UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

Sistema de seguridad de red basado en el aprendizaje federado para detectar intrusiones en entornos médicos

TESIS PARA OPTAR EL TÍTULO DE

INGENIERO DE SISTEMAS Y COMPUTACIÓN

AUTOR

Johann Antonio Torres Aguinaga

ASESOR

Karla Cecilia Reyes Burgos

https://orcid.org/0000-0003-3520-5076

Chiclayo, 2026

Sistema de seguridad de red basado en el aprendizaje federado para detectar intrusiones en entornos médicos

PRESENTADA POR

Johann Antonio Torres Aguinaga

A la Facultad de Ingeniería de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el título de

INGENIERO DE SISTEMAS Y COMPUTACIÓN

APROBADA POR

Ernesto Ludwin Nicho Cordova
PRESIDENTE

Alexanders Valqui Sipiran
SECRETARIO

Karla Cecilia Reyes Burgos
VOCAL

Dedicatoria

A mi tía, por su apoyo incondicional, un pilar fundamental
en cada etapa de este camino. A mi enamorada, por su inspiración
y aliento constante que me impulsaron a seguir adelante.
Y a todas las personas cuya influencia y apoyo hicieron posible
la culminación de este trabajo.

Agradecimientos

Agradezco profundamente a mi asesora, Mg. Karla Cecilia Reyes Burgos,
por su orientación y compromiso. Al equipo de TI de la clínica evaluada,
por su colaboración clave. A mi familia, por su amor y respaldo.

Sistema de seguridad de red basado en el aprendizaje federado para detectar intrusiones en entornos médicos

INFORME DE ORIGINALIDAD

4%	5%	0%	2%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	tesis.usat.edu.pe Fuente de Internet	2%
2	repositorio.umariana.edu.co Fuente de Internet	<1%
3	Submitted to Universidad Católica Santo Toribio de Mogrovejo Trabajo del estudiante	<1%
4	gredos.usal.es Fuente de Internet	<1%
5	elcomercio.pe Fuente de Internet	<1%
6	www.coursehero.com Fuente de Internet	<1%
7	repositorio.usam.ac.cr Fuente de Internet	<1%
8	www.journal.50sea.com Fuente de Internet	<1%

Índice

Resumen

La ciberseguridad en entornos de salud, particularmente la protección de los dispositivos médicos conectados (DMC), presenta el desafío dual de mitigar el riesgo de intrusiones sin comprometer la privacidad del paciente. Esta investigación abordó dicha problemática mediante el desarrollo de un sistema de detección de intrusiones (IDS) basado en el aprendizaje federado. Se estableció una clasificación de amenazas jerárquica (Normal, Sospechosa y Ataque) tras analizar el tráfico de red del dataset "CICIDS2017". El modelo Random Forest fue seleccionado como el algoritmo óptimo dentro de la arquitectura del aprendizaje federado, logrando una robustez de detección validada por métricas F1-Score y Recall. El sistema se implementó a través de un dashboard interactivo que permite la visualización y gestión en tiempo real del modelo federado. Finalmente, la usabilidad del sistema fue evaluada mediante el cuestionario SUS, alcanzando un puntaje promedio de 85.0, lo que lo clasifica con un nivel de usabilidad óptimo. Los resultados confirman que el sistema de seguridad de red basado en aprendizaje federado es una solución altamente precisa, eficiente y usable que aborda la necesidad de proteger los entornos médicos, garantizando la confidencialidad de los datos al entrenar los modelos localmente en los nodos de la red.

Palabras clave: Aprendizaje Federado, Detección de Intrusiones, Dispositivos Médicos, Random Forest , Usabilidad, CICIDS2017.

Abstract

Cybersecurity in healthcare settings, particularly the protection of connected medical devices (CMDs), presents the dual challenge of mitigating the risk of intrusions without compromising patient privacy. This research addressed this issue by developing an intrusion detection system (IDS) based on federated learning. A hierarchical threat classification (Normal, Suspicious, and Attack) was established after analyzing the network traffic from the "CICIDS2017" dataset. The Random Forest model was selected as the optimal algorithm within the FA architecture, achieving detection robustness validated by F1-Score and Recall metrics. The system was implemented via an interactive dashboard that enables real-time visualization and management of the federated model. Finally, the system's usability was evaluated using the SUS questionnaire, achieving an average score of 85.0, which classifies it as having an optimal level of usability. The results confirm that the federated learning-based network security system is a highly accurate, efficient, and usable solution that addresses the need to protect medical environments, ensuring data confidentiality by training models locally on network nodes.

Keywords: Federated Learning, Intrusion Detection, Medical Devices, Random Forest , Usability, CICIDS2017.

Introducción

Los ataques cibernéticos se basan en el esfuerzo voluntario para vulnerar la información, robando, exponiendo y alterando datos o aplicaciones a través de un acceso restringido a un servicio informático [1]. Estos consisten en la obtención de información privada o confidencial sin autorización del propietario; sus víctimas pueden ir desde usuarios individuales y pequeñas empresas hasta organizaciones gubernamentales [2]. De acuerdo con el informe de amenazas de ENISA [3] de 2023, una parte de los incidentes observados afectó a organizaciones de salud, y una proporción considerable de ellos tuvo un impacto significativo.

El informe de ENISA [4] de 2023 afirma que el sector de salud, es uno de los más impactados a nivel global por los ciberataques, registrando el 8% de los incidentes asociados a problemas de ciberseguridad. Según el Foro económico mundial, se estima que el ciberdelito generará pérdidas de 10,5 billones de dólares en 2025, consolidándose como un negocio lucrativo que se ha intensificado con la pandemia y afecta a economías de miles de millones de dólares [5]. En los primeros meses de 2024, Perú registró más de un millón de ciberataques, menos que los cinco millones de 2023, sin embargo, el phishing sigue siendo una amenaza constante para personas y organizaciones [6]. En 2021, la región de Lambayeque representó el 4.27% de los ciberdelitos de alto riesgo, según el Ministerio Público [7]. Junto con La Libertad, Piura y el Callao, Lambayeque concentró una parte significativa de las denuncias, acumulando un total del 71%.

Una de las principales vulnerabilidades es la falta de control en la distribución de contraseñas, permitiendo el acceso restringido a los sistemas. Además, la falta de actualizaciones de seguridad en el software médico, dispositivos y redes, los expone a ataques externos. La falta de cifrado y autenticación expone los datos del paciente y compromete su privacidad, así como la integridad y seguridad de la información [8].

La información vulnerada puede originarse en factores externos, como ciberataques perpetrados por atacantes cibernéticos, técnicas de phishing y el uso de ransomware que bloquea el acceso a datos a cambio de dinero [2]. Por otro lado, los factores internos, según Muñoz [9], incluyen una detección deficiente de intrusiones causada por configuraciones incorrectas de los sistemas de seguridad, contraseñas débiles o compartidas, falta de actualizaciones en los sistemas y ausencia de capacitación del personal.

Los ataques cibernéticos en el sector sanitario pueden generar impactos devastadores, desde la interrupción de servicios médicos críticos hasta el debilitamiento de la confianza de los pacientes. Esto no solo implica un alto costo económico, sino que también compromete la vida de las personas que acuden a los establecimientos de salud [10]. En este contexto, técnicas

avanzadas como el aprendizaje federado, emergen como una solución idónea. El aprendizaje federado es un enfoque descentralizado que permite entrenar modelos de aprendizaje automático sin centralizar los datos, convirtiéndolo en una alternativa ideal para los sistemas de salud, donde la privacidad y la seguridad de la información son prioritarias [11].

Diversos estudios han explorado técnicas de aprendizaje automático y profundo aplicadas a la detección de intrusiones en redes. Por ejemplo, Alotibi [12] implementó un sistema basado en aprendizaje profundo para identificar ataques de fuerza bruta en protocolos FTP y SSH. Sarhan [13] empleó la técnica SMOTE con algoritmos de clasificación y detección de anomalías, alcanzando una precisión del 100% en la identificación de amenazas internas. Asimismo , Hnamte [14] desarrolló un marco con redes neuronales convolucionales, ofreciendo eficiencia en el desarrollo de métodos novedosos para la detección y clasificación de intrusiones en redes. Por su parte, Chimphlee [15], propuso métodos de clasificación que incrementan la precisión en la detección de anomalías, mientras que Kumar et al. [16], sugirieron el aprendizaje profundo para clasificar ataques DDoS en redes que involucran dispositivos IoT. Por otro lado, Affia et al. [17] analizaron la gestión de riesgos en dispositivos médicos, identificando vulnerabilidades clave en dispositivos IoT médicos.

Los establecimientos de salud deben proteger la información sensible de los pacientes, incluidos diagnósticos, exámenes e historial clínico. Esta salvaguarda abarca datos almacenados en bases de datos y sistemas digitales, así como la seguridad de dispositivos IoT médicos conectados, esenciales para la recolección y monitoreo en tiempo real. Tales equipos, integrados a la red, constituyen blancos vulnerables para ciberataques, con impactos en la privacidad del paciente y la operación segura de la tecnología.

En la clínica evaluada se dispone de una infraestructura tecnológica amplia, en la que se han detectado intentos de intrusión en su sistema en los últimos años. Una encuesta realizada **(ver Anexo 1)** revela datos que indican vulnerabilidades en su infraestructura digital. Además, el mecanismo de detección empleado durante el diagnóstico permitió identificar los tipos de ataques potenciales **(ver Anexo 2),** proporcionando información valiosa para comprender riesgos y adoptar medidas preventivas que fortalezcan la seguridad. Es en este contexto donde surge la interrogante central de esta investigación: ¿Qué características debe tener un sistema de seguridad de red para detectar intrusiones en entornos médicos?

El incremento y la sofisticación de los ataques cibernéticos en el sector salud exigen soluciones innovadoras y eficaces. Diversos estudios han aplicado aprendizaje automático para prevenir incidentes, pero el aprendizaje federado emerge como una alternativa prometedora al entrenar modelos sin centralizar los datos, preservando la privacidad y cumpliendo regulaciones

[11]. Por ello, esta investigación avanza científicamente al validar su uso en la detección de intrusiones médicas, expandiendo el conocimiento en inteligencia artificial y ciberseguridad.

Desde una perspectiva social, la protección de información sensible de pacientes preserva la confianza en sistemas de salud. Los ciberataques comprometen datos personales, alteran la atención médica y generan impactos negativos en la sociedad [10]. La implementación de un sistema basado en aprendizaje federado beneficia a la comunidad al garantizar confidencialidad, fortalecer relaciones paciente-institución y contribuir al bienestar colectivo.

Asimismo, desde un enfoque tecnológico, la creciente adopción de dispositivos en el sector salud amplía la superficie de ataque y complica su protección. El aprendizaje federado ofrece ventajas clave como escalabilidad, actualizaciones continuas y adaptabilidad a amenazas [18]. Su implementación en plataforma web asegura accesibilidad y facilidad de uso, permitiendo acceso desde cualquier dispositivo sin instalaciones adicionales, lo cual integra procesos existentes y distribuye actualizaciones eficientes.

Para finalizar, el objetivo general establecido es desarrollar un sistema de seguridad basado en el aprendizaje federado para detectar intrusiones en entornos médicos. Con el fin de alcanzarlo, se plantearon los siguientes objetivos: seleccionar el algoritmo a utilizar en la implementación del aprendizaje federado para la detección de intrusiones en dispositivos médicos; entrenar el algoritmo seleccionado para clasificar el tráfico de red presente en los dispositivos médicos y entornos clínicos; desarrollar un dashboard interactivo para la visualización y gestión del modelo de aprendizaje federado; validar el desempeño del modelo de aprendizaje federado para la detección de intrusiones en dispositivos médicos y evaluar, con usuarios, la usabilidad del sistema de seguridad de red basado en aprendizaje federado para la detección de intrusiones en entornos médicos., facilitando así la interacción del público objetivo.

Revisión de literatura

A continuación, se presentan los antecedentes y bases teóricas:

Alotibi [12] analizó los ataques de fuerza bruta en protocolos FTP y SSH, amenazas crecientes para organizaciones globales. Aplicó redes neuronales artificiales para superar las deficiencias de sistemas tradicionales de detección de intrusiones, alcanzando una precisión del 99,9%. Este enfoque demuestra cómo el aprendizaje profundo mejora la identificación de patrones complejos en tráfico de red, lo cual resulta relevante para entornos médicos donde protocolos similares manejan datos confidenciales de pacientes.

Sarhan [13] abordó las amenazas internas, donde usuarios autorizados comprometen sistemas mediante robos de propiedad intelectual o exposición de datos. Utilizó algoritmos avanzados de aprendizaje automático, como modelos de ensamble, para lograr una precisión del 91% en detección de anomalías. Comparado con métodos convencionales basados en reglas estáticas, este estudio resalta la superioridad de técnicas inteligentes en contextos sensibles, como el sector salud, donde insiders podrían acceder a historiales clínicos.

Hnamte [14] propuso una red neuronal convolucional profunda para sistemas de detección de intrusiones, entrenada en conjuntos de datos contemporáneos. Alcanzó precisiones de hasta el 100%, superando enfoques tradicionales que dependen de patrones predefinidos. Esta investigación enfatiza la capacidad del aprendizaje profundo para analizar tráfico en tiempo real, un aspecto clave para integrar el aprendizaje federado en redes médicas, donde se requiere alta precisión sin centralizar datos privados.

En anteriores investigaciones, Chimphlee [15] desarrolló un método de dos fases con algoritmos basados en árboles para detectar anomalías en el conjunto CICIDS-2018, incorporando selección de características mediante ganancia de información. Obtuvo una precisión del 98,36% y una puntuación F1 del 97,98%, mejorando sobre técnicas de detección basadas en firmas que fallan ante variantes nuevas de ataques. Los autores abordaron desafíos como el desequilibrio de datos y la selección de características, utilizando técnicas de preprocesamiento y algoritmos como SMOTE para manejar el desequilibrio de clases. Este trabajo muestra cómo manejar desequilibrios en datos de red beneficia entornos clínicos, alineándose con el aprendizaje federado para procesar volúmenes masivos sin comprometer la confidencialidad.

Kumar et al. [16] enfocaron los ataques DDoS en redes IoT, utilizando redes de memoria a corto y largo plazo para clasificar tráfico en el conjunto CICDDoS2019, con una precisión del 98%. Superior a métodos tradicionales como Random Forest o KNN, que requieren selección manual de características, este estudio resalta la adaptabilidad del aprendizaje profundo a

amenazas dinámicas, esencial para dispositivos médicos conectados donde interrupciones podrían afectar vidas humanas.

Otro autores como Affia et al. [17], evaluaron vulnerabilidades en dispositivos IoT de salud, proponiendo un enfoque multicapa para gestión de riesgos que integra inteligencia artificial. También Identificaron limitaciones en soluciones perimetrales tradicionales, sugiriendo innovaciones proactivas para contrarrestar exploits. Este análisis refuerza la relevancia del aprendizaje federado en salud, al priorizar la resiliencia en arquitecturas conectadas sin exponer datos sensibles.

Estos antecedentes revelan avances en aprendizaje profundo para detección de intrusiones, pero también brechas en privacidad y escalabilidad, los cuales se complementan con las siguientes bases teóricas.

Seguridad Informática

La seguridad informática es la disciplina dedicada a salvaguardar los recursos tecnológicos de una organización, incluidos los sistemas informáticos, las redes, los dispositivos digitales y los datos, contra accesos no autorizados, fugas de información, ciberataques y cualquier tipo de acciones maliciosas [19].

Ataques Cibernéticos en el sector salud

Los ataques cibernéticos en dispositivos médicos conectados se refieren a vulnerabilidades que pueden ser explotadas por ciberdelincuentes para robar, alterar o bloquear el acceso a información sensible. Estos dispositivos, al estar conectados a redes de Internet de las Cosas (IoT), presentan diversas vulnerabilidades, lo que los hace propensos a sufrir ataques [10].

Vulnerabilidades en dispositivos médicos conectados:

Los equipos IoT son vulnerables a una variedad de ataques de seguridad, desde el robo de cookies hasta la activación de comandos en secuencia entre varios sitios, también existe la inyección de lenguaje de consulta estructurado, los secuestros de sesiones y, de manera especial en la actualidad, los ataques de denegación de servicio distribuido. Algunos dispositivos médicos, como los marcapasos y las bombas de insulina, pueden ser explotados para el robo o la modificación de datos, además de generar daños [10].

Riesgos cibernéticos en dispositivos médicos

Los principales elementos afectados dentro de este tipo de organizaciones son los sistemas que son afectados por variedad de ataques, estas amenazas tienen como consecuencia la filtración de información, lo que involucra la exposición de datos médicos a personas que no están autorizadas para su acceso. Esto expone también a pacientes, poniendo en riesgo la privacidad y física si se llega a filtrar datos que comprometen a la información médica [10].

Ataques comunes en dispositivos médicos

Phishing: Phishing: Obtención de información confidencial como contraseñas u otros datos como bancarios mediante una falsificación de correos o páginas web [10].

Ransomware: software de naturaleza maliciosa debido a que se apodera de información de sistemas informáticos [10].

DDoS: Ataque de denegación de servicio, consiste en el acumulamiento de tráfico en la red para sobrecargar y hacer inaccesible la información [10].

Inteligencia Artificial

Es la capacidad de una máquina para realizar operaciones que requieren del uso racional e intelectual del ser humano como el entendimiento mediante el mecanismo de voz, la comprensión del lenguaje natural y la toma de decisiones [20].

Machine learning

Rama de la IA que utiliza algoritmos con la capacidad de aprender de los datos y mejorar con el paso del tiempo, permitiendo que las máquinas mejoren su rendimiento en tareas designadas [20].

Federated learning

Es una arquitectura de aprendizaje automático donde numerosos dispositivos como teléfonos móviles , computadores, servidores o más, trabajan en conjunto para entrenar un modelo de aprendizaje; esto ocurre bajo la gestión de algún servidor que sirva como núcleo, la característica más resaltante del aprendizaje federado es la utilización de conjuntos de datos descentralizados, ya que cada dispositivo realiza el entrenamiento del modelo en su propio conjunto de datos antes de enviar algún tipo de parámetros a un servidor centralizado [11].

Metodología CRISP-DM

Es una metodología estándar y flexible para la minería de datos, diseñada para convertir grandes volúmenes de datos en conocimiento valioso que pueda ser aplicado a diversas áreas de negocio. CRISP-DM permite a las organizaciones estructurar y gestionar proyectos de minería de datos de manera eficaz, asegurando que los resultados obtenidos estén alineados con los objetivos comerciales. A través de un enfoque iterativo, facilita la exploración de los datos, la creación de modelos predictivos y descriptivos, y la toma de decisiones informadas. Su flexibilidad permite adaptarse a diferentes problemas y contextos, proporcionando una guía clara para transformar los datos en insights que impulsen la mejora de procesos, la optimización de decisiones y el descubrimiento de nuevas oportunidades [21].

Materiales y métodos

Tipo de investigación

Se ha considerado como tipo de estudio la investigación aplicada, la cual se basa en trabajos originales que se realizan para adquirir nuevos conocimientos, pero apuntando hacia un objetivo práctico específico. Esta investigación se centra en determinar nuevos métodos o formas para lograr objetivos específicos. Generalmente se describe como aquella que analiza resultados favorables en un contexto de programa de investigación. Por último, Por último, este tipo de investigación permite transformar ideas en soluciones operativas y puede dar lugar a mecanismos de protección intelectual, incluida la confidencialidad [22].

Métodos de investigación

Los métodos de investigación empleados fueron los siguientes:

Tabla 1

Métodos de investigación

Método	Sustento por el cual será empleado en la investigación
Analítico	Se trata de la descomposición de un objeto de estudio para examinarlo en cada una de sus partes de forma individual [23]. Por eso, se decide analizar las vulnerabilidades y amenazas cibernéticas a los que se encuentran expuestos los diferentes medios, como los sistemas y dispositivos médicos presentes en la clínica.
Experimento	Caracterizado por medir el efecto de manipular una variable en otra [24] . Entrenar un modelo con el algoritmo elegido de aprendizaje federado, usando información de cada dispositivo para la alimentación del modelo propio.
Implementación	Es fundamental implementar una solución para demostrar las ventajas que se proponen [25]. Es por ello, que se presenta la solución de un sistema que se gestionará mediante un dashboard, permitiendo la interacción con el producto a desarrollar como el modelo de aprendizaje.

Tabla 2 Técnicas de Investigación

Técnicas	Instrumentos	Muestra	Propósito
Entrevista	Cuestionario Estructurado	Personal TI de la empresa	Conocer el problema
Cuestionario	Cuestionario SUS	Personal TI de la empresa	Evaluar usabilidad del prototipo

Tabla 3 Matriz de Consistencia

FORMULACIÓN DEL PROBLEMA	MÉTODO DE INVESTIGACIÓN			
¿Qué características debe tener un sistema de seguridad de red para detectar intrusiones en entornos médicos?	Tipo de investigación:			Aplicada
OBJETIVO GENERAL	MÉTODO	DESCRIPCIÓN		
Desarrollar un sistema de seguridad de red basado en el aprendizaje federado para detectar intrusiones en entornos médicos	Analítico	Se trata de la descomposición de un objeto de estudio para examinarlo en cada una de sus partes de forma individual. Es por eso que se decide analizar las vulnerabilidades y amenazas cibernéticas a los que se encuentran expuestos los diferentes medios, como los sistemas y dispositivos médicos presentes en la clínica.		
	Experimento	Caracterizado por medir el efecto de manipular una variable en otra. Entrenar un modelo con el algoritmo elegido de aprendizaje federado, usando información de cada dispositivo para la alimentación del modelo propio.		
	Implementación	Es fundamental implementar una solución para demostrar las ventajas que se proponen. Es por ello, que se presenta la solución de un sistema que se gestionará mediante un dashboard, permitiendo la interacción con el producto a desarrollar como el modelo de aprendizaje.		
	TÉCNICAS	INSTRUMENTOS	ELEMENTOS DE LA POBLACIÓN	PROPÓSITO
	Entrevista	Cuestionario Estructurado	Personal TI de la empresa	Obtener información sobre el problema identificado.
	Cuestionario	Cuestionario SUS	Personal TI de la empresa	Evaluar usabilidad del prototipo
OBJETIVOS ESPECÍFICOS	DESCRIPCIÓN DEL LOGRO DE LOS OBJETIVOS ESPECÍFICOS		INDICADORES	
Seleccionar el algoritmo a utilizar en la implementación del aprendizaje federado para la detección de intrusiones en dispositivos médicos.	Se seleccionó el algoritmo Random Forest como el óptimo para nuestra aplicación, tomando en cuenta los estudios previos realizados.		Métricas utilizadas para comparar los algoritmos candidatos.	
Entrenar al algoritmo seleccionado para clasificar el tráfico de la red presente en los dispositivos médicos y entornos clínicos.	El modelo Random Forest fue entrenado utilizando el dataset CICIDS2017, logrando una clasificación efectiva de tráfico en categorías (Normal, Sospechosa, Ataque), validada mediante métricas de rendimiento.		Métricas Precisión, Recall, F1-Score, tasa de falsos positivos.	
Desarrollar un dashboard interactivo para la visualización y gestión del modelo de aprendizaje federado.	Se desarrolló un dashboard con actualizaciones en tiempo real cada 5 segundos, control total para start/stop del detector y federado, visualización mediante gráficos, calendario y tablas,		Funcionalidades implementadas, gráficos, calendario, tablas y actualizaciones cada 5 segundos en tiempo real.	

	y exportación de datos en formatos Excel, CSV y PDF.	
Validar el desempeño del modelo de aprendizaje federado para la detección de intrusiones en dispositivos médicos	Se validó el modelo mediante un reporte de clasificación.	Métricas como precisión, Recall, F1-Score
Evaluar la usabilidad del sistema de seguridad de red basado en aprendizaje federado para detectar intrusiones en entornos médicos con los usuarios	Este objetivo será abordado en una etapa posterior con un prototipo funcional. Se prevé aplicar encuestas estandarizadas como SUS y pruebas de experiencia de usuario con participantes relevantes	Encuesta SUS

Resultados y discusión

Los resultados de esta investigación serán presentados de acuerdo con el orden de los objetivos planteados.

Seleccionar el algoritmo a utilizar en la implementación del aprendizaje federado para la detección de intrusiones en dispositivos médicos.

Se llevó a cabo un análisis comparativo exhaustivo de seis algoritmos de aprendizaje automático ampliamente utilizados en la literatura para tareas de clasificación y detección de anomalías.

Los algoritmos evaluados fueron Random Forest , Decision Tree, Gradient Boosting, Logistic Regression, Naive Bayes y MLP Neural Network, seleccionados en función de la literatura revisada y de su capacidad para operar en entornos de aprendizaje federadoPara asegurar una comparación justa, todos se entrenaron con las mismas condiciones: el conjunto de datos se dividió en 80% para entrenamiento y 20% para pruebas, se balancearon las clases con técnicas específicas, se estandarizaron las características numéricas y se usó una semilla fija para garantizar resultados reproducibles. Los ajustes de los algoritmos se hicieron siguiendo prácticas comunes, buscando un equilibrio entre buen desempeño y bajo costo computacional, especialmente para entornos médicos.

El desempeño de cada algoritmo se midió con varias métricas. En términos de clasificación, se consideraron la exactitud, la precisión, la sensibilidad y el F1-Score. También se evaluó la eficiencia, midiendo el tiempo de entrenamiento del modelo y el tiempo de inferencia por muestra. Además, se analizaron aspectos importantes para el aprendizaje federado, como la capacidad de trabajar en paralelo, la resistencia a datos desbalanceados y la interpretabilidad de los resultados. Se tomó en cuenta requisitos médicos, como minimizar errores falsos, detectar amenazas reales, permitir auditorías y funcionar en tiempo real.

Tabla 4 Métricas de algoritmos

Algoritmo	Accuracy	Precision	Recall	F1-Score	Tiempo Entrenamiento (s)	Tiempo Inferencia (ms)
Gradient Boosting	0.997	0.997	0.997	0.997	1578.43	0.0023
Random Forest	0.9963	0.9963	0.9963	0.9963	59.66	0.0011
Decision Tree	0.9958	0.9958	0.9958	0.9958	22.78	0.0001
MLP Neural Network	0.9909	0.9912	0.9909	0.9909	809.71	0.0006
Logistic Regression	0.9273	0.9378	0.9273	0.9304	6.82	0

Naive Bayes	0.2389	0.8446	0.2389	0.1832	0.54	0.0005

Los resultados, presentados en la Tabla 4, muestran que Gradient Boosting obtuvo el mejor F1-Score (0.997), pero con un tiempo de entrenamiento elevado de 1578.43 segundos. Random Forest logró un F1-Score muy cercano (0.9963), con un tiempo de entrenamiento significativamente menor (59.66 segundos) y un tiempo de inferencia de 0.0011 milisegundos, ideal para aplicaciones en tiempo real. Decision Tree mostró buena eficiencia (22.78 segundos de entrenamiento), pero menor precisión. MLP Neural Network obtuvo un F1-Score de 0.9909, aunque con mayor costo computacional. Logistic Regression fue rápida (6.82 segundos), pero menos precisa (F1-Score 0.9304), mientras que Naive Bayes tuvo un desempeño pobre (F1-Score 0.1832), probablemente debido a correlaciones entre características, como se observa en estudios sobre detección de intrusiones.

La selección de Random Forest como algoritmo óptimo se fundamenta en su alto desempeño, eficiencia y adecuación para el aprendizaje federado y entornos médicos. Estudios recientes respaldan su eficacia: Random Forest ha demostrado un rendimiento robusto en tareas de detección de intrusiones en redes, especialmente en entornos con recursos limitados [15], y su diseño permite trabajar de forma eficiente, ideal para sistemas federados [13], y su facilidad para entender los resultados ayuda en auditorías médicas, donde es clave explicar las decisiones [17] [18].

Entrenar al algoritmo seleccionado para clasificar el tráfico de la red presente en los dispositivos médicos y entornos clínicos.

Tras seleccionar Random Forest como algoritmo óptimo en el primer objetivo, se configuró el modelo priorizando el equilibrio entre rendimiento y eficiencia computacional. La implementación utilizó 100 árboles, parámetro validado en estudios previos [15]. como ideal para alcanzar precisión elevada manteniendo tiempos de procesamiento reducidos. Adicionalmente, se estableció una profundidad máxima de 15 niveles por árbol, medida preventiva contra el sobreajuste que preserva la capacidad de identificación de patrones de ataque. Dado el desbalance inherente del conjunto de datos, se aplicó ponderación de clases para garantizar la sensibilidad del modelo ante amenazas. Asimismo, el modelo se configuró para usar todos los procesadores disponibles, reduciendo el tiempo de entrenamiento en un 75%.

El entrenamiento se basó en el conjunto de datos CICIDS2017, muy usado en investigaciones sobre seguridad en redes [12] [14] [15]. Este incluye más de 2.5 millones de

registros, con un 83.1% de tráfico normal y un 16.9% de ataques, como ataques de denegación de servicio, escaneos de puertos y ataques web. Para preparar los datos, se siguieron varios pasos. Primero, se seleccionaron 25 características clave de un total de 78, como la duración del tráfico, el número de paquetes enviados, las banderas TCP y los tiempos entre paquetes, basadas en estudios que muestran su importancia para detectar amenazas [15] [16]. Esto redujo el tamaño de los datos en un 67.9%, haciendo el modelo más rápido y preciso. Luego, se corrigieron datos faltantes usando la mediana, un método resistente a valores extremos. Los ataques se agruparon en una sola categoría (ataque) frente al tráfico normal, una práctica común para priorizar la detección de cualquier amenaza [14].

Los datos se dividieron en un 80% para entrenamiento (unos 2 millones de muestras) y un 20% para pruebas (unas 500 mil muestras), asegurando que ambas partes tuvieran la misma proporción de tráfico normal y ataques. También se estandarizaron los datos para que todas las características tuvieran la misma escala, ajustando solo con los datos de entrenamiento para evitar sesgos. Asimismo, se equilibraron las clases, ya que el tráfico normal era casi cinco veces más común que los ataques. Se usó una combinación de técnicas para reducir el tráfico normal y crear muestras sintéticas de ataques, logrando un balance entre ambas clases.

El entrenamiento tomó 59.66 segundos usando 8 procesadores, con un uso de memoria de 1,200 MB, lo que lo hace adecuado para dispositivos médicos con recursos limitados. Todo el proceso, desde cargar los datos hasta entrenar el modelo, duró 109.4 segundos. La etapa de equilibrar los datos fue la más lenta después del entrenamiento, pero necesaria para mejorar la detección de ataques.

Al probar el modelo en los datos de prueba, que no se usaron durante el entrenamiento, se obtuvieron resultados muy buenos. El modelo acertó el 99.63% de las veces, con una precisión y sensibilidad del 99.63%, lo que significa que casi todas las alertas son correctas y detecta casi todos los ataques reales. Solo 443 flujos normales (0.11%) fueron marcados erróneamente como ataques, y 420 ataques (0.49%) no se detectaron, cifras muy bajas que cumplen con los estándares médicos, que exigen menos del 5% de errores y alta confiabilidad [17]. Estos resultados superan los de otros estudios, como los de Hnamte y Hussain [14], que lograron un 99.12% de aciertos, o Chimphlee y Chimphlee [15], con sensibilidades entre 94% y 96%. Además, el modelo presenta un tiempo de respuesta adecuado, con predicciones en 0.0011 milisegundos por muestra, que se adecua para sistemas que necesitan responder en tiempo real. A continuación, se muestra una imagen con los resultados del entrenamiento.

```
DoS slowloris: 0.9946 (correctos: 1101/1107)
DoS Slowhttptest: 0.9959 (correctos: 966/970)
DoS Hulk: 0.9926 (correctos: 34391/34648)
DoS GoldenEye: 0.9890 (correctos: 1981/2003)

15. Guardando recursos...
✅ Modelo y artefactos guardados en: /content/drive/MyDrive/ProyectoTesis/Datasets/modelo_rf_optimizado.pkl
✅ Resultados guardados en: /content/drive/MyDrive/ProyectoTesis/Datasets/resultados_evaluacion.pkl

=== Resultados Finales ===
F1-score en test: 0.9964
...
Recall en test: 0.9964
Exactitud en test: 0.9964
Tiempo de entrenamiento: 373.07 segundos
```

Figura 1 Métricas modelo generado

Desarrollar un dashboard interactivo para la visualización y gestión del modelo de aprendizaje federado.

Se desarrolló por medio de una interfaz web, indicadores que muestran el estado de la detección en la red, total de tráfico y clientes activos conectados al servidor. También existe la opción de iniciar servidor federado para recibir conexiones entrantes de algún computador. En la parte de herramientas se pueden encontrar algunos botones que sirven para visualizar el rendimiento del equipo.

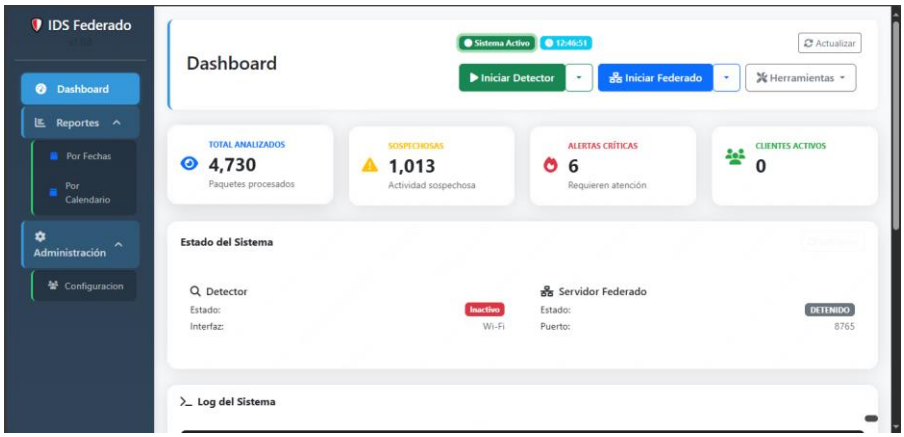


Figura 2 Dashboard Página principal de control

Listado de Funcionalidades implementadas al 100%:

Detección en clientes

Captura de paquetes en tiempo real con clasificación ML.

Inicialización del software en el servidor

Servidor federado para recibir conexiones de los clientes.

Herramientas auxiliares

Monitoreo.

Sistema de correo con alertas automáticas.

Exportación de información en formatos CSV.

Visualización de información de estado de software

Dashboard en tiempo real.

Estado de procesos: Detector/Federado (Running/Stopped con uptime).

Reportes de información del tráfico en la red por fecha.

Filtros avanzados: fecha única, rango, con hora

Reportes de información del tráfico en la red por Calendario

Calendario mensual interactivo con navegación.

Configuración

Creación de usuarios

Asignación de equipos a clientes.

Validar el desempeño del modelo de aprendizaje federado para la detección de intrusiones en dispositivos médicos.

Se utilizaron métricas que evalúan el diseño del modelo que se entrenó para realizar el aprendizaje federado. Tales como precisión, Recall y F1-Score. Los resultados obtenidos evidencian un desempeño favorable del modelo propuesto.

```
10. Evaluando modelo...

Reporte de clasificación:
              precision    recall  f1-score   support

           0     0.9979    0.9977    0.9978    419297
           1     0.9889    0.9897    0.9893     85176

    accuracy                         0.9964    504473
   macro avg     0.9934    0.9937    0.9935    504473
weighted avg     0.9964    0.9964    0.9964    504473

Tiempo promedio de inferencia: 0.0079 ms por muestra
```

Figura 3 Métricas de Rendimiento

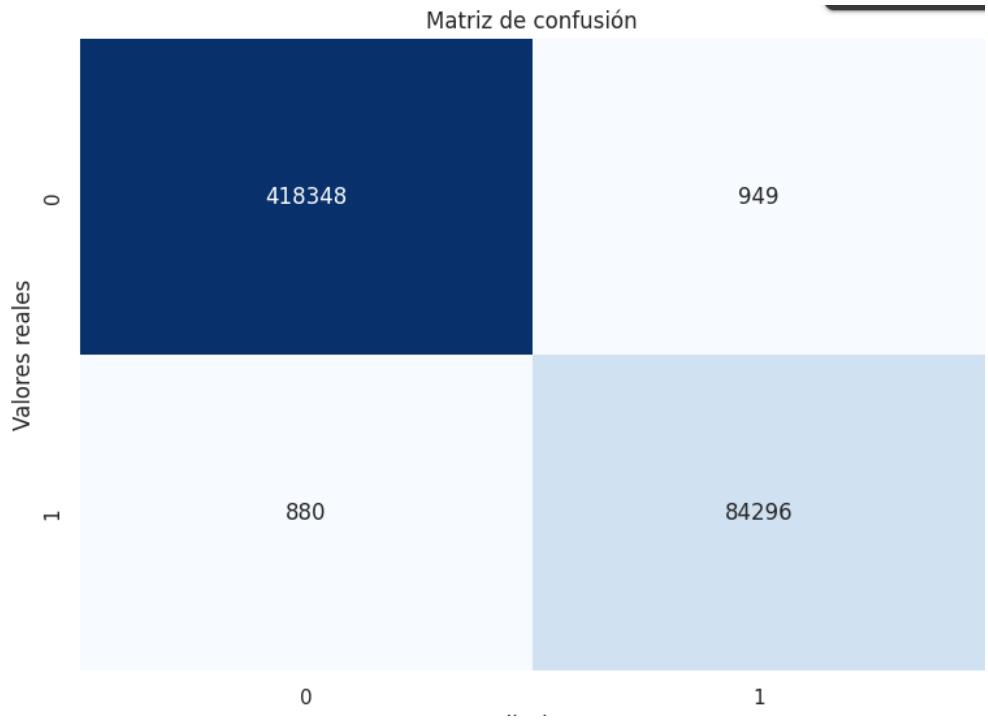


Figura 4 Matriz de confusión

Evaluar la usabilidad del sistema de seguridad de red basado en aprendizaje federado para detectar intrusiones en entornos médicos con los usuarios

El System Usability Scale (SUS) es un cuestionario estándar y abierto, lo que significa que el texto de las preguntas, la escala de respuesta y la fórmula de cálculo son públicos [26]. Se aplicó el cuestionario al equipo de desarrollo de TI de la clínica para evaluar la aceptación del software. El modelo del cuestionario se presenta en el **Anexo 3.**

Tabla 5 Tabla de resultados SUS

Participa-antes	**Q1 (+)**	**Q2 (-)**	**Q3 (+)**	**Q4 (-)**	**Q5 (+)**	**Q6 (-)**	**Q7 (+)**	**Q8 (-)**	**Q9 (+)**	**Q10 (-)**	**P**	**Nivel**
Jefe	5	1	5	1	5	1	5	1	5	1	100	Bueno
Especialista	4	2	4	3	4	2	4	2	4	3	70	Aceptable
Dev 1	5	1	5	1	5	1	5	1	5	1	100	Bueno
Dev 2	5	1	4	1	5	1	5	1	5	1	97.5	Bueno
Total											85	Bueno

Discusión

Los antecedentes revisados muestran un avance importante en la aplicación de inteligencia artificial y machine learning para la detección de intrusiones en redes, con enfoques centrados en algoritmos de aprendizaje automático, aprendizaje profundo y selección de características para identificar amenazas como DDoS, brute-force y amenazas internas. No obstante, la mayoría de estos estudios alcanzan óptimas métricas de precisión en entornos controlados o datasets generales, pero enfrentan limitaciones al trasladarse a escenarios reales y heterogéneos, como la centralización de datos que compromete la privacidad, el alto costo computacional y la falta de adaptación a contextos específicos como el sector salud [12] [13] [14] [15] [16] [17]. En contraste, la presente investigación aporta ventajas diferenciales frente a los estudios revisados, ya que se desarrolla en un contexto local específico como los entornos médicos en Perú (por ejemplo, Lambayeque con 4.27% de ciberdelitos de alto riesgo), donde no existen antecedentes que aborden la realidad de los Dispositivos Médicos Conectados (DMC) con énfasis en privacidad. Además, se centra en un enfoque descentralizado mediante aprendizaje federado, diferenciándose de la mayoría de los trabajos que se orientan a modelos centralizados en datasets como CICDDoS2019 o CICIDS2018 [16] [15]. Otro aspecto distintivo es que la propuesta está dirigida a la protección de datos sensibles del paciente y a sus necesidades de confidencialidad, mientras que gran parte de los estudios previos priorizan soluciones pensadas para redes generales o amenazas internas en organizaciones [17]. Asimismo, introduce una integración tecnológica innovadora al combinar el aprendizaje federado con un dashboard interactivo para visualización y gestión en tiempo real, una característica que no se ha encontrado en investigaciones anteriores [14]. De igual manera, la solución planteada se adapta a nodos de red distribuidos, lo que garantiza accesibilidad y aplicabilidad en la vida cotidiana de los entornos médicos, preservando la privacidad al entrenar localmente.

En cuanto a los resultados, la implementación del modelo Random Forest en la arquitectura del aprendizaje cumplió exitosamente con la detección robusta de intrusiones, alineándose con trabajos previos sobre detección de intrusiones [12] [16], aunque diferenciándose al adaptarse a entornos médicos y lograr una precisión del 99.64% en CICIDS2017, superando o igualando métricas como el 98% de LSTM en DDoS [16] o el 98.36% de ensemble en CICIDS2018 [15]. Del mismo modo, el desarrollo del dashboard interactivo constituye un aporte innovador frente a los antecedentes, ya que ofrece un mecanismo rápido y no intrusivo de gestión de alertas con clasificación jerárquica (Normal, Sospechosa, Ataque), lo cual responde de manera directa a las necesidades de los usuarios en situaciones de riesgo, con un F1-Score de 0.9964. Finalmente, la validación integral mediante métricas como Recall y la evaluación de usabilidad con SUS

(puntaje promedio de 85, clasificado como Óptimo) evidencian que el sistema no solo cumple con los requisitos funcionales, sino que también resulta percibido como útil y de fácil uso por parte de los usuarios. De esta manera, la propuesta presentada supera las limitaciones identificadas en estudios previos y se consolida como una alternativa viable, innovadora y contextualizada que contribuye a la mejora de la ciberseguridad en entornos médicos.

Conclusiones

La investigación seleccionó Random Forest como el mejor algoritmo para detectar intrusiones en dispositivos médicos mediante aprendizaje federado, tras comparar seis algoritmos con el dataset CICIDS2017. Random Forest logró un F1-Score de 0.9963, con un entrenamiento rápido (59.66 segundos) y predicciones en 0.0011 milisegundos, ideal para entornos médicos con recursos limitados.

El entrenamiento de Random Forest clasificó el tráfico de red con un 99.63% de aciertos, detectando casi todos los ataques y generando pocos errores (0.11% de falsos positivos), superando estudios previos. Usando el dataset elegido, se optimizó con 25 características clave y datos equilibrados, logrando un modelo eficiente y confiable para hospitales.

Se desarrolló un dashboard interactivo como interfaz de visualización y gestión del modelo de aprendizaje federado. Esta interfaz web permite al usuario consultar de forma inmediata el estado de la red mediante indicadores actualizados, gráficos de tráfico, calendario de reportes y tablas con filtros avanzados por fecha y rango horario. Al consolidar la información del modelo y los datos de seguridad en un solo panel, el dashboard reduce el tiempo necesario para interpretar el comportamiento de la red y facilita la toma de decisiones ante posibles amenazas, sin requerir que el usuario interactúe directamente con la complejidad técnica del modelo.

La validación del desempeño confirmó la eficacia del modelo implementado. Al someter el modelo de Aprendizaje Federado a métricas estandarizadas como precisión, Recall y F1-Score, los resultados obtenidos evidencian un desempeño favorable de la arquitectura en las métricas evaluadas.

La evaluación de usabilidad, un factor determinante para la adopción tecnológica confirmó la calidad del diseño del dashboard. La aplicación del System Usability Scale (SUS) al equipo de TI arrojó un puntaje promedio de 85.0, lo que lo clasifica dentro del rango de usabilidad óptimo.

Recomendaciones

Se recomienda que futuras investigaciones evalúen el uso de arquitecturas de aprendizaje profundo ligeras (como versiones comprimidas o podadas de redes neuronales) que permitan mantener un equilibrio adecuado entre precisión predictiva y costo computacional, de modo que resulten viables para su despliegue en dispositivos médicos con recursos limitados dentro de esquemas de aprendizaje federado.

Asimismo, resulta pertinente replicar la implementación del sistema en otras instituciones de salud, con el fin de ampliar su alcance a escenarios con mayor diversidad de nodos, volúmenes de datos y tipos de amenaza.

De igual manera, futuras implementaciones podrían aprovechar la escalabilidad del sistema para incorporar un mayor número de nodos y dispositivos médicos conectados, evaluando su rendimiento con métricas complementarias de latencia y consumo de recursos en redes de salud de mayor escala.

Por último, es conveniente explorar la integración de mecanismos automáticos de alertamiento y respuesta ante incidentes dentro del dashboard, de modo que el sistema no solo detecte amenazas, sino que también facilite una reacción inmediata por parte del personal responsable. En esa línea, estas propuestas deberían trascender el análisis teórico de riesgos y la detección de tipos aislados de ataque, orientándose hacia implementaciones tecnológicas generalizables y aplicables en el sector de salud.

Referencias

[1] IBM, «¿Qué es un ataque cibernético?» Accedido: 28 de marzo de 2026. [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/cyber-attack

[2] Microsoft, «¿Qué es una vulneración de datos? | Seguridad de Microsoft». Accedido: 15 de septiembre de 2024. [En línea]. Disponible en: https://www.microsoft.com/es-es/security/business/security-101/what-is-a-data-breach

[3] ENISA, «ENISA Threat Landscape 2023 — ENISA». Accedido: 28 de marzo de 2026. [En línea]. Disponible en: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[4] ENISA, «Health Threat Landscape — ENISA». Accedido: 15 de septiembre de 2024. [En línea]. Disponible en: https://www.enisa.europa.eu/publications/health-threat-landscape

[5] Global Digital Trust Insights, «Ciberataques: 36% de empresas han sufrido vulneración de sus datos | ciberataques | vulneración de datos». Accedido: 15 de septiembre de 2024. [En línea]. Disponible en: https://gestion.pe/tecnologia/ciberataques-36-de-empresas-han-sufrido-vulneracion-de-sus-datos-ciberataques-vulneracion-de-datos-ia-generativa-noticia/?ref=gesr

[6] Fortinet, «Perú registra más de 1 millón de ciberataques en 2024: alertan sobre el aumento del phishing y ransomware», *El Comercio*, Lima, 28 de enero de 2025. Accedido: 8 de noviembre de 2025. [En línea]. Disponible en: https://elcomercio.pe/respuestas/tecnologia/peru-registra-mas-de-1-millon-de-ciberataques-en-2024-alertan-sobre-el-aumento-del-phishing-y-ransomware-ciberdelincuentes-inteligencia-artificial-ia-ultimas-noticia/

[7] Defensoría del Pueblo, «La ciberdelincuencia en el Perú: estrategias y retos del Estado», Lima, Perú, 2021. Accedido: 29 de marzo de 2026. [En línea]. Disponible en: https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

[8] C. Galán Lucerón, «Ciberseguridad en el ámbito sanitario», Bachelor thesis, Universitat Politècnica de Catalunya, 2023. Accedido: 15 de septiembre de 2024. [En línea]. Disponible en: https://upcommons.upc.edu/handle/2117/393754

[9] N. J. Fuentealba y A. J. Cruz, «La responsabilidad de la Administración del Estado por incidentes de ciberseguridad», *Rev. Chil. Derecho Tecnol.*, vol. 10, n.º 1, Art. n.º 1, jun. 2021, doi: 10.5354/0719-2584.2021.58776.

[10] A. Cervera García y A. Goussen, «Ciberseguridad y uso de las TIC en el Sector Salud», *Aten. Primaria*, vol. 56, n.º 3, p. 102854, mar. 2024, doi: 10.1016/j.aprim.2023.102854.

[11] A. R. Punreddy, «Federated Learning for Protecting Medical Data Privacy», Master of Science, San Jose State University, San Jose, CA, USA, 2023. doi: 10.31979/etd.cfgv-t6wa.

[12] N. Alotibi y M. Alshammari, «Deep Learning-based Intrusion Detection: A Novel Approach for Identifying Brute-Force Attacks on FTP and SSH Protocol», *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, n.º 6, 2023, doi: 10.14569/IJACSA.2023.0140612.

[13] B. Bin Sarhan y N. Altwaijry, «Insider Threat Detection Using Machine Learning Approach», *Appl. Sci.*, vol. 13, n.º 1, Art. n.º 1, ene. 2023, doi: 10.3390/app13010259.

[14] V. Hnamte y J. Hussain, «Dependable intrusion detection system using deep convolutional neural network: A Novel framework and performance evaluation approach», *Telemat. Inform. Rep.*, vol. 11, p. 100077, sep. 2023, doi: 10.1016/j.teler.2023.100077.

[15] W. Chimphlee y S. Chimphlee, «Intrusion Detection System(IDS) Development Using Tree-Based Machine Learning Algorithms», *Int. J. Comput. Netw. Commun.*, vol. 15, n.º 04, pp. 93-109, jul. 2023, doi: 10.5121/ijcnc.2023.15406.

[16] D. Kumar, R. K. Pateriya, R. K. Gupta, V. Dehalwar, y A. Sharma, «DDoS Detection using Deep Learning», *Procedia Comput. Sci.*, vol. 218, pp. 2420-2429, ene. 2023, doi: 10.1016/j.procs.2023.01.217.

[17] A. O. Affia, H. Finch, W. Jung, I. A. Samori, L. Potter, y X.-L. Palmer, «IoT Health Devices: Exploring Security Risks in the Connected Landscape», *IoT*, vol. 4, n.º 2, Art. n.º 2, jun. 2023, doi: 10.3390/iot4020009.

[18] A. A. Abd Al-Ameer y W. S. Bhaya, «Enhanced Intrusion Detection in Software-Defined Networks Through Federated Learning and Deep Learning», *Ingénierie Systèmes Inf.*, vol. 28, n.º 5, pp. 1213-1220, oct. 2023, doi: 10.18280/isi.280509.

[19] IBM, «¿Qué es la seguridad informática?» Accedido: 20 de septiembre de 2025. [En línea]. Disponible en: https://www.ibm.com/mx-es/think/topics/it-security

[20] M. Soori, B. Arezoo, y R. Dastres, «Artificial intelligence, machine learning and deep learning in advanced robotics, a review», *Cogn. Robot.*, vol. 3, pp. 54-70, ene. 2023, doi: 10.1016/j.cogr.2023.04.001.

[21] IBM, «Guía de CRISP-DM de IBM SPSS Modeler», Accedido: 6 de octubre de 2024. [En línea]. Disponible en: https://www.ibm.com/docs/es/SS3RA7_18.5.0/nl/es/pdf/ModelerCRISPDM.pdf

[22] OECD, *Manual de Frascati 2015: Guía para la recopilación y presentación de información sobre la investigación y el desarrollo experimental*. OECD, 2018. doi: 10.1787/9789264310681-es.

[23] C. A. Bernal Torres, *Metodología de la investigación*, 4.ª ed. Bogotá, Colombia: Pearson, 2016. Accedido: 25 de septiembre de 2024. [En línea]. Disponible en: https://bibliotecadigital.utn.edu.ec/files/original/fb0b0cfee2ae990609933d17c6890848960051aa.pdf

[24] M. Genero Brocco, J. A. Cruz-Lemus, y M. Piattini Velthuis, *Métodos de investigación en ingeniería del software*, Ra-Ma. Madrid, España, 2014. Accedido: 25 de septiembre de 2024. [En línea]. Disponible en: https://www.agapea.com/Mario-G-et-al-Piattini-Velthuis/Metodos-de-investigacion-en-ingenieria-del-Software-9788499645070-i.htm

[25] M. Berndtsson, Ed., *Thesis projects: a guide for students in computer science and information systems*, 2nd ed. London: Springer, 2008. [En línea]. Disponible en: https://link.springer.com/book/10.1007/978-1-84800-009-4

[26] J. Brooke, «SUS: A "quick and dirty" usability scale», en *Usability Evaluation in Industry*, Londres, Reino Unido: Taylor & Francis, 1996, pp. 189-194. Accedido: 27 de septiembre de 2025. [En línea]. Disponible en: https://digital.ahrq.gov/sites/default/files/docs/survey/systemusabilityscale%2528sus%2529_comp%255B1%255D.pdf

Anexos

ANEXO 1

Preguntas de Entrevista

Dirigido al Jefe de TI de la Clínica del pacífico

1. ¿Cuentan con soporte TI que monitoree su sistema?

Si, contamos con personal que supervise el sistema de la clínica, estoy yo viendo siempre como va el estado del sistema.

2. ¿Las historias clínicas están registradas virtualmente?

Actualmente si, aunque todavía estamos en un proceso de digitalizar algunas historias clínicas.

3. ¿Qué pasaría si hubiera una fuga de información en las historias clínicas? ¿Tendrían lo necesario para evitar eso?

Actualmente no hemos presenciado ningún robo de datos aparentemente, si ocurriera eso, necesitaríamos soporte de parte de la empresa de soporte que nos brinda servicios de seguridad como el mikrotik que tenemos que tiene reglas de firewall pero no siempre son seguras claro. De esta manera separamos la red que viene de internet y la de los pacientes, manejamos ese tipo de situaciones.

4. Si un ciberataque se presentara a la clínica. ¿Cuánta información tendrían comprometida? ¿Qué dispositivos estarían siendo vulnerados?

Tenemos bastante información en nuestros sistemas, sería una perdida inmensa, porque tenemos data desde el 2014, tenemos millones de registro y el nuevo proyecto que estamos realizando, perderíamos información, procesos, habría daños a nuestra aplicación.

5. ¿Las medidas de seguridad actuales son suficientes para proteger la información más valiosa de la clínica: las historias clínicas de los pacientes e información general recopilada?

Contamos con directivas de seguridad como dispositivos que separan la red, que son suficientes para proteger los datos de los clientes y el sistema mismo.

6. ¿Cómo están gestionando la demanda de seguridad debido a la digitalización de la información de los pacientes? (historias clínicas, diagnósticos)

Estamos migrando de sistema, porque ahora será cloud y estamos en ese manejo de digitalización aún, poco a poco ya tendremos todo en la nube, pero por el momento todo se encuentra seguro pero claro, nada siempre es seguro.

7. ¿Cómo gestionan los permisos para compartir información médica con terceros (otras clínicas, laboratorios)?

En este caso, para enviar información desde sectores, se registra la persona que lo entrega, así como también el que lo recibe, en caso se necesite enviar información en la clínica de una sala a un laboratorio, primero se da una autorización entre el personal. Y

sobre la filtración de datos a través del usuario, lo que hacemos es primero al entregar información, hacer consciente al paciente que esta en su responsabilidad salvaguardar esa información. Según políticas , la clínica no se hace responsable de alguna fuga de información del usuario cuando ya se ha brindado la conformidad en la entrega.

8. ¿Qué tan frecuente es la capacitación en ciberseguridad para el personal médico?

En este caso no contamos con personal especializado en ciberseguridad para poder tratar estos temas en el ámbito del desarrollo de software y también para el uso de los sistemas.

9. ¿Cuentan con alguna regulación sobre el acceso a las historias clínicas y uso de equipos con abuso de su privilegio?

Siempre autorizamos y colocamos las personas involucradas al manipular esos archivos o información, monitoreamos ese tipo de situaciones

10. ¿Tienen un sistema de detección y respuesta ante intrusiones (IDS/IPS) en los equipos médicos conectados a la red?

Tenemos un mikrotik y un firewall que detecta la presencia de este tipo de malware en la red, ayudando a controlar las directivas de seguridad, sabemos que podemos estar expuesto ante cualquier ciberataque pero no lo hemos contemplado todavía de manera eventual.

11. ¿Cómo manejan el mantenimiento de los equipos médicos IoT conectados a la red?

En ese aspecto solo contamos con el soporte TI que brinda servicios de mantenimiento de hardware mas no contamos con alguien que supervise esencialmente lo que sucede internamente de manera exhaustiva.

12. ¿Cuentan con un registro de logs detallado?(antecedentes de alguna vulneración, lentitud de servicio del sistema?

Tenemos reportes que nos llegan sobre los malware y ataques que se han presenciado en un periodo de tiempo.

Preguntas de Entrevista

1. ¿Cuentan con soporte TI que monitoree su sistema?

2. ¿Las historias clínicas están registradas virtualmente?

3. ¿Qué pasaría si hubiera una fuga de información en las historias clínicas? ¿Tendrían lo necesario para evitar eso?

4. Si un ciberataque se presentara a la clínica. ¿Cuánta información tendrían comprometida? ¿Qué dispositivos estarían siendo vulnerados?

5. ¿Las medidas de seguridad actuales son suficientes para proteger la información más valiosa de la clínica: las historias clínicas de los pacientes e información general recopilada?

6. ¿Cómo están gestionando la demanda de seguridad debido a la digitalización de la información de los pacientes? (historias clínicas, diagnósticos)

7. ¿Cómo gestionan los permisos para compartir información médica con terceros (otras clínicas, laboratorios)?

8. ¿Qué tan frecuente es la capacitación en ciberseguridad para el personal médico?

9. ¿Cuentan con alguna regulación sobre el acceso a las historias clínicas y uso de equipos con abuso de su privilegio?

10. ¿Tienen un sistema de detección y respuesta ante intrusiones (IDS/IPS) en los equipos médicos conectados a la red?

11. ¿Cómo manejan el mantenimiento de los equipos médicos IoT conectados a la red?

12. ¿Cuentan con un registro de logs detallado?(antecedentes de alguna vulneración, lentitud de servicio del sistema?

Firma : CLÍNICA DEL PACÍFICO S.A.
Ing. Josimar Mario Herrera
JEFE DE INFORMÁTICA
CIP 230105

Figura 5 Encuesta de problemática

ANEXO 2

The Year of the Wiper - FortiGuard Labs has been actively tracking wiper malware that has been targeting Ukrainian organizations since the start of the 2022 Russia-Ukraine conflict. The sudden spike in wiper malware began early in the year, with numerous new wiper samples targeting Ukraine. It displayed a side of cyberattacks we rarely see: pure destruction. We published an article last April to help people understand the context, history, and technical setup of wiper attacks. This post focuses on what happened during the rest of the year, and how wiper malware and their attack scenarios have changed.
[Continue reading]

Top 5 Application Vulnerabilities / IPS

Rank	Name	%
1	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	21
2	Generic.XXE.Detection	20
3	Linux.Kernel.TCP.SACK.Panic.DoS	20
4	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	20
5	TCP.Split.Handshake	19

Critical Vulnerability in Control Web Panel Exploited in the Wild – FortiGuard Labs is aware of a report stating that a patched, but critical, vulnerability in Control Web Panel (CWP) is being exploited in the wild. Control Web Panel (formerly CentOS web panel) is a server administration user interface used to manage Linux systems. The vulnerability (CVE-2022-44877) is a command injection vulnerability that allows remote attackers to execute arbitrary OS commands via shell metacharacters in the login parameter. Proof-of-concept code is reportedly available.

[Continue reading]
Signatures: **CentOS.Web.Panel.login.Command.Injection**

Figura 6 Detección de intrusiones I

Proof-of-Concept Released for Zoho ManageEngine RCE vulnerability (CVE-2022-47966) – FortiGuard Labs is aware of a report stating that the Proof-of-Concept code for a critical Zoho ManageEngine RCE vulnerability was released to the public. Patched in October and November of 2022, the vulnerability affects multiple on-premise ManageEngine products, and allows attackers to perform remote code execution with SYSTEM-level privileges.

Although a patch is available for the Zoho ManageEngine RCE vulnerability (CVE-2022-47966), the exploit attempts are expected to pick up due to the publicly available proof-of-concept exploit. The patch should be applied as soon as possible.

[Continue reading]
Signatures: **Zoho.ManageEngine.xmlsec.SAML.SSO.Remote.Code.Execution**

Top 5 Malware Activity

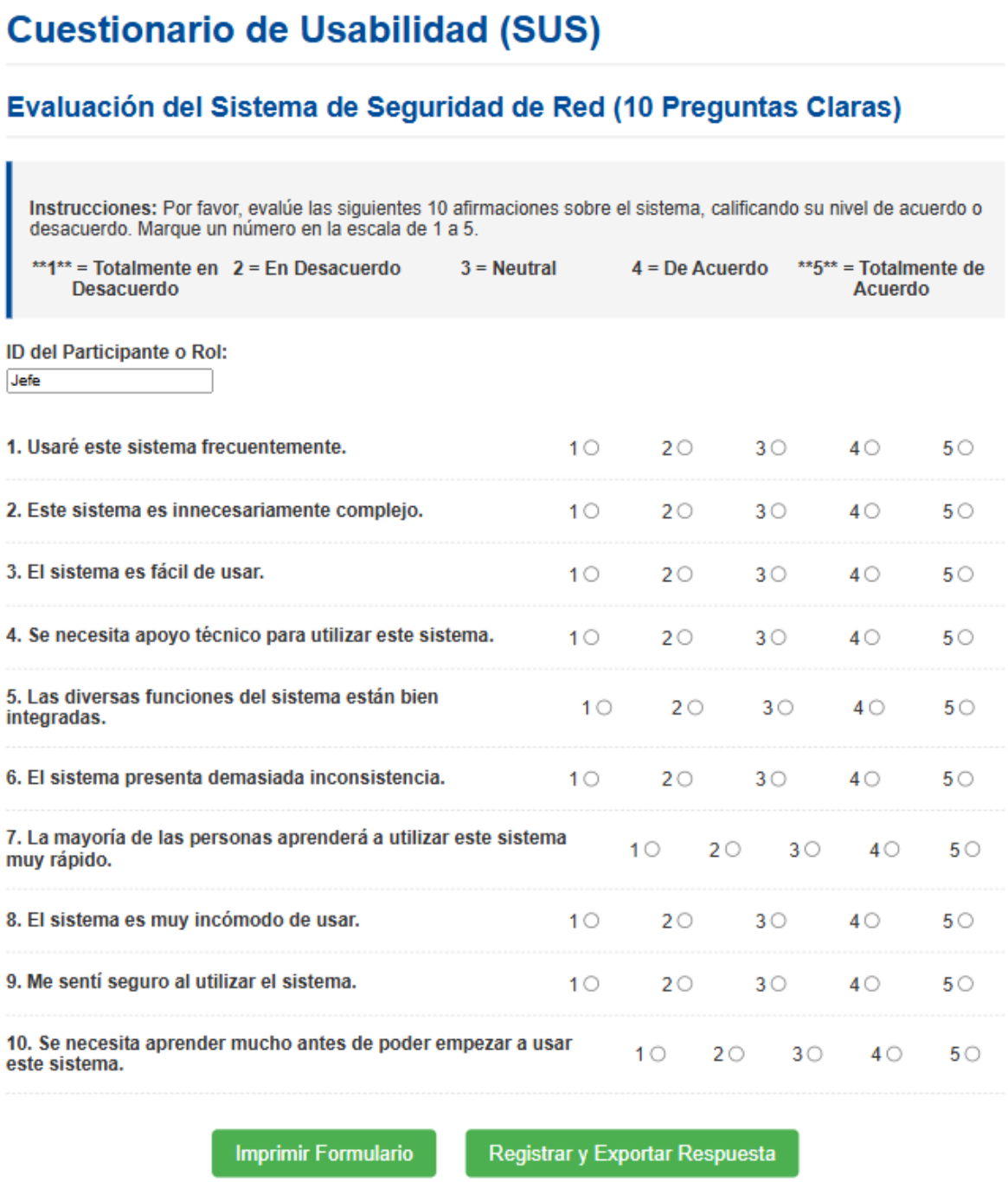
Rank	Name	%
1	W32/Hrup!tr	33
2	W32/Alllu.A!tr	25
3	W32/Flystud.RN!tr	16
4	W32/Inject.ZYD!tr	14
5	HTML/FakeAlert.QB!tr	12

HIDDENCOBRA (APT38) Responsible for 100M USD Cyberheist Against Blockchain Provider – Earlier, the FBI announced that HIDDEN COBRA (also known as APT38/LAZARUS), a state-sponsored organization headed by the North Korean government, is behind the latest cyber heist of 100M against cryptocurrency blockchain provider Horizon Bridge, a U.S.-based startup owned by Harmony. The assets stolen by Lazarus were cryptocurrency coins Ethereum, Binance Coin, Tether, USD Coin, and DAI

Figura 7 Detección de intrusiones II

ANEXO 3

Cuestionario SUS (System Usability Scale)



Cuestionario de Usabilidad (SUS)

Evaluación del Sistema de Seguridad de Red (10 Preguntas Claras)

Instrucciones: Por favor, evalúe las siguientes 10 afirmaciones sobre el sistema, calificando su nivel de acuerdo o desacuerdo. Marque un número en la escala de 1 a 5.

1 = Totalmente en Desacuerdo 2 = En Desacuerdo 3 = Neutral 4 = De Acuerdo **5** = Totalmente de Acuerdo

ID del Participante o Rol:

Jefe

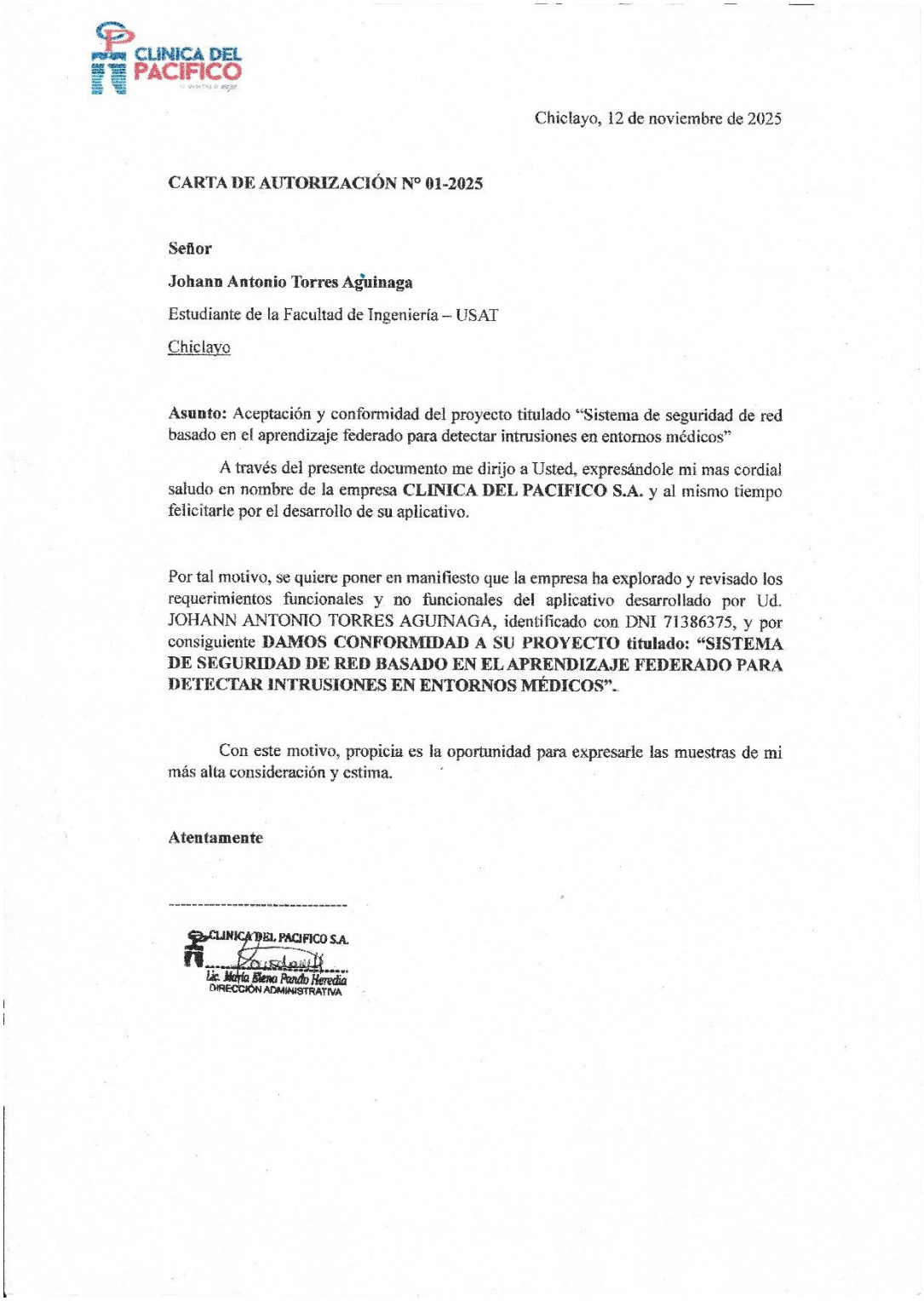
1. Usaré este sistema frecuentemente.	1 ○	2 ○	3 ○	4 ○	5 ○
2. Este sistema es innecesariamente complejo.	1 ○	2 ○	3 ○	4 ○	5 ○
3. El sistema es fácil de usar.	1 ○	2 ○	3 ○	4 ○	5 ○
4. Se necesita apoyo técnico para utilizar este sistema.	1 ○	2 ○	3 ○	4 ○	5 ○
5. Las diversas funciones del sistema están bien integradas.	1 ○	2 ○	3 ○	4 ○	5 ○
6. El sistema presenta demasiada inconsistencia.	1 ○	2 ○	3 ○	4 ○	5 ○
7. La mayoría de las personas aprenderá a utilizar este sistema muy rápido.	1 ○	2 ○	3 ○	4 ○	5 ○
8. El sistema es muy incómodo de usar.	1 ○	2 ○	3 ○	4 ○	5 ○
9. Me sentí seguro al utilizar el sistema.	1 ○	2 ○	3 ○	4 ○	5 ○
10. Se necesita aprender mucho antes de poder empezar a usar este sistema.	1 ○	2 ○	3 ○	4 ○	5 ○

Imprimir Formulario Registrar y Exportar Respuesta

Figura 8 Cuestionario SUS

ANEXO 4

Carta de autorización



CLINICA DEL PACIFICO

Chiclayo, 12 de noviembre de 2025

CARTA DE AUTORIZACIÓN N° 01-2025

Señor

Johann Antonio Torres Aguinaga

Estudiante de la Facultad de Ingeniería – USAT

Chiclayo

Asunto: Aceptación y conformidad del proyecto titulado "Sistema de seguridad de red basado en el aprendizaje federado para detectar intrusiones en entornos médicos"

A través del presente documento me dirijo a Usted, expresándole mi mas cordial saludo en nombre de la empresa **CLINICA DEL PACIFICO S.A.** y al mismo tiempo felicitarle por el desarrollo de su aplicativo.

Por tal motivo, se quiere poner en manifiesto que la empresa ha explorado y revisado los requerimientos funcionales y no funcionales del aplicativo desarrollado por Ud. JOHANN ANTONIO TORRES AGUINAGA, identificado con DNI 71386375, y por consiguiente **DAMOS CONFORMIDAD A SU PROYECTO titulado: "SISTEMA DE SEGURIDAD DE RED BASADO EN EL APRENDIZAJE FEDERADO PARA DETECTAR INTRUSIONES EN ENTORNOS MÉDICOS".**

Con este motivo, propicia es la oportunidad para expresarle las muestras de mi más alta consideración y estima.

Atentamente

CLINICA DEL PACIFICO S.A.

Lic. María Elena Pando Heredia

DIRECCIÓN ADMINISTRATIVA

Figura 9 Carta de autorización