica. De forma general, el problema de optimización puede expresarse como:

$$\theta^* = arg\min_{\theta} L(\theta)$$

donde:

$\boldsymbol{\theta}$ → representa el conjunto de parámetros entrenables del modelo;

$\boldsymbol{L(\theta)}$ → corresponde a la función objetivo empleada durante el entrenamiento;

$\boldsymbol{\theta^*}$ → representa el conjunto de parámetros óptimos obtenidos al finalizar el proceso de optimización.

- Votación ponderada suave del ensamble

$\boldsymbol{M}$ = número total de clasificadores que conforman a Xander, y la probabilidad final asociada a la clase positiva se calcula mediante

$$\hat{p}\,(y = 1|x) = \sum_{k=1}^{M} w_k \,.p_k\,(y = 1|x)$$

donde:

$\boldsymbol{M}$→ representa el número total de modelos participantes;

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

w_k → corresponde al peso asignado al clasificador k;

$p_k\,(y = 1|x)$ → representa la probabilidad estimada por dicho clasificador para la muestra x.

Los pesos satisfacen las siguientes restricciones:

- Ajuste dinámico de pesos.

Para reducir el impacto de resultados inestables, los pesos cuánticos se ajustan según su confianza c_k;

donde:

w'_k → representa el nuevo peso asignado al clasificador k;
c_k → corresponde al índice de confianza del clasificador k;
$c_k \in [0, 1]$ → donde valores próximos a uno indican mayor estabilidad experimental.

- Regla de decisión final

La predicción final se define como:

donde:

$\hat{y}$ → representa la clase predicha;

τ → corresponde al umbral de decisión.

$\tau = 0,5$

- Mecanismo de respaldo (Fallback)

Con el fin de garantizar la continuidad del proceso de inferencia cuando la ejecución cuántica no pueda completarse debido a limitaciones del hardware, tiempos de espera o errores de ejecución, se implementó un mecanismo de respaldo (fallback) definido como:

donde:

$\hat{y}Q$ → representa la predicción obtenida mediante el clasificador cuántico;

$\hat{y}C$ → corresponde a la predicción generada por el clasificador clásico de respaldo;

$Fallback = False$ → indica que la inferencia cuántica se ejecutó correctamente;

z$Fallback = True$ → indica que el sistema activó el mecanismo de respaldo clásico.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Métricas de evaluación

El rendimiento del modelo se evalúa utilizando métricas de clasificación estándar:

- Exactitud, precisión, recall, puntuación F1, área bajo la curva ROC.

Se usaron pruebas estadísticas para validar resultados. Se usó un nivel de importancia de $\alpha = 0.05$. Se hizo una prueba τ para datos emparejados. También un ANOVA de un factor. Se probó normalidad y varianza con: Shapiro-Wilk y la de Levene para los supuestos.

Resultados

Comparación de conjuntos de datos

El conjunto CIC-IDS-2017 presentó mejores resultados en la clasificación que el CIC-IDS-2018, mejorando en un 1% aproximadamente en todas las mediciones. El dataset CIC-IDS-2018, al ser más variable y desajustado de preparar, presentó un desafío extra para clasificar con las configuraciones que fueron probadas. Como se observa en la Tabla 1, el conjunto CIC-IDS-2017 alcanzó valores ligeramente superiores a los obtenidos con CIC-IDS-2018 en todas las métricas evaluadas.

Tabla 1

Análisis Comparativo: CIC-IDS-2017 vs. CIC-IDS-2018

Métrica	*CIC-IDS-2018*	*CIC-IDS-2017*	*diferencia*
Accuracy total	0.98	0.99	+1.0%
F1-Score	0.98	0.99	+1.0%
Precisión	0.98	0.99	+1.0%
Recall	0.98	0.99	+1.0%

Resultados obtenidos en la ejecución con Estimator local de Qiskit GPU

La Tabla 2 presenta el desempeño de los modelos clásicos, cuánticos y del ensamble híbrido durante la ejecución con el Estimator local de Qiskit GPU.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

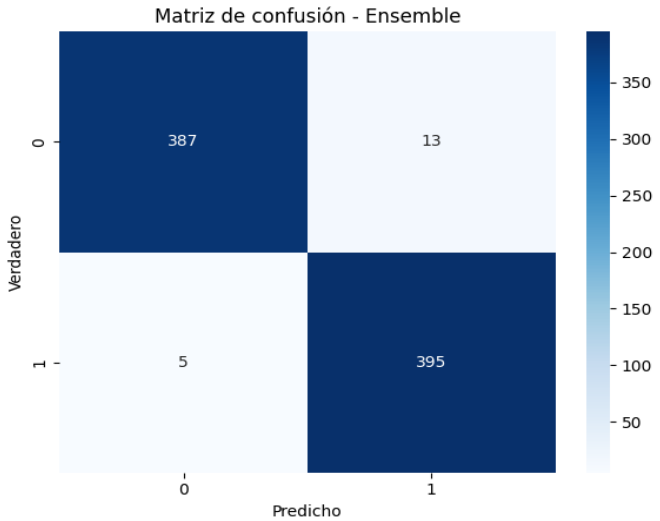
Tabla 2
Resumen del desempeño en estimator local de qiskit GPU

Modelo	accuracy	precision	recall	F1-score	fallback
QSVM	0.916	0.918	0.916	0.916	False
VQC	0.749	0.756	0.749	0.747	False
QCNN-like	0.490	0.468	0.490	0.384	False
SVC (clásico)	0.895	0.898	0.895	0.895	False
Random Forest	0.981	0.981	0.981	0.981	False
MLP (clásico)	0.954	0.954	0.954	0.954	False
XGBoost (XGB)	0.979	0.979	0.979	0.979	False
Ensamble híbrido	0.978	0.978	0.978	0.978	False

Desempeño del Ensamble Híbrido

El ***Ensamble híbrido XANDER*** logró **97.8%** de *accuracy*, con métricas homogéneas precision, *recall* o sensibilidad o tasa de verdaderos positivos y *F1* **≈ 97.8%**. Para examinar la distribución de los aciertos y errores de clasificación del ensamble híbrido, se presenta la matriz de confusión en la Figura 2.

Figura 2
Matriz de confusión del ensamble



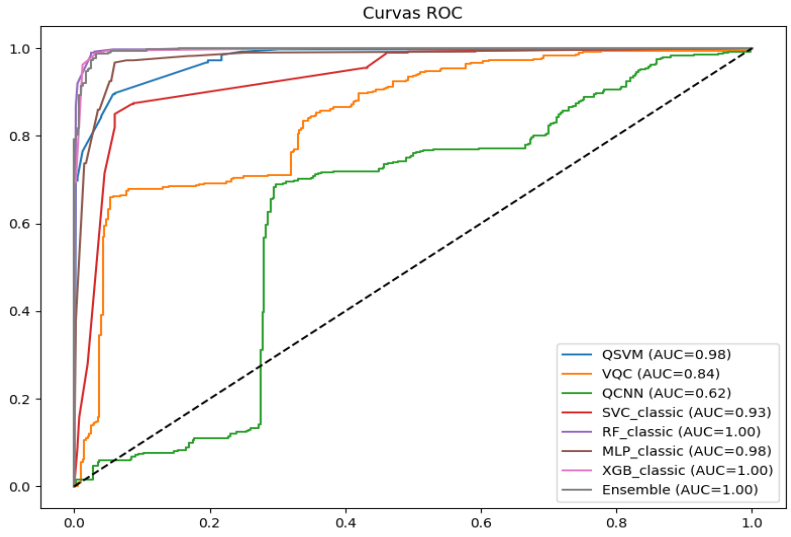
Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

En la Figura 2, se puede observar;

- Verdaderos Positivos TP: 395
- Verdaderos Negativos TN: 387
- Falsos Positivos FP: 13
- Falsos Negativos FN: 5

La capacidad discriminativa de cada modelo y del ensamble híbrido se compara mediante las curvas ROC presentadas en la Figura 3.

Figura 3
Curvas ROC – características operativas



En la Figura 3, se pueden observar que el área bajo la curva *AUC*, indica qué tan bien cada modelo distingue entre tráfico normal y tráfico malicioso. El ensamble híbrido alcanza un área bajo la curva *AUC* **= 1.00**, reflejando un desempeño considerable.

Resultados obtenidos en la ejecución con IBM Quantum Simulador

Los resultados obtenidos mediante el simulador de IBM Quantum para cada uno de los modelos evaluados se presentan en la Tabla 3.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Tabla 3

Resumen del desempeño en IBM quantum simulador

Modelo	accuracy	precision	recall	f1	fallback
QSVM	0.91625	0.916461	0.91625	0.916239	True
VQC	0.85750	0.861485	0.85750	0.857106	True
QCNN	0.98125	0.981253	0.98125	0.981250	True
SVC_classic	0.81875	0.826858	0.81875	0.817619	False
RF_classic	0.97875	0.978753	0.97875	0.978750	False
MLP_classic	0.94500	0.945178	0.94500	0.944994	False
XGB_classic	0.98125	0.981253	0.98125	0.981250	False
Ensamble	0.97625	0.976754	0.97625	0.976244	False

El **ensamble híbrido Xander** se presenta con una Precisión y F1 ≈0.976 → ligeramente por debajo de *RF* y *XGB,* pero más estable.

Resultados obtenidos en la ejecución con el procesador Heron r2 ibm_kingston de 156 qubits

Los backends de **IBM** dentro del **Plan Open NO** permiten: Trabajos largos, ni circuitos profundos, tampoco demasiados shots, ni demasiados circuitos en la relación tiempo de cola más ejecución y circuitos con un mayor de 6 qubits en los procesadores pequeños. Las ventajas de realizar estos ajustes son qué; nos permiten una profundidad mínima, un entrelazamiento lineal y estable, lo que lo hace 100% compatible con hardware real.

La Tabla 4 resume las restricciones identificadas durante la ejecución en la QPU real, sus consecuencias para el modelo y las soluciones implementadas en el pipeline híbrido.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Tabla 4

Ajustes y mitigaciones para el lanzamiento en la QPU real ibm_kingston.

Restricción IBM (Plan Open)	Consecuencia en el Modelo	Solución Aplicada en el Pipeline Híbrido
(Límite de tiempo por trabajo y cuota mensual).	Algoritmos cuánticos altamente iterativos (como VQC o QCNN)	**Enfoque Híbrido Indexado:** Se migró a un QSVM con Nyström.
Arquitectura de ibm_kingston *(156 Qubits físicos disponibles).*	Mapear un dataset clásico de muchas dimensiones satura y escala el error exponencialmente.	**Compresión por PCA Atómica:** Reducción dimensional previa a **4 o 6 componentes.**
(Decoherencia y error en compuertas).	Circuitos cuánticos muy profundos.	**Profundidad:** Uso de ZZFeatureMap restringido a (reps=1)
Escalabilidad Cuadrática del Kernel *(Problema de n^2 circuitos cuánticos).*	Calcular la matriz de similitud completa, haciendo inviable el proyecto en la cola pública.	**Aproximación Nyström por Lotes:** Selección de *m* puntos de anclaje (30 a 100).
Protocolo de SamplerV2 *(Requisito de salida explícita en Qiskit Runtime).*	ClassicalRegister required.	**Registro Clásico Estricto:** Se inyecta dinámicamente ClassicalRegister(N_QUBITS, 'c_reg') en cada circuito y las frecuencias de probabilidad se extraen mediante .data.c_reg.get_counts().
(Tiempos de espera prolongados en la plataforma).	Enviar un bloque masivo de circuitos expone el trabajo a ser cancelado por expiración de tiempo de vida (Time-To-Live).	**Segmentación Asíncrona:** Volumen fijo de **1024 shots**, asegurando transpilaciones rápidas

Se tomó la arquitectura híbrida de 6 qubits con aproximación Nyström (m=50) y 2 500 muestras estratificadas debido a que demostró el mejor balance entre representatividad de la varianza clásica (64.32%), coste temporal de cómputo emulado (~25 minutos) y capacidad de generalización en datos no vistos, alcanzando un rendimiento óptimo del 97.20% de exactitud sin incurrir en sobreajuste por fuga de datos.

Los resultados finales obtenidos con el método de seis qubits y la aproximación Nyström se presentan en la Tabla 5.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Tabla 5

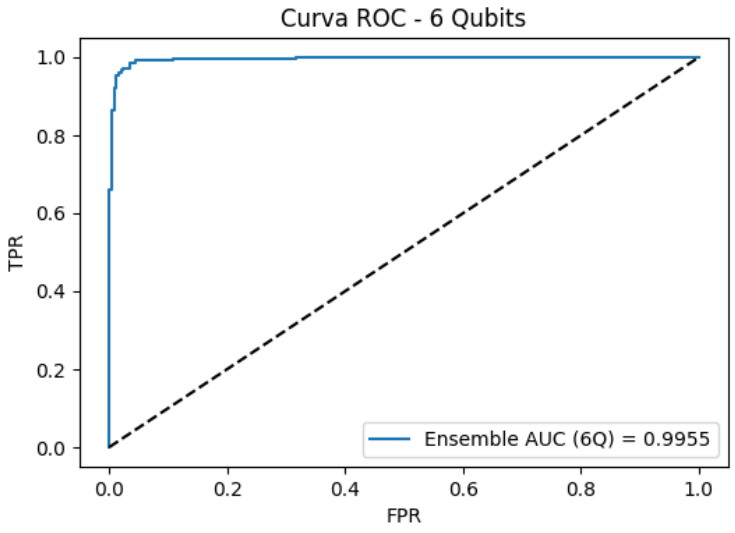
Resultados finales Simulador (método 6 qubits con aproximación Nyström).

Exactitud: 0.9720				
F1-Score: 0.9718				
Reporte:				
	precision	recall	f1-score	support
0	0.96	0.98	0.97	250
1	0.98	0.96	0.97	250
accuracy			0.97	500
macro avg	0.97	0.97	0.97	500
weighted avg	0.97	0.97	0.97	500

La Figura 4 muestra la curva ROC obtenida con la arquitectura de seis qubits y permite valorar la capacidad discriminativa del modelo mediante el área bajo la curva.

Figura 4

Curvas ROC – características operativas

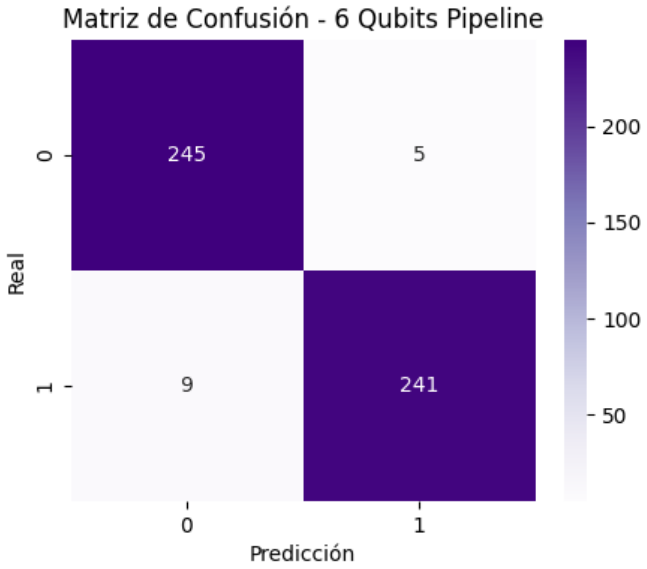


La distribución de las predicciones correctas e incorrectas obtenidas con esta configuración se presenta en la matriz de confusión de la Figura 5.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Figura 5

Matriz de confusión



Curva ROC: Discriminación óptima

- Métrica: El área bajo la curva alcanza un AUC de 0.9955.

Matriz de confusión: Comportamiento Simétrico y Balanceado

- Falsos Positivos (5 casos)
- Falsos Negativos (9 casos)
- Diagnóstico: Los errores están distribuidos de manera muy homogénea (5 y 9). Esto demuestra que el submuestreo estratificado funcionó a la perfección y el modelo no está sesgado hacia ninguna de las dos etiquetas.

Ejecución con el procesador Heron r2 ibm_kingston de 156 qubits

La información relativa al trabajo ejecutado, el estado de finalización, el procesador utilizado y el tiempo de uso de la QPU se presenta en la Tabla 6.

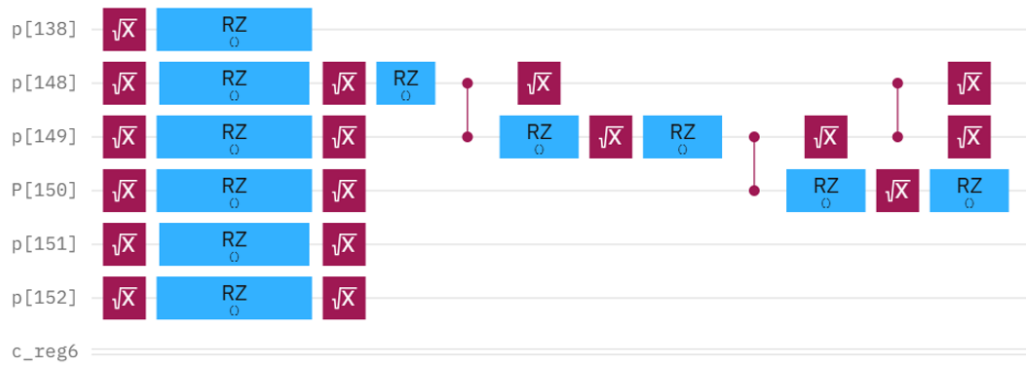
Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Tabla 6
Carga de trabajo IBM plan open

ID	Status	Instance	Mode	Created
d8ibdf66983c73drul20	Completed	QNN_23Qubits	Job	6/6/26, 7:09 PM
	Completed	**QPU**	**Usage**	**User**
	6/6/26, 7:15 PM	ibm_kingston	4m 29s	Oscar Peñaloza

La configuración y la topología del circuito ejecutado en el procesador cuántico se presentan en la Figura 6.

Figura 6
Circuito cuántico



La topología del circuito Xander presenta una profundidad optimizada de $(N_{train} = 150)$ capas de entrelazamiento, lo que permite minimizar el ruido por decoherencia en los qubits físicos de *ibm_kingston*.

Configuración Experimental y Arquitectura del Modelo Híbrido

La configuración experimental se definió bajo los siguientes parámetros:

- Se seleccionó un subconjunto estratificado de 200 muestras, dividido en un conjunto de entrenamiento $(N_{train} = 150)$ de prueba independiente $(N_{test} = 50)$.
- Se establecieron 5 puntos de anclaje fijos dentro del conjunto de entrenamiento.

$$Circuitos\ Totales = (N_{train} + N_{test})\ x\ M_{anchors} = (150 + 50)\ x\ 5 = 1$$

Los resultados obtenidos con esta configuración experimental en el procesador cuántico Heron ibm_kingston se presentan en la Tabla 7.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Tabla 7

Resultados finales en el Procesador Cuántico Heron ibm_kingston

Exactitud (Accuracy): 76.00%				
Reporte:				
	precision	recall	f1-score	support
0	0.71	0.88	0.79	25
1	0.84	0.64	0.73	25
accuracy			0.76	50
macro avg	0.78	0.76	0.76	50
weighted avg	0.78	0.76	0.76	50

Análisis estadístico e inferencia

Las pruebas inferenciales se realizaron sobre las métricas obtenidas en los cinco pliegues de validación cruzada estratificada. Cada pliegue se evalúo utilizando un conjunto independiente de 500 registros derivado del submuestreo experimental de 2.500 observaciones. Las evaluaciones sobre hardware cuántico real se presentan de forma independiente debido a las limitaciones inherentes de los dispositivos NISQ.

Los resultados de las pruebas de normalidad, homogeneidad de varianzas y comparación inferencial entre los modelos se resumen en la Tabla 8.

Tabla 8

Resultados de pruebas estadísticas inferenciales

Prueba	Estadístico	Grados de libertad	Valor p	Interpretación
Shapiro-Wilk	0.9774	–	0.9202	Normalidad no rechazada
Levene	1,9557	(5,24)	0.1995	Homogeneidad de varianzas
t-test pareado	18,0076	4	5.59×10^{-5}	Diferencia significativa
ANOVA	181.6286	(5,24)	2.97×10^{-18}	Diferencias globales significativas

Los intervalos de confianza del ensamble y los tamaños del efecto correspondientes a las comparaciones realizadas se presentan en la Tabla 9.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Tabla 9

Tabla Intervalos de confianza y tamaños de efecto

Comparación	Intervalo de confianza (95%)	Tamaño de efecto	Interpretación
Accuracy del Ensamble	[0.964, 0.972]	–	Alta estabilidad
F1-score del Ensamble	[0.964, 0.972]	–	Alta estabilidad
Ensamble vs VQC	–	Cohen's d = 8.05	Efecto muy grande
ANOVA (Global)	–	η² parcial = 0.97	Efecto muy grande

Shapiro-Wilk $W = 0.9774, p = 0.9202$ → indicó que no se rechazó la hipótesis de normalidad para las métricas del ensamble. La prueba de **Levene** $F = 1{,}9557, p = 0.1995$ → confirmó la homogeneidad de varianzas entre los modelos evaluados. La independencia de las observaciones estuvo garantizada mediante validación cruzada estratificada de cinco pliegues. El **t-test pareado** entre el ensamble y VQC → mostró diferencias estadísticamente significativas $t(4) = 18{,}0076, p = 5.59 \times 10^{-5}$. El **ANOVA** de un factor realizado sobre el conjunto de modelos evaluados evidenció diferencias globales significativas; $F(5{,}24) = 181.6286, p = 2.97 \times 10^{-18}$. El intervalo de confianza del 95% para el accuracy y el F1-score del ensamble fueron; [0.964, 0.972] y [0.964, 0.972], respectivamente. El tamaño del efecto para la comparación entre el ensamble y el VQC fue muy grande $Cohen´s\ d \approx 8.05$. Asimismo, el ANOVA presentó un $\eta^2\ parcial = 0.97$ indicando que el tipo de modelo explicó una elevada proporción de la variabilidad observada en el rendimiento bajo las condiciones experimentales evaluadas.

Discusión

La implementación del marco Xander en el procesador cuántico de IBM Kingston, representa un avance importante en la aplicación de modelos híbridos dentro de las limitaciones del NISQ. El cambio de simulación a entorno real mostró una caída controlada en el rendimiento, pasando de un AUC de 0.995 en simulación a una precisión del 76% en QPU. De igual manera, los resultados obtenidos con Xander se alinean con estudios recientes que emplean QSVM híbridos y arquitecturas cuánticas inspiradas en IDS. Al igual que en Chen et al. (2025), se observan modelos híbridos que mantienen desempeño

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

competitivo en hardware real, mitigando parcialmente el ruido. Por otra parte, la revisión sistemática de Premalatha, (2025), respalda la conclusión de que los híbridos son actualmente la vía más viable para integrar QML en ciberseguridad bajo las restricciones NISQ.

Interpretación de la diferencia en los resultados

La diferencia observada entre los resultados simulados y los del hardware real es un fenómeno esperado y esencial para validar el modelo. Esta variación puede explicarse por tres factores técnicos clave:

- Ruido y Decoherencia: A diferencia del simulador Aer, donde las puertas lógicas funcionan perfectamente, el procesador ibm_kingston opera en condiciones físicas donde el entrelazamiento circular que es la topología sugerida, provoca errores en la tasa de puertas CNOT, esto afecta ligeramente la pureza de las matrices de Nyström.
- Limitaciones de Recursos Computacionales: La decisión de optimizar utilizando la aproximación de Nyström con cinco puntos de anclaje fue estratégica para asegurar la viabilidad del experimento dentro de los límites del Plan Open de IBM.
- Propagación de Errores en el Circuito: Al reducir la profundidad del circuito (reps=1), se priorizó la estabilidad sobre la expresividad profunda. Aunque esto ayudó a reducir los errores de calibración, también limitó la complejidad del espacio de Hilbert explorado.

Valor del Ensamble Híbrido

Xander no supera de manera consistente a los mejores modelos clásicos en métricas absolutas de desempeño. Sin embargo, su aporte principal radica en la **estabilidad intermodelo**, la **integración híbrida cuántico-clásica**, la **exploración práctica en entornos NISQ** y la **reproducibilidad experimental**. Estos aspectos lo convierten en una propuesta relevante para avanzar hacia aplicaciones reales de QML en ciberseguridad, aun bajo las limitaciones actuales del hardware cuántico.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Conclusiones

Los resultados obtenidos permiten extraer tres conclusiones fundamentales que respaldan la contribución científica de este trabajo:

- Los resultados experimentales obtenidos indican que es posible implementar pipelines híbridos cuántico-clásicos en los procesadores cuánticos actuales de IBM, respetando las limitaciones de tiempo de ejecución y de profundidad de circuito. La reducción de la complejidad del kernel cuántico se logra mediante la aplicación de la aproximación de Nyström y la aplicación de PCA estableciéndose como métodos clave.
- El ensamble Xander indica que la incorporación de clasificadores clásicos para respaldar los componentes cuánticos resulta en una solución más estable en comparación con los modelos cuánticos por separado.
- La técnica usada, fue estructurada con un modelo de ocho fases que facilita la reproducibilidad del estudio.

En resumen, Xander no solo identifica intrusiones, sino que aporta evidencia sobre el potencial híbrido, demostrando que la colaboración entre modelos clásicos y la infraestructura cuántica ruidosa puede ser una posibilidad práctica.

Por otra parte, para futuras líneas de investigación: Se tienen planeadas más pruebas con procesadores cuánticos. Se intentará utilizar un mejor método para reducir el ruido. Y explorar el área de la cuántica generativa.

Limitaciones

El estudio se realizó con las limitaciones de la era NISQ. Qubits limitados. Circuitos superficiales. Tiempo en hardware cuántico real limitado. Las pruebas utilizaron poca data. La data utilizada fue CIC-IDS-2017 y de CIC-IDS-2018. Esto dificulta la aplicación de sus resultados a tráfico muy intenso. Tampoco fue posible utilizar modelos como VQC y QCNN en hardware real. Los circuitos eran muy complejos. La corrección de ruido era limitada.

Implicaciones prácticas

Los resultados muestran grupos cuánticos y clásicos que en conjunto pueden emplearse en sistemas que detectan y prevén ataques. No se necesita ventaja cuántica ahora. Esto

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

permite utilizar a Xander en la seguridad de empresas y redes actuales. La estructura pensada puede ser un punto de partida para usarla después en SOAR.

Disponibilidad de datos y código

Los datos utilizados (CIC-IDS-2017 y CIC-IDS-2018) pueden encontrarse en internet, son de carácter público. Se relaciona el link donde puede validarse el código fuente. https://github.com/openaloza/Xander.git

Declaración ética

El trabajo usó datos públicos, que simulaban tráfico. No se utilizó información privada. Tampoco se puso en riesgo la privacidad. No se atacaron sistemas en funcionamiento. No se dañaron redes externas. Esta investigación sigue reglas de seguridad y se realiza con el fin de aprender sobre ciberseguridad y computación cuántica.

Uso de inteligencia artificial

En la elaboración del documento se utilizó inteligencia artificial generativa (Microsoft Copilot) como apoyo en la expresión académica y organización de apartados.

- Objetivo: mejorar la claridad, cohesión y estilo científico de la redacción.
- Extensión: únicamente en el aspecto académico de la expresión del documento, sin generar resultados experimentales.
- Responsabilidad del autor: los resultados, interpretaciones y conclusiones son exclusivamente responsabilidad del autor, quien revisó y confirmó todo el material producido.

Declaración de conflicto de interés

El autor, declara no tener conflicto de intereses; financiero, personal o profesional, que haya influido en el desarrollo del estudio o en los resultados presentados. La investigación se realizó independientemente y bajo lineamientos académicos de la Universidad Internacional de La Rioja.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Referencias

Abdulrazzaq Altarraji, M. A., & Mokdad, A. (2024). Quantum-Assisted Machine Learning for Enhanced Fraud Detection in Cybersecurity. *International Research Journal of Innovations in Engineering and Technology, 08*(05),319 – 324. https://doi.org/10.47001/IRJIET/2024.805042

Abreu, D., Rothenberg, C. E., & Abelem, A. (2024). *QML-IDS: Quantum Machine Learning Intrusion Detection System*. Proceedings - IEEE Symposium on Computers and Communications. https://doi.org/10.1109/ISCC61673.2024.10733655

Ajdani, M. (2025). Deep Learning-Based Intrusion Detection Systems: A Novel Approach Using Generative Adversarial Networks (GANs). *International Journal of Information Security and Privacy (IJISP), 19*(1), 1-15. https://doi.org/10.4018/IJISP.383299

Akif, M. A., Butun, I., Williams, A., & Mahgoub, I. (2025). *Hybrid Machine Learning Models for Intrusion Detection in IoT: Leveraging a Real-World IoT Dataset* (No. arXiv:2502.12382). arXiv. https://doi.org/10.48550/arXiv.2502.12382

Alluhaibi, R. (2024). *Quantum Machine Learning for Advanced Threat Detection in Cybersecurity*. *International Journal of Safety and Security Engineering, 14*(3), 875–883. https://doi.org/10.18280/IJSSE.140319

Almseidin, M., Alzubi, M., Kovacs, S., & Alkasassbeh, M. (2018). *Evaluation of Machine Learning Algorithms for Intrusion Detection System* (No. arXiv:1801.02330). arXiv. https://doi.org/10.48550/arXiv.1801.02330

Alotaibi, A., & Rassam, M. A. (2023). *Adversarial Machine Learning Attacks against Intrusion Detection Systems: A Survey on Strategies and Defense*. *Future Internet, 15*(2), 62. https://doi.org/10.3390/fi15020062

Camargo, J. A. F., Aguilar, J., & Pinto, Á. (2024, agosto). *Analysis of Quantum Support Vector Machines in Classification Problems*. https://doi.org/10.1109/CLEI64178.2024.10700573

Cerezo, M., Arrasmith, A., Babbush, R., Benjamin, S. C., Endo, S., Fujii, K., McClean, J. R., Mitarai, K., Yuan, X., Cincio, L., & Coles, P. J. (2021). *Variational quantum algorithms*. *Nature Reviews Physics, 3*(9), 625–644. https://doi.org/10.1038/s42254-021-00348-9

Chen, Z., Zhu, Z., & Li, X. (2025). *Cyber threat detection enabled by quantum computing*.

arXiv preprint arXiv:2512.18493. https://doi.org/10.48550/arXiv.2512.18493

Danso, P. K., Neto, E. C. P., Dadkhah, S., Zohourian, A., Molyneaux, H., & Ghorbani, A. A. (2022). *Ensemble-based Intrusion Detection for Internet of Things Devices*. 2022 IEEE 19th International Conference on Smart Communities (HONET), 034–039. https://doi.org/10.1109/HONET56683.2022.10019140

Dong, Y., Hu, W., Zhang, J., Chen, M., Liao, W., & Chen, Z. (2022). *Quantum beetle swarm algorithm optimized extreme learning machine for intrusion detection*. *Quantum Information Processing, 21*(1), 9. https://doi.org/10.1007/s11128-021-03311-w

Elsedimy, E. I., Elhadidy, H., & Abohashish, S. M. M. (2024). *A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer*. *Cluster Computing, 27*(7), 9917–9935. https://doi.org/10.1007/s10586-024-04458-8

Fan, F., Shi, Y., Guggemos, T., & Zhu, X. X. (2024). *Hybrid Quantum-Classical Convolutional Neural Network Model for Image Classification*. IEEE *Transactions on Neural Networks and Learning Systems, 35*(12), 18145–18159. https://doi.org/10.1109/TNNLS.2023.3312170

Farhi, E., & Neven, H. (2018). *Classification with Quantum Neural Networks on Near Term Processors* (No. arXiv:1802.06002). arXiv. https://doi.org/10.48550/arXiv.1802.06002

Ganapathi, P., & Shanmugapriya, D. (2019). *Handbook of research on machine and deep learning applications for cyber security*. IGI Global. ISBN: 9781522596106. https://books.google.com/books?id=vK2rDwAAQBAJ

Gong, C., Guan, W., Gani, A., & Qi, H. (2022). *Network attack detection scheme based on variational quantum neural network*. *The Journal of Supercomputing, 78*(15), 16876–16897. https://doi.org/10.1007/s11227-022-04542-z

Havlíček, V., Córcoles, A. D., Temme, K., Harrow, A. W., Kandala, A., Chow, J. M., & Gambetta, J. M. (2019). *Supervised learning with quantum-enhanced feature spaces*. Nature, 567(7747), 209–212. https://doi.org/10.1038/s41586-019-0980-2

Hozouri, A., Mirzaei, A., & Effatparvar, M. (2025). *A comprehensive survey on intrusion detection systems with advances in machine learning, deep learning and emerging cybersecurity challenges*. *Discover Artificial Intelligence, 5*(1), 314.

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

https://doi.org/10.1007/s44163-025-00578-1

Kadry, H., Farouk, A., Zanaty, E. A., & Reyad, O. (2023). *Intrusion detection model using optimized quantum neural network and elliptical curve cryptography for data security*. *Alexandria Engineering Journal, 71,* 491–500. https://doi.org/10.1016/j.aej.2023.03.072

Kalinin, M., & Krundyshev, V. (2023). *Security intrusion detection using quantum machine learning techniques*. *Journal of Computer Virology and Hacking Techniques, 19*(1), 125–136. https://doi.org/10.1007/s11416-022-00435-0

Kalyan, B. K. P., Chandana, M. S., Karimalla, N., & Bukaita, W. (2025). *Generative Adversarial Network–based Intrusion Detection for Securing In-vehicle Communication in Electric Vehicles*. *American Journal of Information Science and Technology, 9*(4), 304–323. https://doi.org/10.11648/j.ajist.20250904.16

Khan, F. A., Gumaei, A., Derhab, A., & Hussain, A. (2019). *A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection. IEEE Access, 7*, 30373–30385. https://doi.org/10.1109/ACCESS.2019.2899721

Khan, N., Mohmand, M. I., Rehman, S. ur, Ullah, Z., Khan, Z., & Boulila, W. (2024). *Advancements in intrusion detection: A lightweight hybrid RNN-RF model*. *PLoS One, 19*(6). https://doi.org/10.1371/journal.pone.0299666

Kim, T. H., & Madhavi, S. (2024). *Quantum intrusion detection system using outlier analysis*. *Scientific Reports, 14*(1), 27114. https://doi.org/10.1038/s41598-024-78389-0

Li, D., Chen, D., Shi, L., Jin, B., Goh, J., & Ng, S.-K. (2019). *MAD-GAN: Multivariate Anomaly Detection for Time Series Data with Generative Adversarial Networks* (No. arXiv:1901.04997). arXiv. https://doi.org/10.48550/arXiv.1901.04997

Maseer, Z. K., Yusof, R., Al-Bander, B., Saif, A., & Kadhim, Q. K. (2023). *Meta-Analysis and Systematic Review for Anomaly Network Intrusion Detection Systems* (No. arXiv:2308.02805). arXiv. https://doi.org/10.48550/arXiv.2308.02805

Metawei, M. A., Said, H., Taher, M., Eldeib, H., & Nassar, S. M. (2020). *Survey on Hybrid Classical-Quantum Machine Learning Models*. 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), 1–6. https://doi.org/10.1109/CCCI49893.2020.9256649

Musa, U. S., Chhabra, M., Ali, A., & Kaur, M. (2020). *Intrusion Detection System using*

Machine Learning Techniques: A Review. 2020 International Conference on Smart Electronics and Communication (ICOSEC), 149–155. https://doi.org/10.1109/ICOSEC49089.2020.9215333

Nazim, S., Hussain, S. S., Yousuf, B., Sultana, S., & Tanweer, E. (2025). *An innovative intrusion detection framework using GAN-augmented Deep Ensemble Neural Network for cross-domain IoT–cloud security*. Internet of Things, 34, 101773. https://doi.org/10.1016/j.iot.2025.101773

Nicesio, O. K., Leal, A. G., & Gava, V. L. (2023). *Quantum Machine Learning for Network Intrusion Detection Systems, a Systematic Literature Review*. 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC). https://doi.org/10.1109/ICAIC57335.2023.10044125

Noor, K., Agbotiname, L. I., Chun-Ta, L., & Chi-Yao, W. (2025). *A Review of Machine Learning and Transfer Learning Strategies for Intrusion Detection Systems in 5G and Beyond*. *Mathematics, 13*(7). https://doi.org/10.3390/math13071088

Noor, M., Abbas, H., & Shahid, W. B. (2018). *Countering cyber threats for industrial applications*. Journal of Network and Computer Applications, 103, 249–261. https://doi.org/10.1016/j.jnca.2017.10.004

Odeh, A., & Abu Taleb, A. (2023). *Ensemble-Based Deep Learning Models for Enhancing IoT Intrusion Detection*. Applied Sciences, 13(21), 11985. https://doi.org/10.3390/app132111985

Orazi, F., Gasperini, S., Lodi, S., & Sartori, C. (2024). *Hybrid Quantum Technologies for Quantum Support Vector Machines*. Information, 15(2), 72. https://doi.org/10.3390/info15020072

Pinto, A., Herrera, L.-C., Donoso, Y., & Gutierrez, J. A. (2023). *Survey on Intrusion Detection Systems Based on Machine Learning Techniques for the Protection of Critical Infrastructure*. *Sensors, 23*(5), 2415. https://doi.org/10.3390/s23052415

Premalatha, D. V. (2025). *Ensemble-Based Intrusion Detection for IoT Networks Using the CICIoT2023 Dataset*. Journal of Information Systems Engineering and Management, 10(21s), 743–755. https://doi.org/10.52783/jisem.v10i21s.3407

Rawat, S., Srinivasan, A., Ravi, V., & Ghosh, U. (2022). *Intrusion detection systems using classical machine learning techniques vs integrated unsupervised feature learning*

and deep neural network. Internet Technology Letters, 5(1). https://doi.org/10.1002/ITL2.232

Rehman, H. M. R. U., Liaquat, S., Gul, M. J., Jhandir, M. Z., Gavilanes, D., Vergara, M. M., & Ashraf, I. (2025). *A systematic literature study of machine learning techniques based intrusion detection*. *Journal of Big Data, 12*(1), 264. https://doi.org/10.1186/s40537-025-01323-2

Sarker, I. H. (2021). *Machine Learning: Algorithms, Real-World Applications and Research Directions*. *SN Computer Science, 2*(3), 160. https://doi.org/10.1007/s42979-021-00592-x

Sharafaldin, I., Habibi Lashkari, A., & Ghorbani, A. A. (2018). *Toward Generating a New Intrusion Detection Dataset*. Proceedings of the 4th International Conference on Information Systems Security and Privacy, 108–116. https://doi.org/10.5220/0006639801080116

Shen, J.-Y., Wu, C.-H., Hua, C.-Y., Chang, M.-H., Kuo, S.-Y., Chou, Y.-H., & Kuo, S.-Y. (2024). *An Efficient Quantum-inspired Computing Approach for Intrusion Detection System*. 2024 IEEE 24th International Conference on Nanotechnology (NANO), 306–310. https://doi.org/10.1109/NANO61778.2024.10628664

Solar, M., Alvarez, F. C., Villacura, J.-P., & Dombrovskaia, L. (2024). *A Review on Quantum Machine Learning and Quantum Cryptography*. *Memoria Investigaciones En Ingeniería, 27*, 180–199. https://doi.org/10.36561/ING.27.12

Talukder, Md. A., Hasan, K. F., Islam, Md. M., Uddin, Md. A., Akhter, A., Yousuf, M. A., Alharbi, F., & Moni, M. A. (2023). *A dependable hybrid machine learning model for network intrusion detection*. Journal of Information Security and Applications, 72, 103405. https://doi.org/10.1016/j.jisa.2022.103405

Vol. 3, No. 2, julio-diciembre, 2026 ISSN L2992-6440
REVISTA IBEROAMERICANA DE INNOVACIÓN CIENTÍFICA
JA TUAIDA
revistas.unachi.ac.pa revista.jatuaida@unachi.ac.pa David, Chiriquí, República de Panamá
Universidad Autónoma de Chiriquí pp. 4-36 Extensión Universitaria de Boquete

Anexo A: Diagrama de la Arquitectura del Circuito Cuántico

La Figura 7 presenta de manera ampliada el diagrama de la arquitectura del circuito cuántico empleado en la implementación de Xander.

Figura 7
Circuito cuántico