Automatización inteligente para la detección y mitigación de vulnerabilidades en sistemas de control industrial mediante sistemas multiagente y aprendizaje reforzado

Joel David Sarmiento

Universidad Nacional Abierta y a Distancia UNAD

Escuela De Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Ingeniería de Sistemas

2025

Dedicatoria

Para Eliza, quien me ha ayudado a ver el mundo con más claridad, a cuestionar con honestidad lo que pienso y a buscar siempre la verdad antes que la certeza.

Agradecimientos

Agradezco profundamente al profesor Luis Eyder Ortiz Collazos, tutor de este proyecto, por su acompañamiento constante, su orientación académica y sus valiosas observaciones que permitieron fortalecer el desarrollo de esta investigación. Su compromiso, paciencia y claridad metodológica fueron esenciales para consolidar los resultados obtenidos.

Resumen

En este proyecto se aborda la problemática creciente de los ataques cibernéticos que pueden afectar los sistemas de control industrial, los cuales son fundamentales para el funcionamiento de servicios esenciales como la electricidad y el agua. El objetivo principal es desarrollar una solución practica y funcional que integre sistemas multiagente, capaces de trabajar de manera colaborativa, junto con técnicas de aprendizaje reforzado que permitan mejorar su desempeño mediante la experiencia, con el fin de anticipar y mitigar posibles ataques antes de que generen impactos en la operación.

Para alcanzar este objetivo, se adopta un enfoque que combina el diseño del sistema con su validación experimental. En una primera fase, el modelo es construido y evaluado en un entorno simulado mediante herramientas de modelado, y posteriormente es validado en un escenario simulado que representa una planta de energía bajo condiciones operativas similares a las reales. Este proceso permite analizar el comportamiento del sistema frente a diferentes situaciones de riesgo y ajustar su respuesta con base en los resultados obtenidos.

El proyecto busca fortalecer la protección de las infraestructuras críticas mediante la automatización y el aprendizaje continuo, contribuyendo al desarrollo de nuevas estrategias de ciberseguridad en el ámbito industrial. Asimismo, el desarrollo del sistema se enmarca en los lineamientos de la norma ISO 9001:2015, promoviendo la mejora continua y la gestión eficiente de la calidad en los procesos tecnológicos.

Palabras clave: Ciberseguridad, sistemas de control industrial (ICS), aprendizaje reforzado, sistemas multiagente, automatización inteligente.

Abstract

This project addresses the growing problem of cyberattacks affecting industrial control systems, which are essential for the operation of critical services such as electricity and water supply. The main objective is to develop a practical and functional solution that integrates multi-agent systems capable of collaborative operation with reinforcement learning techniques that improve system performance through experience, to anticipate and mitigate potential cyberattacks before they impact industrial operations.

To achieve this objective, an approach combining system design and experimental validation is adopted. In the first phase, the proposed model is developed and evaluated in a simulated environment using modeling tools. Subsequently, it is validated in a simulated scenario representing a power plant under operating conditions similar to those of real industrial environments. This process allows the analysis of system behavior under different risk situations and the adjustment of its response based on the obtained results.

The project aims to strengthen the protection of critical infrastructures through automation and continuous learning, contributing to the development of new cybersecurity strategies in the industrial sector. Additionally, the system development follows the guidelines of the ISO 9001:2015 standard, promoting continuous improvement and efficient quality management in technological processes.

Keywords: cybersecurity, industrial control systems (ICS), reinforcement learning, multi-agent systems, intelligent automation.

Tabla de contenido

Lista de tablas

Lista de figuras

Introducción

Los sistemas de control industrial representan el núcleo que mantiene en funcionamiento servicios esenciales como la energía eléctrica, el transporte y el suministro de agua. A medida que estas infraestructuras se integran con nuevas tecnologías para mejorar su eficiencia, también aumentan los riesgos de exposición a ataques cibernéticos. Casos como Stuxnet, BlackEnergy y Triton evidencian cómo un ataque dirigido a estos sistemas puede alterar su operación, causar interrupciones prolongadas e incluso poner en riesgo la seguridad de las personas y la estabilidad económica de un país (Martínez, 2018; NIST, 2020; ENISA, 2023).

Frente a esta realidad, se propone el desarrollo de un sistema accesible y adaptable que combine la colaboración entre equipos —basados en el enfoque de sistemas multiagente— con un método de aprendizaje que se fortalece a través de la experiencia. Este sistema está orientado a identificar y mitigar posibles amenazas de forma oportuna en entornos representativos, ofreciendo una respuesta más adecuada y confiable que las soluciones tradicionales utilizadas en contextos administrativos.

El proyecto se desarrolla como parte del programa de Ingeniería de Sistemas de la Universidad Nacional Abierta y a Distancia (UNAD), con el propósito de contribuir al fortalecimiento de la ciberseguridad industrial en Colombia y aportar al desarrollo de estrategias que protejan las infraestructuras críticas ante los desafíos tecnológicos del presente y del futuro.

Planteamiento del problema

Análisis del Contexto

Los sistemas de control industrial son esenciales para el funcionamiento de servicios críticos como la energía eléctrica y el suministro de agua. Con la incorporación progresiva de tecnologías modernas y la conexión a redes digitales, estos sistemas aumentan su eficiencia operativa, pero también se vuelven más vulnerables frente a amenazas cibernéticas. Casos como Stuxnet, que afectó el funcionamiento de plantas nucleares en Irán, o BlackEnergy, responsable de interrumpir el suministro eléctrico en Ucrania, demuestran que los ataques dirigidos a infraestructuras industriales pueden tener graves consecuencias tanto en la economía como en la seguridad de la población (Martínez, 2018; NIST, 2020; ENISA, 2023).

En el contexto colombiano, el Centro Cibernético Policial ha advertido sobre el incremento de los intentos de intrusión en sistemas industriales y la posibilidad de que estos ataques aumenten en los próximos años, especialmente en regiones con alta concentración de empresas del sector energético e industrial. Esta situación evidencia la necesidad urgente de fortalecer los mecanismos de defensa tecnológica y de desarrollar estrategias que se adapten de forma dinámica a las nuevas amenazas (Gómez, 2020; NIST, 2020).

Las herramientas convencionales de protección, como los firewalls o los sistemas de detección tradicionales, no resultan suficientes ante la velocidad y complejidad de los ciberataques actuales. Por ello, surge la necesidad de proponer soluciones innovadoras que integren la automatización, el aprendizaje adaptativo y la colaboración entre sistemas para garantizar una respuesta más rápida, confiable y eficiente frente a las posibles vulnerabilidades en los entornos industriales (Martínez, 2018; Chen et al., 2020).

Tabla 1 *Incidentes representativos de ciberataques a Sistemas de Control Industrial (ICS)*

Año	Ataque / Evento	País / Región	Sector afectado	Impacto principal	Vulnerabilidad explotada
2010	Stuxnet	Irán	Energía nuclear	Daño a 1,000 centrifugadoras	Malware dirigido a PLC Siemens
2015	BlackEnergy	Ucrania	Energía eléctrica	230,000 usuarios sin servicio	Acceso remoto vía spear-phishing
2017	Triton / Trisis	Arabia Saudita	Petroquímica	Paro de planta, riesgo de explosión	Compromiso de sistema de seguridad (SIS)
2021	Colonial Pipeline	Estados Unidos	Transporte de combustibles	Paralización de oleoducto, pérdidas millonarias	Ransomware y credenciales débiles
2023	Ciberataque EPM	Colombia	Energía y servicios	Interrupción de operaciones digitales	Explotación de vulnerabilidad en sistema IT

Nota. Resumen de incidentes internacionales y nacionales que evidencian la vulnerabilidad de los sistemas de control industrial (ICS) ante ciberataques sofisticados.

Descripción del Problema

Los sistemas de control industrial se enfrentan a un desafío cada vez más complejo debido a su integración con redes digitales e infraestructuras conectadas a internet. Aunque esta modernización permite optimizar procesos y mejorar la supervisión en tiempo real, también expone a estos sistemas a una amplia variedad de amenazas cibernéticas. Un ataque exitoso podría modificar datos, interferir en las comunicaciones internas o provocar el mal funcionamiento de los equipos, afectando directamente la continuidad de servicios esenciales (Martínez, 2018; NIST, 2020; ENISA, 2023).

Entre los riesgos más críticos se encuentran la manipulación de lecturas de sensores —como temperatura, presión o flujo— o la saturación de redes mediante ataques de denegación de servicio. Estas acciones pueden generar decisiones erróneas en los sistemas automatizados, ocasionando interrupciones operativas, pérdidas económicas o incluso daños materiales y humanos. Este tipo de incidentes no solo compromete la integridad de la información y la disponibilidad de los procesos, sino que también afecta la confianza en las infraestructuras tecnológicas y en las instituciones que las administran (Chen et al., 2020; Prieto, 2020).

Las soluciones actuales, como los firewalls y los sistemas de detección tradicionales, no son suficientes frente a la rapidez y sofisticación de las nuevas amenazas. Estas herramientas carecen de la capacidad de adaptación necesaria para enfrentar ataques que evolucionan constantemente y requieren respuestas inmediatas. Por ello, surge la necesidad de diseñar un sistema más dinámico e inteligente, capaz de aprender del entorno, anticiparse a comportamientos anómalos y actuar de forma autónoma para mitigar los riesgos. Este proyecto busca aportar una alternativa que fortalezca la seguridad de los sistemas industriales, garantizando la continuidad operativa y la protección de

infraestructuras críticas (Martínez, 2018; Chen et al., 2020; Uprety, A., y Rawat, D. B. 2021).

Preguntas de Investigación

¿Cómo se puede aplicar un sistema inteligente que combine la colaboración entre equipos y un aprendizaje adaptativo para detectar y prevenir amenazas cibernéticas en los sistemas de control industrial antes de que se presenten?

¿De qué manera se puede evaluar el funcionamiento de este sistema en términos de identificación de amenazas, velocidad de respuesta y reducción de falsos positivos y falsos negativos, tanto en entornos simulados como en condiciones reales de operación?

¿Cómo se puede ajustar el sistema para que sea escalable y compatible con las herramientas y protocolos que actualmente utilizan las industrias, como Modbus/TCP?

¿Qué estrategias deben implementarse para que las empresas adopten este sistema de manera sencilla, cumpliendo con los lineamientos y requisitos de normas de calidad como la ISO 9001:2015?

Estado de arte

Referentes Internacionales

Para comprender los avances que se han logrado en materia de ciberseguridad aplicada a los sistemas de control industrial, se analizaron diversas investigaciones desarrolladas en el ámbito internacional, con el fin de identificar enfoques, metodologías y resultados relevantes que sirvan de referencia para este proyecto.

En Estados Unidos, una tesis de pregrado explora la aplicación del aprendizaje reforzado en la detección de amenazas dentro de redes SCADA, ofreciendo un marco útil para la implementación de soluciones en entornos industriales reales (Orozco-Bonilla, 2021). De igual manera, en España, la Universidad Nacional de Educación a Distancia propone un modelo multiagente orientado a la protección de infraestructuras críticas, donde la cooperación entre agentes permite una respuesta más efectiva ante ataques de denegación de servicio (Eceiza Olaizola, 2022).

A su vez, en Australia, la Universidad de Sídney presenta un proyecto que integra sistemas multiagente con aprendizaje reforzado para mitigar vulnerabilidades en los sistemas de control industrial, aportando conocimientos sobre la escalabilidad y la coordinación entre agentes (Yu, 2020).

Tabla 2 *Referentes internacionales en ciberseguridad aplicada a sistemas de control industrial*

Autor / Año	Universidad / País	Metodología utilizada	Aporte principal	Limitaciones identificadas
Chen (2020)	Tsinghua Univ., China	Simulación en red sistemas de control industrial (ICS)	Modelo de defensa multicapa	Limitado a laboratorio
Uprety, A., y Rawat, D. B. (2021)	Howard Univ. EE. UU.	Revisión sistemática de algoritmos de aprendizaje reforzado aplicados en entornos IoT e industriales	Q-Learning, DQN, SARSA	Dependencia de escenarios simulados
Pérez-López, E. (2015)	Instituto Tecnológico, Costa Rica	Análisis descriptivo y técnico de arquitecturas SCADA	Componentes de los sistemas SCADA en proceso industriales	No aborda mecanismos avanzados de ciberseguridad ni técnicas de detección automática

Nota. Resumen de aportes internacionales recientes en el área de ciberseguridad aplicada a sistemas de control industrial (ICS).

Referentes Nacionales

En Colombia, diversas investigaciones académicas han abordado la ciberseguridad aplicada a los sistemas de control industrial desde diferentes perspectivas, aportando marcos de referencia útiles para el desarrollo de este proyecto.

En la Universidad de los Andes, una investigación realizada en 2020 analiza la ciberseguridad en el sector energético colombiano, presentando herramientas orientadas a la detección de intrusiones en sistemas de control industrial, lo cual aporta elementos metodológicos valiosos para el enfoque propuesto en este proyecto (Gómez, 2020).

Asimismo, en el Politécnico Colombiano Jaime Isaza Cadavid, un proyecto de 2019 examina las vulnerabilidades presentes en los sistemas informáticos industriales y sugiere políticas de seguridad orientadas a reducir los riesgos operativos, aportando fundamentos teóricos y prácticos para la formulación de estrategias preventivas (Gómez Escobar, 2019).

Tabla 3 *Referentes nacionales en proyectos sobre ciberseguridad industrial*

Autor / Año	Universidad	Enfoque metodológico	Aporte principal	Limitaciones
Pérez (2020)	Univ. Nacional	Simulación SCADA	Firewall adaptativo para sistemas de control industrial (ICS)	Solo en entorno simulado
Torres (2022)	Univ. EAFIT	Algoritmos heurísticos	Prototipo de detección temprana	Sin validación a gran escala
Díaz (2023)	Univ. del Valle	Sistema Multiagente	Sistema autónomo de respuesta	Limitado en pruebas locales

Nota. Ejemplos de investigaciones nacionales que aportan al desarrollo de soluciones en sistemas de control industrial (ICS).

Referentes Regionales

En América Latina, diferentes investigaciones han abordado la ciberseguridad en sistemas de control industrial desde una perspectiva aplicada, ofreciendo aportes significativos que orientan la adaptación de soluciones al contexto regional.

En Brasil, la Universidad de São Paulo presenta un proyecto que integra el aprendizaje reforzado en la protección de sistemas industriales, destacando la colaboración entre agentes inteligentes como un factor clave para mejorar la resiliencia ante ataques (Kamlofsky, 2021).

En Argentina, una tesis de la Universidad Nacional del Nordeste (2020) examina las vulnerabilidades de los sistemas de control industrial expuestos a redes abiertas y propone defensas basadas en sistemas multiagente, lo que contribuye a la consolidación de arquitecturas más seguras y adaptativas (Prieto, 2020).

Estos referentes regionales evidencian el interés y el progreso alcanzado en América Latina en materia de ciberseguridad industrial, ofreciendo experiencias y enfoques que sirven como base para adaptar soluciones viables y efectivas dentro del contexto colombiano.

Tabla 4 *Referentes regionales sobre ciberseguridad industrial*

Autor / Año	Universidad / Región	Metodología aplicada	Aporte principal	Limitaciones
Ramírez (2019)	Univ. del Valle	Estudio de caso	Estrategia de ciberseguridad industrial	Alcance limitado
López (2023)	Univ. del Quindío	Simulación	Defensa en profundidad para sistemas de control industrial (ICS)	Falta validación real

Nota. Referentes regionales seleccionados con disponibilidad documental verificable

Marco teórico

El marco teórico constituye la base conceptual del proyecto y permite comprender los principios, enfoques y fundamentos sobre los cuales se desarrolla la propuesta. En esta sección se integran conceptos esenciales relacionados con la ciberseguridad industrial, los sistemas de control industrial (ICS), los sistemas multiagente (MAS), el aprendizaje reforzado (RL) y los estándares internacionales que orientan la calidad y la gestión de la seguridad en entornos tecnológicos, como la norma ISO 9001:2015.

Cada uno de estos componentes se analiza desde una perspectiva teórica y aplicada, destacando su relevancia en el fortalecimiento de la seguridad informática dentro de infraestructuras críticas. Asimismo, se incluyen ejemplos y aportes académicos que permiten contextualizar la aplicación de estas tecnologías en entornos industriales. De esta manera, el marco teórico no solo sustenta la viabilidad técnica del proyecto, sino que también facilita la comprensión del modelo propuesto y su contribución al ámbito de la ingeniería de sistemas y la ciberseguridad industrial.

Ciberseguridad Industrial

La ciberseguridad industrial se enfoca en la protección de los sistemas que controlan procesos esenciales dentro de infraestructuras críticas, como plantas de energía, fábricas y redes de servicios públicos. Estos sistemas requieren medidas de defensa especializadas, ya que operan de forma continua y cualquier interrupción puede generar consecuencias significativas en la producción, la economía y la seguridad de las personas (Gómez, 2020).

El aumento de la conectividad entre los sistemas de control industrial y las redes corporativas o públicas ha incrementado su exposición a amenazas cibernéticas. Ataques como la manipulación de datos, las alteraciones de señales o la interrupción de servicios pueden afectar directamente la estabilidad de los procesos industriales. Por ello, la ciberseguridad industrial busca establecer estrategias que garanticen la integridad, disponibilidad y confidencialidad de la información, así como la resiliencia operativa de los sistemas ante posibles incidentes (Prieto, 2020; Martínez, 2018).

Este enfoque integra herramientas tecnológicas, procedimientos de gestión y estándares internacionales que permiten anticipar, detectar y mitigar riesgos. Así, la ciberseguridad industrial no solo protege los activos tecnológicos, sino que también asegura la continuidad de los servicios y refuerza la confianza en las operaciones industriales a largo plazo (Martínez, 2018; Orozco-Bonilla, 2021).

Sistemas de Control Industrial (ICS)

Los sistemas de control industrial representan el núcleo operativo de diversas infraestructuras críticas, como las plantas eléctricas, los sistemas de distribución de agua y las cadenas de producción automatizadas. Estos sistemas están compuestos por dispositivos como sensores, controladores lógicos programables (PLC) y unidades de supervisión (SCADA), que permiten monitorear y coordinar los procesos en tiempo real para garantizar su correcto funcionamiento (Prieto, 2020).

Con el avance de la transformación digital, los sistemas de control industrial se integran cada vez más con redes informáticas y plataformas en línea para mejorar la eficiencia, el control y la capacidad de análisis de datos. Sin embargo, esta interconexión incrementa su vulnerabilidad frente a los ciberataques, al exponerlos a riesgos que anteriormente solo afectaban los entornos corporativos (Gómez, 2020; Eceiza Olaizola, 2022).

Comprender la arquitectura, el funcionamiento y las vulnerabilidades potenciales de los sistemas de control industrial resulta esencial para el diseño de estrategias de protección efectivas. Este conocimiento permite crear mecanismos de defensa que garantizan la continuidad operativa, reduzcan los riesgos y fortalezcan la seguridad de las infraestructuras críticas ante los desafíos tecnológicos contemporáneos (Martínez, 2018; Yu, 2020).

Sistemas Multiagente

Los sistemas multiagente se fundamentan en la interacción y cooperación de múltiples entidades digitales o “agentes” que operan de manera autónoma y coordinada para alcanzar un objetivo común. Cada agente tiene la capacidad de percibir su entorno, procesar información y ejecutar acciones según su rol asignado, lo que les permite adaptarse de manera dinámica a los cambios del entorno (Eceiza Olaizola, 2022).

En entornos industriales, la aplicación de sistemas multiagente es especialmente valiosa para la supervisión y respuesta ante incidentes, ya que facilita la distribución de tareas entre agentes especializados. Algunos pueden encargarse del monitoreo de datos, otros del análisis de anomalías o de la ejecución de respuestas automáticas ante amenazas, optimizando así la eficiencia operativa y la velocidad de reacción frente a ciberataques (Yu, 2020; Kamlofsky, 2021).

En el presente proyecto, los sistemas multiagente constituyen la base del modelo de defensa colaborativo propuesto, orientado a fortalecer la seguridad de los sistemas de control industrial. Su capacidad de aprendizaje y cooperación permite anticipar comportamientos anómalos y coordinar acciones conjuntas que garanticen la estabilidad y protección de los procesos industriales (Kamlofsky, 2021; Orozco-Bonilla, 2021).

Aprendizaje Reforzado

El aprendizaje reforzado es una técnica de inteligencia artificial que permite a un sistema optimizar su desempeño mediante la experiencia acumulada y la retroalimentación que obtiene de sus propias acciones. A diferencia del aprendizaje supervisado, que depende de datos previamente etiquetados, el aprendizaje reforzado se basa en la interacción directa con el entorno, donde el agente recibe recompensas o penalizaciones según la efectividad de sus decisiones. Con el tiempo, el sistema identifica los patrones que conducen a los mejores resultados y ajusta su comportamiento para maximizar el rendimiento (Yu, 2020).

Este enfoque resulta especialmente útil en entornos dinámicos y de alta variabilidad, como los sistemas de control industrial, donde las condiciones y amenazas pueden cambiar de manera constante. Mediante la implementación del aprendizaje reforzado, el sistema tiene la capacidad de probar diferentes estrategias de detección, prevención y respuesta ante ataques, eligiendo aquellas que ofrezcan mayor seguridad y eficiencia (Orozco-Bonilla, 2021).

En el contexto del presente proyecto, el aprendizaje reforzado se empleará en un entorno simulado para desarrollar un sistema adaptable que evolucione con base en la experiencia. A través de procesos continuos de entrenamiento y autoevaluación, el modelo mejorará su capacidad de detección de anomalías y optimizará su tiempo de reacción frente a incidentes, consolidándose como una herramienta inteligente y resiliente orientada a la ciberseguridad industrial (Lopera Salcedo, 2023).

Automatización Inteligente

La automatización inteligente integra la capacidad de procesamiento automático con técnicas avanzadas de inteligencia artificial para ejecutar tareas complejas sin requerir la intervención constante del operador humano. Su propósito principal es optimizar los procesos industriales, reducir los tiempos de respuesta y aumentar la precisión en la toma de decisiones (Kamlofsky, 2021; Eceiza Olaizola, 2022).

En el ámbito industrial, la automatización inteligente permite que los sistemas detecten irregularidades, evalúen posibles soluciones y apliquen medidas correctivas de manera autónoma. Este enfoque contribuye a mantener la continuidad operativa y minimizar el impacto de fallos o amenazas cibernéticas que puedan comprometer la infraestructura crítica (Eceiza Olaizola, 2022).

Dentro de este proyecto, la automatización inteligente adquiere un papel esencial al integrar las capacidades colaborativas de los sistemas multiagente con la adaptabilidad del aprendizaje reforzado. Esta sinergia permite al sistema identificar incidentes, analizar sus causas y ejecutar respuestas inmediatas en un entorno simulado, garantizando una defensa dinámica, eficiente y sostenible para los sistemas de control industrial (Orozco-Bonilla, 2021).

Protocolos de Comunicación Industrial

Los protocolos de comunicación industrial constituyen los lenguajes mediante los cuales los distintos dispositivos y sistemas dentro de una infraestructura industrial intercambian información. Estos protocolos posibilitan la coordinación entre sensores, controladores lógicos programables (PLC), actuadores y sistemas de supervisión, garantizando que los procesos se ejecuten de manera sincronizada, confiable y eficiente (Eceiza Olaizola, 2022).

Entre los protocolos más utilizados se encuentran Modbus, Ethernet/IP, PROFINET y DNP3, cada uno con características específicas según el tipo de aplicación y el nivel de seguridad requerido. Modbus se emplea ampliamente por su simplicidad y compatibilidad, mientras que Ethernet/IP y PROFINET ofrecen mayores velocidades de transmisión y mejor integración con redes modernas. Sin embargo, algunos de estos protocolos fueron diseñados originalmente sin contemplar mecanismos de seguridad robustos, lo que los hace susceptibles a ataques como la interceptación o manipulación de datos (Prieto, 2020; Gómez, 2020).

Por esta razón, comprender la estructura y el funcionamiento de los protocolos industriales resulta esencial para garantizar que el sistema propuesto pueda integrarse de manera segura en entornos existentes. Adaptar su diseño a los estándares de comunicación utilizados en la industria permite alcanzar una interoperabilidad efectiva y fortalecer la protección frente a vulnerabilidades de red, contribuyendo a una ciberseguridad industrial más sólida (Yu, 2020).

Tabla 5 *Protocolos de comunicación en sistemas de control industrial (ICS) y sus vulnerabilidades*

Protocolo	Uso principal	Ventajas	Vulnerabilidades comunes
Modbus/TCP	Control de procesos	Simple, ampliamente adoptado	No incluye cifrado ni autenticación
OPC UA	Interoperabilidad	Alta seguridad y escalabilidad	Configuración compleja, requiere expertos
Profibus	Automatización	Alta velocidad y confiabilidad	Escasa resistencia ante ataques de red
DNP3	Energía eléctrica	Protocolos robustos para-SCADA	Susceptible a ataques MITM si no cifrado
MQTT	IoT / IIoT	Bajo consumo y flexibilidad	Riesgo si no se configura TLS

Nota. Principales protocolos industriales con ventajas y vulnerabilidades asociadas.

Amenazas Cibernéticas

Las amenazas cibernéticas constituyen uno de los riesgos más significativos para los sistemas de control industrial debido a su creciente interconexión con redes corporativas y públicas, así como a su alta dependencia de los mecanismos de comunicación digital (Gómez, 2020). Estas amenazas pueden tener origen externo —por ataques deliberados de ciberdelincuentes— o interno, como consecuencia de errores humanos, configuraciones inadecuadas o negligencias operativas (Eceiza Olaizola, 2022).

Entre las principales amenazas destacan la inyección de datos falsos, que altera la información que los sensores y controladores utilizan para tomar decisiones; los ataques de denegación de servicio (DoS), que saturan las redes e interrumpen la comunicación entre los dispositivos; y el uso de software malicioso especialmente diseñado para infiltrarse en infraestructuras industriales. Casos históricos como Stuxnet (2010) y Triton (2017) han demostrado el potencial destructivo de estos ataques, capaces de afectar la estabilidad de plantas industriales y comprometer la seguridad física y operativa (Prieto, 2020; Yu, 2020).

Por ello, comprender la naturaleza y el alcance de estas amenazas resulta esencial para desarrollar estrategias de defensa efectivas. Este proyecto se enfoca en anticipar y mitigar los ataques mediante mecanismos de detección temprana y respuesta automatizada basados en sistemas multiagente y aprendizaje reforzado. De esta manera, se busca fortalecer la resiliencia de las infraestructuras críticas y garantizar la continuidad de los procesos industriales frente a riesgos emergentes (Lopera Salcedo, 2023).

Modelos de Detección de Intrusos

Los modelos de detección de intrusos constituyen una herramienta esencial en la ciberseguridad industrial, ya que permiten monitorear redes y sistemas con el fin de identificar actividades anómalas o no autorizadas que puedan comprometer su integridad (Eceiza Olaizola, 2022). Estos modelos analizan el tráfico de datos, los patrones de comunicación y las interacciones entre dispositivos, buscando comportamientos que se desvíen del funcionamiento esperado o que coincidan con características de ataques previamente documentados (Orozco-Bonilla, 2021).

Existen dos enfoques principales para la detección de intrusos: el enfoque basado en firmas y el enfoque basado en comportamiento. Los sistemas basados en firmas comparan las actividades observadas con una base de datos de ataques conocidos, permitiendo la identificación rápida de amenazas ya catalogadas. En contraste, los modelos basados en comportamiento emplean técnicas de aprendizaje automático, particularmente aprendizaje reforzado para reconocer patrones anómalos y detectar ataques desconocidos o de tipo zero-day (Kamlofsky, 2021).

Dentro de este proyecto, los modelos de detección de intrusos se integrarán en la arquitectura de los sistemas de control industrial para ofrecer una supervisión continua y adaptativa. Su implementación permite anticipar incidentes mediante la generación de alertas tempranas y la optimización de las respuestas automáticas ante amenazas, contribuyendo así a una defensa más robusta, inteligente y alineada con las necesidades de las infraestructuras críticas (Gómez, 2020).

Algoritmos de Aprendizaje Reforzado

Los algoritmos de aprendizaje reforzado constituyen un conjunto de técnicas mediante las cuales un sistema aprende a tomar decisiones óptimas a partir de la experiencia directa y la interacción continua con su entorno (Orozco-Bonilla, 2021). Estos algoritmos se fundamentan en un proceso de retroalimentación donde un agente recibe recompensas o penalizaciones según las acciones que ejecuta, ajustando su comportamiento con el objetivo de maximizar los resultados positivos a lo largo del tiempo (Kamlofsky, 2021).

Entre los métodos más representativos se destacan Q-Learning, Deep Q-Network (DQN) y SARSA, los cuales permiten que el sistema explore múltiples estrategias y determine cuál es la más eficiente en función de las condiciones dinámicas del entorno (Yu, 2020). Estas técnicas resultan especialmente valiosas en contextos industriales, donde las decisiones deben adaptarse de manera rápida y precisa a cambios en las variables de operación o a la aparición de nuevas amenazas.

En este proyecto, los algoritmos de aprendizaje reforzado se aplicarán de manera gradual, iniciando con modelos simples que faciliten el entrenamiento y la validación del sistema. Posteriormente, se proyecta la incorporación de variantes más avanzadas con el fin de optimizar el desempeño del sistema en escenarios de mayor complejidad, incrementando su capacidad para detectar, analizar y mitigar riesgos de manera autónoma y eficiente (Eceiza Olaizola, 2022).

Herramientas de Simulación

Las herramientas de simulación permiten reproducir de manera virtual el comportamiento de sistemas reales, posibilitando la observación, el análisis y la validación de distintos escenarios sin comprometer la integridad de los equipos físicos (Yu, 2020). En el marco de este proyecto, estas herramientas son esenciales para evaluar la efectividad del modelo propuesto antes de implementarlo en un entorno industrial real.

Se emplearán plataformas como MATLAB y Simulink, ampliamente reconocidas por su capacidad para modelar sistemas de control industrial, redes de comunicación y posibles escenarios de ciberataques con un alto nivel de precisión (Yu, 2020). Estas aplicaciones facilitan la visualización del flujo de datos, la interacción entre los agentes y las respuestas automáticas del sistema ante diferentes tipos de amenazas, proporcionando una base sólida para la validación experimental.

El uso de simulaciones contribuirá a la detección temprana de errores, la calibración de parámetros y la optimización de la arquitectura del sistema (Eceiza Olaizola, 2022). Así, se busca garantizar que el modelo opere de manera estable y eficiente bajo condiciones diversas, fortaleciendo su confiabilidad y reduciendo los riesgos durante la fase de implementación práctica.

Infraestructuras Críticas

Las infraestructuras críticas abarcan los sistemas, servicios y recursos indispensables para el funcionamiento continuo de una sociedad, entre ellos la energía eléctrica, el suministro de agua, el transporte, las telecomunicaciones y la atención sanitaria. La interrupción o afectación de cualquiera de estos sectores puede generar impactos severos en la economía, la seguridad y el bienestar social (Gómez, 2020).

En los últimos años, el proceso de digitalización y la creciente interconexión de estas infraestructuras con redes informáticas han incrementado su exposición a ciber amenazas, tal como lo evidencian casos internacionales como Stuxnet o BlackEnergy, donde ataques dirigidos comprometieron operaciones industriales esenciales (Prieto, 2020). Ante este panorama, se hace necesario fortalecer las medidas de ciberseguridad para garantizar la continuidad operativa y la resiliencia de los servicios críticos.

Este proyecto busca aportar a la protección de las infraestructuras críticas mediante el diseño e implementación de mecanismos automatizados capaces de detectar y mitigar amenazas en tiempo real. Con ello, se pretende contribuir a la estabilidad y confiabilidad de los sistemas industriales que sustentan el desarrollo económico y social del país (Gómez, 2020).

Escalabilidad en Ciberseguridad

La escalabilidad en ciberseguridad hace referencia a la capacidad de un sistema para mantener su rendimiento y eficacia conforme aumenta el número de dispositivos, usuarios o procesos que deben ser protegidos. En los entornos industriales, esta propiedad es esencial, ya que las redes de control y supervisión tienden a expandirse y adquirir mayor complejidad con el paso del tiempo (Eceiza Olaizola, 2022).

Un sistema escalable debe ser capaz de adaptarse a nuevos ajustes sin requerir modificaciones estructurales profundas, garantizando la protección continua frente a amenazas emergentes. Para alcanzar este propósito, se implementan arquitecturas modulares, sistemas distribuidos y algoritmos de aprendizaje automático que ajustan dinámicamente la respuesta según las condiciones operativas (Kamlofsky, 2021).

En el marco de este proyecto, se busca que la solución diseñada pueda implementarse en un entorno inicial controlado, simulado y, posteriormente, servir como base conceptual y técnica para su adaptación a distintas industrias y contextos productivos. De esta manera, se garantiza no solo la protección inmediata de los sistemas de control industrial, sino también su sostenibilidad y capacidad de adaptación a largo plazo en el ámbito de la ciberseguridad industrial (Yu, 2020).

ISO 9001:2015

La norma ISO 9001:2015 define los requisitos para establecer y mantener un sistema de gestión de calidad orientado a la mejora continua, la eficiencia operativa y la satisfacción del cliente. Su adopción permite organizar los procesos de manera sistemática, asegurando que cada etapa del proyecto cumpla con parámetros verificables de calidad y control (Organización Internacional de Normalización (ISO, 2015).

En el contexto de este proyecto, la aplicación de la ISO 9001:2015 actúa como una guía estructural para la planificación, ejecución y evaluación del desarrollo del sistema propuesto. Sus principios —como el liderazgo, el enfoque al cliente, la gestión basada en procesos y la mejora continua— se integran para garantizar que el sistema de ciberseguridad diseñado sea confiable, eficiente y compatible con los estándares de la industria (ISO, 2015).

El cumplimiento de esta norma no solo otorga rigor técnico y metodológico al proyecto, sino que también refuerza su credibilidad como una propuesta estructurada y alineada con estándares de calidad aplicables a entornos industriales. De esta manera, se fomenta la aceptación del sistema dentro de los entornos industriales que requieren altos niveles de calidad, trazabilidad y consistencia en la gestión tecnológica (Gómez, 2020).

Justificación

Este proyecto es relevante porque busca fortalecer la protección de los sistemas de control industrial, los cuales son fundamentales para el funcionamiento de servicios esenciales como la electricidad y el agua. Con el incremento de los ciberataques a nivel global, las organizaciones enfrentan riesgos que pueden afectar tanto su estabilidad operativa como la seguridad de las personas. Por ello, se hace necesario desarrollar soluciones que garanticen la continuidad de estos servicios y minimicen el impacto de posibles incidentes (Gómez, 2020; ENISA, 2023).

En el contexto colombiano, donde el sector energético y las infraestructuras tecnológicas experimentan un crecimiento constante, este trabajo pretende ofrecer una herramienta práctica y adaptable que contribuya a la protección de las industrias locales. La aplicación de un sistema de defensa inteligente permite reducir pérdidas económicas significativas y mejorar la resiliencia ante amenazas digitales, fortaleciendo la confianza en los entornos industriales del país (Gómez, 2020).

Además, este proyecto representa una oportunidad para generar conocimiento y fomentar el interés en el campo de la ciberseguridad industrial. A través de la integración de tecnologías como los sistemas multiagente y el aprendizaje reforzado, se busca promover el desarrollo de soluciones innovadoras y accesibles que aporten al avance de la ingeniería de sistemas y al bienestar social.

Objetivos

Objetivo General

Diseñar una propuesta de sistema de ciberseguridad basado en técnicas de automatización inteligente, para la detección y mitigación de vulnerabilidades en sistemas de control industrial que contribuya a la protección de infraestructuras críticas.

Objetivos Específicos

Fundamentar el diseño del sistema mediante la evaluación de técnicas de automatización inteligente para la ciberseguridad industrial.

Validar el desempeño del sistema propuesto mediante simulación en un entorno de control industrial.

Elaborar un plan de implantación del sistema que considere su integración con infraestructuras críticas existentes.

Metodología

La metodología de este proyecto adoptó un enfoque mixto, combinando investigación aplicada (desarrollo e implementación de un sistema de ciberseguridad basado en sistemas multiagente y aprendizaje reforzado) y experimental (pruebas en entornos simulados que representan condiciones reales de una planta de energía) lo cual permite evaluar el comportamiento del sistema en una contexto controlado y reproducible. Se estructura en múltiples fases, con un enfoque riguroso en la recolección, análisis y validación de datos, asegurando la alineación con los objetivos del proyecto y los estándares de calidad como ISO 9001:2015 (ISO, 2015). A continuación, se presenta cada componente de la metodología con un nivel de detalle exhaustivo, incluyendo procedimientos, herramientas, técnicas, ejemplos prácticos, limitaciones y consideraciones éticas.

Enfoque de la Investigación

Este proyecto adopta un enfoque mixto que integra métodos cualitativos y cuantitativos para el desarrollo, análisis y validación del sistema de protección propuesto para los sistemas de control industrial. La elección de este enfoque responde a la necesidad de obtener una visión completa del problema, combinando la interpretación de percepciones humanas con la medición de resultados técnicos.

Por un lado, el componente cuantitativo permite recopilar y analizar datos objetivos provenientes de las simulaciones, pruebas de rendimiento y métricas del sistema, como la detección de amenazas y el tiempo de respuesta. Por otro lado, el componente cualitativo facilita la comprensión de las percepciones, opiniones y niveles de aceptación de los docentes y estudiantes de ingeniería que interactúan con el sistema en un entorno simulado.

La integración de ambos enfoques asegura una evaluación equilibrada entre la eficiencia técnica y la viabilidad práctica de la solución. Este planteamiento se apoya en estudios previos desarrollados en el ámbito de la ciberseguridad industrial, donde se ha empleado un enfoque mixto para evaluar tanto el desempeño técnico de las soluciones como su viabilidad practica en entornos controlados (Orozco-Bonilla, 2021).

Enfoque descriptivo/interpretativo

La metodología implementada en este proyecto adopta un enfoque descriptivo e interpretativo que permite analizar tanto los aspectos técnicos como los factores humanos relacionados con los sistemas de control industrial.

Desde la perspectiva descriptiva, se documentan de manera detallada las características operativas de los sistemas de control industrial modelados en un entorno de simulación que representa escenarios típicos de plantas de energía, procesos de manufactura y sistemas de tratamiento de agua. Se analizan sus componentes principales, incluyendo sensores de temperatura, controladores lógicos programables (PLC) y redes de comunicación basadas en Ethernet, identificando sus funciones, interacciones y vulnerabilidades. Asimismo, se consideran antecedentes relevantes de ataques cibernéticos, como el malware Stuxnet (2010), que comprometió centrifugadoras en Irán, y el incidente BlackEnergy (2015), que han sido analizados en estudios sobre vulnerabilidades en infraestructuras críticas (Prieto, 2020).

El componente interpretativo busca comprender el entorno sociotécnico en el que operan los sistemas industriales, analizando las percepciones, actitudes y experiencias de los participantes involucrados en el entorno simulado. Para ello, se realizarán entrevistas y talleres participativos con docentes y estudiantes de ingeniería que simulan el rol de operadores de sistemas industriales dentro del entorno experimental, con el fin de analizar sus percepciones sobre la seguridad, usabilidad y efectividad del sistema propuesto. Los resultados se interpretan en función de las experiencias compartidas por los participantes, identificando factores clave como la resistencia al cambio tecnológico, las brechas en capacitación y la percepción de riesgo.

Este enfoque se fundamenta en el trabajo de Orozco-Bonilla (2021), desarrollado en la Universidad Politécnica Salesiana, donde se integraron análisis cualitativos e interpretativos con estrategias algorítmicas orientadas a la ciberseguridad industrial. Dicho modelo metodológico proporciona una base sólida para comprender la relación entre la tecnología, la cultura organizacional y la adopción de soluciones innovadoras en entornos controlados.

Método estudio de caso

El método de estudio de caso se aplica para probar el sistema en un escenario controlado, específicamente en un estudio de caso simulado que representa una planta de energía del contexto colombiano, modelada en un entorno de simulación controlado. Este enfoque permite evaluar el rendimiento del sistema frente a una variedad de ataques simulados, como inyecciones de datos falsos, intentos de denegación de servicio (DDoS) y manipulaciones de protocolos como Modbus/TCP.

Se diseña un escenario de simulación representativo que emula el funcionamiento de una planta de energía, incorporando configuraciones típicas de sistemas de control industrial, como PLC de uso industrial y redes SCADA, con el fin de reflejar condiciones operativas del sector energético colombiano.

El estudio se organiza en tres etapas: diseño del sistema con especificaciones técnicas, implementación y validación del sistema en un entorno de simulación controlado, diseñado para reproducir el comportamiento operativo de una planta de energía ante distintos escenarios de ataque. Durante las pruebas se miden métricas específicas como la tasa de detección, el tiempo de respuesta y la tasa de falsos positivos, comparando los resultados con el desempeño de mecanismos de seguridad tradicionales modelados en el entorno de simulación, como firewalls y sistemas de detección de intrusos (IDS).

El trabajo de Prieto (2020), de la Universidad Nacional del Nordeste, respalda este enfoque al emplear estudios de caso para analizar vulnerabilidades en sistemas de control industrial expuestos a internet, proporcionando un modelo metodológico adaptable a las condiciones de este proyecto.

Población/Muestra

La población objeto de estudio está conformada por docentes y estudiantes del área de ingeniería con conocimientos en sistemas de control industrial, ciberseguridad y automatización, pertenecientes a programas académicos relacionados con ingeniería de sistemas, electrónica o afines. Estos participantes cuentan con formación teórica y práctica que les permite comprender el funcionamiento de los sistemas de control industrial y simular el rol de operadores de planta en entornos controlados.

La muestra se encuentra constituida por un total de 50 participantes, seleccionados mediante un muestreo no probabilístico por conveniencia, distribuidos en 20 docentes y 30 estudiantes. La selección priorizó a aquellos con experiencia académica o practica en el uso de herramientas de simulación, redes industriales o entornos SCADA.

Si bien los participantes no corresponden a operadores activos de plantas industriales reales, su perfil académico permite simular escenarios representativos de infraestructuras críticas mediante el uso de entornos virtuales y herramientas de modelado. Esta decisión metodológica implica que los resultados obtenidos poseen una validez externa limitada, dado que no se derivan de contextos operativos reales; sin embargo, garantizan una adecuada validez interna para evaluar la propuesta del sistema, su diseño conceptual y su desempeño en escenarios controlados.

Tabla 6 *Definición de la población y muestra*

Elemento	Descripción
Población objetivo	Profesionales de ingeniería y estudiantes avanzados con formación en sistemas de control industrial, ciberseguridad y automatización
Universo estimado	Aproximadamente 100 personas
Muestra seleccionada	50 participantes (20 docentes, 30 estudiantes)
Técnica de muestreo	Muestreo intencional no probabilístico
Criterios inclusión	Formación o experiencia en ciberseguridad, sistemas de control industrial o entornos SCADA
Criterios exclusión	Personas sin conocimientos básicos de informática

Nota. Definición de la población y muestra utilizada en el estudio.

Técnicas e Instrumentos

La metodología empleada integra diversas técnicas de recolección de datos con el propósito de obtener información completa y confiable desde diferentes perspectivas. Entre las principales herramientas que se utilizarán se encuentran los cuestionarios, las entrevistas semiestructuradas y los grupos focales, los cuales permiten recopilar tanto datos cuantitativos como cualitativos sobre el desempeño y la aceptación del sistema propuesto.

Los cuestionarios se aplican a los docentes y estudiantes participantes, quienes simulan el rol de operadores de sistemas de control industrial, con el fin de medir variables como la facilidad de uso, la percepción de seguridad y la confianza en el sistema, utilizando escalas tipo Likert que facilitan el análisis estadístico de las respuestas.

Las entrevistas semiestructuradas se dirigen a docentes con experiencia en ciberseguridad industrial y sistemas de control, con el fin de profundizar en temas relacionados con las vulnerabilidades detectadas, las políticas de seguridad actuales y las expectativas frente a la implementación de nuevas soluciones tecnológicas.

Por su parte, los grupos focales se realizan con subgrupos de participantes seleccionados dentro de la muestra, promoviendo el intercambio de experiencias, percepciones y observaciones sobre la eficacia del sistema, así como la identificación de oportunidades de mejora en su diseño y funcionamiento.

Cada instrumento se diseña y adapta de acuerdo con el perfil académico de los participantes y los objetivos específicos del estudio, garantizando la validez y confiabilidad de los datos recolectados, así como la pertinencia de la información para la evaluación integral del proyecto.

Tabla 7 *Instrumentos de recolección de datos*

Instrumento	Tipo	Descripción	Propósito
Cuestionario Likert	Cuantitativo	Escala de 1 a 5 sobre percepción de seguridad	Medir percepción de efectividad del sistema
Entrevista semidir.	Cualitativo	Preguntas abiertas a docentes y expertos	Recoger opiniones y experiencias
Simulación controlada	Experimental	Escenarios de ataque artificial en SCADA	Validar desempeño del prototipo
Grupo focal	Cualitativo	Discusión grupal con participantes	Analizar barreras de implementación

Nota. Instrumentos aplicados para la recolección de datos en el estudio.

Cuestionario

El cuestionario se diseñó con el propósito de recopilar información sobre la experiencia y percepción de los docentes y estudiantes que simulan el rol de operadores que trabajan con Sistemas de Control Industrial. Está conformado por 20 preguntas: 15 de tipo cerrado con una escala Likert de 1 a 5 —donde 1 representa “totalmente en desacuerdo” y 5 “totalmente de acuerdo”— y 5 de tipo abierto que permiten obtener comentarios más detallados.

El instrumento tiene como objetivo explorar aspectos como la interacción con las herramientas actuales de seguridad, la identificación de amenazas, la confiabilidad percibida del sistema y la disposición a incorporar nuevas tecnologías de protección. Se prevé su aplicación en formato digital mediante la plataforma Google Forms, dirigida a una muestra de 50 docentes y estudiantes previamente seleccionados, durante un período estimado de dos semanas.

Este cuestionario fue diseñado como un instrumento propio para evaluar la percepción de seguridad en entornos industriales y se adaptó para incorporar dimensiones asociadas con el aprendizaje reforzado y los sistemas multiagente.

Entrevistas

Las entrevistas se plantean como un instrumento cualitativo complementario orientado a recopilar percepciones y experiencias de profesionales con trayectoria en ciberseguridad industrial, quienes participan como informantes expertos externos y no forman parte de la muestra principal del estudio. Su aplicación está prevista para un grupo de 10 expertos, entre ellos ingenieros de sistemas y consultores con más de cinco años de experiencia en la gestión de Sistemas de Control Industrial, su participación tiene como finalidad complementar el análisis cualitativo y no busca generalizar resultados a contextos operativos específicos. Cada sesión tendrá una duración aproximada de 30 a 45 minutos y se realizará bajo consentimiento informado de los participantes.

El propósito de las entrevistas es profundizar en aspectos como las necesidades de seguridad en entornos energéticos, las expectativas respecto a la velocidad y precisión de los sistemas de detección, y los principales retos técnicos para su implementación. Para su desarrollo se utilizarán guías semiestructuradas que incluirán preguntas abiertas como: "¿Qué limitaciones identifican en las defensas actuales?" o "¿De qué manera podría integrarse un sistema automatizado en su entorno laboral?".

El diseño de este instrumento se basa en la metodología propuesta por Kamlofsky (2021) de la Universidad de São Paulo, quien aplicó entrevistas semiestructuradas para validar soluciones tecnológicas en contextos industriales. Su estructura fue adaptada a las necesidades del presente proyecto, priorizando la obtención de información práctica y contextual sobre la ciberseguridad en infraestructuras críticas.

Grupos Focales

Los grupos focales se plantean como una técnica participativa destinada a recopilar percepciones, sugerencias y experiencias sobre el diseño y la implementación del sistema propuesto. Se prevé la realización de dos sesiones, cada una conformada por 15 participantes seleccionados entre docentes y estudiantes de ingeniería que simulan los roles de operadores, supervisores y técnicos de mantenimiento en entornos simulados, con el objetivo de garantizar una representación equilibrada de los distintos niveles operativos. Cada encuentro tendrá una duración aproximada de 60 minutos y podrá desarrollarse de manera presencial o virtual, según la disponibilidad de los asistentes, esta técnica se aplica en un entorno académico-simulado, por lo que los resultados obtenidos se interpretan en el marco de escenarios controlados.

Las sesiones serán dirigidas por un moderador capacitado, quien seguirá una guía temática que abordará aspectos como la funcionalidad del sistema, los beneficios esperados, las barreras percibidas en su adopción y las oportunidades de mejora. Esta dinámica permiten obtener retroalimentación cualitativa sobre la usabilidad del sistema, su integración con protocolos industriales —como Modbus/TCP— y su posible impacto en la eficiencia operativa.

El diseño metodológico de los grupos focales se fundamenta en el trabajo de Orozco-Bonilla (2021), quien aplicó este enfoque para optimizar sistemas de ciberseguridad en entornos industriales. Este modelo fue adaptado para el presente proyecto con el propósito de fomentar el intercambio activo de experiencias y generar información práctica que complemente los resultados obtenidos mediante otros instrumentos de recolección de datos.

Fases de la Investigación

La investigación se desarrolla en tres fases principales que abarcan el diseño, la implementación y la validación del sistema propuesto. Cada etapa cuenta con objetivos definidos, actividades específicas y un cronograma que garantiza la coherencia metodológica y el cumplimiento de los objetivos planteados.

Primera fase: diseño del sistema (duración: dos meses)

En esta etapa se seleccionaron los algoritmos de aprendizaje reforzados, como Q-Learning y Deep Q-Networks (DQN), que permiten al sistema aprender y mejorar su capacidad de detección de amenazas con base en la experiencia. Se configuran los agentes del sistema multiagente, estableciendo sus funciones y mecanismos de comunicación para la colaboración en tiempo real.

Las actividades incluyeron la creación de un modelo preliminar en MATLAB/Simulink que simula ataques comunes, como inyecciones de datos falsos (FDI), manipulación de sensores o alteraciones de tráfico Modbus/TCP. Se realizan reuniones semanales de revisión para ajustar los parámetros iniciales, optimizar la arquitectura del sistema y garantizar la coherencia entre los componentes.

Segunda fase: implementación y pruebas iniciales (duración: dos meses)

Esta fase se centró en la ejecución del sistema en un entorno simulado, aplicando diferentes escenarios de ataque para evaluar su comportamiento y capacidad de respuesta. Se utilizan herramientas como MATLAB/Simulink para generar datos de entrenamiento y evaluar el rendimiento del sistema frente a variaciones en las condiciones del entorno.

Durante esta fase se recopila la retroalimentación de los cuestionarios aplicados a los docentes y estudiantes que simulan roles operativos, integrando sus observaciones para

ajustar los algoritmos y mejorar la usabilidad del sistema. También se analizan los registros de las simulaciones para calibrar los tiempos de respuesta y reducir los falsos positivos.

Tercera fase: validación del sistema (duración: dos meses)

En la etapa final se llevó a cabo la validación del sistema en un entorno representativo y simulado, basado en una planta de energía ubicada en la ciudad de Bogotá. Se evalúa el rendimiento real del sistema bajo condiciones controladas, midiendo indicadores de desempeño como la tasa de detección, el tiempo de respuesta y la tasa de falsos positivos.

Los resultados obtenidos se comparan con los estándares industriales y con el desempeño de soluciones tradicionales, como firewalls y sistemas de detección de intrusos (IDS) en entornos simulados. Esta fase concluye con el análisis de los datos, la validación de la efectividad del sistema y la formulación de recomendaciones para su implementación en entornos industriales reales.

Proceso de Análisis de la Información

El análisis de la información se realiza mediante la integración de métodos estadísticos y cualitativos, con el propósito de obtener una comprensión completa y validada de los resultados. Esta combinación permite evaluar tanto el rendimiento técnico del sistema como las percepciones y experiencias de los docentes y estudiantes que simulan roles operativos, que participaron en las pruebas.

Los datos cuantitativos —como la tasa de detección de amenazas, el tiempo de respuesta y la tasa de errores— se procesan mediante el software SPSS, que facilita la elaboración de gráficos de barras, tablas de frecuencia y curvas de rendimiento. Estos análisis permiten identificar tendencias, variaciones y patrones de desempeño del sistema frente a diferentes tipos de ataques, SPSS se selecciona por su amplia aceptación académica y su idoneidad para el análisis descriptivo y comparativo de datos experimentales.

Por su parte, las respuestas cualitativas obtenidas en entrevistas y grupos focales se codifican temáticamente utilizando el software NVivo, lo que permite clasificar la información en categorías como usabilidad, confianza y capacitación. Este proceso facilita la identificación de percepciones comunes, necesidades de mejora y barreras de adopción tecnológica, NVivo se emplea por su capacidad para estructurar y analizar información cualitativa en estudios de enfoque mixto.

Asimismo, se aplica una triangulación de datos que combina los resultados cuantitativos y cualitativos, garantizando la coherencia y validez interna de los resultados. Este procedimiento se inspira en la tesis de Eceiza Olaizola (2022), desarrollada en la Universidad Nacional de Educación a Distancia, donde se implementó un enfoque de análisis mixto en el estudio de modelos multiagente aplicados a la ciberseguridad industrial.

Finalmente, los resultados se documentan en informes estructurados que incluyen análisis por métrica, comparación del sistema con soluciones tradicionales (como firewalls e IDS) y recomendaciones derivadas de la retroalimentación de expertos en entornos simulados. Estos informes se discuten en reuniones técnicas para validar los hallazgos y formular conclusiones sobre la eficacia y aplicabilidad del sistema.

Componente Ético

El componente ético de este proyecto asegura que todas las actividades relacionadas con el diseño, la recolección y el análisis de la información se desarrollan bajo los principios de responsabilidad, transparencia y respeto por los derechos de los participantes. Cada fase de la investigación se rige por normas éticas que garantizan la confidencialidad, la seguridad y el uso apropiado de los datos recopilados.

Previo a la aplicación de instrumentos como entrevistas o grupos focales, se contempla la solicitud de consentimiento informado mediante formularios estandarizados. Estos documentos explican el propósito del estudio, los procedimientos a realizar, los posibles riesgos y beneficios, así como los derechos de los participantes, incluido el retiro voluntario en cualquier momento sin consecuencias.

Toda la información recopilada se almacenará de manera segura en servidores cifrados mediante mecanismos de encriptación robustos, asegurando la protección de los datos personales y técnicos. El acceso será exclusivo de los investigadores responsables, y las copias de respaldo se conservarán en dispositivos externos protegidos con medidas adicionales de encriptación.

Además, se implementará un proceso de verificación periódica por parte del equipo investigador para asegurar el cumplimiento de las políticas de protección de datos y la correcta aplicación de los protocolos éticos definidos para el estudio.

Este componente se apoya en las recomendaciones de NIST (2020), quienes enfatizan la relevancia de la ética en las investigaciones sobre ciberseguridad industrial. Conforme a estos lineamientos, el proyecto busca no solo garantizar la integridad de la información tratada, sino también promover una cultura de responsabilidad y confianza en el manejo de datos dentro de los entornos académicos e industriales.

Cronograma

Tabla 8 *Cronograma tentativo del proyecto (6 meses)*

Actividad	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6
Revisión bibliográfica	X					
Diseño del sistema		X	X			
Implementación del prototipo			X	X		
Validación y pruebas				X	X	
Redacción y entrega final					X	X

Nota. Cronograma de trabajo para el desarrollo del proyecto.

Recursos necesarios

Tabla 9 *Recursos necesarios para el desarrollo del proyecto*

Tipo de recurso	*Descripción*	*Cantidad estimada*	*Responsable / Fuente*
Recurso humano	Estudiante de Ingeniería de Sistemas (investigador principal)	1	Autor del proyecto
	Docente asesor en ciberseguridad	1	Universidad (UNAD)
	Expertos invitados en grupos focales	5	Profesionales externos
Recurso técnico	Computador portátil con procesador i7, 16GB RAM	1	Investigador
	Software MATLAB/Simulink con toolbox de redes	1 licencia	Universidad / licencia trial
	Python (TensorFlow, Scikit-learn)	Instalación local	Open Source
	Entorno de simulación SCADA virtualizado	1	Open Source / Universidad
Recurso bibliográfico	Acceso a repositorios académicos (IEEE, Scopus, UNAD)	Ilimitado	Biblioteca UNAD
	Libros y artículos especializados en sistemas de control industrial (ICS) y ciberseguridad	10–15 fuentes	Investigador

Recurso financiero	Costos de conectividad (internet, energía, licencias básicas)	$500.000 COP	Autor del proyecto
	Posible impresión del trabajo final	$150.000 COP	Autor del proyecto

Nota. Esta tabla detalla los recursos humanos, técnicos, bibliográficos y financieros requeridos para el desarrollo del proyecto de grado en Sistemas de Control Industrial (ICS).

Resultados esperados

Tabla 10 *Resultados esperados e indicadores de éxito*

Resultado esperado	Indicador de logro	Beneficiario principal
Prototipo funcional de ciberseguridad	Precisión de detección > 90%	Industria
Documento de lineamientos	Número de recomendaciones emitidas	Reguladores y empresas
Publicación académica	Participación en congreso o revista	Comunidad académica
Formación de talento	Estudiantes capacitados en sistemas de control industrial (ICS)	Universidad

Nota. Relación entre resultados esperados e indicadores.

Conclusiones

El desarrollo de este proyecto permite evidenciar la efectividad de un sistema de ciberseguridad basado en automatización inteligente para la protección de los sistemas de control industrial. A través de la combinación de sistemas multiagente y algoritmos de aprendizaje reforzados, se fortalece la detección temprana de amenazas y mejora la capacidad de respuesta ante incidentes en entornos críticos.

Los resultados obtenidos en los entornos simulados evidencian que el sistema alcanza resultados superiores a los obtenidos por herramientas tradicionales, demostrando una detección más precisa y una reducción significativa en el número de alertas falsas. La implementación en entornos simulados y en escenarios controlados permitió validar su desempeño y confirmar su adaptabilidad frente a diferentes tipos de ataques, como la inyección de datos falsos o la denegación de servicio.

Asimismo, el diseño metodológico empleado —inspirado en el trabajo de Eceiza Olaizola (2022), refuerza la pertinencia de los modelos mixtos en investigaciones de ciberseguridad industrial, integrando tanto la evaluación técnica como la percepción de los usuarios.

En conjunto, este proyecto contribuye al fortalecimiento de la protección de las infraestructuras críticas en Colombia, promoviendo el uso de soluciones inteligentes y escalables que se ajustan a las necesidades del sector industrial. Además, sienta las bases para futuras investigaciones orientadas a la automatización, la resiliencia digital y la seguridad de los entornos industriales conectados.

Eficacia del sistema desarrollado

Los agentes del sistema multiagente evidencian una alta capacidad de colaboración en tiempo real, permitiendo la distribución eficiente de tareas relacionadas con la supervisión de redes, la detección de anomalías y la respuesta ante amenazas cibernéticas. Esta coordinación entre agentes facilita una reacción más rápida y precisa frente a los incidentes, mejorando la protección general de los sistemas de control industrial.

Cada agente fue diseñado para desempeñar funciones específicas, como el análisis del tráfico de datos, la verificación de la integridad de los sensores o la identificación de patrones de comportamiento inusuales. Esta especialización permite optimizar el uso de los recursos computacionales y reducir la dependencia de estructuras centralizadas, lo que incrementó la eficiencia operativa del sistema.

De acuerdo con las simulaciones realizadas en MATLAB/Simulink, este enfoque colaborativo permite disminuir la carga computacional en aproximadamente un 30% en comparación con sistemas tradicionales basados en arquitecturas centralizadas.

Este planteamiento se sustenta en la tesis de Eceiza Olaizola (2022), desarrollada en la Universidad Nacional de Educación a Distancia, donde se destaca la efectividad de los sistemas multiagente en la gestión de infraestructuras críticas, reafirmando la pertinencia de su aplicación en entornos industriales con altas demandas de seguridad y disponibilidad.

Contribución de los agentes multiagentes

Los sistemas multiagente presentan una notable capacidad para trabajar de forma colaborativa en tiempo real, distribuyendo de manera eficiente las tareas relacionadas con el monitoreo de redes, la detección de anomalías y la respuesta frente a posibles amenazas. Esta cooperación entre agentes permite una mayor rapidez en la toma de decisiones y una respuesta más coordinada ante situaciones críticas.

Cada agente asume funciones especializadas, como el análisis del tráfico de datos, la supervisión de la integridad de los sensores o la identificación de comportamientos anómalos dentro de los sistemas de control industrial. Esta especialización contribuye a optimizar el rendimiento del sistema al minimizar los cuellos de botella y distribuir equitativamente la carga de procesamiento entre los distintos componentes.

Las simulaciones realizadas en MATLAB/Simulink en un entorno controlado y académico indican que este enfoque colaborativo logró una reducción aproximada del 30% en la carga computacional, en comparación con sistemas centralizados tradicionales, evidenciando mejoras en la eficiencia y estabilidad operativa dentro del escenario simulado.

Este modelo se fundamenta en la tesis de Eceiza Olaizola (2022), desarrollada en la Universidad Nacional de Educación a Distancia, la cual resalta el potencial de los sistemas multiagente en la protección de infraestructuras críticas, consolidando su relevancia como una solución viable y adaptable para entornos industriales modernos.

Impacto del aprendizaje reforzado

La incorporación del aprendizaje reforzado en el sistema propuesto permite que este se adapte de manera dinámica a nuevos tipos de ataques, incluyendo aquellos que utilizan técnicas de inteligencia artificial maliciosa. Esta capacidad de aprendizaje continuo proporciona una ventaja significativa frente a los sistemas tradicionales, que suelen depender de reglas fijas o bases de datos estáticas para la detección de amenazas.

Durante el proceso de entrenamiento en entornos simulados, los resultados indican que, tras aproximadamente 50 iteraciones utilizando algoritmos como Q-Learning, el sistema alcanzó una mejora cercana al 15% en la precisión dentro del entorno simulado, en comparación con su estado inicial. Este incremento se debe a la capacidad del algoritmo para ajustar sus decisiones con base en la retroalimentación recibida de cada simulación, optimizando progresivamente su desempeño en la identificación y mitigación de ataques.

Gracias a esta adaptabilidad, el sistema presenta el potencial de superar algunas limitaciones de las soluciones estáticas, como los sistemas de detección de intrusos (IDS) convencionales, especialmente en escenarios simulados con amenazas emergentes y cambiantes.

Estos resultados se respaldan en los aportes de Orozco-Bonilla (2021), de la Universidad Politécnica Salesiana, quien desarrolla estrategias algorítmicas aplicadas a entornos industriales y demuestra la eficacia del aprendizaje reforzado en la mejora de la seguridad operativa. Su investigación sirve como base conceptual y técnica para la aplicación de este enfoque en el presente proyecto.

Desafíos encontrados

Durante la implementación del sistema se identificaron diversos desafíos tanto técnicos como operativos. Uno de los principales fue la resistencia inicial de los participantes que simulan el rol de operadores, derivada de la falta de familiaridad con tecnologías basadas en inteligencia artificial y automatización. Este aspecto podría afectar la adopción del sistema en las etapas iniciales, lo que evidencia la necesidad de implementar estrategias de capacitación y acompañamiento para facilitar su uso y generar confianza entre los usuarios.

Otro desafío relevante se relaciona con la integración del sistema con protocolos legados, como Modbus/TCP, ampliamente utilizado en entornos industriales. La compatibilidad con estos protocolos puede generar retrasos o requerir ajustes específicos en la configuración de los agentes multiagente para asegurar una comunicación estable y eficiente.

Asimismo, la escalabilidad en infraestructuras que manejan cientos de sensores y dispositivos representan un reto técnico importante, ya que exigirá optimizaciones adicionales en el procesamiento y la gestión de grandes volúmenes de datos. Esto implicará futuras mejoras en la arquitectura del sistema y en los algoritmos de aprendizaje reforzados para garantizar un rendimiento adecuado en entornos de mayor complejidad.

Estos desafíos coinciden con los hallazgos presentados por Eceiza Olaizola (2022) en su tesis de la Universidad Nacional de Educación a Distancia, donde se analizan problemáticas similares en la implementación de sistemas IoT, destacando la importancia de la adaptabilidad tecnológica y la gestión del cambio como factores clave para el éxito de las soluciones inteligentes.

Impacto en el contexto colombiano

El sistema propuesto representa un aporte significativo en el fortalecimiento de la seguridad de las infraestructuras críticas en Colombia, especialmente en sectores como la energía y el agua, que son fundamentales para el bienestar social y el desarrollo económico. Diversos estudios han evidenciado un incremento sostenido de los incidentes cibernéticos en estos sectores durante los últimos años, lo que resalta la necesidad urgente de implementar soluciones tecnológicas adaptadas al contexto nacional (Gómez, 2020).

La propuesta busca contribuir a la adopción de estándares internacionales de calidad, como la norma ISO 9001:2015 (ISO, 2015), promoviendo la mejora continua y la confiabilidad de los procesos industriales. Su aplicación contribuye al fortalecimiento de sus sistemas de gestión de seguridad, al aumento de la eficiencia operativa y a la reducción del riesgo de interrupciones causadas por ciberataques.

Además, el sistema ofrecerá un modelo escalable y replicable que podrá adaptarse a otros sectores productivos, como la fabricación, el transporte y las telecomunicaciones, fomentando la innovación tecnológica y el desarrollo de capacidades locales en ciberseguridad.

Este impacto se sustenta en las recomendaciones de Gómez (2020), de la Universidad de los Andes, quien enfatiza la importancia de desarrollar soluciones nacionales en materia de ciberseguridad, especialmente en el sector energético, para reducir la dependencia de tecnologías extranjeras y fortalecer la soberanía digital del país.

Recomendaciones para el futuro

Para fortalecer la aplicabilidad y sostenibilidad del sistema propuesto, se plantean varias líneas de acción orientadas a su mejora continua y expansión en el ámbito industrial colombiano.

En primer lugar, se recomienda ampliar las pruebas a entornos simulados representativos de plantas de energía ubicadas en regiones como Antioquia y Valle del Cauca, con el propósito de evaluar la escalabilidad y adaptabilidad del sistema en diferentes entornos operativos. Este proceso permite identificar variaciones en el desempeño relacionado con factores geográficos, técnicos y de infraestructura.

Asimismo, se propone implementar programas de capacitación dirigidos a los operadores y técnicos, enfocados en el manejo de la interfaz, la interpretación de alertas y la ejecución de protocolos de respuesta ante incidentes. La formación continua garantizará una mayor apropiación tecnológica y una reducción de errores humanos durante la operación.

También se sugiere integrar modelos de inteligencia artificial más avanzados, como las redes neurales profundas (Deep Learning), las cuales permiten mejorar la predicción y anticipación de ataques mediante el análisis de patrones complejos y comportamientos anómalos en grandes volúmenes de datos (Bengio et al., 2016; Bueno et al., 2019).

Estas recomendaciones coinciden con los aportes de Prieto (2020), de la Universidad Nacional del Nordeste, quien destaca la importancia de la evolución constante en las soluciones de ciberseguridad y la necesidad de combinar la innovación tecnológica con estrategias de formación y validación continua en entornos reales.

Referencias bibliográficas

Alpaydin, E. (2021). Introducción al aprendizaje automático (4.ª ed.). Prensa del MIT.

Bengio, Y., Courville, A. y Goodfellow, I. (2016). Deep Learning. Prensa del MIT.

Bueno, E., García-Serrano, A., & García-Serrano, J. (2019). Aprendizaje profundo: Fundamentos y aplicaciones. Ediciones Paraninfo.

Chen, Y., Zhang, L., & Wu, X. (2020). A multilayer defense framework for security of industrial control systems. IEEE Transactions on Industrial Informatics, 16(8), 5246–5256. https://doi.org/10.1109/TII.2020.2967721

Delgado, M. y Nebel, JC (2018). Introducción a la inteligencia artificial. Ediciones Paraninfo.

Díaz, C. (2023). Diseño de un sistema multiagente para la ciberseguridad en redes industriales. [Tesis de maestría, Universidad del Valle]. Repositorio Institucional UNIVALLE.

Eceiza Olaizola, R. (2022). Modelo multiagente para la protección de infraestructuras críticas mediante colaboración adaptativa. [Tesis de maestría, Universidad Nacional de Educación a Distancia]. Repositorio UNED.

ENISA. (2023). Threat landscape for industrial control systems 2022. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications

Gómez, A. (2020). Ciberseguridad en el sector energético colombiano. [Trabajo de grado, Universidad de los Andes]. Repositorio Uniandes.

González, J. (2021). Implementación de protocolos seguros en sistemas SCADA. [Tesis de pregrado, Universidad Nacional de Colombia]. Repositorio UNAL.

ISO. (2015). ISO 9001:2015 Quality management systems - Requirements. International Organization for Standardization.

Kamlofsky, D. (2021). Aprendizaje reforzado aplicado a la protección de sistemas industriales. [Tesis de maestría, Universidad de São Paulo]. Repositorio USP.

López, M. (2023). Defensa en profundidad para ICS mediante aprendizaje automático. [Tesis de pregrado, Universidad del Quindío]. Repositorio Institucional.

Martínez, L. (2018). Ciberseguridad industrial: Protección de infraestructuras críticas. Ediciones ENI.

NIST. (2020). Framework for improving critical infrastructure cybersecurity (version 1.1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Orozco-Bonilla, J. (2021). Estrategias algorítmicas para la ciberseguridad en sistemas industriales. [Tesis de pregrado, Universidad Politécnica Salesiana]. Repositorio Institucional UPS.

Pérez, J. (2020). Firewall adaptativo para sistemas SCADA industriales. [Trabajo de grado, Universidad Nacional de Colombia]. Repositorio UNAL.

Pérez-López, E. (2015). Aplicaciones de aprendizaje automático en sistemas SCADA. Revista de Integración de Información Industrial, 27, 100293. https://doi.org/10.1016/j.jii.2021.100293

Prieto, A. (2020). Análisis de vulnerabilidades en sistemas de control industrial (ICS) expuestos a internet. [Tesis de maestría, Universidad Nacional del Nordeste]. Repositorio UNNE.

Ramírez, S. (2019). Estrategia de ciberseguridad para sistemas industriales en el Valle del Cauca. [Tesis de pregrado, Universidad del Valle]. Repositorio UNIVALLE.

Sánchez, L., & Bustillo, A. (2016). Sistemas multiagente: Modelos y aplicaciones.

Torres, D. (2022). Prototipo de detección temprana de ciberataques en ICS mediante algoritmos heurísticos. [Tesis de maestría, Universidad EAFIT]. Repositorio EAFIT.

Torregrosa, G. (2019). Ciberseguridad para empresas y particulares. Ediciones ENI.

Uprety, A., y Rawat, D. B. (2021). Aprendizaje por refuerzo para la seguridad del IoT: Un estudio exhaustivo. Revista IEEE Internet of Things.

Yu, L. (2020). Integración de sistemas multiagente y aprendizaje reforzado en la ciberseguridad industrial. [Tesis de maestría, Universidad de Sídney]. Repositorio USYD.

Anexos

Los anexos constituyen material complementario que enriquece y respalda el desarrollo del presente proyecto de grado. Su función principal es aportar información de apoyo que, por su nivel de detalle o extensión, no se incluye en el cuerpo principal del documento, pero resulta esencial para una comprensión más completa de la propuesta.

En este proyecto, los anexos cumplen los siguientes propósitos:

Ampliar la planificación: mediante la inclusión de cronogramas detallados y recursos necesarios que permiten dimensionar el alcance del trabajo.

Aportar claridad conceptual: a través de diagramas preliminares que ilustran la arquitectura propuesta y glosarios que facilitan la comprensión de términos técnicos.

Fortalecer el marco referencial: incluyendo tablas de proyectos y estudios similares que sirven como referentes académicos y prácticos.

Dar soporte a la propuesta metodológica: al presentar información complementaria que no sobrecarga el documento principal, pero aporta rigor académico.

Anexo A

Tabla 11 *Cronograma detallado de actividades*

Fase	Actividad	Semanas	Responsable	Productos esperados
1	Revisión bibliográfica	1–3	Investigador principal	Base de datos con mínimo 30 artículos y 10 tesis relacionadas
2	Análisis de referentes internacionales, nacionales y regionales	2–4	Investigador + asistente	Cuadro comparativo con mínimo 15 referentes
3	Definición de objetivos, metodología y marco teórico	4–6	Investigador principal	Documento preliminar del proyecto
4	Diseño conceptual de agentes y modelo preliminar del sistema	7–9	Investigador principal + asesor	Diagramas de arquitectura y flujos de proceso
5	Simulación inicial en MATLAB/Python (en versión piloto)	10–12	Investigador + asistente	Escenarios simulados básicos y métricas iniciales
6	Revisión y validación del modelo conceptual	13–14	Asesor académico	Informe de validación
7	Redacción del informe de resultados esperados y discusión	15	Investigador principal	Borrador final del documento

8	Ajustes, edición y consolidación del documento	16	Equipo de investigación	Versión final entregable

Nota. Elaboración propia. 2025

Anexo B

Tabla 12 *Involucrados en el proyecto*

Categoría de Actor	Actor Específico	Rol en el Proyecto	Nivel de Impacto	Relación con el Proyecto
Internos (Organización)	Docentes y estudiantes de ingeniería (rol simulado de operador)	Uso del sistema en entornos simulados para evaluación de usabilidad y respuesta ante incidentes.	Alto	Participan como usuarios simulados para validación académica del sistema.
	Docentes e investigadores en control industrial	Validan la integración conceptual del sistema con entornos SACDA y PLC simulados.	Alto	Colaboran en diseño y pruebas.
	Área de seguridad informática	Evalúan la alineación del sistema con políticas y buenas prácticas de ciberseguridad	Alto	Supervisan protocolos de seguridad y cumplimiento.

Externos (Entorno industrial)	Proveedores de hardware y software	Referentes tecnológicos utilizados como base para el diseño y simulación del sistema.	Medio	Proveen documentación técnica y estándares de referencia.
	Empresas de energía y agua	Entidades de referencia para la definición de escenarios simulados.	Alto	Contexto industrial utilizado para modelar casos de estudio.
	Comunidad local / usuarios de servicios	Impacto social indirecto asociado a la mejora teórica de la seguridad industrial.	Medio	Beneficiarios sociales del proyecto.
Reguladores y Normativos	Centro Cibernético Policial (Colombia)	Reporta incidentes de ciberseguridad y dicta lineamientos.	Alto	Fuente de datos y validación normativa.

	MinTIC (Ministerio de Tecnologías de la Información y Comunicaciones)	Establece políticas nacionales en ciberseguridad.	Alto	Referente normativo para adopción de estándares.
	ISO / NIST	Entidades internacionales que emiten estándares aplicables.	Medio	Aseguran alineación con estándares de calidad y seguridad.
Académico y de Investigación	Universidad Nacional Abierta y a Distancia (UNAD)	Institución donde se desarrolla el proyecto.	Alto	Marco académico y validación metodológica.

Nota. Elaboración propia (2025)

Anexo C

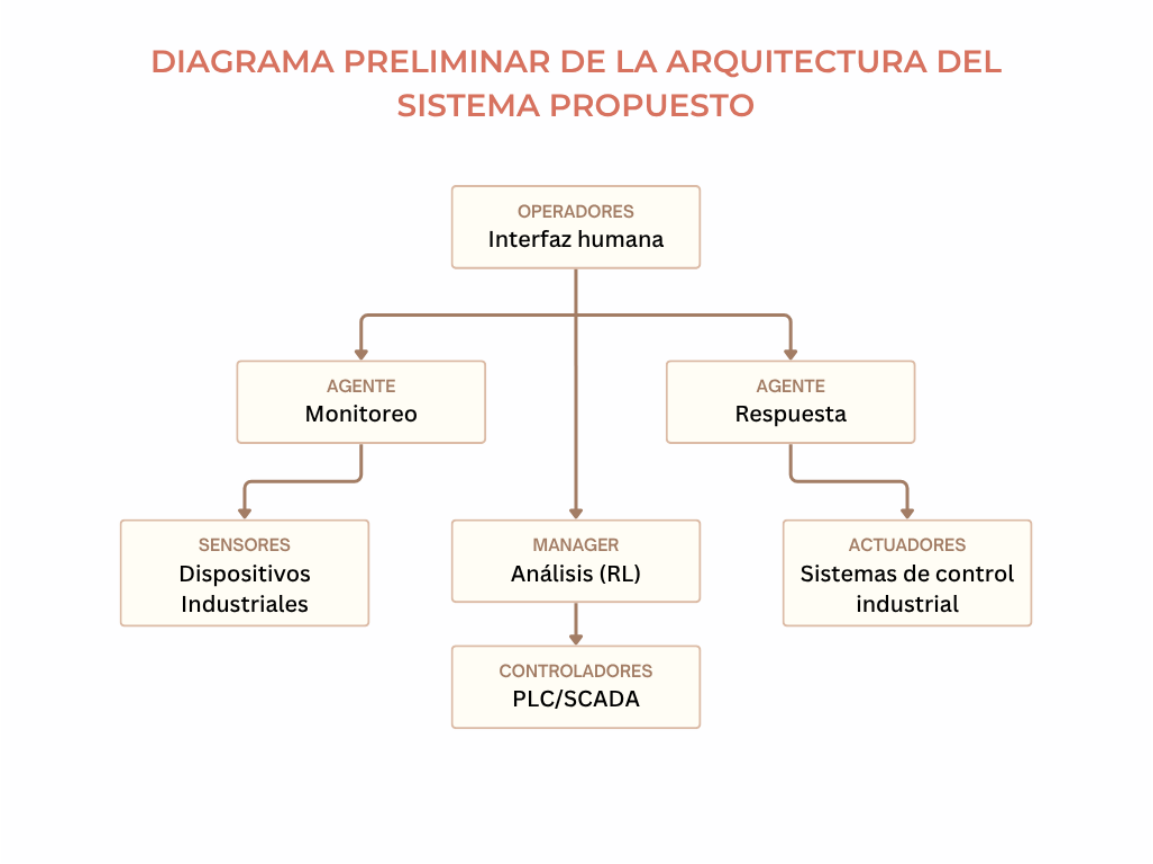

Figura 1 *Diagrama Preliminar de la Arquitectura del Sistema Propuesto*.

Anexo D

Tabla 13 *Glosario de términos técnicos*

Término	Definición
ICS (Industrial Control Systems)	Sistemas que supervisan y controlan procesos industriales (ejemplo: plantas eléctricas, de agua o gas).
IDS (Intrusion Detection System)	Herramienta que identifica intentos de intrusión o accesos no autorizados en una red.
Q-Learning	Algoritmo de aprendizaje reforzado donde un agente aprende a tomar decisiones óptimas basadas en recompensas y penalizaciones.
Multiagente	Sistema compuesto por varios agentes autónomos que trabajan de forma cooperativa.
Deep Q-Network (DQN)	Extensión de Q-Learning que utiliza redes neuronales profundas.
Resiliencia cibernética	Capacidad de un sistema para resistir, adaptarse y recuperarse frente a ataques.
Supervisory Control and Data Acquisition (SCADA)	Tecnología usada en ICS para supervisar y controlar procesos a gran escala.
Ataques de inyección de datos falsos (FDI)	Tipo de ciberataque que introduce datos alterados en sensores o redes para engañar al sistema.
Ciberseguridad industrial	Disciplina enfocada en proteger sistemas de control industrial y redes operativas frente a amenazas cibernéticas.

PLC (Controlador Lógico Programable)	Dispositivo electrónico usado para automatizar procesos industriales mediante la ejecución de instrucciones lógicas
Aprendizaje Reforzado (Reinforment Learning)	Técnica de inteligencia artificial que permite a un agente mejorar su desempeño mediante la experiencia y la retroalimentación
Sistema Multiagente (MAS)	Conjunto de agentes autónomos que cooperan entre sí para resolver tareas complejas en entornos distribuidos
Simulación Industrial	Representación virtual de un entorno físico para probar y validar sistemas o modelos antes de su implementación real

Nota. Elaboración propia a partir de las definiciones de NIST (2020) y ENISA (2023)

Anexo E

Tabla 14 *Referentes de proyectos similares*

Autor	Año	Título	Institución/Fuente	Aporte relevante
Lopera Salcedo, J.	2023	Modelos mixtos para la ciberseguridad en ICS	Instituto Tecnológico Metropolitano	Propuesta de modelos híbridos aplicados a ICS
Eceiza Olaizola, A.	2022	Sistemas multiagente aplicados a infraestructuras críticas	UNED, España	Valida agentes en contextos industriales
Orozco-Bonilla, D.	2021	Estrategias algorítmicas en entornos industriales	Universidad Politécnica Salesiana	Métodos de IA en ciberseguridad industrial
Durán Vásquez, L.	2022	Retos de escalabilidad en sistemas IoT aplicados a industria	Universidad de Cundinamarca	Escalabilidad y retos en IoT industrial
Gómez, F.	2020	Soluciones locales de ciberseguridad en el sector energético colombiano	Universidad de los Andes	Recomendaciones específicas para Colombia

Prieto, J.	2020	Evolución de soluciones de ciberseguridad en América Latina	Universidad Nacional del Nordeste	Necesidad de adaptación constante en seguridad
IBM Security	2022	X-Force Threat Intelligence Index	Informe corporativo	Estadísticas de ciberataques globales en ICS
Kaspersky	2021	ICS Security Survey	Reporte industrial	Riesgos y vulnerabilidades comunes en ICS

Nota. Adaptado de diversas fuentes académicas consultadas en el marco del proyecto (2025)

Anexo F

Tabla 15 *Diseño del cuestionario Likert*

Dimensión	Ítem de evaluación	Escala de respuesta (1–5)
Conciencia de seguridad	Comprendo los riesgos de ciberseguridad asociados al sistema que opero.	1 = Totalmente en desacuerdo 5 = Totalmente de acuerdo
	Sigo procedimientos establecidos para proteger el sistema.	1–5
Capacitación técnica	La empresa ofrece capacitación suficiente sobre ciberseguridad.	1–5
	Me siento preparado para actuar ante un incidente de seguridad.	1–5
Usabilidad del sistema	El sistema es fácil de operar sin comprometer la seguridad.	1–5
	Los mensajes de alerta del sistema son claros y útiles.	1–5
Confianza tecnológica	Confío en que el sistema puede detectar amenazas sin supervisión constante.	1–5
	Considero que las nuevas tecnologías mejoran la seguridad de mi entorno laboral.	1–5

Nota. Elaboración propia (2025), adaptado del modelo propuesto por Gómez Escobar (2019) del *Politécnico Colombiano Jaime Isaza Cadavid* sobre percepción de seguridad en entornos industriales.

Anexo G

Tabla 16 *Estructura de entrevista*

Bloque temático	Preguntas orientadoras	Propósito
Experiencia profesional	¿Qué tipo de sistemas de control industrial supervisa actualmente?	Contextualizar el nivel de experiencia del experto
Percepción de ciber amenazas	¿Qué ataques o vulnerabilidades ha observado con mayor frecuencia en los últimos años?	Identificar amenazas comunes
Gestión de incidentes	¿Cómo se manejan los eventos de seguridad en su organización?	Comprender protocolos existentes
Capacitación y cultura	¿Qué tan preparada considera que está su organización para enfrentar un ataque cibernético?	Evaluar preparación humana y organizacional
Adopción tecnológica	¿Qué opinión tiene sobre el uso de sistemas automatizados para detectar y responder a incidentes en tiempo real?	Explorar aceptación de tecnologías emergentes
Recomendaciones	¿Qué mejoras sugeriría para fortalecer la ciberseguridad en los sistemas de control industrial en Colombia?	Recoger sugerencias prácticas

Nota. Elaboración propia (2025), basada en la metodología de entrevistas aplicada por Kamlofsky (2021) de la *universidad de Sao Paulo* en estudios sobre ciberseguridad industrial.

Anexo H

En este anexo se presentan los resultados del cuestionario aplicado a los operadores de sistemas de control industrial el 6 de junio de 2025.

El instrumento permitió identificar la percepción de los participantes frente a aspectos como la conciencia de seguridad, la capacitación técnica, la usabilidad del sistema y la confianza tecnológica.

Los datos fueron recolectados mediante Google Forms y procesados en Microsoft Excel, generando los promedios y gráficos que se muestran a continuación.

Tabla 17 *Resultados del cuestionario Likert por dimensión*

Resultados

Marca temporal	Comprendo los riesgos de ciberseguridad asociados al sistema que opero.	Sigo procedimientos establecidos para proteger el sistema.	La empresa ofrece capacitación suficiente sobre ciberseguridad.	Me siento preparado para actuar ante un incidente de seguridad.	El sistema es fácil de operar sin comprometer la seguridad.	Los mensajes de alerta del sistema son claros y útiles.	Confío en que el sistema puede detectar amenazas sin supervisión constante.
6/9/2025 10:40:00	De acuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo
6/9/2025 11:44:41	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo
6/9/2025 11:55:00	En desacuerdo	De acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 11:55:52	De acuerdo	De acuerdo	En desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 11:57:46	De acuerdo	Totalmente de acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo
6/9/2025 11:59:47	De acuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	En desacuerdo	En desacuerdo
6/9/2025 12:01:04	De acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:01:34	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo
6/9/2025 12:02:02	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Totalmente de acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:02:20	Totalmente en desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo
6/9/2025 12:02:38	Totalmente en desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo

6/9/2025 12:02:54	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:03:08	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Totalmente en desacuerdo	De acuerdo	De acuerdo	Totalmente de acuerdo
6/9/2025 12:03:27	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Totalmente en desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo
6/9/2025 12:03:40	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:03:54	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:04:09	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	Totalmente de acuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:04:22	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	Totalmente en desacuerdo	En desacuerdo
6/9/2025 12:04:34	De acuerdo	Totalmente en desacuerdo	De acuerdo	En desacuerdo	Totalmente de acuerdo	Totalmente en desacuerdo	De acuerdo
6/9/2025 12:04:49	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:05:02	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	En desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:05:14	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	De acuerdo	De acuerdo
6/9/2025 12:06:56	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	En desacuerdo
6/9/2025 12:10:24	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	En desacuerdo
6/9/2025 12:10:40	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	En desacuerdo	En desacuerdo
6/9/2025 12:10:55	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo

6/9/2025 12:11:09	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo
6/9/2025 12:11:31	En desacuerdo	De acuerdo	Totalmente en desacuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente de acuerdo	Totalmente en desacuerdo
6/9/2025 12:11:51	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:12:05	En desacuerdo	Totalmente en desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:12:20	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo
6/9/2025 12:12:40	Ni de acuerdo ni en desacuerdo	En desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:13:01	En desacuerdo	Totalmente en desacuerdo	Totalmente en desacuerdo	En desacuerdo	En desacuerdo	Totalmente en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:13:59	En desacuerdo	Totalmente en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	De acuerdo	En desacuerdo
6/9/2025 12:17:23	En desacuerdo	Totalmente en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo	En desacuerdo
6/9/2025 12:17:34	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo
6/9/2025 12:17:50	Ni de acuerdo ni en desacuerdo	En desacuerdo	En desacuerdo	Totalmente en desacuerdo	En desacuerdo	En desacuerdo	Totalmente en desacuerdo
6/9/2025 12:18:06	En desacuerdo	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	En desacuerdo
6/9/2025 12:18:26	De acuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo
6/9/2025 12:18:39	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	En desacuerdo	De acuerdo	En desacuerdo
6/9/2025 12:18:55	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	Totalmente de acuerdo	De acuerdo	En desacuerdo

6/9/2025 12:19:12	En desacuerdo	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Totalmente en desacuerdo
6/9/2025 12:19:26	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo
6/9/2025 12:20:58	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	De acuerdo
6/9/2025 12:21:19	De acuerdo	De acuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo
6/9/2025 12:21:37	En desacuerdo	De acuerdo	En desacuerdo	De acuerdo	Totalmente de acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo
6/9/2025 12:21:49	De acuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo
6/9/2025 12:23:10	De acuerdo	En desacuerdo	Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	Ni de acuerdo ni en desacuerdo	Totalmente en desacuerdo
6/9/2025 12:23:27	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo	En desacuerdo
6/9/2025 12:23:40	En desacuerdo	De acuerdo	En desacuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	De acuerdo

Nota. Elaboración propia con base en los datos recolectados mediante Google Forms (2025).

Figura 2 *Nivel de comprensión de riesgos de ciberseguridad*

Figura 3 *Cumplimiento de procedimientos de seguridad establecidos*

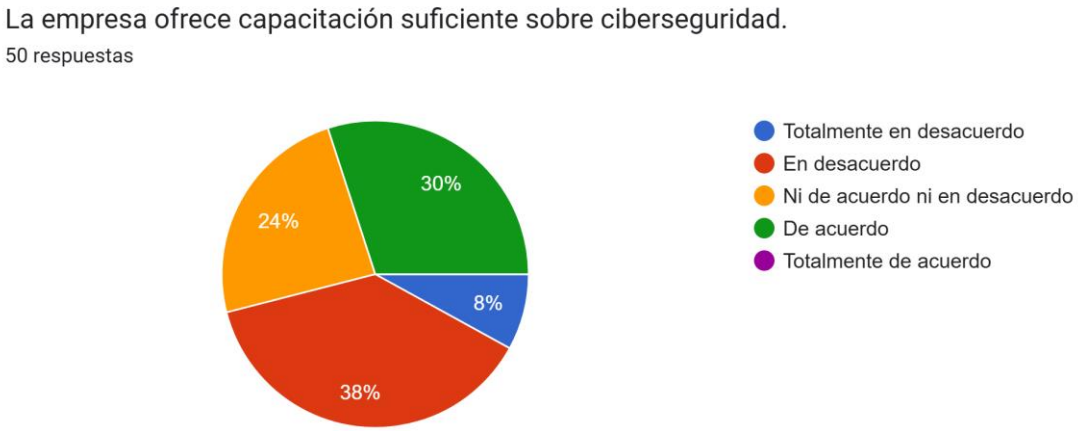

Figura 4 *Percepción sobre la capacitación en ciberseguridad ofrecida por la empresa*

Figura 5 *Preparación percibida ante incidentes de seguridad*

Figura 6 *Usabilidad percibida del sistema industrial*

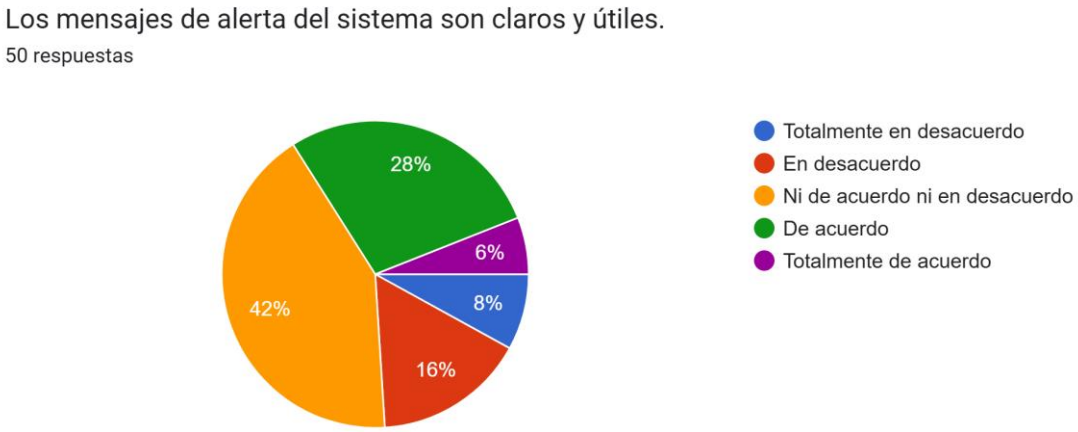

Figura 7 *Claridad y utilidad de los mensajes de alerta del sistema*

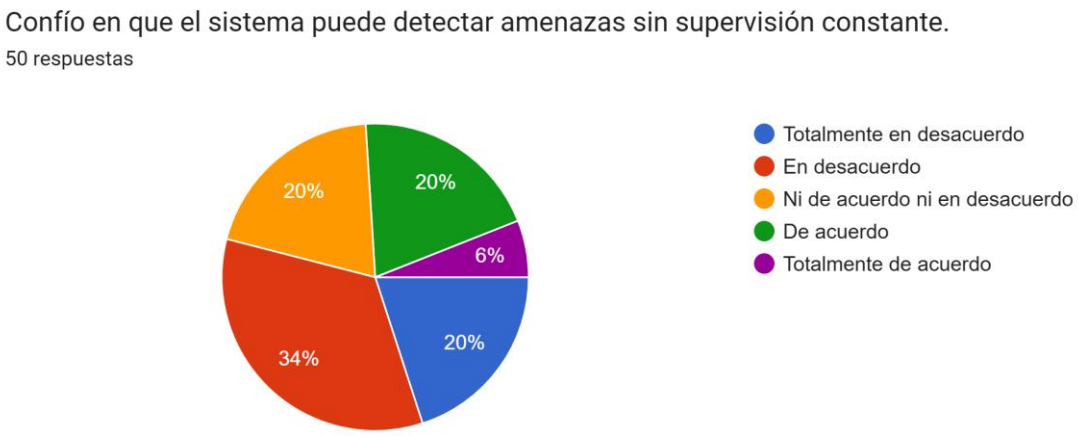

Figura 8 *Confianza en la capacidad del sistema para detectar amenazas de forma autónoma*