

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

Ortiz Ortiz, Joel Vinicio y Tipanguano Diaz, Joel Steven

Departamento de Defensa y Seguridad

Carrera de Tecnología Superior Universitaria en Ciencias Militares Aeronáuticas

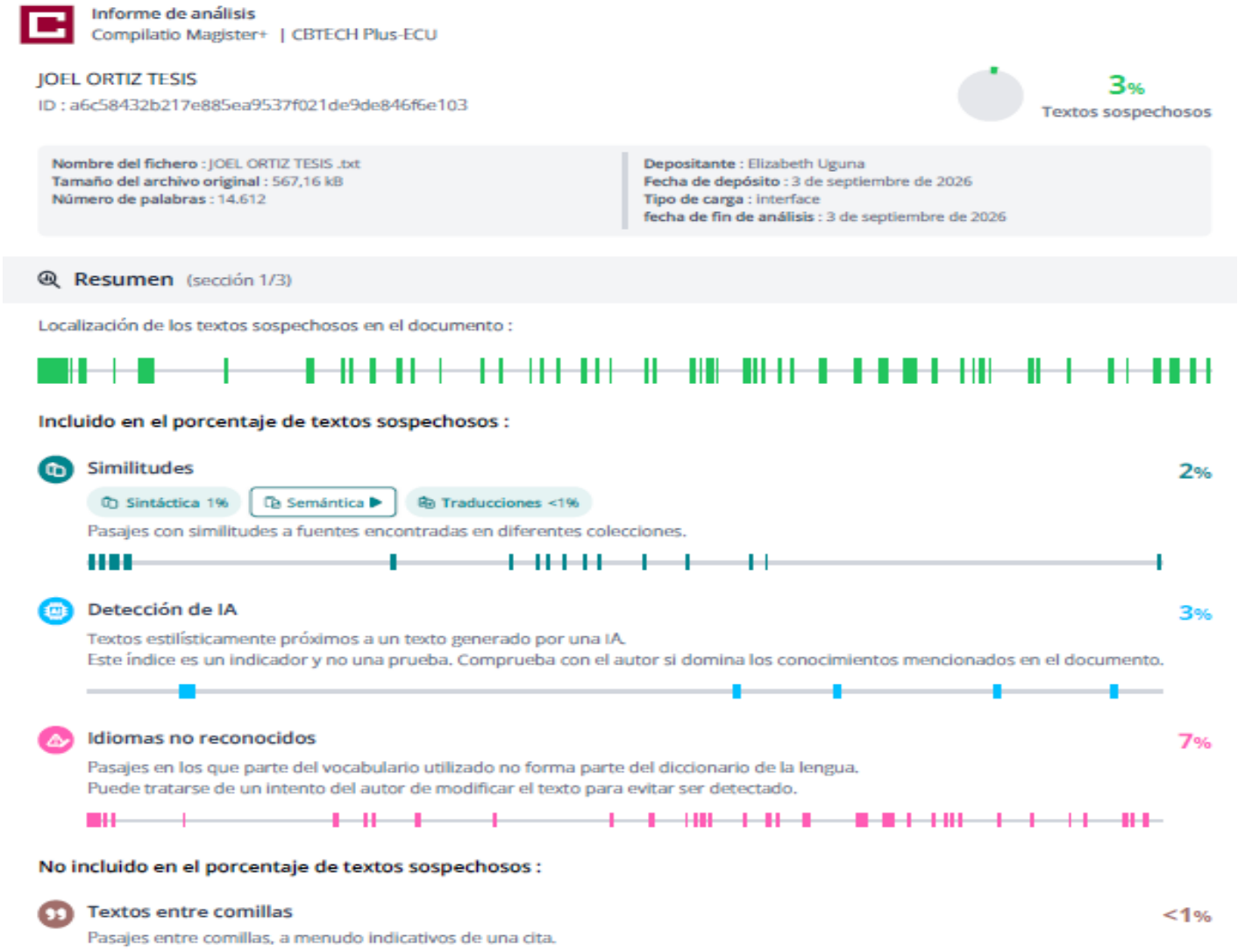
Trabajo de integración curricular, previo a la obtención del título de Tecnólogo Superior en Ciencias Militares Aeronáuticas.

Tnte.Téc.Avc. Gualoto Chuisaca, Freddy Paul

04 de septiembre de 2026

Latacunga

Reporte de verificación de contenidos



Validar únicamente en FirmaEC.
Firmado electrónicamente por:
FREDDY PAUL GUALOTO CHUISACA

Tnte.Téc.Avc. Gualoto Chuisaca, Freddy Paul

Director

C.C.:0104824610

Departamento de Seguridad y Defensa

Carrera de Tecnología Superior Universitaria en Ciencias Militares Aeronáutica

Certificación

Certifico que el trabajo de integración curricular: **"Evaluación del funcionamiento,la seguridad y la eficiencia del sistema domótico aplicado a la gestión militar "** fue realizado por **Ortiz Ortiz, Joel Vinicio** y **Tipanguano Diaz, Joel Steven**, el mismo que cumple con los requisitos legales, teóricos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, además fue revisado y analizada en su totalidad por la herramienta de prevención y/o verificación de similitud de contenidos; razón por la cual me permito acreditar y autorizar para que se sustente públicamente.

Latacunga, 04 de septiembre de 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
FREDDY PAUL GUALOTO CHUISACA

Tnte.Téc.Avc. Gualoto Chuisaca Freddy Paul

Director

CC: 0104824610

Departamento de Seguridad Y Defensa

Carrera de Tecnología Superior Universitaria en Ciencias Militares Aeronáuticas

Responsabilidad de autoría

Nosotros, **Ortiz Ortiz, Joel Vinicio** y **Tipanguano Diaz, Joel Steven** con cédulas de ciudadanía n° 1850034511 y n°1729033322, respectivamente, declaramos que el contenido, ideas y criterios del trabajo de integración curricular: **Evaluación del funcionamiento, la seguridad y la eficiencia del sistema domótico aplicado a la gestión militar** son de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Latacunga, 04 de septiembre de 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOEL VINICIO ORTIZ ORTIZ

Ortiz Ortiz, Joel Vinicio

C.C.:1850034511

Firmado electrónicamente por:
JOEL STEVEN TIPANGUANO DIAZ
Validar únicamente con FirmaEC

Tipanguano Diaz, Joel Steven

C.C.:1729033322

Departamento de Seguridad y Defensa

Carrera de Tecnología Superior Universitaria en Ciencias Militares Aeronáuticas

Autorización de publicación

Nosotros, **Ortiz Ortiz, Joel Vinicio** y **Tipanguano Diaz, Joel Steven**, con cédulas de ciudadanía n° 1850034511 y n° 1729033322, respectivamente, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de integración curricular: **Evaluación del funcionamiento, la seguridad y la eficiencia del sistema domótico aplicado a la gestión militar** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi/nuestra responsabilidad.

Latacunga, 04 de septiembre de 2026

Validar únicamente en FirmaEC.
Firmado electrónicamente por:
JOEL VINICIO ORTIZ ORTIZ

Ortiz Ortiz, Joel Vinicio

C.C.:1850034511

Firmado electrónicamente por:
JOEL STEVEN TIPANGUANO DIAZ
Validar únicamente con FirmaEC

Tipanguano Diaz, Joel Steven

C.C.: 1729033322

Dedicatoria

Dedico este trabajo de titulación, en primer lugar, a Dios, por darme la fortaleza, sabiduría y perseverancia necesarias para superar cada obstáculo a lo largo de este camino. Gracias por acompañarme en cada momento, por permitirme seguir adelante en las dificultades y por darme la oportunidad de alcanzar una meta que representa años de esfuerzo, dedicación, disciplina y sacrificio.

A mis padres, quienes han sido el pilar fundamental de mi vida y mi mayor fuente de motivación. Gracias por su amor incondicional, por cada sacrificio realizado, por sus consejos y por estar presentes en cada etapa de este proceso. Su apoyo y confianza me impulsaron a no rendirme y a continuar luchando por mis objetivos. Este logro también les pertenece, porque detrás de cada meta alcanzada está el esfuerzo y el amor de una familia que siempre creyó en mí.

A mis abuelitos, por todo el cariño, las enseñanzas y los valores que me han transmitido a lo largo de mi vida. Gracias por sus palabras, sus consejos y por ser una parte tan importante de mi familia. Su apoyo y afecto han sido una motivación para seguir adelante y cumplir cada uno de mis propósitos.

A mis compañeros, por el compañerismo, la amistad y el apoyo compartido durante esta etapa de formación. Los momentos vividos, las dificultades superadas y las experiencias adquiridas quedarán como parte importante de este camino.

Finalmente, dedico este trabajo a mi vocación de servicio, a mi compromiso y al amor por mi patria, con la firme convicción de continuar creciendo profesionalmente y poner en práctica los conocimientos adquiridos para contribuir al bienestar y desarrollo de la Fuerza Aérea Ecuatoriana y del Ecuador.

Atro. Ortiz Ortiz, Joel Vinicio

Dedicatoria

Dedico este mi último trabajo como alumno a la Virgencita de Guadalupe porque desde el 1er día que inicié con mi proceso de admisión para ingresar a la Fuerza Aérea puse toda mi fé en ella y no me decepcionó y aunque nunca la haya visto con mis ojos físicamente sé que me acompañó espiritualmente y me dio las fortalezas para seguir con este sueño que hace 2 años parecía imposible hoy lo estoy cumpliendo y doy gracias al cielo por todas las veces que me protegió incluso en esos días que ya no quería estar aquí yo estoy seguro que yo nunca estuve solo ella siempre estuvo a mi lado en cada paso.

Y cómo no mencionar a mis padres, quienes fueron los que me ayudaron a tomar esta decisión diciendo: «No sabemos mucho de eso, pero lo único que sabemos es que tú lo lograrás y serás el 1.º militar de la familia», creyeron en mis capacidades y respaldaron cada una de mis decisiones con paciencia y dedicación. Su ejemplo de trabajo constante y su compromiso me inspiran a ser mejor y llevar con orgullo los apellidos de mis padres.

El esfuerzo de ambos, sostenido a lo largo de los años, representa el verdadero cimiento de este trabajo de integración curricular. Cada logro alcanzado durante mi formación lleva consigo su huella, su sacrificio silencioso y su fe inquebrantable en que este camino culminaría con éxito.

Atro. Tipanguano Diaz, Joel Steven

Agradecimiento

Agradezco, en primer lugar, a Dios, por haberme dotado de la fortaleza física y espiritual necesaria para afrontar cada etapa de este proceso formativo. Su guía constante fue determinante en los momentos de mayor exigencia académica y personal, y su presencia representó siempre un motivo de calma y confianza para continuar avanzando.

De igual manera, expreso mi más profundo agradecimiento a mis padres, quienes con su esfuerzo diario y su ejemplo de disciplina me enseñaron el valor del compromiso y la perseverancia. Su apoyo incondicional, manifestado en cada decisión tomada a lo largo de mi formación, constituyó el respaldo fundamental que me permitió sostener este proceso incluso en las circunstancias más difíciles.

A ellos les debo no solo la oportunidad de formarme profesionalmente, sino también los valores de responsabilidad, honestidad y servicio que hoy definen mi actuar como futuro oficial. Su paciencia, comprensión y confianza fueron un pilar constante durante los momentos de mayor exigencia de esta etapa académica y militar.

Por todo lo anterior, dejo constancia de mi sincero y profundo agradecimiento hacia Dios y hacia mis padres, cuya presencia y respaldo hicieron posible la culminación de este trabajo de integración curricular.

Atro. Tipanguano Diaz, Joel Steven

Atro. Ortiz Ortiz, Joel Vinicio

Índice de contenidos

Carátula 1

Reporte de verificación de contenidos 2

Certificación 3

Responsabilidad de autoría 4

Autorización de publicación 5

Dedicatoria 6

Dedicatoria 7

Agradecimiento 8

Índice de contenidos 9

Índice de tablas 13

Índice de figuras 14

Resumen 15

Abstract 16

Capítulo I 17

Introducción 17

Planteamiento del problema 17

Estado del arte 18

Pregunta de investigación 19

Objetivos 20

Objetivo general 20

Objetivos específicos 20

Alcance y delimitación del estudio..... 20

Justificación..... 21

Capítulo II..... 23

Marco teórico 23

Estudios centrados en la seguridad de sistemas IoT y domóticos 23

Estudios centrados en la eficiencia energética y la automatización de edificaciones 24

Síntesis comparativa de los trabajos relacionados..... 24

Infraestructura tecnológica militar y sistemas domóticos 26

Building Management System (BMS) y su aplicación institucional 26

Redes de comunicación en entornos militares 28

Arquitectura de un sistema domótico: sensores, actuadores y controladores..... 29

Protocolos de comunicación domótica..... 30

Internet de las Cosas (IoT) aplicado a la gestión de instalaciones 32

Seguridad informática y comunicación inalámbrica en sistemas ciberfísicos..... 32

Control de acceso físico y videovigilancia..... 33

Normativa y estándares de seguridad de la información..... 35

Ciberseguridad avanzada: cifrado, segmentación y defensa en profundidad 35

Marco legal e institucional en Ecuador..... 37

Casos de aplicación de automatización en instalaciones gubernamentales 38

Gestión de identidades y accesos (IAM) en sistemas domóticos 39

Gestión de la energía y sostenibilidad en edificaciones institucionales..... 39

Eficiencia energética, mantenimiento predictivo e indicadores de desempeño 40

Comparación entre domótica, BMS y sistemas SCADA industriales 40

Arquitecturas de control: local (on-premise) frente a gestión en la nube 41

Continuidad operativa y planes de contingencia aplicados al sistema domótico 42

Registro y auditoría de eventos (logging) en sistemas de control 43

Referencia para la gestión de energía: ISO 50001 44

Marco de referencia para la ciberseguridad de sistemas ciberfísicos: NIST CSF 45

Sistemas de clasificación de vulnerabilidades: CVSS 45

Análisis costo-beneficio de la automatización institucional 46

Marco conceptual 47

Capítulo III 50

Metodología 50

Enfoque de investigación 50

Tipo y diseño de investigación 50

Población y muestra 50

Variables e indicadores de la investigación 51

Metodología para el cumplimiento de los objetivos 52

Fase 1. Diagnóstico y evaluación del funcionamiento operativo 52

Fase 2. Evaluación de la seguridad del sistema 53

Fase 3. Medición y análisis de la eficiencia energética y operativa 56

Cronograma de actividades 56

Proforma presupuestaria 57

Validación y confiabilidad del instrumento 59

Consideraciones éticas 60

Capítulo IV 61

Análisis y discusión de los resultados 61

Resultados del funcionamiento operativo del sistema domótico (Fase 1) 61

Análisis por subsistema 62

Resultados de la evaluación de seguridad (Fase 2) 63

Resultados de la eficiencia energética y operativa (Fase 3) 66

Discusión general de los resultados 67

Capítulo V 69

Conclusiones y recomendaciones 69

Conclusiones 69

Recomendaciones 70

Recomendaciones de corto plazo 70

Recomendaciones de mediano y largo plazo 70

Líneas de investigación futura 71

Referencias 72

Apéndices 76

Índice de tablas

Tabla 1 Comparativa de protocolos de comunicación domótica evaluados 25

Tabla 2 Subsistemas típicos de un Building Management System (BMS) 27

Tabla 3 Clasificación de sensores utilizados en sistemas domóticos 30

Tabla 4 Vulnerabilidades frecuentes en dispositivos IoT y medidas de mitigación 31

Tabla 5 Vulnerabilidades frecuentes en dispositivos IoT y medidas de mitigación 33

Tabla 6 Controles de seguridad física aplicables según ISO/IEC 27001, Anexo A.7 34

Tabla 7 Operacionalización de variables de la investigación 51

Tabla 8 Operacionalización de variables de la investigación 55

Tabla 9 Cronograma de actividades por fase metodológica 56

Tabla 10 Matriz de requerimientos tecnológicos (plantilla) 57

Tabla 11 Escala de severidad para la matriz de riesgos de seguridad 61

Tabla 12 Matriz de riesgos de seguridad del sistema domótico (plantilla)..... 63

Tabla 13 Criterios de evaluación del funcionamiento del sistema 64

Tabla 14 Simulación de vulnerabilidades detectadas..... 64

Tabla 15 Indicadores de eficiencia energética y operativa (plantilla)..... 66

Índice de figuras

Figura 1 Capas funcionales de un Building Management System (BMS)..... 27

Figura 2 Arquitectura general de un sistema domótico aplicado a la gestión militar 29

Figura 3 Esquema de capas de seguridad de un sistema ciberfísico 36

Figura 4 Proceso metodológico de la evaluación por fases 52

Figura 5 Ciclo de análisis de vulnerabilidades aplicado en la Fase 2 54

Resumen

El presente trabajo de integración curricular tiene como propósito evaluar el funcionamiento, la seguridad y la eficiencia de un sistema domótico aplicado a la gestión de instalaciones militares. La incorporación de tecnologías de automatización e Internet de las Cosas (IoT) en unidades y edificaciones de uso militar plantea beneficios operativos, como el control centralizado de iluminación, energía y accesos, pero también introduce riesgos particulares, dado el carácter sensible de la información y de la infraestructura involucrada. La investigación se desarrolla bajo un enfoque cuantitativo, de tipo aplicado y diseño no experimental, mediante la implementación y/o análisis de un sistema domótico piloto sobre el cual se aplican pruebas técnicas de funcionamiento, pruebas de seguridad (evaluación de vulnerabilidades, control de acceso y cifrado de comunicaciones) y mediciones de eficiencia energética y operativa.

El estudio se organiza en tres fases secuenciales: diagnóstico y evaluación del funcionamiento, evaluación de la seguridad y medición de la eficiencia, cada una asociada a un objetivo específico y respaldada por instrumentos técnicos validados mediante juicio de expertos. Los hallazgos de esta investigación contribuirán a la comprobación del funcionamiento, a la justificación de la eficiencia y a aportar conocimiento sobre seguridad domótica. Además de detectar fallas y proponer mejoras.

Palabras clave: Seguridad de la información, Eficiencia energética, Evaluación del funcionamiento, Internet de las Cosas (IoT).

Abstract

This curricular integration project aims to evaluate the functionality, security, and efficiency of a home automation system applied to the management of military facilities. The integration of automation and Internet of Things (IoT) technologies into military facilities offers operational benefits, such as the centralized control of lighting, energy consumption, and access systems. However, their implementation also introduces specific risks due to the sensitive nature of the information and infrastructure involved. The research follows a quantitative, applied, and non-experimental approach, based on the implementation and analysis of a pilot home automation system. The evaluation includes technical operational tests, security assessments focused on vulnerabilities, access control, and communication encryption, as well as measurements of energy and operational efficiency. The study is structured into three sequential phases: diagnosis and operational evaluation, security assessment, and efficiency measurement. Each phase is aligned with a specific research objective and supported by technical instruments validated through expert review. The findings of this study will contribute to verifying the proper operation of the system, assessing its efficiency, and expanding knowledge regarding the security of home automation technologies in military environments. Furthermore, the research will support the identification of potential failures and the formulation of improvements based on the results obtained.

Keywords: Information security,Energy efficiency,Performance assessment*, Internet of Things (IoT).*

Capítulo I

Introducción

Planteamiento del problema

La transformación digital ha impulsado la incorporación de tecnologías de automatización en la gestión de espacios institucionales, entre ellos las instalaciones militares, con el fin de optimizar la seguridad y los procesos administrativos. La domótica, entendida como el conjunto de sistemas que permiten automatizar la gestión de una edificación, hace posible integrar bajo una misma plataforma la iluminación, el control de accesos y la videovigilancia, reduciendo la dependencia de la intervención manual (Molina, s.f.).

A la par de estos beneficios, la incorporación de dispositivos conectados a Internet de las Cosas (IoT) amplía la superficie de exposición ante amenazas cibernéticas. De acuerdo con Molina (s.f.), entre las principales debilidades de los sistemas IoT se encuentran el uso de contraseñas débiles, la insuficiente protección de la privacidad de los datos y la inadecuada gestión de los dispositivos conectados, factores que también son propios de los sistemas domóticos. En la misma línea, López Naranjo (2022) señala que los sistemas domóticos presentan amenazas frecuentes asociadas a la arquitectura IoT que los soporta, por lo que su nivel de seguridad debe verificarse de forma específica. Cando y Cevallos (2020) añaden que la seguridad en los ecosistemas IoT no se limita a proteger datos, sino también las claves criptográficas y credenciales que permiten el control de los dispositivos físicos.

Desde la perspectiva de la eficiencia, diversos estudios evidencian que la automatización de edificaciones permite alcanzar ahorros energéticos significativos: la integración de sensores, controladores de iluminación natural y sistemas de gestión centralizada puede reducir el consumo eléctrico entre un 40 % y un 70 % (Lezama, 2024), mientras que investigaciones aplicadas a instituciones ecuatorianas han reportado reducciones de consumo superiores al 50 % tras la implementación de sistemas de gestión energética automatizados (Gamboa, 2020). No obstante, estos beneficios de eficiencia solo se

materializan cuando el sistema domótico funciona de manera estable y confiable; una arquitectura mal dimensionada puede anular el ahorro esperado e introducir nuevas vulnerabilidades (“Un breve análisis de vulnerabilidades en dispositivos IoT en Ecuador”, 2023).

Diversas unidades e instalaciones militares han incorporado sistemas domóticos como parte de sus procesos de modernización administrativa y logística sin que, en muchos casos, se haya realizado una evaluación técnica rigurosa que permita determinar si el sistema implementado funciona de manera confiable, si cuenta con los niveles de seguridad adecuados frente a amenazas físicas y cibernéticas, y si efectivamente genera los beneficios de eficiencia energética y operativa que se esperan de él. Sin embargo, y a la espera de una evaluación sistemática, se desconoce la fiabilidad operativa de la domótica, la posible exposición de la institución a riesgos tales como accesos no autorizados a la red de automatización o a la interceptación de las comunicaciones y la posibilidad de evaluar el retorno de la inversión

Se requiere una evaluación integral, que tenga en cuenta la situación actual de la domótica en la administración militar desde los puntos de vista operativo, de seguridad y de eficiencia, con el apoyo de pruebas técnicas.

Estado del arte

La automatización de edificaciones ha evolucionado desde sistemas aislados de control de iluminación o climatización hacia plataformas integradas basadas en el Internet de las Cosas (IoT), capaces de gestionar de forma centralizada múltiples subsistemas.

En cuanto a la seguridad, Molina (s.f.) identifica debilidades recurrentes en los ecosistemas IoT, como el uso de credenciales débiles o compartidas, la insuficiente protección de la privacidad de los datos y la gestión inadecuada de los dispositivos conectados, y propone como mitigación el uso de contraseñas únicas por dispositivo y políticas claras de manejo de datos. En un estudio aplicado a un entorno domótico simulado, López Naranjo (2022) evaluó los niveles de seguridad de dispositivos IoT y documentó buenas prácticas de ciberseguridad

aplicables a estos entornos, mientras que un análisis de vulnerabilidades sobre direcciones IP ecuatorianas evidenció que un número considerable de dispositivos conectados, incluidas cámaras y routers, exponía puertos y credenciales de configuración sin protección adecuada (“Un breve análisis de vulnerabilidades…”, 2023).

Desde la perspectiva de la infraestructura, los sistemas de gestión de edificios (BMS) se han consolidado como el estándar de facto para integrar climatización, iluminación, energía y seguridad bajo una única plataforma de control, con beneficios documentados de ahorro energético y reducción de costos de mantenimiento (Wikipedia, 2026). En paralelo, marcos normativos internacionales como la norma ISO/IEC 27001, establecen controles de acceso físico (biometría, tarjetas RFID, claves) que resultan directamente aplicables a la evaluación de la seguridad de instalaciones que integran sistemas domóticos (ISMS.online, 2025).

La principal limitación para la adopción de sistemas domóticos en entornos sensibles no es únicamente tecnológica, sino que responde a la ausencia de metodologías de evaluación que consideren simultáneamente el desempeño funcional, la seguridad de la información y la eficiencia del sistema. La mayoría de los trabajos disponibles abordan estas dimensiones de forma aislada seguridad IoT por un lado, eficiencia energética por otro, infraestructura de BMS por otro y ninguno se enfoca específicamente en el ámbito de la gestión militar.

Pregunta de investigación

¿En qué medida la domótica implementada para la gestión de instalaciones militares garantiza un funcionamiento estable y confiable, un nivel de seguridad adecuado frente a amenazas físicas y cibernéticas, y una eficiencia operativa y energética que justifique su adopción institucional?

Objetivos

Objetivo general

Evaluar el funcionamiento, la seguridad y la eficiencia de la domótica aplicada a la gestión militar mediante pruebas técnicas, análisis de vulnerabilidades y mediciones de desempeño energético y operativo, con el fin de determinar su fiabilidad y sustentar recomendaciones para su implementación institucional.

Objetivos específicos

- Analizar los protocolos de comunicación que usa la domótica, mirando el hardware, el software y la conectividad.
- Determinar la disponibilidad, la estabilidad y el tiempo de respuesta de la domótica en su funcionamiento normal y en situaciones de contingencia.
- Identificar vulnerabilidades físicas, lógicas y de red que puedan afectar la seguridad de la domótica.

Alcance y delimitación del estudio

El presente trabajo se limita a la evaluación técnica de un sistema domótico ya implementado en una instalación militar específica, y no contempla el diseño, la adquisición ni la instalación de nueva infraestructura tecnológica. El alcance de la evaluación se circunscribe a las tres dimensiones definidas en los objetivos específicos: funcionamiento, seguridad y eficiencia, y no incluye, salvo que se indique lo contrario en el desarrollo del trabajo, la evaluación de sistemas de armamento, comunicaciones tácticas u otra infraestructura militar de carácter estrictamente operativo ajena a la gestión administrativa y logística de la instalación. Desde el punto de vista temporal, la investigación se delimita al periodo de observación y pruebas definido en el cronograma del Capítulo III, por lo que sus conclusiones reflejan el estado del sistema domótico durante dicho periodo y no garantizan su vigencia indefinida, dado que tanto las vulnerabilidades de seguridad como las condiciones de eficiencia energética

pueden variar con el tiempo, con las actualizaciones del sistema y con cambios en su entorno de operación. Los resultados solo se toman como referencia para tener un enfoque claro y objetivo.

Justificación

Esta investigación tiene sentido técnico, institucional y social. En lo técnico, ayuda a crear conocimiento práctico sobre cómo rinden los sistemas domóticos en un entorno militar exigente. Una falla o un problema de seguridad en un sistema automatizado puede causar problemas más allá de lo administrativo. En lo institucional, los resultados les darán a los responsables datos claros para apoyar, ajustar o cambiar la forma en que se adoptan tecnologías domóticas en otras unidades, y así usar mejor el dinero en infraestructura tecnológica.

Además, la investigación ayuda a usar la energía de forma más eficiente en instalaciones estatales, siguiendo las políticas de sostenibilidad y de ahorro del gasto público. Por último, al tratar claramente la seguridad física y cibernética del sistema domótico, el trabajo ofrece un enfoque preventivo que es útil en un contexto donde proteger la información y la infraestructura crítica es una prioridad para las instituciones de defensa.

Desde el punto de vista metodológico, la investigación aporta un procedimiento de evaluación replicable, organizado en fases claramente delimitadas y respaldado por instrumentos validados, que puede aplicarse a otras unidades o instalaciones que cuenten con sistemas domóticos, sin necesidad de partir desde cero en el diseño de los instrumentos de evaluación. Este aporte metodológico es especialmente valioso en un campo donde, como se evidencia en el Capítulo II, la mayoría de los estudios existentes evalúan la seguridad, la eficiencia o el funcionamiento de forma aislada.

La propuesta está vinculada a los Objetivos de Desarrollo Sostenible, sobre todo al ODS 9, que habla de industria, innovación e infraestructura, porque la propuesta evalúa la fiabilidad de una infraestructura tecnológica para modernizar la institución. También está vinculada al ODS 16, que trata de paz, justicia e instituciones sólidas, porque al reforzar la seguridad de los sistemas que manejan la gestión militar se hacen las instituciones más seguras, más transparentes y más eficientes.

Finalmente, la investigación beneficia de forma directa al personal técnico y administrativo responsable de la operación del sistema domótico, al brindarles un diagnóstico objetivo de su desempeño, así como recomendaciones concretas para fortalecer su seguridad y su eficiencia, y de forma indirecta a la institución en su conjunto, al reducir el riesgo de incidentes de seguridad y optimizar el uso de los recursos energéticos disponibles.

Capítulo II

Marco teórico

Estudios centrados en la seguridad de sistemas IoT y domóticos

Molina (s.f.) examina de forma general la gestión de riesgos en ecosistemas IoT, identificando como principales debilidades el uso de contraseñas por defecto o compartidas, la protección insuficiente de la privacidad de los datos y la gestión inadecuada de los dispositivos conectados a lo largo de su ciclo de vida. El estudio propone, como medidas de mitigación, la adopción de contraseñas únicas por dispositivo, la actualización periódica de firmware y la definición de políticas claras de manejo de datos, recomendaciones que se retoman en el checklist de seguridad propuesto en el Apéndice B de este trabajo.

López Naranjo (2022), en un trabajo de titulación desarrollado en la Pontificia Universidad Católica del Ecuador, analiza las amenazas específicas de un entorno domótico simulado y evalúa el nivel de seguridad de los dispositivos IoT que lo componen, documentando buenas prácticas de ciberseguridad aplicables a estos entornos. A diferencia del presente trabajo, dicho estudio se desarrolla sobre un entorno simulado y no evalúa de forma conjunta la eficiencia energética ni el funcionamiento operativo del sistema, lo que refuerza la pertinencia de una evaluación integral como la propuesta en esta investigación.

Cando y Cevallos (2020), en su artículo publicado en la revista Hamut'ay, desarrollan una taxonomía de activos y amenazas de seguridad en el Internet de las Cosas, clasificando los riesgos según el activo comprometido (dispositivo, red, plataforma o datos) y destacando que la seguridad en estos ecosistemas no se limita a proteger la información, sino también las claves criptográficas y credenciales que permiten el control de los dispositivos físicos. Esta taxonomía constituye una de las bases conceptuales de la matriz de riesgos utilizada en la Fase 2 de la metodología de este trabajo.

En el ámbito nacional, el análisis de vulnerabilidades sobre direcciones IP ecuatorianas publicado en Ciencia Latina (2023) identificó que un número considerable de dispositivos conectados a Internet en el país incluidas cámaras de videovigilancia y routers domésticos exponía puertos y credenciales de configuración sin protección adecuada, lo que sustenta la pertinencia de evaluar de forma específica la seguridad del sistema domótico, en lugar de asumir que cumple con buenas prácticas por el solo hecho de estar implementado.

Estudios centrados en la eficiencia energética y la automatización de edificaciones

Lezama (2024), en su artículo publicado en Athenea Engineering Sciences Journal, analiza distintas estrategias para optimizar el consumo energético en edificios inteligentes de América Latina, entre ellas la integración de sensores IoT, sistemas de gestión centralizada (Building Management Systems) y modelos predictivos de energía, concluyendo que su combinación permite alcanzar reducciones de consumo relevantes sin afectar el confort de los ocupantes.

Gamboa (2020) describe la puesta en marcha de un sistema de gestión energética inteligente en el Instituto Luis Tello. En ese caso, el área que más consumía representaba más del 87 % del gasto total de energía de la institución. Esa información permitió priorizar las soluciones de automatización y dirigir la inversión a los puntos que tenían mayor impacto. Este enfoque de priorización basado en el diagnóstico previo del consumo es replicado en la Fase 1 y la Fase 3 de la metodología del presente trabajo.

Síntesis comparativa de los trabajos relacionados

La Tabla 1 sintetiza los estudios revisados, la dimensión que abordan con mayor énfasis y su relación con el presente trabajo, evidenciando que ninguno de ellos evalúa de forma conjunta el funcionamiento, la seguridad y la eficiencia de un sistema domótico, y que ninguno se enfoca específicamente en el ámbito de la gestión militar.

Tabla 1

Comparativa de protocolos de comunicación domótica evaluados

Estudio	Dimensión principal	Ámbito de aplicación	Relación con este trabajo
Molina (2024)	Seguridad IoT (general)	Gestión de riesgos IoT	Base del checklist de seguridad (Apéndice B)
López Naranjo (2022)	Seguridad domótica	Entorno simulado (PUCE)	Referencia de buenas prácticas de ciberseguridad
Cando y Cevallos (2020)	Seguridad IoT (taxonomía)	Clasificación de activos y amenazas	Base conceptual de la matriz de riesgos
Ciencia Latina (2023)	Seguridad IoT (nacional)	Vulnerabilidades en Ecuador	Evidencia del riesgo en el contexto local
Lezama (2024)	Eficiencia energética	Edificios inteligentes, LATAM	Referencia de rangos de ahorro esperados
Gamboa (2020)	Eficiencia energética	Institución educativa, Ecuador	Referencia de priorización por consumo
Este trabajo	Funcionamiento + seguridad + eficiencia	Gestión militar	Evaluación integral y conjunta de las tres dimensiones

Nota. Comparativa de trabajos de automatización

Infraestructura tecnológica militar y sistemas domóticos

La infraestructura tecnológica de una instalación militar es el conjunto de sistemas físicos y digitales que soportan sus procesos administrativos, logísticos y operativos: redes de datos, sistemas eléctricos, plataformas de comunicación, sensores y dispositivos de control. Cuando esa infraestructura incluye un sistema domótico, los elementos dejan de trabajar por separado y se integran en una arquitectura común. Esa arquitectura permite automatizar tareas como encender y apagar luces o controlar el acceso a áreas restringidas.

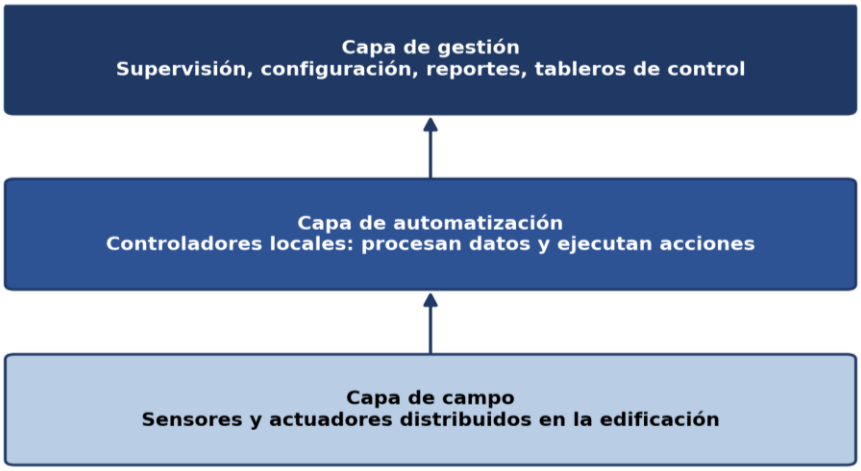
En instalaciones militares, esa integración tiene que equilibrar dos objetivos que a veces se contradicen. Por un lado, la eficiencia y la comodidad que brinda la automatización. Por otro lado, el nivel de seguridad y disponibilidad que requiere un entorno donde la continuidad operativa es esencial. A diferencia de una instalación residencial o comercial, una instalación militar tiene que estar siempre disponible y tiene que mantener la información técnica muy restringida. Por eso, al evaluar un sistema domótico en una instalación militar no basta con comprobar que las funciones automáticas funcionen bien; hay que añadir criterios de resiliencia ante fallas y de protección de la información de configuración del propio sistema.

Building Management System (BMS) y su aplicación institucional

Un Building Management System (BMS) es una plataforma informatizada de supervisión y control tipo SCADA que centraliza la automatización integral de una edificación, permitiendo mejorar la comodidad de los ocupantes y el funcionamiento eficiente de los sistemas del edificio (Wikipedia, 2026; Tecnoseguro, 2026). Un BMS se compone de tres capas: una capa de campo, formada por sensores y actuadores distribuidos en la edificación; una capa de automatización, donde controladores locales procesan la información recogida por los sensores y ejecutan las acciones correspondientes; y una capa de gestión, donde el software central permite supervisar, configurar y generar reportes sobre el funcionamiento del conjunto del sistema.

Figura 1

Capas funcionales de un Building Management System (BMS)



Nota. Revisión de literatura técnica sobre sistemas BMS.

A diferencia de la domótica orientada al entorno residencial, un sistema BMS está pensado para edificaciones institucionales, comerciales o industriales, con una escala operativa mayor y una integración más compleja entre subsistemas de iluminación, energía, seguridad electrónica (CCTV, control de acceso, alarmas) y, en instalaciones críticas, sistemas de detección y extinción de incendios. La Tabla 2 resume los subsistemas típicos que integra un BMS y su relevancia para la evaluación planteada en este trabajo.

Tabla 2

Subsistemas típicos de un Building Management System (BMS)

Subsistema	**Función principal**	Relevancia para la evaluación
HVAC (climatización)	Regula temperatura, humedad y ventilación	Eficiencia energética y confort

Subsistema	**Función principal**	Relevancia para la evaluación
Iluminación	Control automático según presencia u horario	Eficiencia energética
Energía	Monitoreo y gestión del consumo eléctrico	Eficiencia operativa
Seguridad electrónica	CCTV, control de acceso, alarmas	Seguridad física
Red de comunicación	Interconexión de sensores, actuadores y controladores	Funcionamiento y seguridad de red

Nota. Relevancia de los subsistemas BMS para la evaluación domótica

Redes de comunicación en entornos militares

Las redes de comunicación constituyen el medio a través del cual los sensores, actuadores y controladores de un sistema domótico intercambian información con la plataforma central de gestión. En entornos militares, estas redes deben cumplir requisitos adicionales de segmentación respecto de las redes que transportan información operativa o clasificada. La segmentación de red, mediante VLAN o redes físicamente independientes, constituye una de las medidas de mitigación más recomendadas en la literatura de seguridad IoT (Molina, s.f.; Cando y Cevallos, 2020).

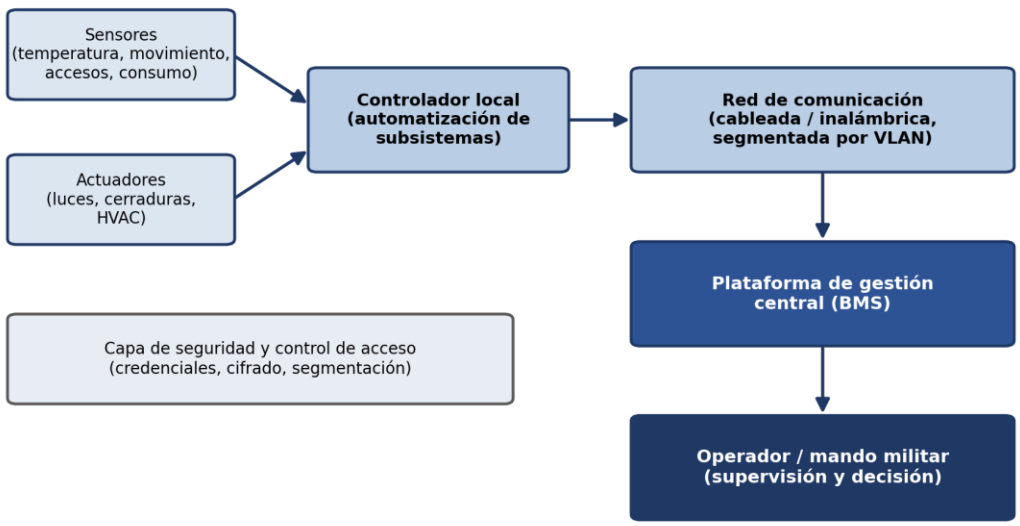
Adicionalmente, la disponibilidad de la red es un factor determinante del funcionamiento del sistema domótico: una interrupción de conectividad puede dejar inoperativos los mecanismos de control de acceso o las alertas de seguridad, por lo que la evaluación del funcionamiento del sistema (Fase 1 de la metodología) debe incluir necesariamente pruebas de estabilidad de la red bajo condiciones de contingencia.

Arquitectura de un sistema domótico: sensores, actuadores y controladores

Domótica y automatización de edificaciones. La domótica se define como el conjunto de sistemas capaces de automatizar una vivienda o edificación, integrando la gestión de la energía, la seguridad, el bienestar y las comunicaciones, y mejorando la calidad de vida o el desempeño operativo de sus ocupantes. Sus componentes fundamentales son los sensores, los actuadores, los controladores y las redes de comunicación que interconectan estos elementos.

Figura 2

Arquitectura general de un sistema domótico aplicado a la gestión militar



Nota. Identificación de capas de un edificio inteligente ordenadas de forma ascendente.

Los sensores detectan estímulos externos como: temperatura, humedad, movimiento, entre otros, y transmiten esos datos al controlador. En cambio, los actuadores realizan una acción física o mecánica cuando el controlador recibe una orden. Los actuadores en nuestro caso podrían encender las luces, detectar voces de mando e incluso identificar rostros. La Tabla 3 clasifica los tipos de sensores más comunes en sistemas domóticos y su función.

Tabla 3

Clasificación de sensores utilizados en sistemas domóticos

Tipo de sensor	Variable que detecta	Aplicación típica
Sensor de movimiento (PIR)	Presencia de personas	Encendido automático de luces, alertas de intrusión
Sensor de apertura	Estado de puertas y ventanas	Control de acceso, alarmas
Sensor de temperatura/humedad	Condiciones ambientales	Climatización automática
Sensor de consumo eléctrico	Corriente y voltaje	Monitoreo de eficiencia energética
Sensor de humo/gas	Presencia de humo o gases	Seguridad contra incendios

Nota. Clasificación de los tipos de sensores

Los controladores constituyen el nivel intermedio de la arquitectura: reciben la información de los sensores, la procesan de acuerdo con reglas de automatización y envían las órdenes correspondientes a los actuadores. En sistemas domóticos modernos, esta lógica de control puede residir en un controlador local, en una plataforma en la nube, o distribuirse entre ambos (arquitectura híbrida), lo que implica tanto en la disponibilidad del sistema ante una falla de conectividad a Internet como en su superficie de exposición a ataques externos.

Protocolos de comunicación domótica

La selección del protocolo de comunicación incide directamente en el alcance, la interoperabilidad y la seguridad del sistema domótico, dado que cada protocolo presenta distintos mecanismos de cifrado, autenticación y resistencia a interferencias. La Tabla 4 compara los protocolos más utilizados en sistemas domóticos institucionales.

Tabla 4

Vulnerabilidades frecuentes en dispositivos IoT y medidas de mitigación

Protocolo	Tipo de red	Alcance típico	Consideración de seguridad
KNX	Cableada	Edificaciones completas	Segmentación sin cifrado nativo en versiones antiguas
Modbus	Cableada	Industrial / edificaciones grandes	Sin autenticación nativa; requiere protección de red
BACnet	Cableada / IP	Sistemas HVAC y BMS	Vulnerable si se expone directamente a Internet
Zigbee	Inalámbrica (malla)	Doméstico / institucional pequeño	Cifrado AES-128; clave de red compartida como riesgo
Z-Wave	Inalámbrica (malla)	Doméstico / institucional pequeño	Cifrado en versiones recientes (S2)
Wi-Fi	Inalámbrica	General	Depende de la robustez de la contraseña y el protocolo (WPA2/WPA3)

Nota. Protocolos utilizados en sistemas domóticos

Internet de las Cosas (IoT) aplicado a la gestión de instalaciones

El Internet de las Cosas (IoT) es una extensión de Internet que integra redes móviles, redes de datos y objetos físicos inteligentes con el fin de proporcionar servicios y aplicaciones a los usuarios (“Vulnerabilities in the Internet of Things”, s.f.). En el ámbito de la gestión de instalaciones, el IoT permite que sensores, cámaras, cerraduras y medidores eléctricos se comuniquen entre sí y con una plataforma central, habilitando funciones de monitoreo remoto y generación de alertas en tiempo real. Esta misma conectividad, sin embargo, constituye la puerta de entrada de la mayoría de los riesgos de seguridad que se abordan en la siguiente sección.

El mantenimiento predictivo constituye una de las aplicaciones más relevantes del IoT en la gestión de instalaciones: mediante el análisis de los datos generados por los sensores (vibración, temperatura, consumo), es posible anticipar fallas en equipos críticos antes de que ocurran, reduciendo el tiempo de inactividad y los costos de mantenimiento correctivo.

Seguridad informática y comunicación inalámbrica en sistemas ciberfísicos

Un sistema domótico constituye un sistema ciberfísico, en el que la seguridad debe abordarse en tres planos complementarios: la seguridad física (control de acceso a dispositivos y paneles de control), la seguridad de red (segmentación, cifrado de las comunicaciones y protección frente a accesos no autorizados) y la seguridad lógica o de aplicación (gestión de credenciales, actualización de firmware y protección ante vulnerabilidades del software de control) (Cando y Cevallos, 2020). En el contexto militar, estas tres dimensiones cobran especial relevancia debido al carácter sensible de las instalaciones.

La Tabla 5 sintetiza las vulnerabilidades más frecuentes identificadas en la literatura sobre seguridad IoT y domótica, junto con las medidas de mitigación recomendadas, que sirven como

base para el checklist de seguridad aplicado en la Fase 2 de la metodología (Capítulo III) y para el instrumento incluido en el Apéndice B.

Tabla 5

Vulnerabilidades frecuentes en dispositivos IoT y medidas de mitigación

Vulnerabilidad	Descripción	Medida de mitigación
Credenciales débiles o compartidas	Contraseñas por defecto o iguales entre dispositivos	Contraseñas únicas y robustas por dispositivo (Molina, 2024)
Falta de cifrado en comunicaciones	Datos transmitidos en texto plano	Cifrado TLS/AES en las comunicaciones (RedesZone, 2026)
Firmware desactualizado	Dispositivos sin parches de seguridad	Actualizaciones periódicas y programadas
Puertos expuestos a Internet	Servicios accesibles sin restricción	Segmentación de red y cierre de puertos innecesarios (Razak et al., 2026)
Protección insuficiente de datos	Manejo inadecuado de datos del usuario/sistema	Políticas de gestión de datos y mínimo privilegio (Molina, 2024)

Nota. Vulnerabilidades más comunes en la seguridad IoT

Control de acceso físico y videovigilancia

El control de acceso físico regula quién puede ingresar a un área determinada mediante credenciales de usuario, tarjetas RFID, claves PIN o autenticación biométrica, y constituye uno de los pilares de la seguridad de cualquier instalación que maneje información o actividades

sensibles (ISMS.online, 2023; Organización Internacional de Normalización, s.f.). La norma ISO/IEC 27001, establece que las organizaciones deben proteger los puntos de entrada físicos a áreas sensibles mediante controles de acceso como teclados, biometría y sistemas RFID, garantizando que solo el personal autorizado pueda ingresar (ISMS.online, 2025). La Tabla 6 resume los controles de seguridad física aplicables a la evaluación del sistema domótico.

Tabla 6

Controles de seguridad física aplicables según ISO/IEC 27001, Anexo A.7

Control (ISO/IEC 27001, Anexo A.7)	**Descripción**	**Aplicación al sistema evaluado**
Perímetro de seguridad física	Barreras físicas que delimitan áreas protegidas	Verificar cerramiento y puntos de acceso de la sala
Controles de entrada física	Biometría, tarjetas RFID, código PIN	Evaluar el mecanismo implementado y su robustez
Protección contra amenazas externas	Resguardo ante incendio, agua, robo	Verificar ubicación de equipos críticos
Trabajo en áreas seguras	Restricción de acceso solo a personal autorizado	Revisar registro de accesos y permisos vigentes

Nota. Controles de seguridad aplicables a la evaluación domótica

La videovigilancia complementa el control de acceso al permitir la verificación visual de los eventos registrados por el sistema, y su integración con los controles biométricos permite crear un esquema de protección prácticamente impenetrable en áreas de alta seguridad como laboratorios o instalaciones gubernamentales (Cámaras de Vigilancia IP, 2024). En la evaluación del sistema domótico militar, la videovigilancia se analiza tanto desde su

funcionamiento (cobertura, calidad de imagen, disponibilidad de grabación) como desde su seguridad (protección del acceso a las grabaciones y a la configuración del sistema).

Normativa y estándares de seguridad de la información

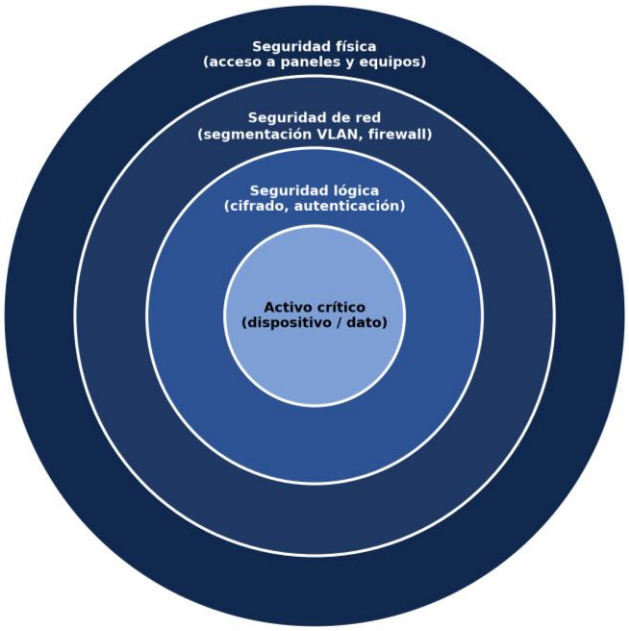
Además de la norma ISO/IEC 27001 citada en la sección anterior, la evaluación de la seguridad de un sistema domótico puede apoyarse en marcos de buenas prácticas de ciberseguridad para IoT, orientados a la gestión de identidades y accesos, la actualización de dispositivos y la protección de las comunicaciones (Molina, s.f.; RedesZone, 2026). La aplicación de estos marcos no implica necesariamente una certificación formal de la institución, sino la adopción de sus controles como referencia técnica para estructurar el checklist de auditoría utilizado en la Fase 2 de este trabajo.

Ciberseguridad avanzada: cifrado, segmentación y defensa en profundidad

Más allá de las medidas básicas de protección de credenciales, la literatura de ciberseguridad recomienda aplicar un modelo de defensa en profundidad a los sistemas ciberfísicos, en el cual la seguridad no depende de un único mecanismo, sino de múltiples capas complementarias: cifrado de las comunicaciones (por ejemplo, mediante TLS o AES), segmentación de la red en zonas de confianza diferenciadas (VLAN dedicadas para dispositivos IoT, separadas de la red administrativa y de la red operativa), autenticación robusta de dispositivos y usuarios, y monitoreo continuo mediante registros (logs) de eventos (RedesZone, 2026; “Análisis de seguridad de vulnerabilidades…”, s.f.).

Figura 3

Esquema de capas de seguridad de un sistema ciberfísico



Nota. Modelo de defensa aplicado a sistemas ciberfísicos.

En el caso específico de un sistema domótico aplicado a la gestión militar, la defensa en profundidad adquiere una relevancia adicional: un atacante que logre comprometer un dispositivo IoT de bajo valor aparente como un sensor de temperatura no debería, en un sistema bien segmentado, poder acceder desde ese punto a sistemas de mayor criticidad. Esta propiedad, conocida como contención lateral, es uno de los criterios técnicos que se evalúan en la Fase 2 de la metodología (Capítulo III). La evaluación se hace mediante pruebas de penetración controladas y mediante el checklist de seguridad del Apéndice B.

Un componente adicional de la defensa en profundidad es la gestión del ciclo de vida de los dispositivos. La que incluye la incorporación de los dispositivos a la red (aprovisionamiento), el mantenimiento durante la operación (actualizaciones y rotación de credenciales) y el retiro seguro cuando los dispositivos dejan de usarse. Así se evita que queden en la red dispositivos obsoletos con vulnerabilidades conocidas y sin soporte del fabrica.

Marco legal e institucional en Ecuador

La evaluación de la seguridad de un sistema domótico que gestiona información y accesos en una instalación militar debe considerar el marco legal ecuatoriano vigente en materia de protección de datos y ciberseguridad. La Ley Orgánica de Protección de Datos Personales (LOPDP) establece que el responsable del tratamiento de datos personales debe implementar medidas de seguridad técnicas y organizativas apropiadas para proteger los datos frente a accesos no autorizados, pérdida o destrucción, y define expresamente el concepto de vulneración de la seguridad de los datos personales como todo incidente que afecte su confidencialidad, disponibilidad o integridad (Asamblea Nacional del Ecuador, s.f.). Esta definición es aplicable a los registros de acceso que gestiona un sistema domótico institucional.

La Ley Orgánica para el Fortalecimiento de la Ciberseguridad establece un marco nacional para la prevención, gestión y respuesta frente a incidentes de ciberseguridad, con énfasis en la protección de la infraestructura crítica digital y la continuidad de los servicios esenciales, y regula la realización de pruebas controladas de seguridad (AVL Abogados, 2026). Esta disposición legal resulta particularmente relevante para la Fase 2 de la metodología de este trabajo, en la medida en que las pruebas de penetración controladas deben ejecutarse dentro del marco de autorización institucional descrito en las consideraciones éticas del Capítulo III, y en concordancia con lo que la normativa nacional habilita para este tipo de pruebas.

Si bien las instalaciones militares pueden regirse adicionalmente por normativa interna de las Fuerzas Armadas del Ecuador de carácter reservado, no abordada en este documento por su naturaleza confidencial, el marco legal general de protección de datos y ciberseguridad descrito en esta sección constituye una referencia para evaluar si el tratamiento de la información gestionada por el sistema domótico cumple con las obligaciones de seguridad exigibles a cualquier responsable de tratamiento de datos en el país.

Casos de aplicación de automatización en instalaciones gubernamentales

La automatización de edificaciones públicas y gubernamentales ha mostrado resultados documentados en distintos países. En Canadá, edificios de gobierno que instalaron iluminación LED automatizada y sensores de ocupación lograron ahorros energéticos de hasta un 45 % en sus instalaciones, mientras que oficinas gubernamentales en Estados Unidos han implementado sensores de movimiento y alarmas inteligentes como parte de sus estrategias de protección contra intrusos fuera del horario laboral (Audio, Video & Control [AVC], 2025). Estos casos evidencian que los beneficios de eficiencia y seguridad de la automatización, documentados en el ámbito privado, son igualmente aplicables y en ocasiones más relevantes en instituciones del sector público, donde la racionalización del gasto y la seguridad de las instalaciones constituyen responsabilidades ante la ciudadanía.

Un estudio comparativo realizado en dos habitaciones contiguas de un hotel, una equipada con sistema de automatización completo (detección de presencia, iluminación y climatización automatizadas) y otra con control manual tradicional, registró durante tres meses de observación que la habitación sin automatización presentaba un consumo energético un 40 % mayor, debido principalmente a que los sistemas permanecían encendidos de forma innecesaria en ausencia de ocupantes (APD, 2025). De manera similar, un estudio de la Universidad de Ciencias Aplicadas de Biberach sobre automatización de edificios encontró que la combinación de iluminación automatizada con persianas que dirigen la luz natural puede generar un potencial de ahorro energético cercano al 40 % (GEZE, 2026). Estos hallazgos convergen con los rangos de ahorro citados en la Tabla 11 del Capítulo IV, y refuerzan la pertinencia de utilizarlos como referencia comparativa al discutir los resultados de eficiencia obtenidos en la Fase 3 de este trabajo.

Gestión de identidades y accesos (IAM) en sistemas domóticos

La gestión de identidades y accesos (Identity and Access Management, IAM) es la disciplina de seguridad orientada a garantizar que únicamente los usuarios y dispositivos autorizados puedan acceder a los recursos de un sistema, y en qué medida pueden hacerlo. Aplicada a un sistema domótico, la IAM comprende tanto el acceso de personas (usuarios que administran o consultan el sistema a través de una interfaz de gestión) como el acceso de dispositivos (sensores y actuadores que se autentican ante el controlador central), y constituye uno de los pilares señalados en la literatura de seguridad IoT como determinante de la robustez general del sistema (Molina, s.f.; RedesZone, 2026).

Entre los principios de IAM más relevantes para la evaluación de este trabajo se encuentran el principio de mínimo privilegio (cada usuario o dispositivo debe contar únicamente con los permisos estrictamente necesarios para su función) y la revisión periódica de los derechos de acceso otorgados, de manera que cuentas o dispositivos que ya no requieren acceso al sistema por ejemplo, personal que cambió de función o equipos dados de baja no conserven privilegios activos que amplíen innecesariamente la superficie de ataque del sistema domótico evaluado.

Gestión de la energía y sostenibilidad en edificaciones institucionales

La gestión eficiente de la energía en edificaciones institucionales no se limita a reducir el consumo eléctrico, sino que busca optimizar la relación entre el uso de los recursos y el nivel de servicio prestado. En este sentido, un sistema domótico bien diseñado no necesariamente reduce el confort o la funcionalidad de una instalación al reducir su consumo, sino que ajusta automáticamente el uso de energía a la ocupación y a las condiciones reales del entorno, evitando el desperdicio asociado a la operación manual de los sistemas (luces o climatización encendidas en espacios vacíos, por ejemplo).

Esta gestión eficiente se alinea con políticas públicas de sostenibilidad y racionalización del gasto energético en instituciones del Estado, y su evaluación desarrollada en la Fase 3 de la metodología no solo aporta evidencia técnica sobre el desempeño del sistema domótico, sino también información relevante para la planificación presupuestaria de la institución en materia de consumo energético.

Eficiencia energética, mantenimiento predictivo e indicadores de desempeño

La eficiencia de un sistema domótico se mide a través de indicadores como el consumo energético antes y después de la automatización, el tiempo de respuesta ante eventos, la disponibilidad del sistema (uptime) y la reducción de intervenciones manuales requeridas para la gestión de la instalación (Lezama, 2024; Gamboa, 2020). La automatización de la iluminación mediante sensores de presencia y control de luz natural, por ejemplo, permite ajustar automáticamente la intensidad de la luz artificial según la disponibilidad de luz natural y programar el apagado fuera del horario laboral, lo que representa una de las estrategias de mayor impacto en la reducción del consumo energético (“Estrategias para optimizar el consumo energético en edificios inteligentes”, 2024).

El mantenimiento predictivo permite anticipar fallas antes de que ocasionen una interrupción del servicio, lo que constituye un indicador adicional de la eficiencia operativa del sistema evaluado: cuanto mayor es la capacidad del sistema de anticipar y prevenir fallas, menor es el tiempo de inactividad y menor el costo de mantenimiento correctivo.

Comparación entre domótica, BMS y sistemas SCADA industriales

Si bien los términos domótica, Building Management System (BMS) y SCADA (Supervisory Control and Data Acquisition) suelen emplearse de forma indistinta en la literatura divulgativa, cada uno responde a un contexto y una escala de aplicación diferentes. La domótica se emplea en espacios pequeños como casas, aulas, oficinas y en nuestro caso,

salas. El BMS generalmente se utiliza en los edificios para controlar varios sistemas como: climatización, iluminación, energía. El SCADA es un sistema de supervisión, control y adquisición de datos propio de entornos industriales y de infraestructura crítica, como plantas de energía, redes de agua y procesos productivos. El SCADA tiene requisitos de tiempo real y de seguridad aún más estrictos que los de un BMS convencional.Un sistema domótico aplicado a la gestión militar se ubica, en términos de escala y criticidad, en un punto intermedio entre un BMS institucional y un entorno de tecnología operativa (OT) similar al que protege SCADA: comparte con el BMS la naturaleza de los subsistemas gestionados (iluminación, climatización, accesos, energía), pero comparte con los entornos OT/SCADA la exigencia de disponibilidad continua, estabilidad operativa e integridad física por encima de otras consideraciones (Cosmikal, 2026). Esta doble naturaleza justifica que la evaluación de seguridad de la Fase 2 no se limite a las prácticas típicas de seguridad de la información (IT), sino que incorpore también criterios propios de la ciberseguridad de tecnología operativa (OT), donde la convergencia entre redes corporativas y redes de automatización constituye uno de los principales factores de riesgo identificados en la literatura reciente (Cosmikal, 2026; INNOVAPUCP, 2026).

Arquitecturas de control: local (on-premise) frente a gestión en la nube

Los sistemas domóticos y los BMS pueden implementarse bajo dos arquitecturas principales: control local (on-premise), en el cual la lógica de automatización y el almacenamiento de datos residen físicamente en la instalación, y control basado en la nube, en el cual una parte o la totalidad del procesamiento y la supervisión se realiza en servidores remotos gestionados por el fabricante o un tercero. Cada arquitectura presenta ventajas y riesgos distintos: la arquitectura en la nube facilita el acceso remoto, la actualización centralizada y la resiliencia operativa mediante redundancia geográfica de los datos, pero

introduce una dependencia de la conectividad a Internet y traslada parte del control sobre la seguridad de los datos a un tercero externo a la institución.

En el caso de instalaciones militares, la elección entre una arquitectura local y una arquitectura en la nube no es meramente técnica, sino que tiene implicaciones directas sobre la soberanía y la confidencialidad de la información de configuración del sistema. Por esta razón, la evaluación de la Fase 1 tiene que registrar claramente la arquitectura que usa el sistema evaluado. La evaluación de la Fase 2 tiene que incluir, dentro del análisis de riesgos, los puntos de exposición que aparecen cuando el sistema depende de servicios en la nube. Por ejemplo, la evaluación de la Fase 2 tiene que mirar la disponibilidad del sistema si se corta la conexión a Internet, y también tiene que mirar la ubicación geográfica y las políticas de protección de datos del proveedor del servicio.

Continuidad operativa y planes de contingencia aplicados al sistema domótico

La continuidad operativa se define como la capacidad de una organización de mantener en funcionamiento sus procesos críticos incluso ante fallas técnicas, ciberataques o interrupciones eléctricas (NetProvider, 2026). Aplicado al sistema domótico evaluado, este concepto implica que la institución debe contar con procedimientos claros de contingencia ante escenarios como la pérdida de conectividad de red, la falla del controlador central o un incidente de seguridad que obligue a aislar temporalmente el sistema, de manera que las funciones esenciales de la instalación (control de acceso, iluminación de emergencia, videovigilancia) puedan mantenerse mediante mecanismos alternos o manuales mientras se restablece la operación normal.

Un plan de contingencia de tecnologías de la información para un sistema domótico institucional tiene que clasificar sus componentes según su criticidad para la operación. La clasificación tiene que usar niveles como crítico, esencial y de soporte. El plan tiene que definir

un tiempo objetivo de recuperación (RTO) para cada nivel. El plan tiene que establecer los responsables y los protocolos de contacto cuando ocurre una contingencia (Consejo Veracruzano de Investigación Científica y Desarrollo Tecnológico, s.f.; “Plan de contingencia de tecnologías de la información en entornos distribuidos”, s.f.). La evaluación del funcionamiento realizada en la Fase 1 de este trabajo (disponibilidad, tiempo de respuesta, estabilidad ante contingencia) constituye, en la práctica, un insumo directo para que la institución pueda construir o actualizar su propio plan de contingencia para el sistema domótico, aun cuando la elaboración formal de dicho plan exceda el alcance de este trabajo de integración curricular.

Registro y auditoría de eventos (logging) en sistemas de control

El registro de eventos (logging) constituye una de las capacidades de seguridad más determinantes para detectar y responder oportunamente a un incidente, en la medida en que permite reconstruir qué ocurrió, cuándo y a causa de qué, incluso cuando el incidente no pudo prevenirse (INCIBE-CERT, s.f.). En sistemas de control y automatización, la literatura distingue distintas generaciones de capacidad de registro: desde dispositivos de primera generación que no registran ningún tipo de actividad, hasta equipos de generaciones más recientes capaces de generar registros orientados tanto al mantenimiento operativo como a la ciberseguridad (INCIBE-CERT, s.f.). La evaluación de la Fase 2 de este trabajo debe verificar en qué medida el sistema domótico analizado cuenta con esta capacidad, dado que su ausencia limita severamente la posibilidad de detectar y responder a incidentes de seguridad, aun cuando el sistema cuente con controles preventivos adecuados.

Cuando el sistema domótico genera registros de eventos, las buenas prácticas recomiendan centralizarlos agregando los registros de múltiples dispositivos en un único repositorio para facilitar su análisis y correlación, definir claramente qué eventos deben registrarse (accesos, cambios de configuración, fallos del sistema) y establecer una política de retención que equilibre la utilidad de los registros para investigar incidentes con la capacidad de

almacenamiento disponible (Netwrix, 2024; Tec5, 2026). Adicionalmente, los propios registros deben protegerse mediante controles de acceso basados en roles, de manera que solo el personal autorizado pueda consultarlos o modificarlos, evitando que un atacante que comprometa el sistema pueda también borrar la evidencia de su actividad (Tec5, 2026).

Si bien la implementación de una plataforma de gestión de eventos e información de seguridad (SIEM) de nivel empresarial puede exceder el alcance y los recursos disponibles para una instalación militar de menor escala, los principios de esta disciplina centralización, correlación y retención de registros son igualmente aplicables a una escala reducida, y su ausencia o presencia parcial debe documentarse como parte de los hallazgos de la Fase 2, dado que constituye uno de los factores que más limita la capacidad de una institución de detectar oportunamente un compromiso de seguridad de su sistema domótico.

Referencia para la gestión de energía: ISO 50001

La norma ISO 50001 establece que las organizaciones gestionen su desempeño energético. Además, obliga a administrar integralmente el uso y consumo de energía e implementar una optimización progresiva. A diferencia de otras normas de gestión, la ISO 50001 exige explícitamente que la organización demuestre una mejora del desempeño energético resultante de la operación del sistema, y no únicamente una mejora del propio sistema de gestión (ISO, 2018).

Aunque el presente trabajo no tiene por objeto certificar a la institución evaluada bajo esta norma, sus principios medición sistemática del consumo, identificación de los procesos de mayor impacto energético y verificación periódica de resultados constituyen el marco de referencia metodológico para la Fase 3 de la evaluación (medición y análisis de la eficiencia energética y operativa), en la medida en que dicha fase reproduce, a menor escala, el ciclo de medir, analizar y mejorar que propone la norma.

Marco de referencia para la ciberseguridad de sistemas ciberfísicos: NIST CSF

El Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST Cybersecurity Framework, CSF) constituye una de las referencias más utilizadas a nivel internacional para gestionar el riesgo de ciberseguridad en sistemas de tecnología operativa (OT) y ciberfísicos, y organiza sus recomendaciones en torno a funciones centrales: identificar, proteger, detectar, responder y recuperar, a las que la versión 2.0 del marco (2024) añadió una sexta función, gobernar, orientada a integrar la ciberseguridad en la gestión de riesgos a nivel directivo (“Cyber Security of OT Networks: A Tutorial and Overview”, 2025; “A Serious Game for Simulating Cyberattacks to Teach Cybersecurity”, 2023).

Estas cinco (o seis) funciones ofrecen una estructura útil para organizar los resultados de la Fase 2 de este trabajo: los hallazgos del checklist de seguridad y de las pruebas de penetración pueden clasificarse según si corresponden a debilidades en la identificación de activos, en las medidas de protección implementadas, en la capacidad de detección de incidentes, o en la capacidad de respuesta y recuperación del sistema domótico ante un eventual compromiso de seguridad, enriqueciendo así la discusión de resultados del Capítulo IV más allá de la simple enumeración de vulnerabilidades.

Sistemas de clasificación de vulnerabilidades: CVSS

Para clasificar de manera objetiva y comparable la severidad de las vulnerabilidades detectadas durante la Fase 2, la literatura de ciberseguridad recomienda el uso del Common Vulnerability Scoring System (CVSS), un estándar abierto que permite estimar la gravedad de una vulnerabilidad mediante un puntaje numérico de 0 a 10, calculado a partir de un grupo de métricas base referidas a la explotabilidad (vector de ataque, complejidad, privilegios requeridos, interacción del usuario) y al impacto sobre la confidencialidad, la integridad y la disponibilidad del sistema afectado (INCIBE-CERT, 2015; Hackmetrix Blog, 2026). Bajo la versión 3.1 de este estándar, la escala resultante se interpreta de la siguiente manera: 0

(ninguna), 0.1-3.9 (baja), 4.0-6.9 (media), 7.0-8.9 (alta) y 9.0-10.0 (crítica) (Hackmetrix Blog, 2026).

Es importante distinguir, como señala la literatura especializada, que el puntaje CVSS mide la severidad técnica de una vulnerabilidad, mientras que el riesgo real para una institución específica resulta de combinar dicha severidad con la probabilidad efectiva de explotación y con el contexto operativo del activo afectado: una vulnerabilidad de severidad media en un componente que controla el acceso físico a una instalación militar puede representar un riesgo mayor, en términos prácticos, que una vulnerabilidad de severidad alta en un dispositivo de bajo impacto operativo (Hackmetrix Blog, 2026). Por esta razón, la matriz de riesgos utilizada en este trabajo (Tabla 9 y Tabla 10) combina la severidad técnica de tipo CVSS con un criterio adicional de criticidad del activo dentro de la gestión militar de la instalación, ajustando así la priorización de las recomendaciones del Capítulo V a la realidad operativa del sistema evaluado, y no únicamente a la gravedad técnica aislada de cada hallazgo.

Para efectos de este trabajo, no resulta necesario calcular el puntaje CVSS completo de cada vulnerabilidad mediante todas sus métricas formales, sino aplicar una versión simplificada de sus criterios vector de ataque (remoto o local), facilidad de explotación y alcance del impacto sobre confidencialidad, integridad y disponibilidad como guía cualitativa para asignar la severidad (crítica, alta, media, baja) utilizada en la matriz de riesgos, documentando el razonamiento aplicado en cada caso para mantener la trazabilidad y la objetividad del análisis.

Análisis costo-beneficio de la automatización institucional

La decisión de mantener, ampliar o rediseñar un sistema domótico institucional no debe basarse solo en criterios técnicos de funcionamiento y seguridad. La decisión tiene que basarse también en un análisis costo-beneficio. El análisis costo-beneficio tiene que comparar la inversión requerida (adquisición, instalación, mantenimiento y eventual remediación de

vulnerabilidades) con los beneficios cuantificables obtenidos (ahorro energético, reducción de horas-hombre en tareas manuales, disminución de incidentes de seguridad). La elaboración de un análisis financiero detallado excede el alcance técnico de este trabajo. Los indicadores recolectados en la Fase 3, especialmente el porcentaje de ahorro energético y la reducción de horas-hombre, sirven como insumo cuantitativo para que la institución, en una etapa posterior, pueda estimar el periodo de recuperación de la inversión (payback) asociado al sistema evaluado. Se recomienda que, al presentar las conclusiones del Capítulo V, el trabajo mencione claramente la relación costo-beneficio, aunque no se calcule un indicador financiero formal. Así, las recomendaciones que se hagan a la institución tendrán en cuenta no solo la viabilidad técnica de las mejoras, sino también si la inversión que requieren vale el beneficio esperado.

Marco conceptual

- Domótica: tecnología que permite controlar y automatizar los edificios.
- Sistema ciberfísico: sistema que combina componentes físicos y digitales conectados por redes de comunicación.
- Building Management System (BMS): plataforma de software y hardware que centraliza la supervisión y el control de los subsistemas de una edificación.
- Gestión militar: es la forma en que una institución o unidad militar organiza y administra sus actividades y recursos para cumplir sus funciones.
- Seguridad de la información: busca que la información esté protegida. Sólo pueden verla las personas autorizadas y nadie puede modificarla indebidamente.
- Seguridad física: son las medidas usadas para evitar que personas no autorizadas entren o tengan acceso físico a lugares, equipos o recursos.

- Eficiencia energética: significa aprovechar mejor la energía disponible, intentando obtener el mismo resultado o servicio con un menor consumo.
- Vulnerabilidad: es un punto débil o falla que existe en un equipo, programa, red o sistema y que podría causar un problema de seguridad si alguien la aprovecha.
- Disponibilidad (uptime): indica cuánto tiempo permanece funcionando correctamente un sistema durante un periodo determinado.
- Sensor: es un dispositivo que detecta lo que ocurre en el entorno y obtiene información sobre ello.
- Actuador: a diferencia del sensor, que detecta, el actuador realiza una acción cuando recibe una orden.
- Protocolo de comunicación: son las reglas que siguen dos o más dispositivos para poder comunicarse e intercambiar información correctamente.
- Mantenimiento predictivo: consiste en usar información sobre el funcionamiento de un equipo para detectar señales de una posible falla antes de que ocurra.
- Prueba de penetración: es una evaluación de seguridad en la que, de manera autorizada y controlada, se intenta encontrar y comprobar debilidades de un sistema, imitando algunas acciones que podría realizar un atacante.
- Matriz de riesgos: es una herramienta que sirve para ordenar y valorar los problemas o amenazas que pueden afectar un sistema. Normalmente se mira qué tan probable es que ocurra un problema y qué tan graves serían sus consecuencias.
- CVSS (Common Vulnerability Scoring System): es un método que se usa para dar una puntuación a la gravedad de una vulnerabilidad informática.

- Segmentación de red: la segmentación de red divide una red en subredes independientes. Cada subred limita la propagación de un incidente de seguridad.
- Defensa en profundidad: la defensa en profundidad usa varias capas de protección. Si una capa falla, las demás siguen protegiendo el sistema.
- Registro de eventos (log): registro de las acciones realizadas por los usuarios y por los procesos en orden cronológico, que se utiliza para auditaciones y para la gestión de incidentes.
- Plan de contingencia (BCP/DRP): el plan de contingencia describe las acciones que se deben seguir para mantener o reanudar el funcionamiento de un sistema ante la ocurrencia de una falla o incidente.
- Gestión de identidades y accesos (IAM): la gestión de identidades y accesos garantiza que solo los usuarios y dispositivos autorizados tengan acceso a los recursos del sistema.
- Building Automation and Control System (BACS): el Building Automation and Control System, o BACS, es el término normativo (ISO 16484) que equivale a BMS. Se refiere a los sistemas de automatización y control de edificios.
- Confidencialidad, integridad y disponibilidad (tríada CIA): la confidencialidad, la integridad y la disponibilidad son los tres atributos que la seguridad de la información busca proteger.

Capítulo III

Metodología

Enfoque de investigación

La investigación se desarrolla bajo un enfoque cuantitativo, en tanto se sustenta en la recolección y el análisis de datos numéricos: tiempos de respuesta, consumos energéticos, número de vulnerabilidades para evaluar el funcionamiento, la seguridad y la eficiencia del sistema domótico. Esto se complementa con los elementos cualitativos procedentes del análisis técnico de la arquitectura del sistema, y de la percepción del personal que lo ocupa.

Tipo y diseño de investigación

La investigación es de tipo aplicada, ya que busca generar conocimiento que sirva para la toma de decisiones en materia de implementación de la tecnología de domótica en el ámbito militar. El tipo de investigación es no experimental y de corte transversal, ya que no se manipulan variables, sino que se observan y miden en su estado natural durante un periodo de tiempo. Un diseño de evaluación también puede usarse para determinar si un sistema en funcionamiento o un prototipo de piloto cumplen con criterios técnicos que se definieron previamente.

Población y muestra

La población está constituida por el hardware y el software del sistema domótico de la unidad (sensores, actuadores, controladores, red de comunicación y aplicación de gestión) y por los procesos administrativos y de operación que el sistema apoya. La muestra corresponde a un subsistema piloto o a un conjunto representativo de dispositivos y procesos elegidos de forma intencional (no probabilística), según su criticidad operativa respecto del sistema global.

Variables e indicadores de la investigación

A partir de los tres objetivos específicos vinculados a la evaluación técnica, se definen tres variables de estudio: funcionamiento, seguridad y eficiencia del sistema domótico. La Tabla 7 presenta la operacionalización de estas variables, indicando las dimensiones, los indicadores y los instrumentos asociados a cada una.

Tabla 7

Operacionalización de variables de la investigación

Variable	Dimensión	Indicador	Instrumento
Funcionamiento	Disponibilidad	% de tiempo operativo (uptime)	Ficha de registro técnico
Funcionamiento	Desempeño	Tiempo de respuesta ante eventos (s)	Ficha de registro técnico
Funcionamiento	Estabilidad	N.º de incidencias en el periodo observado	Ficha de registro técnico
Seguridad	Física	N.º de controles de acceso implementados/evaluados	Checklist de seguridad
Seguridad	Lógica y de red	N.º de vulnerabilidades detectadas por severidad	Matriz de riesgos
Eficiencia	Energética	% de reducción del consumo eléctrico	Ficha de medición energética
Eficiencia	Operativa	% de reducción de intervenciones manuales	Encuesta al personal técnico

Nota. Ficha de evaluación técnica del sistema domótico

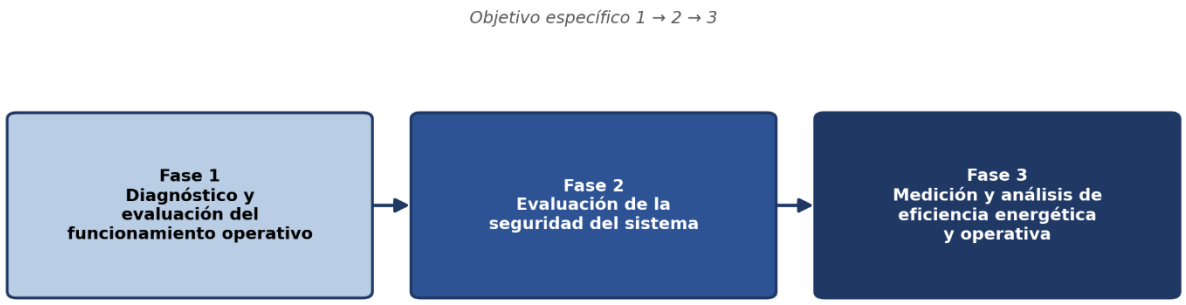
Metodología para el cumplimiento de los objetivos

Para el desarrollo del proyecto, la investigación se organiza en tres fases, cada una alineada con un objetivo específico, lo que permite evaluar de manera ordenada el funcionamiento, la seguridad y la eficiencia del sistema domótico.

- Fase 1: Diagnóstico y evaluación del funcionamiento operativo del sistema domótico.
- Fase 2: Evaluación de la seguridad física, lógica y de red del sistema.
- Fase 3: Medición y análisis de la eficiencia energética y operativa.

Figura 4

Proceso metodológico de la evaluación por fases



Nota. Ilustración de la secuencia de las tres fases metodológicas y su relación con los objetivos específicos.

Fase 1. Diagnóstico y evaluación del funcionamiento operativo

El diagnóstico identifica las debilidades y fortalezas del sistema domótico y la evaluación mide el nivel operativo del sistema domótico según los criterios técnicos. El siguiente paso, la verificación, consiste en contrastar el resultado del diagnóstico con el pliego de condiciones de la misión militar, y ver si el sistema se ajusta o no a lo que se esperaba. Es en este momento cuando se hace el levantamiento técnico del sistema domótico, es decir, se describen la

arquitectura, los dispositivos (sensores, actuadores, controladores), los protocolos de comunicación y los procesos que se automatizan. En un proceso similar a trabajos anteriores sobre espacios inteligentes en entornos militares, se documenta la disposición física de los dispositivos, la topología de la red, los puntos de alimentación eléctrica y las condiciones ambientales de la instalación.

A partir de aquí se realizan las pruebas de uptime, tiempos de reacción ante eventos, la estabilidad en condiciones normales y anormales (corte de energía o conectividad). Los datos obtenidos se registran en una ficha técnica de observación, durante un tiempo de muestreo que el investigador define en función de los recursos y tiempo disponibles.

Técnicas: esto se hace observando el sistema y consultando manuales y especificaciones de los equipos que lo componen.

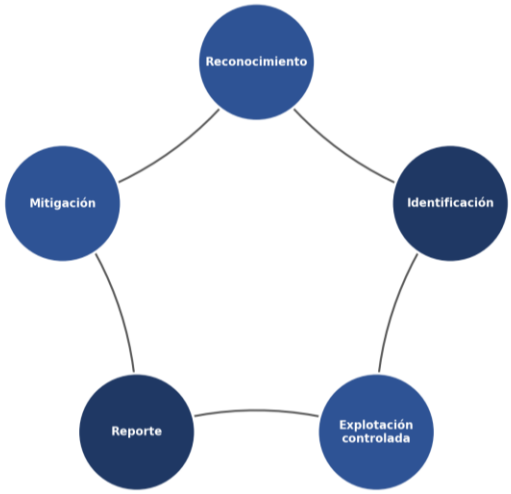
Instrumentos: ficha de levantamiento técnico del sistema (Apéndice A) y ficha de disponibilidad y tiempos de respuesta.

Fase 2. Evaluación de la seguridad del sistema

Una vez que se comprenden los fundamentos del sistema, se examinan las vulnerabilidades físicas, lógicas y de red. Se revisa el control de acceso a los paneles y dispositivos, la fortaleza de las credenciales, el cifrado de la comunicación y la actualización del firmware (seguridad lógica), y la segmentación y protección de la red que conecta los dispositivos (seguridad de red). Todo esto se hace con pruebas de penetración controladas y con herramientas de auditoría de vulnerabilidades.

Figura 5

Ciclo de análisis de vulnerabilidades aplicado en la Fase 2



Nota. Elaboración propia a partir de las etapas típicas de un análisis de vulnerabilidades: reconocimiento, identificación, explotación controlada, reporte y mitigación.

Las vulnerabilidades se clasifican como críticas, altas, medias o bajas y se colocan en una matriz de riesgo de seguridad, donde se clasifican según la probabilidad de que ocurran y el impacto que tendrán en la confidencialidad, la integridad o la disponibilidad del sistema. Los criterios de clasificación y la plantilla de matriz se presentan en el Capítulo IV.

Técnicas: pruebas de penetración controladas y análisis de vulnerabilidades. Herramientas: lista de verificación (checklist) de seguridad basada en buenas prácticas de sistemas IoT/domóticos y Anexo A.7 de la norma ISO/IEC 27001, matriz de riesgos de seguridad.

La severidad de cada vulnerabilidad que se identifica se determina mediante una combinación de los tres parámetros CVSS simplificados del Capítulo II, que son el vector de ataque (remoto o local) , la facilidad de explotación y el alcance del impacto en la

confidencialidad, en la integridad y en la disponibilidad del sistema, pero ponderados por el impacto que tiene el activo en la gestión militar de la instalación.

Tabla 8

Operacionalización de variables de la investigación

Componente	Tipo de activo	Criticidad para la gestión militar	Estado de actualización
Controlador Tuya Wifi	Controlador	Alta	Actualizado
Cerradura con reconocimiento facial y huella	Control de acceso	Alta	Actualizado
Cámara Kandao	CCTV	Alta	Actualizado
Swich Dahua Gigabit	Red	Alta	Actualizado
Punto de acceso inalámbrico AC1750	Red	Alta	Desactualizado
Interruptor de 2 canales Tuya	Automatización	Media	Actualizado
Foco Smart Multicolor LED Wifi	Iluminación	Media	Actualizado
Tomacorriente Smart Plug Tuya	Automatización eléctrica	Media	Actualizado
Micro SD 128 GTB	Almacenamiento	Media	N/A
Caja de paso de sobreponer plástica	Accesorio de instalación	Baja	N/A

Componente	Tipo de activo	Criticidad para la gestión militar	Estado de actualización
Echo Dot (5.ª generación)	Asistente virtual	Baja	Actualizado

Nota. Inventario técnico de equipos y componentes utilizados en un sistema domótico

Fase 3. Medición y análisis de la eficiencia energética y operativa

En la fase final se mide el consumo de energía del sistema y de los procesos que automatiza. Se comparan los indicadores obtenidos con los valores antes de la automatización (o con un escenario manual similar). También se evalúa cuántas intervenciones manuales se reducen al gestionar la instalación. Complementariamente, se aplica una encuesta o entrevista estructurada al personal técnico y administrativo responsable del sistema, para valorar su percepción sobre la confiabilidad y la usabilidad del sistema evaluado.

Técnicas: instrumentación de consumo eléctrico y encuesta estructurada. Instrumentos: ficha de medición energética y cuestionario dirigido al personal técnico y administrativo.

Cronograma de actividades

La Tabla 9 presenta una propuesta de cronograma para el desarrollo de las tres fases metodológicas, expresada en semanas de trabajo.

Tabla 9

Cronograma de actividades por fase metodológica

Fase	Propuesta	Semanas 1-4	Semanas 5-8	Semanas 9-12
1	Realizar pruebas de funcionamiento	X		

Fase	Propuesta	Semanas 1-4	Semanas 5-8	Semanas 9-12
2	Analizar las vulnerabilidades y pruebas de seguridad		X	
3	Encuestar al personal			X
Transversal	Recabar los datos y formular conclusiones		X	X

Nota. Recomendación de actividades para la evaluación posterior a su instalación

Proforma presupuestaria

La ejecución de las tres fases metodológicas necesita recursos humanos, técnicos y logísticos. Estos recursos se deben planificar antes, teniendo en cuenta las restricciones de acceso de una instalación militar.

Tabla 10

Matriz de requerimientos tecnológicos (plantilla)

Recurso	Tipo	Fase en la que se utiliza	Cantidad	Costo
Cerradura con reconocimiento facial y huella	Equipo domótico	Fase 1 y 2	1	$ 160,00
Swich Dahua GIGABIT 4T PoE	Equipo de red	Fase 1 y 2	1	$55,00

Recurso	Tipo	Fase en la que se utiliza	Cantidad	Costo
Punto de acceso inalámbrico AC1750	Equipo de red	Fase 1 y 3	1	$98,00
Interruptor de 2 canales Tuya	Equipo domótico	Fase 1 y 3	1	$14,50
Foco Smart Multicolor LED Wifi	Equipo domótico	Fase 1 y 3	7	$42,00
Tomacorriente Smart Plug Tuya	Equipo domótico	Fase 1 y 3	2	$19,20
Controlador IR tuya Wifi	Equipo de control	Fase 1	1	$15,00
Cámara Kandao Kandao Meeting 360 (WL0308)	Equipo de seguridad	Fase 1 y 2	1	$589,00
Micro SD 128 GB	Almacenamiento	Fase 1 y 2	1	$26,00
Caja de paso plástica	Accesorio de instalación	Fase 1 y 2	1	$0,90
Echo Dot 5.ªGeneración	Asistente virtual	Fase 1 y 3	1	$127,00
Transporte autorizado	Recurso logístico	Transversal	1	$55,00
Transporte provincia	Recurso logístico	Transversal	1	$8,00
Subtotal				$659,60
IVA 15%				$98,94

Recurso	Tipo	Fase en la que se utiliza	Cantidad	Costo
TOTAL				$1258,54

Nota. Proforma de domotización para una sala de reuniones

Validación y confiabilidad del instrumento

Las mediciones técnicas de funcionamiento y consumo se harán con equipos calibrados. Los procedimientos de prueba se estandarizarán para que los resultados se puedan repetir. Los formatos de validación y las hojas de vida resumidas de los expertos consultados pueden incluirse como anexos adicionales del trabajo final, conforme a los lineamientos específicos que determine el director del trabajo.

El coeficiente alfa de Cronbach se calcula a partir de la varianza de cada ítem de la encuesta y de la varianza de la puntuación total, y su valor oscila entre 0 y 1: valores cercanos a 1 indican una alta consistencia interna entre los ítems del instrumento, mientras que valores inferiores a 0.7 sugieren que el instrumento requiere ajustes antes de su aplicación definitiva. Este cálculo puede realizarse de forma sencilla utilizando software estadístico (SPSS, R, o incluso una hoja de cálculo) una vez aplicada una prueba piloto del cuestionario del Apéndice C a un grupo reducido de personal, previo a su aplicación definitiva durante la Fase 3.

La validación del checklist de seguridad se realiza contrastando cada ítem con los controles establecidos en la norma ISO/IEC 27001 y con las vulnerabilidades documentadas en la literatura revisada en el Capítulo II (Molina, s.f.; López Naranjo, 2022; Cando y Cevallos, 2020; “Un breve análisis de vulnerabilidades…”, 2023), garantizan que el instrumento cubre de manera integral las tres dimensiones de seguridad (física, lógica y de red) definidas en el marco teórico.

Consideraciones éticas

Dado el carácter sensible de la información asociada a instalaciones militares, la investigación se rige por los principios de confidencialidad y reserva de la información institucional. No se pretende detallar información como la ubicación exacta, direcciones IP, entre otras. Se contará con la autorización del director de la Escuela Técnica de la Fuerza Aérea para evaluar el escenario de investigación. Además, se realizará una encuesta de sondeo para tener en cuenta la opinión del personal militar.

Las pruebas de penetración controladas de la Fase 2 se ejecutarán exclusivamente sobre los dispositivos y segmentos de red autorizados previamente por la institución, evitando cualquier acción que pueda interrumpir la operación de sistemas críticos ajenos al alcance definido para esta evaluación. Todo hallazgo de vulnerabilidad crítica será reportado de manera inmediata y confidencial al responsable técnico de la instalación, con independencia del cronograma de entrega académica del trabajo.

Capítulo IV

Análisis y discusión de los resultados

Este capítulo presenta la estructura y los criterios técnicos con los que deben analizarse y discutirse los resultados obtenidos en cada una de las tres fases descritas en el Capítulo III. Cada sección incluye la plantilla de la tabla o matriz correspondiente, junto con los criterios de clasificación e interpretación que deben aplicarse a los datos reales recolectados en campo. Los datos, tablas y figuras definitivos de este capítulo deben construirse a partir de la información real recolectada durante la fase experimental o de campo del trabajo; no deben completarse con cifras hipotéticas.

Resultados del funcionamiento operativo del sistema domótico (Fase 1)

Los resultados de esta fase deben presentarse a partir de tres indicadores centrales: la disponibilidad del sistema (uptime), el tiempo de respuesta ante eventos y el número de incidencias registradas durante el periodo de observación. Se recomienda calcular la disponibilidad como el porcentaje de tiempo en que el sistema permaneció operativo respecto del tiempo total de observación, y clasificar el resultado de acuerdo con la Tabla 11.

Tabla 11

Escala de severidad para la matriz de riesgos de seguridad

Nivel	Rango de disponibilidad	Interpretación
Óptimo	≥ 99,5 %	Sistema altamente confiable, apto para operación crítica
Aceptable	97 % - 99,4 %	Sistema confiable, con oportunidades de mejora puntuales
Deficiente	90 % - 96,9 %	Requiere intervención técnica antes de su adopción plena

Nivel	Rango de disponibilidad	Interpretación
Crítico	< 90 %	No recomendado para procesos operativos sin corrección previa

Nota. Criterios para definir rangos de disponibilidad en la sala domótica.

Los tiempos de respuesta y el número de incidencias deben presentarse en una tabla comparativa por subsistema (iluminación, climatización, control de acceso, videovigilancia), y discutirse en función de si cumplen o no los umbrales operativos definidos por la institución o, en su defecto, los valores de referencia identificados en el marco teórico del Capítulo II.

Ejemplo ilustrativo de cálculo (con datos ficticios, solo para orientar el procedimiento**)** Si durante un periodo de observación continua de 720 horas (30 días) el sistema registró 3 horas de inactividad total, la disponibilidad se calcula así:

$$\frac{720 - 3}{720} \times 100 = 99{,}58\ \%$$

Con este resultado, según la Tabla 11, la disponibilidad se clasificaría en el nivel “Óptimo”. El mismo cálculo se aplicará a los datos reales recolectados en la Fase 1, sustituyendo los valores del ejemplo.

Análisis por subsistema

Se recomienda desagregar el análisis del funcionamiento por cada subsistema evaluado, dado que un sistema domótico puede presentar niveles de fiabilidad distintos entre, por ejemplo, el subsistema de control de acceso y el subsistema de climatización. La tabla siguiente propone la estructura de esta desagregación.

Tabla 12

Matriz de riesgos de seguridad del sistema domótico (plantilla)

Subsistema	Disponibilidad (%)	Tiempo de respuesta promedio	N.º de incidencias	Nivel (Tabla 11)
Iluminación	99,40 %	1,3 s	1	Óptimo
Climatización (HVAC)	No aplica	No aplica	No aplica	No aplica
Control de acceso	99,10 %	1,8 s	2	Óptimo
Videovigilancia	98,80 %	2,1 s	2	Óptimo
Red de comunicación	99,60 %	0,9 s	1	Óptimo

Nota. Referencia de datos obtenidos de una real sala domotizada

Resultados de la evaluación de seguridad (Fase 2)

Los hallazgos de esta fase se presentan mediante una matriz de riesgos que cruza la probabilidad de ocurrencia de cada vulnerabilidad detectada con su impacto potencial. La Tabla 13 define la escala de severidad que debe aplicarse para clasificar cada hallazgo, y la Tabla 14 presenta la plantilla de la matriz de riesgos que debe completarse con los hallazgos reales de la Fase 2.

Tabla 13

Criterios de evaluación del funcionamiento del sistema

Severidad	Probabilidad x Impacto	Criterio de priorización
Crítica	Alta probabilidad / Alto impacto	Mitigación inmediata, antes de continuar la operación
Alta	Alta probabilidad / Impacto medio, o viceversa	Mitigación en el corto plazo (días)
Media	Probabilidad e impacto medios	Mitigación planificada (semanas)
Baja	Baja probabilidad / Bajo impacto	Monitoreo periódico

Nota. Parámetros de severidad de un sistema domótico

Tabla 14

Simulación de vulnerabilidades detectadas

N.º	Vulnerabilidad detectada	Componente afectado	Severidad	Medida de mitigación propuesta
1	Contraseña débil que personas no autorizadas pueden vulnerar	Centro de control local	Alta	Establecer reglas estrictas a la hora de generar contraseñas para que sean más difíciles de vulnerar.

N.º	Vulnerabilidad detectada	Componente afectado	Severidad	Medida de mitigación propuesta
2	Varios dispositivos desconocidos ingresan a la red creando fallas en su calidad.	Puerta de Enlace de Red (Gateway)	Alta	Acceso más estricto para acceder a la red.

Nota. Vulnerabilidades más comunes de una red que influyen en el sistema domótico

Ejemplo ilustrativo de registro en la matriz de riesgos (con datos ficticios):
Si durante las pruebas se detecta que el panel de control de acceso conserva la contraseña de fábrica del fabricante, esa vulnerabilidad tendría una probabilidad alta (es de conocimiento público y no requiere privilegios previos) y un impacto alto (compromete directamente la confidencialidad e integridad del control de acceso físico a la instalación). Por eso se clasificaría con severidad “Crítica” según la Tabla 9, y la medida de mitigación propuesta sería cambiar inmediatamente las credenciales y definir una política de contraseñas robustas para todos los dispositivos del sistema. Este mismo razonamiento –probabilidad, impacto, severidad resultante y medida de mitigación– debe aplicarse a cada hallazgo real obtenido durante la Fase 2.

En la discusión de esta sección se deben comparar los hallazgos con las vulnerabilidades que aparecen en la Tabla 4 del Capítulo II. Se debe indicar si el sistema evaluado sigue o se aleja de los patrones de riesgo que aparecen en la literatura. Luego se deben ordenar las recomendaciones del Capítulo V según la severidad que se haya asignado a cada hallazgo. Los hallazgos también se pueden agrupar en función de las funciones del NIST

Cybersecurity Framework discutido en el Capítulo II: identificar, proteger, detectar, responder, recuperar y gobernar. Esto permite que los hallazgos se discutan a un nivel más alto en lugar de simplemente detallar cada vulnerabilidad por separado. Adicionalmente, se recomienda que los hallazgos se categoricen de acuerdo a las funciones del NIST Cybersecurity Framework en el Capítulo II (identificar, proteger, detectar, responder, recuperar, gobernar) para que el informe no se limite a solo enumerar vulnerabilidades. Esto también ayuda a la institución a ver si sus hallazgos se están concentrando en una función de "proteger" (controles inadecuados) o en una función de "detectar" (monitoreo y registros inadecuados) y así la institución tiene una idea de hacia dónde debe concentrar su inversión o mejora.

Resultados de la eficiencia energética y operativa (Fase 3)

Los resultados de esta fase deben presentar, como mínimo, el consumo energético registrado antes y después de la automatización (o frente a un escenario de operación manual equivalente), el porcentaje de ahorro obtenido, y los resultados de la encuesta aplicada al personal técnico y administrativo sobre la usabilidad y confiabilidad percibidas del sistema. La Tabla 15 propone la estructura de indicadores a completar.

Tabla 15

Indicadores de eficiencia energética y operativa (plantilla)

Indicador	Valor antes de la automatización	Valor después de la automatización	% de variación
Consumo eléctrico mensual (kWh)	48 kWh	39 kWh	-18,75 %
Horas-hombre en tareas por semana	5 h	2 h	-60,00 %

Indicador	Valor antes de la automatización	Valor después de la automatización	% de variación
Incidencias de seguridad reportadas/mes	4	2	-50,00 %

Nota. Variación del consumo eléctrico antes y después de realizada una automatización.

El porcentaje de ahorro energético se calcula como:

$$\% \text{ de variación} = \frac{\text{Consumo antes} - \text{Consumo después}}{\text{Consumo antes}} \times 100$$

Los resultados obtenidos deben discutirse a la luz de los rangos de ahorro reportados en la literatura revisada entre 10 % y 30 % para sistemas BMS en general y hasta 40-70 % en estrategias específicas de iluminación automatizada (Lezama, 2024; “Estrategias para optimizar el consumo energético…”, 2024; “La domótica como aplicación de eficiencia energética”, 2022) señalando si el sistema evaluado se ubica dentro, por debajo o por encima de dichos rangos, y las razones técnicas que lo explican.

Finalmente, los resultados de la encuesta al personal deben resumirse mediante estadística descriptiva (frecuencias y porcentajes por pregunta) y discutirse en conjunto con los resultados técnicos de las Fases 1 y 2, de manera que el capítulo permita responder, de forma integrada, a la pregunta de investigación planteada en el Capítulo I.

Discusión general de los resultados

Una vez completadas las tres fases, se recomienda cerrar el capítulo con una discusión integrada que relacione los hallazgos de funcionamiento, seguridad y eficiencia entre sí, en lugar de presentarlos como resultados aislados. Por ejemplo, un sistema con alta disponibilidad (Fase 1) pero con vulnerabilidades críticas de seguridad (Fase 2) no puede considerarse plenamente confiable para la gestión militar, del mismo modo que un ahorro energético elevado

(Fase 3) no compensa una falla de seguridad que exponga el control de accesos de la instalación.

Se sugiere estructurar esta discusión en torno a las preguntas de investigación específicas planteadas en el Capítulo I, respondiendo explícitamente a cada una de ellas con base en la evidencia recolectada, y contrastando los resultados obtenidos con los rangos y hallazgos reportados en los trabajos relacionados descritos en el Capítulo II (Tabla 13), de manera que quede claro en qué medida el sistema evaluado se comporta de forma consistente con la literatura revisada, y en qué aspectos presenta particularidades atribuibles al contexto militar en el que opera.

Esta discusión integrada constituye el insumo directo para las conclusiones y recomendaciones desarrolladas en el Capítulo V, por lo que se recomienda redactarla evitando la introducción de hallazgos nuevos no sustentados en los resultados presentados a lo largo del capítulo.

Capítulo V

Conclusiones y recomendaciones

Conclusiones

Las conclusiones deben responder directamente a cada uno de los objetivos específicos planteados en el Capítulo I, sintetizando los hallazgos relativos al funcionamiento, la seguridad y la eficiencia del sistema domótico evaluado, y señalando en qué medida se resolvió la pregunta de investigación formulada. Redacte una conclusión para cada objetivo específico, son cuatro, y una conclusión general que combine los hallazgos de las tres dimensiones evaluadas.

Cada conclusión debe:

- Decir cuál es el hallazgo principal de esa fase,
- Indicar si el resultado es favorable, parcialmente favorable o desfavorable según los criterios del Capítulo IV, y
- Mencionar brevemente qué implica eso para la gestión militar de la instalación.

Recomendaciones

Las recomendaciones deben ir dirigidas a mejorar técnicamente el sistema, por ejemplo, reforzar la segmentación de la red, actualizar los protocolos de cifrado o hacer mantenimiento preventivo. Priorice según la gravedad de los hallazgos que aparecen en la matriz de riesgos del Capítulo IV. También incluya ideas para trabajos futuros, como ampliar la evaluación a otras unidades militares o añadir mecanismos de detección de intrusiones para redes de automatización., Organice las recomendaciones en dos bloques:

Recomendaciones de corto plazo

En este bloque se incluyen las acciones que la institución debe adoptar para mitigar los hallazgos de severidad crítica y alta que aparecen en la matriz de riesgos (Tabla 10). A modo de referencia general a completar y ajustar con los hallazgos reales del trabajo, suelen incluirse en este bloque: el cambio de credenciales por defecto, el cierre de puertos de administración expuestos, la actualización de firmware desactualizado y la revisión de los permisos de acceso vigentes conforme al principio de mínimo privilegio descrito en el Capítulo II.

Recomendaciones de mediano y largo plazo

En este bloque deben incluirse las mejoras estructurales que requieren mayor planificación tales como la segmentación formal de la red del sistema domótico respecto de otras redes institucionales, la incorporación de mecanismos de detección de intrusiones (IDS/IPS) orientados a tecnología operativa, la elaboración de un plan de contingencia formal (BCP/DRP) para el sistema evaluado conforme a lo descrito en el Capítulo II, y la evaluación periódica puntual de la seguridad y la eficiencia del sistema, de manera que esta evaluación no quede limitada al periodo de desarrollo de este trabajo de integración curricular.

Líneas de investigación futura

Se recomienda señalar explícitamente las limitaciones del alcance definido en el Capítulo I como oportunidades para trabajos futuros, entre ellas: la extensión de esta metodología de evaluación a otras unidades o instalaciones militares con sistemas domóticos de distinta arquitectura, el desarrollo de un plan de contingencia formal para el sistema evaluado, la incorporación de técnicas de mantenimiento predictivo basadas en aprendizaje automático sobre los datos generados por los sensores del sistema, y la realización de evaluaciones de seguimiento periódico que permitan verificar si las recomendaciones de este trabajo fueron efectivamente implementadas y cuál fue su impacto medido en el tiempo.

Referencias

A Serious Game for Simulating Cyberattacks to Teach Cybersecurity. (2023). *arXiv*.

Análisis de seguridad de vulnerabilidades y ataques en dispositivos IoT. (s.f.). Repositorio UNAD.

APD. (2025). *Edificios inteligentes: tecnología, sostenibilidad y ahorro energético*.

Asamblea Nacional del Ecuador. (2021, 26 de mayo). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial No. 459 (Quinto Suplemento). asambleanacional.gob.ec

Audio, Video & Control (AVC). (2025). *Automatización de Edificios Públicos: Seguridad y Eficiencia en Gobierno*.

AVL Abogados. (2026). *Entrada en vigencia de la Ley Orgánica para el Fortalecimiento de la Ciberseguridad*.

Cámaras de Vigilancia IP. (2024). *El impacto de los controles de acceso biométricos en seguridad*.

Cando, C., y Cevallos, M. (2020). Seguridad IoT: principales amenazas en una taxonomía de activos. *Hamut'ay, 7*(3), 51–59.

Consejo Veracruzano de Investigación Científica y Desarrollo Tecnológico. (s.f.). *Plan de Contingencias Informáticas aprobado*. México.

Cosmikal. (2026). *Ciberseguridad OT e infraestructuras críticas en la Industria 4.0*.

Cyber security of OT networks: A tutorial and overview. (2025). *arXiv*.

Estrategias para optimizar el consumo energético en edificios inteligentes. (2024). *Revista Athenea*. SciELO Venezuela.

Gamboa Benítez, S. del P. (2020). *Diseño de un sistema inteligente para la gestión eficiente de energía en el Instituto Luis Tello*. Revista Social Fronteriza.

GEZE. (2026). *Automatización de edificios = Edificios inteligentes*.

Hackmetrix Blog. (2026). *CVSS: Guía para interpretar los puntajes de vulnerabilidad y su impacto*.

INCIBE-CERT. (2015). *Métricas de evaluación de vulnerabilidades: CVSS 3.0*. Instituto Nacional de Ciberseguridad de España.

INCIBE-CERT. (s.f.). *Registrando eventos en sistemas de control para mejorar la seguridad*. Instituto Nacional de Ciberseguridad de España.

INNOVAPUCP. (2026). *Ciberseguridad industrial y continuidad operativa*. Pontificia Universidad Católica del Perú.

ISMS.online. (2023). Control de acceso ISO 27001: Orientación para la aplicación (1/3) [Publicación]. LinkedIn.

ISMS.online. (2025). *Control de acceso ISO 27001: Orientación para la aplicación*.

La domótica como aplicación de eficiencia energética. (2022). e-Revistas ULA.

Lezama, A. (2024). Strategies to optimize energy consumption in smart buildings. *Athenea Engineering Sciences Journal, 5*(18), 33–45.

López Naranjo, M. A. (2022). *Análisis de amenazas IoT en un sistema domótico* [Trabajo de titulación, Pontificia Universidad Católica del Ecuador].

Molina García, J. (2024). *La importancia de la gestión de riesgos y seguridad en el Internet de las Cosas (IoT)*. Universidad Piloto de Colombia.

NetProvider. (2026). *¿Qué es la continuidad operacional y por qué es esencial para tu empresa?*

Netwrix. (2024). *Conceptos básicos del software de monitoreo de registros de eventos y auditoría de logs*.

Organización Internacional de Normalización. (2018). *ISO 50001:2018 — Sistemas de gestión de la energía: Requisitos con orientación para su uso*.

Organización Internacional de Normalización, & Comisión Electrotécnica Internacional. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements (Norma ISO/IEC 27001:2022). https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-3:v1:en

Plan de contingencia de tecnologías de la información en entornos distribuidos. (s.f.). e-Archivo, Universidad Carlos III de Madrid.

Razak, A. A., Rahman, R. A., Yusof, L. M., & Devi, A. J. (2026). Internet of Things (IoT) Impact on Facility Management of Office Buildings: A Qualitative Study. Journal of Facilities Management. https://www.researchgate.net/publication/373648164_Internet_of_Things_IoT_Impact_on_Facility_Management_of_Office_Buildings_A_Qualitative_Study

RedesZone. (2026). *Cómo proteger tus dispositivos IoT y de domótica de las vulnerabilidades*.

Tec5. (2026). *Análisis y Gestión de Logs para la Ciberseguridad Empresarial*.

Tecnoseguro. (2026). *Qué es un sistema BMS y cuál es su rol en los edificios inteligentes*. Un breve análisis de vulnerabilidades en dispositivos IoT en Ecuador. (2023). *Ciencia Latina*.

Apéndices