Departamento de Seguridad y Defensa

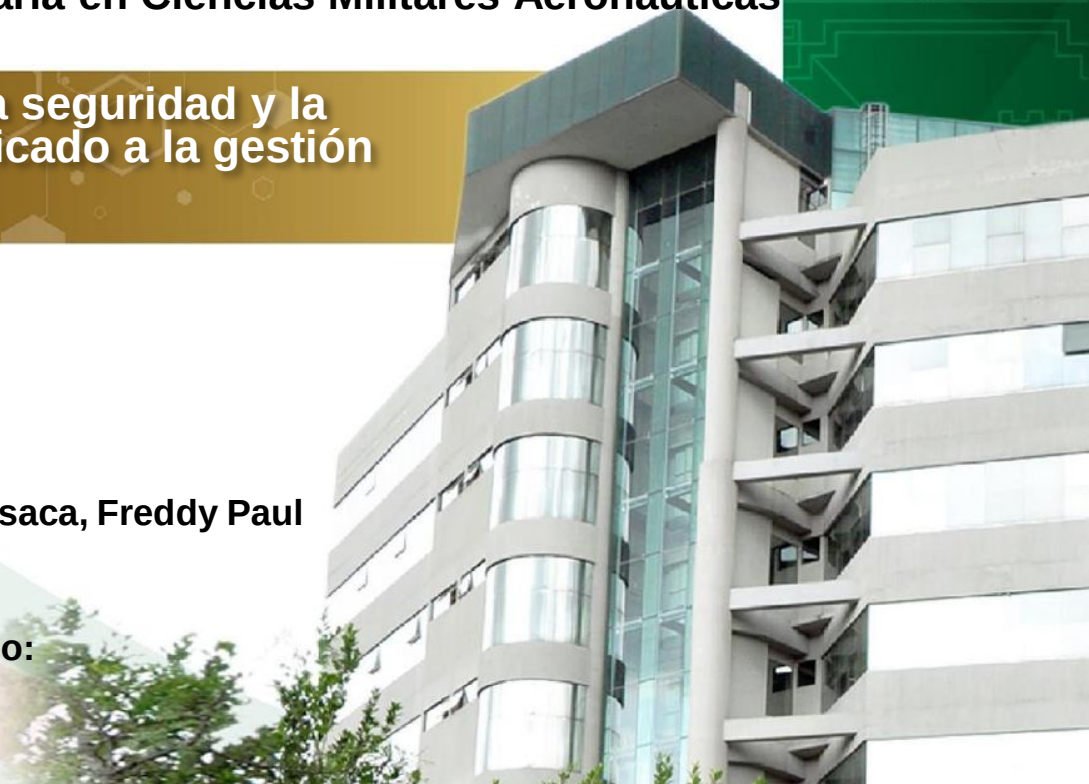
Carrera deTecnología Superior Universitaria en Ciencias Militares Aeronáuticas

Evaluación del funcionamiento, la seguridad y la eficiencia del sistema domótico aplicado a la gestión militar

AUTORES: Ortiz Ortiz, Joel Vinicio
Tipanguano Díaz, Joel Steven

Director: Tnte. Tec. Avc. Gualoto Chuisaca, Freddy Paul

Periodo Académico:
2026



ÍNDICE





CAPÍTULO 1
Introducción,problemay objetivos

CAPÍTULO 2
Metodología

CAPÍTULO 3
Evaluación del sistema domótico

CAPÍTULO 4
Resultados y diagnóstico

CAPÍTULO 5
Conclusiones y recomendaciones

CAPÍTULO 1
Introducción, problema y objetivos

Introducción

Automatización y transformación digital en instalaciones militares.

Mejora la eficiencia y reduce intervenciones manuales.

Integra iluminación, energía, accesos y videovigilancia.

Exige seguridad, continuidad operativa y protección de la información.

ANTECEDENTES

Transformación digital

Internet de las Cosas (IoT) conecta sensores, actuadores y sistemas de gestión.

Los sistemas BMS centralizan iluminación, energía, seguridad y supervisión.

La ciberseguridad es crítica por el carácter sensible de la infraestructura.

La automatización puede disminuir consumo y tareas manuales.

En gestión militar se requiere disponibilidad continua y resiliencia ante fallas.

Planteamiento del Problema

Falta de evaluación integral

No siempre se verifica de manera conjunta el funcionamiento, la seguridad y la eficiencia del sistema domótico.

Riesgos de ciberseguridad

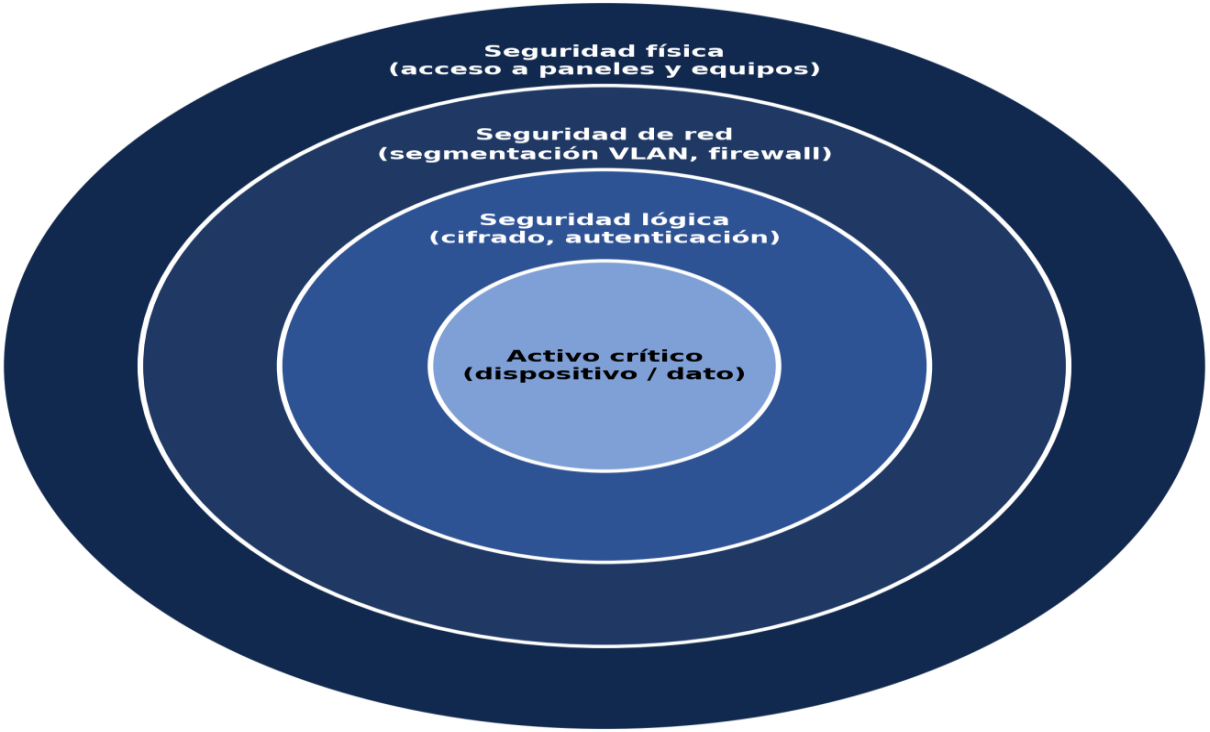
Credenciales débiles, dispositivos no autorizados y fallas de segmentación pueden comprometer el sistema.

Dependencia de conectividad

Una interrupción de red puede afectar el control de acceso, las alertas y la supervisión centralizada.

¿En qué medida la domótica implementada garantiza funcionamiento estable, seguridad adecuada y eficiencia energética y operativa para su uso institucional?

Argumentación del Problema



Objetivo general

Evaluar el funcionamiento, la seguridad y la eficiencia de la domótica aplicada a la gestión militar mediante pruebas técnicas y mediciones de desempeño.

Objetivo específico 1

Analizar los protocolos de comunicación, hardware, software y conectividad del sistema.

Objetivo específico 2

Medir disponibilidad, estabilidad y tiempo de respuesta en condiciones normales y de contingencia.

Objetivo específico 3

Identificar vulnerabilidades físicas, lógicas y de red que puedan afectar la seguridad.

Objetivos específicos complementarios

Objetivo específico 4

Medir la eficiencia energética alcanzada, comparando el consumo y el desempeño antes y después de la automatización.

Objetivo específico 5

Proponer recomendaciones técnicas para fortalecer la seguridad, la confiabilidad y la eficiencia del sistema domótico.

Justificación del problema

Técnica
Evaluar el desempeño real del sistema y detectar fallas o vulnerabilidades que afecten su operación.

Institucional
Aportar evidencia para decidir mejoras, ajustes o adopción de soluciones domóticas en otras unidades.

Eficiencia
Optimizar el uso de energía, reducir tareas manuales y fortalecer la protección de la infraestructura.

Marco teórico

Internet de las Cosas (IoT)
Integra sensores, actuadores, redes y objetos inteligentes para ofrecer servicios interconectados (Cando y Cevallos, 2020).

Building Management System (BMS)
Centraliza la supervisión de iluminación, energía, seguridad y otros subsistemas de una edificación.

Ciberseguridad en domótica
Requiere credenciales robustas, segmentación de red, control de acceso y actualización de dispositivos.

Marco conceptual

Sensores

Capturan variables del entorno y generan datos para el sistema: movimiento, apertura, consumo y otras señales.

Actuadores

Ejecutan acciones físicas, como encendido, apertura, cierre o activación de dispositivos.

Controladores

Procesan la información recibida y coordinan las órdenes de automatización y supervisión.

Marco conceptual

Control de acceso

Mecanismos físicos y digitales —biometría, credenciales y permisos— para proteger áreas restringidas.

Segmentación de red

Separación lógica o física de la red domótica respecto de redes institucionales de mayor criticidad.

Eficiencia energética

Reducción medible del consumo y de las intervenciones manuales mediante automatización y monitoreo.

CAPÍTULO 2
Metodología

Metodología

Enfoque

- Cuantitativo: mide disponibilidad, tiempo de respuesta, incidencias, consumo energético y reducción de tareas manuales.

Tipo

- Aplicado y evaluativo: valora técnicamente un sistema domótico ya implementado o un subsistema piloto representativo.

Alcance

- Descriptivo-evaluativo, organizado en tres dimensiones: funcionamiento, seguridad y eficiencia.



Diseño de la investigación
- No experimental y transversal.
- Variables observadas en su estado natural.
- Diseño evaluativo con criterios técnicos predefinidos.

Población y muestra
Población: componentes, red y procesos del sistema domótico.
Muestra: subsistema piloto o conjunto representativo seleccionado según criticidad.

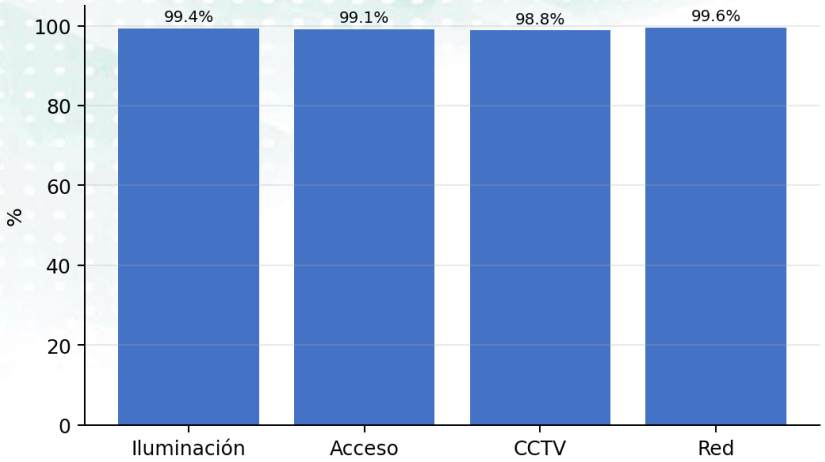
Técnicas e instrumentos
- Ficha de registro técnico.
- Checklist y matriz de riesgos.
- Medición energética.
- Encuesta al personal técnico y administrativo.

CAPÍTULO 3
Evaluación del sistema domótico

Sistema evaluado

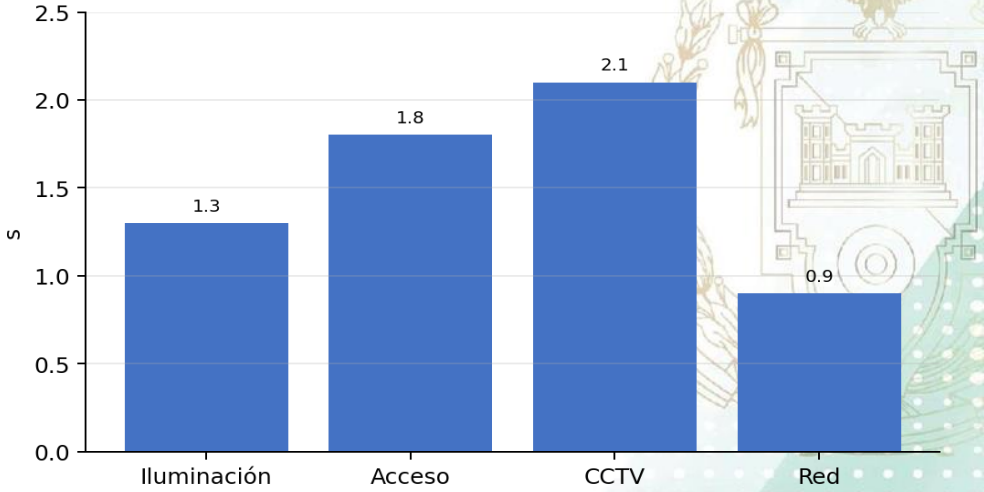
La población está formada por sensores, actuadores, controladores, red de comunicación, aplicación de gestión y procesos administrativos u operativos soportados por la domótica.

La muestra corresponde a un subsistema piloto o a dispositivos representativos seleccionados por criticidad operativa.

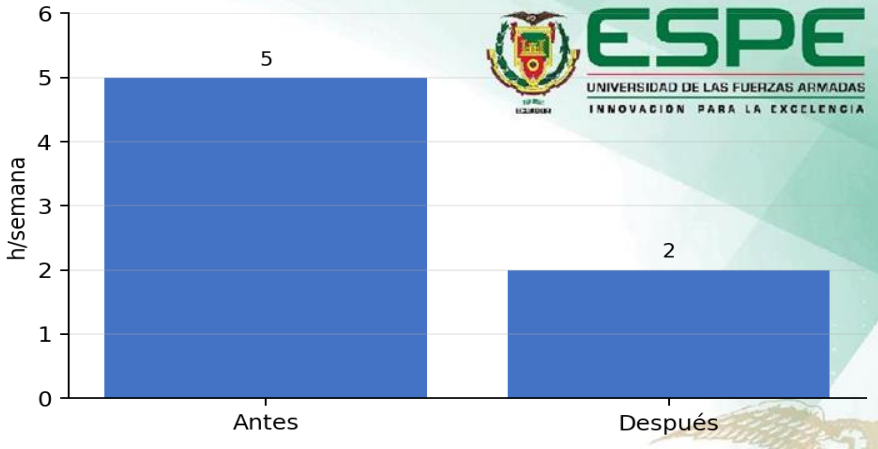


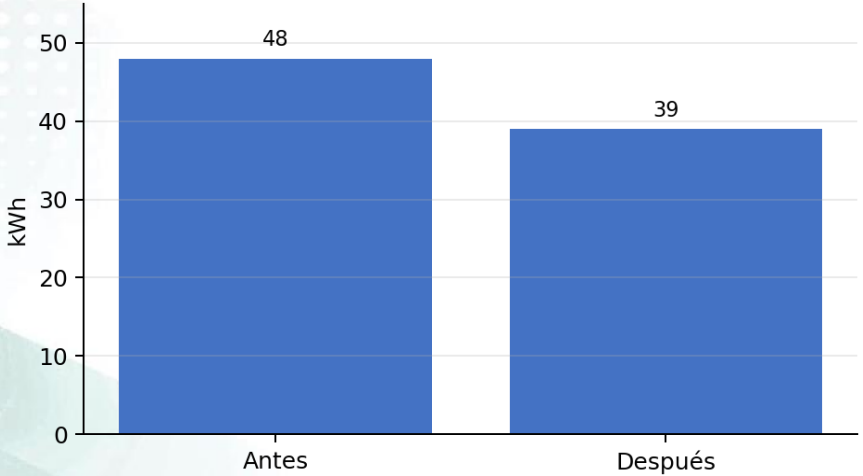
Disponibilidad por subsistema (%)

Tiempo de respuesta promedio (s)

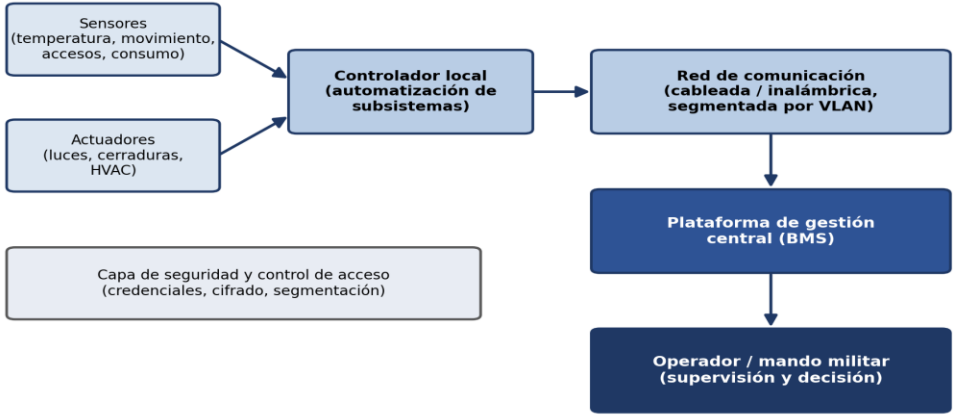


Consumo eléctrico mensual: 48 → 39 kWh
Reducción: 18,75 %





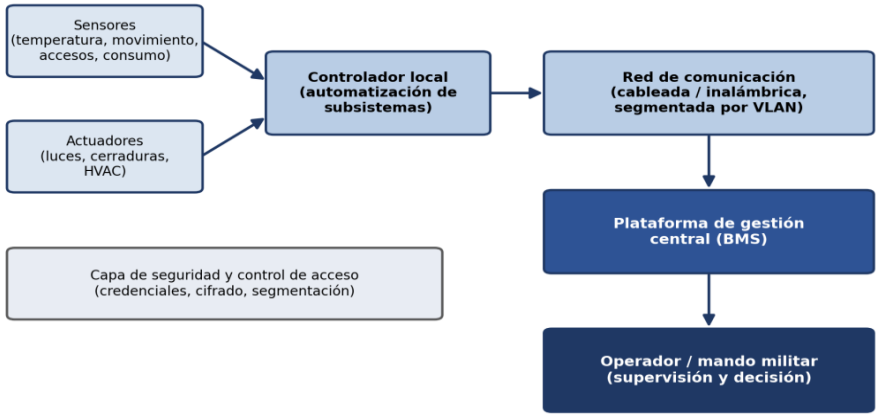
Horas-hombre en tareas manuales: 5 → 2 h/semana
Reducción: 60 %



Síntesis de resultados

Evaluación parcialmente favorable

El sistema presenta alta disponibilidad y mejoras de eficiencia; sin embargo, se identifican vulnerabilidades de severidad alta relacionadas con credenciales y control de acceso a la red.



CAPÍTULO 4
Resultados y diagnóstico

Activos principales del sistema domótico

Inventario técnico

Componente	Criticidad	Estado
Cerradura biométrica	Alta	Actualizado
Cámara Dahua 4MP PoE	Alta	Desactualizado

Desempeño de subsistemas críticos

Evaluación técnica

Subsistema	Disponibilidad	Respuesta
Red de comunicación	99,60 %	0,9 s
Control de acceso	99,10 %	1,8 s

Matriz de Riesgos

Riesgos principales

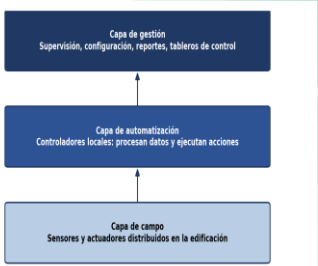
Severidad ALTA: requiere corrección prioritaria y control más estricto de la red.

Contraseña débil y acceso de dispositivos no autorizados.



Valoración del funcionamiento del sistema

Disponibilidad y estabilidad



- ❖ Disponibilidad entre 98,80 % y 99,60 % en los subsistemas evaluados.
- ❖ Los tiempos de respuesta se mantienen entre 0,9 s y 2,1 s.
- ❖ El desempeño operativo se clasifica como óptimo en los registros consignados.

Valoración de la seguridad

Credenciales y acceso a la red

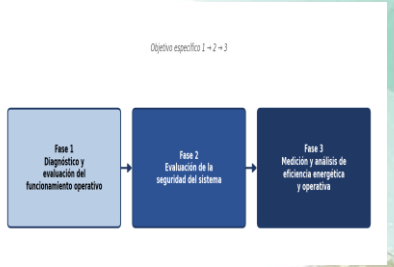
❖ ❖ Se identificó una contraseña débil en el centro de control local.

❖ El ingreso de dispositivos desconocidos a la red puede degradar la calidad del servicio.

❖ Ambos hallazgos fueron clasificados con severidad alta.

Valoración de la eficiencia energética

Consumo eléctrico



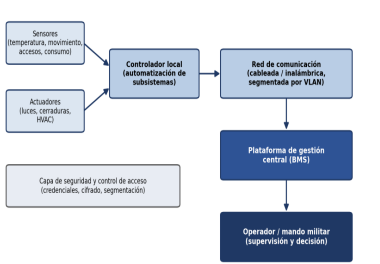
❖ ❖ El consumo mensual registrado pasa de 48 kWh a 39 kWh.

❖ La variación corresponde a una reducción del 18,75 %.

❖ El resultado se ubica dentro del rango de ahorro reportado para sistemas BMS.

Valoración de la eficiencia operativa

Reducción de tareas e incidencias



❖ ❖ Las horas-hombre destinadas a tareas manuales disminuyen de 5 a 2 h por semana (−60 %).

❖ Las incidencias de seguridad reportadas pasan de 4 a 2 por mes (−50 %).

❖ La automatización mejora la supervisión, aunque requiere fortalecer la ciberseguridad.

CAPÍTULO 5
Conclusiones y recomendaciones

Conclusiones

Funcionamiento favorable: Disponibilidad > 98,8 % y tiempos de respuesta entre 0,9 y 2,1 s.

- Seguridad parcialmente favorable:
• 2 vulnerabilidades de severidad alta.
• Se deben reforzar credenciales, permisos y control de red.

Eficiencia favorable: Consumo −18,75 %, tareas manuales −60 % e incidencias −50 %.



Recomendaciones

Cambiar credenciales débiles y aplicar contraseñas robustas con mínimo privilegio.

Segmentar la red y controlar los dispositivos autorizados con monitoreo de eventos.

Actualizar firmware y realizar evaluaciones periódicas de seguridad, funcionamiento y eficiencia.

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA
1922
ECUADOR

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACION PARA LA EXCELENCIA

Gracias por su atención