RESUMEN – TRABAJO DE GRADO

AUTORES	Yeison Rafael Navarro Mendoza
FACULTAD	Facultad de Ingeniería
PLAN DE ESTUDIOS	Maestría en Gobierno de TI
DIRECTOR	Dairon Torrado Castro
CODIRECTOR (si aplica)	No Aplica
TÍTULO DE LA TESIS	Diseño de un modelo de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey S.A.
TITULO EN INGLES	Design of an information security model for the cold chain supervision system in Camagüey S.A.

RESUMEN
(70 palabras)

El objetivo del documento se centró en diseñar un modelo de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey S.A., uno de los principales hallazgos fue el análisis exhaustivo del estado actual del sistema de supervisión de la cadena de frío en Camagüey S.A., la validación del modelo por parte de expertos confirmó su viabilidad y aplicabilidad.

RESUMEN EN INGLES

The objective of the document focused on on designing an information security model for the cold chain for the cold chain supervision system in Camagüey S.A., one of the main findings was the exhaustive analysis of the current state of the one of the main findings was the exhaustive analysis of the current state of the cold chain the current state of the cold chain supervision system at Camagüey S.A., the validation of the model by experts confirmed its viability and applicability. its viability and applicability.

PALABRAS CLAVES	Seguridad, Información, Tecnología, Gobierno, Supervisión
PALABRAS CLAVES EN INGLES	Security, Information, Technology, Governance, Oversight

CARACTERÍSTICAS

PÁGINAS: 98	PLANOS:	ILUSTRACIONES:	CD-ROM:

Diseño de un modelo de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey S.A.

Yeison Rafael Navarro Mendoza

Facultad de Ingeniería, Universidad Francisco de Paula Santander Ocaña

Maestria en Gobierno de TI

Magister Dairon Torrado Castro

31 de mayo de 2025

Índice

Capitulo 1. Modelo de seguridad de la información en el sistema de supervisión de la cadena de frío de los productos cárnicos en Camagüey S.A. 9

1.1 Planteamiento del problema 9

1.2 Formulación del problema 12

1.3 Objetivos 13

1.3.1 Objetivo general 13

1.3 .2 Objetivos específicos 13

1.4 Justificación 14

1.5 Delimitaciones 16

1.5.1 Delimitación conceptual 16

1.5.2 Delimitación geográfica 16

1.5.3 Delimitación temporal 16

1.5.4 Delimitación operativa 16

Capitulo 2. Marco referencial 18

2.1 Marco histórico 18

2.1.1 Antecedentes. 18

2.2 Marco conceptual 24

2.3 Marco contextual 27

2.4 Marco teórico 32

2.5 Marco legal 37

Capitulo 3. Diseño metodológico 41

3.1 Tipo de investigación 41

3.2 Seguimiento metodológico del proyecto. 41

3.3 Población 44

3.4 Muestra 44

3.5 Técnicas de recolección de la información 44

Capítulo 4. Resultados 45

Conclusiones 82

Lista de figuras

Figura 1. Cifras productivas Camagüey S.A. Fuente: Camagüey S.A. 28

Figura 2. Trazabilidad de procesos de la empresa Camaguey S.A. Fuente: Camaguey S.A. 28

Figura 3. Certificaciones de Camaguey S.A Fuente: Camaguey S.A. 31

Figura 4. Procesos de aseguramiento de la calidad..... 32

Figura 5. Dominios de ISO 27000. Fuente: Adaptado de la Norma ISO/IEC 270001.... 34

Figura 6. Cascada de metas de COBIT 2019. Fuente: ISACA. 35

Figura 7. Principios de COBIT 2019. Fuente: ISACA. 36

Figura 8. Dominios de COBIT 2019. Fuente: ISACA..... 36

Figura 9. Modelo Core de COBIT 2019. Fuente: ISACA. 37

Figura 10. Sistema de refrigeración. 47

Figura 11. Sistema electrónico para control de refrigeración. 47

Figura 12. Controlador de IOT. 47

Figura 13. Cuartos de refrigeración o cavas. 48

Figura 14. Monitoreos de sistema de refrigeración. 48

Figura 15. Supervisión de la cadena de frío en Camagüey S.A. 70

Figura 16. Modelo MSISSCF. 75

lista de tablas

Tabla 1. *Marco normativo Colombia.*..... 38

Tabla 2. Matriz de Objetivos. Fuente: Autor. 41

Tabla 3. Ind. 1. Cuadro de diagnóstico de seguridad de la información. Fuente: Autor.46

Tabla 4. *Mecanismos de protección.*..... 49

Tabla 5. *Áreas de mejora.* 50

Tabla 6. *Ind. 2. Lista documentada de vulnerabilidades encontradas* 52

Tabla 7. *Riesgos en los dispositivos IoT.* 52

Tabla 8. *Ind. 3. Cuadro de análisis de políticas de seguridad y su aplicabilidad.*..... 54

Tabla 9. *Deficiencias en seguridad.*..... 55

Tabla 10. *Ind. 4 . Cuadro de análisis comparativo de estándares internacionales*..... 59

Tabla 11. *Ind. 4. Análisis Taxonómico de Estudios sobre Seguridad en la Cadena de Frío con IoT.* 62

Tabla 12. *Ind. 5. Listado estructurado de mejores prácticas recomendadas.* 66

Tabla 13. *Coeficiente de argumentación.* 78

Apéndice

Apéndice A. *Formulario de Evaluación de Competencia del Experto*..... 96

Introducción

En la actualidad, la industria cárnica enfrenta desafíos significativos en términos de calidad y seguridad alimentaria, especialmente en la gestión de la cadena de frío. La compañía Camagüey S.A., dedicada a la producción y distribución de productos cárnicos en Colombia, ha implementado un sistema de supervisión de la cadena de frío basado en tecnologías IoT para garantizar la conservación óptima de sus productos. Sin embargo, la creciente digitalización y la interconectividad de estos sistemas han incrementado los riesgos de seguridad de la información, exponiendo los datos críticos a amenazas cibernéticas como accesos no autorizados, manipulación de información y vulnerabilidades en los dispositivos conectados.

La seguridad de la información es un componente esencial para la operación confiable de sistemas tecnológicos en la industria alimentaria. La falta de medidas adecuadas de protección puede comprometer la integridad, disponibilidad y confidencialidad de los datos recopilados por dispositivos IoT en la supervisión de la cadena de frío. En este contexto, es fundamental el diseño de un modelo de seguridad que permita mitigar los riesgos asociados a la infraestructura tecnológica utilizada en la supervisión de la cadena de frío, alineado con estándares internacionales y buenas prácticas de gobernanza de TI.

El presente estudio tiene como objetivo diseñar un Modelo de Seguridad de la Información para el sistema de supervisión de la cadena de frío en Camagüey S.A., asegurando la protección de los datos y la mitigación de vulnerabilidades en los dispositivos IoT utilizados. Para ello, se analizará el estado actual de la seguridad en la empresa, se identificarán los principales riesgos y se propondrá un marco de control basado en estándares y metodologías reconocidas. La investigación adoptará un enfoque cuantitativo y descriptivo, empleando

técnicas de análisis de riesgos, auditorías de seguridad y validación del modelo propuesto en términos de efectividad y cumplimiento normativo.

La importancia de esta investigación radica en su contribución al fortalecimiento de la seguridad de la información en la industria cárnica, proporcionando un modelo replicable que pueda ser adoptado por otras empresas del sector. Con el incremento de regulaciones en torno a la seguridad alimentaria y la ciberseguridad, el diseño de un modelo específico para la supervisión de la cadena de frío se convierte en una necesidad estratégica para garantizar la calidad del producto y la confianza del consumidor.

Capítulo 1. Modelo de seguridad de la información en el sistema de supervisión de la cadena de frío de los productos cárnicos en Camagüey S.A.

1.1 Planteamiento del problema

En las últimas dos décadas, la tecnología ha experimentado un crecimiento y evolución acelerados (Mazó Pozuelo & Torrado Castro, 2024), la industria cárnica en Colombia es uno de los sectores estratégicos que lo ha experimentado. Sin embargo, este crecimiento ha traído consigo desafíos significativos en términos de calidad y seguridad alimentaria, especialmente en lo que respecta a la gestión de la cadena de frío. La supervisión eficiente de la temperatura y otros factores críticos es esencial para garantizar la inocuidad de los productos cárnicos, evitando su deterioro y la proliferación de microorganismos que puedan comprometer la salud pública (Huang & Leong, 2023).

En este contexto, la compañía Camagüey S.A., dedicada a la producción y distribución de productos cárnicos en Colombia, ha implementado un sistema de supervisión basado en tecnologías IoT con el fin de optimizar la gestión de la cadena de frío. Dicho sistema permite el monitoreo en tiempo real de variables como temperatura y humedad, asegurando que los productos sean almacenados y transportados en condiciones óptimas. Sin embargo, la digitalización de estos procesos ha generado una nueva problemática: la seguridad de la información (Zhang et al., 2024).

Uno de los principales riesgos asociados a la supervisión de la cadena de frío mediante IoT es la exposición de los datos críticos a amenazas cibernéticas. La interconectividad de los dispositivos de monitoreo con redes corporativas y la transmisión constante de datos a plataformas digitales incrementa la superficie de ataque para actores malintencionados. En

consecuencia, la ausencia de un modelo de seguridad adecuado expone a Camagüey S.A. a múltiples riesgos, como accesos no autorizados, alteración de registros de temperatura, interrupción del servicio y, en casos extremos, sabotaje del sistema (Liu, H., 2024).

El cumplimiento de estándares internacionales de seguridad, como la norma (*ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, s/f), se ha convertido en una necesidad imperante para empresas que dependen de tecnologías digitales en sus operaciones. Esta normativa establece directrices para la gestión de la seguridad de la información, proporcionando un marco para la identificación y mitigación de riesgos. Sin embargo, muchas empresas del sector alimentario aún no han implementado un enfoque estructurado de seguridad, lo que las hace vulnerables a ciberataques y fallos en la integridad de sus datos (Raj & Ghosh, 2023).

Además de los riesgos cibernéticos, la falta de medidas de seguridad en la supervisión de la cadena de frío puede tener repercusiones económicas y de reputación para la empresa. Un fallo en la cadena de frío ya sea por un ciberataque o por errores en la configuración del sistema, puede derivar en la pérdida de grandes volúmenes de productos, afectando no solo las finanzas de la empresa, sino también su credibilidad en el mercado. Estudios recientes han demostrado que los consumidores confían cada vez más en la transparencia de las empresas en cuanto a sus procesos de producción y distribución, por lo que una vulnerabilidad en el sistema puede impactar negativamente la percepción del cliente (Ashok & Gopikrishnan, 2023).

A pesar de los avances en tecnologías de seguridad, muchas organizaciones en la industria alimentaria han adoptado sistemas IoT sin implementar estrategias robustas de ciberseguridad. Esto se debe, en parte, a la falta de modelos específicos para la protección de la información en la supervisión de la cadena de frío, lo que dificulta la integración de medidas

efectivas para mitigar riesgos. La falta de mecanismos de cifrado adecuados, el uso de contraseñas débiles en los dispositivos IoT y la ausencia de protocolos de respuesta ante incidentes cibernéticos son algunos de los factores que agravan la problemática (Nguyen et al., 2020).

Desde una perspectiva operativa, la seguridad de la información en la supervisión de la cadena de frío no solo involucra la protección de datos, sino también la garantía de continuidad en las operaciones. La indisponibilidad del sistema debido a una vulnerabilidad de seguridad puede interrumpir el monitoreo de los productos cárnicos, generando problemas en la trazabilidad de los alimentos y afectando el cumplimiento normativo. Por esta razón, las empresas deben adoptar un enfoque integral que no solo aborde la seguridad tecnológica, sino también la capacitación del personal y la implementación de controles de acceso adecuados (Azizi et al., 2021).

Dado el contexto anterior, resulta necesario el diseño de un modelo de seguridad de la información específicamente adaptado al sistema de supervisión de la cadena de frío de Camagüey S.A. Este modelo debe permitir la evaluación y mitigación de vulnerabilidades en los dispositivos IoT, establecer controles adecuados de acceso y encriptación, y alinearse con estándares de ciberseguridad reconocidos a nivel internacional. La implementación de este modelo no solo fortalecerá la protección de los datos, sino que también garantizará la operatividad continua del sistema y el cumplimiento de regulaciones en materia de seguridad alimentaria (Huang & Leong, 2023).

En síntesis, la creciente digitalización de los procesos de supervisión de la cadena de frío en la industria cárnica ha generado la necesidad de reforzar la seguridad de la información. Camagüey S.A., como empresa líder en el sector, enfrenta el desafío de proteger los datos

generados por su sistema de monitoreo IoT, minimizando riesgos operativos y garantizando la confiabilidad de la información. Por ello, la presente investigación se enfocará en el diseño de un modelo de seguridad de la información que permita mitigar vulnerabilidades, optimizar la gestión de riesgos y fortalecer la infraestructura tecnológica de la empresa.

1.2 Formulación del problema

¿Cómo garantizar la seguridad de la información en el sistema de supervisión de la cadena de frío de los productos cárnicos en Camagüey S.A., mitigando vulnerabilidades en los dispositivos IoT y alineándose con estándares internacionales de ciberseguridad?

1.3 Objetivos

1.3.1 Objetivo general

Diseñar un modelo de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey S.A., con el fin de mitigar vulnerabilidades en los dispositivos IoT, proteger la integridad y confidencialidad de los datos y garantizar el cumplimiento de estándares internacionales de ciberseguridad.

1.3 .2 Objetivos específicos

- Diagnosticar el estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., identificando vulnerabilidades en dispositivos IoT y procesos tecnológicos, así como los estándares internacionales y buenas prácticas de ciberseguridad aplicables a su entorno.
- Diseñar un modelo de seguridad de la información basado en las mejores prácticas y estándares de ciberseguridad, alineado con las necesidades y características del sistema de supervisión de la cadena de frío en Camagüey S.A.
- Validar el modelo de seguridad propuesto, evaluando su efectividad en la mitigación de riesgos, la protección de la información y el cumplimiento normativo.

1.4 Justificación

Al analizar la apropiación de la tecnología en diversos sectores sociales, culturales, políticos y educativos, así como su impacto en la humanidad, es fundamental explorar alternativas que permitan establecer los fundamentos epistémicos y operativos para el aseguramiento de infraestructuras tecnológicas (Torrado Castro et al., 2023). Teniendo como base el objetivo de esta investigación, la creciente digitalización de los procesos industriales ha impulsado la adopción de tecnologías emergentes como el Internet de las Cosas (IoT) en la supervisión de la cadena de frío en la industria cárnica. Estas tecnologías permiten un monitoreo continuo de variables críticas como la temperatura y la humedad, optimizando la conservación de los productos y reduciendo el desperdicio. Sin embargo, el incremento en la interconectividad también ha expuesto a las organizaciones a nuevos riesgos de seguridad de la información, comprometiendo la integridad, confidencialidad y disponibilidad de los datos en los sistemas de supervisión (Brandao, 2019).

Camagüey S.A., como empresa del sector cárnico en Colombia, ha implementado un sistema de supervisión de la cadena de frío basado en IoT para garantizar la calidad y seguridad de sus productos. No obstante, la falta de un modelo de seguridad de la información adecuado representa un desafío significativo. La exposición a ciberataques, accesos no autorizados y alteración de datos puede comprometer la operación del sistema y afectar la trazabilidad y confiabilidad de los productos comercializados (Florrence, 2025).

La importancia de este estudio radica en la necesidad de diseñar un modelo de seguridad de la información específico para la supervisión de la cadena de frío en Camagüey S.A., alineado con estándares internacionales de ciberseguridad, como la (*ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management*

systems — Requirements, s/f). Este modelo permitirá mitigar vulnerabilidades en los dispositivos IoT, optimizar la protección de los datos y fortalecer la infraestructura tecnológica de la empresa (Etemadi et al., 2021).

Además, la implementación de un modelo de seguridad contribuirá a mejorar el cumplimiento normativo y la confianza del consumidor en los productos cárnicos de la empresa. Diversos estudios han demostrado que la seguridad de la información es un factor determinante en la trazabilidad de los alimentos y en la capacidad de respuesta ante incidentes de seguridad en la industria alimentaria (Santos & Martins, 2020).

Desde una perspectiva económica y operativa, la seguridad de la información en los sistemas de supervisión de la cadena de frío no solo minimiza los riesgos de incidentes cibernéticos, sino que también mejora la eficiencia en la gestión de la información y optimiza la toma de decisiones basada en datos confiables (Nyamuchiwa et al., 2022). Asimismo, la reducción de incidentes de seguridad disminuye las pérdidas económicas por fallos en la cadena de frío, garantizando la competitividad y sostenibilidad de la empresa en un entorno de mercado altamente regulado. La implementación de medidas de seguridad robustas no solo impacta en la operatividad interna, sino que también refuerza la reputación corporativa y fortalece la relación con los clientes y proveedores.

En síntesis, este estudio es relevante tanto para Camagüey S.A. como para otras empresas del sector cárnico, ya que proporciona un modelo replicable de seguridad de la información en la supervisión de la cadena de frío. La investigación contribuye a la generación de conocimiento en el área de la ciberseguridad aplicada a la industria alimentaria y ofrece herramientas prácticas para la mitigación de riesgos en infraestructuras tecnológicas altamente interconectadas, permitiendo a las empresas mejorar la eficiencia operativa, cumplir con normativas

internacionales y garantizar la seguridad de sus productos a lo largo de toda la cadena de suministro.

1.5 Delimitaciones

1.5.1 Delimitación conceptual

El desarrollo de la presente investigación estará fundamentado en referentes tales como la Seguridad de la Información, Internet de las Cosas (IoT), Cadena de Frío, Gobierno de TI, Normativa ISO/IEC 27001:2022, Productos Cárnicos, Ciberseguridad en IoT, Gestión de Riesgos en Seguridad de la Información.

1.5.2 Delimitación geográfica

El estudio se llevará a cabo en las instalaciones de la compañía Camagüey S.A. ubicada en el Municipio de Galapa, Departamento del Atlántico.

1.5.3 Delimitación temporal

El presente proyecto de investigación se desarrollará en un lapso de 12 meses, contados a partir de la aprobación de la presente propuesta; a fin de dar cumplimiento a los objetivos propuestos.

1.5.4 Delimitación operativa

Esta investigación se enfocará exclusivamente en la formulación de un modelo de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey

S.A., estableciendo límites claros en su desarrollo y validación. Se trabajará en la identificación de vulnerabilidades y riesgos en los dispositivos IoT y procesos tecnológicos de dicho sistema. El modelo de seguridad diseñado será de carácter teórico, alineado con estándares internacionales, sin ejecución práctica ni implementación operativa en la empresa.

El estudio considerará los protocolos de comunicación, almacenamiento de datos y medidas de ciberseguridad aplicadas en el sistema de supervisión de la cadena de frío. La validación del modelo se llevará a cabo a través de simulaciones y análisis de escenarios de riesgo, sin intervención directa en la infraestructura de Camagüey S.A. Además, no se abordará la implementación del modelo ni se modificarán las infraestructuras tecnológicas actuales de la empresa, limitándose al diseño y validación conceptual.

Capitulo 2. Marco referencial

2.1 Marco histórico

2.1.1 Antecedentes.

El presente estudio sobre el diseño de un Modelo de Seguridad de la Información en la supervisión de la cadena de frío en Camagüey S.A. se fundamenta en diversas investigaciones previas. Estas investigaciones han explorado enfoques similares en distintos sectores, lo que permite identificar oportunidades y desafíos para su aplicación en la industria cárnica.

Uno de los estudios más relevantes es el de (Arriaga-Lorenzo et al., 2024), que evaluó la gestión de la cadena de frío en supermercados de México. Su investigación destaca la importancia de la calibración y monitoreo constante de los equipos de refrigeración para prevenir fallos que puedan comprometer la calidad de los productos cárnicos. Esto es aplicable a nuestro estudio en la medida en que refuerza la necesidad de implementar un sistema de monitoreo en tiempo real para garantizar la estabilidad de la cadena de frío.

(Zhang et al., 2024) proponen un modelo de trazabilidad basado en blockchain para la logística de cadena de frío, asegurando la integridad de los datos y la privacidad de la información mediante firmas de anillos enlazables. Su aplicación en el sector cárnico garantizaría la inmutabilidad y seguridad de los registros de temperatura y condiciones de almacenamiento.

Otro estudio relevante es el de (Huang & Leong, 2023), que explora el uso de blockchain para la trazabilidad de la información en la cadena de frío de alimentos. En su propuesta, el uso de sensores RFID y pruebas de desempeño validan la eficacia del modelo implementado. Su implementación en Camagüey S.A. permitiría garantizar transparencia y confianza en el monitoreo de los productos cárnicos.

Desde una perspectiva financiera, (Liu, H., 2024) analiza la aplicación de blockchain en modelos de negocio logísticos para la cadena de frío. Su investigación resalta la importancia de eliminar la asimetría de la información y mejorar la confianza en el transporte de productos perecederos. La incorporación de estas estrategias permitiría a Camagüey S.A. mejorar su eficiencia operativa y optimizar su sistema de distribución.

(Priya et al., 2023) presentan un enfoque basado en IoT para la logística de la cadena de frío, destacando el uso de sensores, bases de datos en la nube y sistemas de monitoreo remoto. Esta investigación demuestra cómo el IoT puede mejorar la eficiencia del transporte y almacenamiento de productos perecederos.

(Cheung & Bell, 2021) desarrollan un modelo de defensa ante ataques cibernéticos en la cadena de suministro basada en IoT, resaltando la importancia de la seguridad en infraestructuras tecnológicas críticas. Su enfoque es esencial para comprender los riesgos asociados con la digitalización de la cadena de frío y cómo mitigarlos.

(Tang, 2023) propone un sistema basado en computación en la nube para la logística de la cadena de frío, optimizando costos y reduciendo la variabilidad en la entrega de productos refrigerados. En el caso de Camagüey S.A., este enfoque podría aplicarse para mejorar la planificación y distribución de los productos.

(Davoudi et al., 2024) realizan un análisis de los avances en la logística de la cadena de frío durante las últimas dos décadas, con un enfoque en la industria cárnica. Identifican estrategias innovadoras para la reducción de desperdicios y la mejora de la sostenibilidad en el transporte de carne refrigerada.

(Ren et al., 2023) desarrollan un modelo basado en redes bayesianas para la gestión de riesgos en el embalaje de la cadena de frío, proporcionando herramientas útiles para evaluar la

eficiencia de las estrategias de mitigación de riesgos en el almacenamiento de productos cárnicos.

(Vilaginés Iglesias, 2023) identifica los dispositivos IoT actuales de una empresa del sector cervecero, proponiendo acciones de mejora para la infraestructura tecnológica, en pro de mantener su competitividad y evitar problemas que puedan afectar su reputación y la continuidad del negocio.

(Martínez & Mesías, 2021) recopila herramientas innovadoras, describiendo la forma en que las tecnologías disruptivas están cambiando los procesos de la cadena alimentaria, mejorando la seguridad y la calidad de los productos obtenidos y evaluando las consecuencias sociales asociadas.

(Miñan Parrales, 2022), basado en el método empírico analítico, de tipo experimental, con un enfoque descriptivo y cualitativo, que apunta a una adecuada gestión logística de la información asociada a materia prima y productos, que les permita a los consumidores verificar su trazabilidad.

El artículo llamado “Principales técnicas criptográficas aplicadas a la seguridad de la información en IoT: una revisión sistemática”, desarrollado en Perú, ofrece un análisis detallado de los métodos criptográficos más populares utilizados para proteger la información en el Internet de las Cosas, mediante el análisis de una variedad de artículos de investigación recopilados de una variedad de bases de datos académicas, como MDPI, Scopus y ScienceDirect (Dionicio et al., 2023)

“Proposal for a Forensic Action Guide for Internet of Things (IoT) Environments”, es un artículo presentado en Argentina. Estudia el entorno de Internet de las cosas, proponiendo pautas para realizar un análisis forense adecuado y suficiente cuando se necesita buscar evidencia

digital en estos contextos. La investigación abarca la evaluación de una variedad de técnicas de análisis forense, especialmente en lo que respecta al Internet de las cosas (IoT), y la creación de una Guía de Actuación Forense para Entornos IoT (Gallo & Beatriz, 2022).

En México, el boletín científico de ciencias básicas e ingenierías del ICBI, presenta el artículo denominado “Internet de las Cosas (IoT) Retos para las Empresas en la era de la Industria 4.0”, el cual señala la integración del Internet de las Cosas como una oportunidad para la manufactura sustentable en la Industria 4.0 y la generación de nuevos servicios cualitativos, que representan una evolución del internet y sus desafíos (Ávila-Camacho & Moreno-Villalba, 2023).

(Jaén-Barrantes, 2022) en su proyecto “Desarrollo de un modelo de gestión de energía basado en la Norma ISO 50001 en el Ingenio La Azucarera La Estrella de Grupo Calesa, bajo concepto de Internet de las Cosas (IoT)” estudio realizado en Costa Rica, realiza una propuesta de cuadro de mando integral que incorpora las perspectivas del cliente, las perspectivas financieras, los procesos internos y el aprendizaje y el crecimiento, junto con indicadores y metas estratégicas que permitan monitorear el cumplimiento del modelo de gestión de energía basado en IoT.

Otra importante investigación citada, es la llevada a cabo en Panamá, mediante el artículo “Integración del internet de las cosas en la gestión de la cadena de suministro de alimentos: una revisión sistemática de la literatura”, que explora el impacto que tiene la integración del IoT en la gestión de la cadena de suministro de alimentos, a través de una revisión sistemática de la literatura (Torres et al., 2021).

En Colombia, existe una amplia variedad de estudios en materia de Internet de las cosas, entre los cuales se destacan los siguientes:

“Optimización de Cultivos de Fresas en Cundinamarca mediante la Integración de Plataformas Cloud e IoT”, cuya propuesta incluye la instalación de sensores en el campo que recopilen datos en tiempo real sobre variables importantes como la temperatura, la humedad del suelo y la calidad del agua para monitorear y controlar de manera remota varios aspectos del cultivo (Hernández Mendoza & Martínez Rojas, s/f).

Por otra parte se encuentra el proyecto “Prototipo de una ruta tecnológica para el IOT, enfocada en las tecnologías de riego, para los agricultores de pequeña escala en Colombia”. El objetivo de este proyecto es crear una estrategia tecnológica para crear mapas de rutas tecnológicas para la agricultura en Colombia mediante la utilización de la minería de texto e inteligencia artificial. El objetivo es encontrar una alternativa adecuada y planificada a los sistemas de riego actuales, así como a la tecnología que actualmente se está implementando para solucionar este problema (Aceros Orduz, 2020).

La revista Publicaciones e Investigación, especializada en Ingenierìa, presenta el artículo titulado “Tópicos de investigación de internet de las cosas en la cadena de suministro”, cuyo objetivo es identificar y analizar los temas de investigación de las publicaciones sobre el internet de las cosas, así como los beneficios y desafíos del IoT y sus aplicaciones en sectores tales como el industrial, automotriz, comercio minorista, farmacéutico, transporte, energía, atención médica, marketing, logística inversa, alimentos, agrícola, calzado, textil y postal, estableciendo una conexión entre tecnologías como RFID, computación en la nube, geoposicionamiento, sensores, sistemas ciberfísicos, telemática y dispositivos móviles; para procesos de identificación, comunicación y seguimiento que mejoran la trazabilidad en tiempo real entre los actores y los objetos de la cadena, para tener información precisa, reducir costos y ser más eficientes (Castellanos et al., 2022).

Una investigación con aportes significativos al presente proyecto es la denominada "Sistema IoT para monitoreo de productos cárnicos", desarrollada en la ciudad de Tunja para simular la interconexión de los dispositivos sensoriales utilizados en la plataforma Azure IoT Central, recopilar datos y generar reportes. De igual forma, se pusieron en práctica conceptos importantes sobre Internet de las cosas, como el papel que juegan los dispositivos, los sensores y cómo se conectan a la nube para intercambiar datos (Vargas Caballero, 2023).

El estudio "Modelo de integración tecnológica en la implementación de sistemas de gestión de inocuidad y seguridad alimentaria en empresas del sector Agro alimentos", ofrece soluciones para la adopción de prácticas de gestión que integran el conocimiento, la automatización de procesos y la incorporación de motores predictivos a través de tecnologías como la inteligencia artificial e Internet de las cosas. Estos cambios tendrán un impacto en la reducción de tiempos, la calidad de la intervención, la mejora de la especialización en el conocimiento y la efectividad, así como en la optimización de los recursos (Rangel Gómez, 2022).

A nivel regional, se estudian investigaciones tales como "Desarrollo de un sistema IoT de monitoreo de temperatura, humedad relativa y estado ON/OFF de un cuarto frío de Inversiones Medina Verbel S.A.S.", desarrollado en la ciudad de Cartagena, la cual señala las condiciones necesarias para el levantamiento y tratamiento de información en campo para el diseño del sistema de monitoreo con arquitectura IoT en la bodega de pescados y mariscos de la empresa mencionada (Ibarguen Cabrera & Martínez Contreras, s/f).

La "Propuesta de optimización de los procesos de almacenamiento y transporte en alimentos cárnicos S.A.S., regional Montería", que desarrolla un estudio descriptivo utilizando un enfoque mixto utilizando información recopilada por encuestas y entrevistas. El objetivo del

diagnóstico es evaluar el nivel de madurez de los procesos e identificar las principales brechas, utilizando como referente varios modelos teóricos y casos de implementación que se encuentran en la revisión de la literatura (Álvarez Polo, 2021).

Al igual que el proyecto llamado “El impacto de la industria 4.0 en los procesos logísticos del sector alimentario de Barranquilla”, que constituye un importante referente, debido a que presenta una propuesta para mejorar la producción y procesos logísticos de las organizaciones del sector en la ciudad (Rangel Tapia et al., 2021).

Estos antecedentes demuestran la relevancia de implementar modelos de seguridad de la información en la supervisión de la cadena de frío mediante IoT, asegurando la calidad de los productos cárnicos y fortaleciendo la ciberseguridad en la industria. El estudio propuesto toma como base estos enfoques para diseñar un modelo adaptado a las necesidades de Camagüey S.A., integrando tecnologías innovadoras y estrategias de seguridad para optimizar la gestión de la cadena de frío.

2.2 Marco conceptual

El desarrollo de un Modelo de Seguridad de la Información para la supervisión de la cadena de frío mediante tecnologías IoT requiere una base conceptual sólida. A continuación, se presentan los conceptos clave que sustentan esta investigación, acompañados de su respectiva fundamentación teórica y referencias actualizadas.

Seguridad de la Información, la seguridad de la información se refiere a la protección de los datos contra accesos no autorizados, alteraciones y pérdida de integridad. La implementación de modelos de seguridad en entornos IoT es fundamental debido a la cantidad de dispositivos interconectados que pueden ser vulnerables a ciberataques (Mnushka & Savchenko, 2019).

Modelo de Seguridad de la Información, los modelos de seguridad de la información establecen directrices para gestionar y mitigar los riesgos en sistemas digitales. En el contexto de IoT y la supervisión de la cadena de frío, estos modelos deben garantizar la confidencialidad, integridad y disponibilidad de los datos generados por sensores (Toapanta et al., 2024).

Internet de las Cosas (IoT) IoT es un ecosistema de dispositivos conectados que recopilan, procesan y transmiten datos en tiempo real. En la cadena de frío, el IoT permite monitorear variables críticas como temperatura y humedad, asegurando la calidad de los productos cárnicos (Yiming et al., s/f).

Supervisión de la Cadena de Frío La supervisión de la cadena de frío implica el monitoreo continuo de las condiciones ambientales de almacenamiento y transporte de productos perecederos. La integración de IoT y blockchain ha permitido mejorar la trazabilidad y la seguridad en este proceso (Sunny et al., 2020).

Trazabilidad de Productos Cárnicos La trazabilidad es la capacidad de seguir el recorrido de un producto a lo largo de la cadena de suministro. La combinación de blockchain e IoT permite registrar y verificar cada etapa del proceso, mejorando la transparencia y seguridad de los alimentos (Huang & Leong, 2023).

Ciberseguridad en IoT La ciberseguridad en IoT abarca estrategias para proteger dispositivos interconectados de accesos no autorizados y ataques malintencionados. La descentralización de datos mediante blockchain ha surgido como una solución efectiva para mitigar riesgos (Ahmed et al., 2023).

Gestión de Riesgos en Seguridad de la Información La gestión de riesgos en seguridad de la información identifica y evalúa amenazas potenciales en sistemas digitales. En el contexto de

la cadena de frío, un enfoque proactivo en la seguridad minimiza las vulnerabilidades operativas (Sargsyan et al., 2019).

Gobierno de TI El gobierno de TI define las políticas y estrategias para garantizar el alineamiento de las tecnologías de la información con los objetivos de negocio. Un gobierno de TI eficaz facilita la implementación segura de IoT en la supervisión de la cadena de frío (Alshahrani, s/f).

Norma ISO/IEC 27001:2022 Este estándar internacional establece los requisitos para un sistema de gestión de seguridad de la información, garantizando la implementación de controles adecuados para mitigar riesgos y mejorar la protección de datos en sistemas IoT (Raj & Ghosh, 2023).

Blockchain en la Trazabilidad de la Cadena de Frío Blockchain permite almacenar registros inmutables sobre la temperatura y condiciones de almacenamiento de los productos, garantizando su autenticidad y seguridad (Asokan et al., 2022).

Big Data en la Supervisión de la Cadena de Frío Big Data permite el análisis de grandes volúmenes de datos generados por sensores IoT en la cadena de frío, facilitando la toma de decisiones basada en evidencia (Brandín & Abrishami, 2021).

Logística Inteligente La logística inteligente integra tecnologías avanzadas como IoT y blockchain para optimizar la planificación, transporte y distribución de productos refrigerados (Benjamín Teisserenc & Samad Sepasgozar, s/f).

Infraestructura Crítica en la Industria Alimentaria Los sistemas tecnológicos utilizados en la cadena de frío forman parte de la infraestructura crítica de la industria alimentaria, y su protección es fundamental para evitar interrupciones en la distribución de alimentos (Kumar & Sharma, 2023).

Computación en la Nube para IoT La computación en la nube permite almacenar y procesar datos IoT de manera eficiente y segura, facilitando la supervisión remota de la cadena de frío (Gonzalez-Amarillo et al., 2023).

Inteligencia Artificial en la Gestión de la Cadena de Frío La inteligencia artificial optimiza el control de la temperatura y la predicción de fallas en sistemas de refrigeración, mejorando la eficiencia y reduciendo desperdicios (Herrmann & Pridöhl, 2020).

2.3 Marco contextual

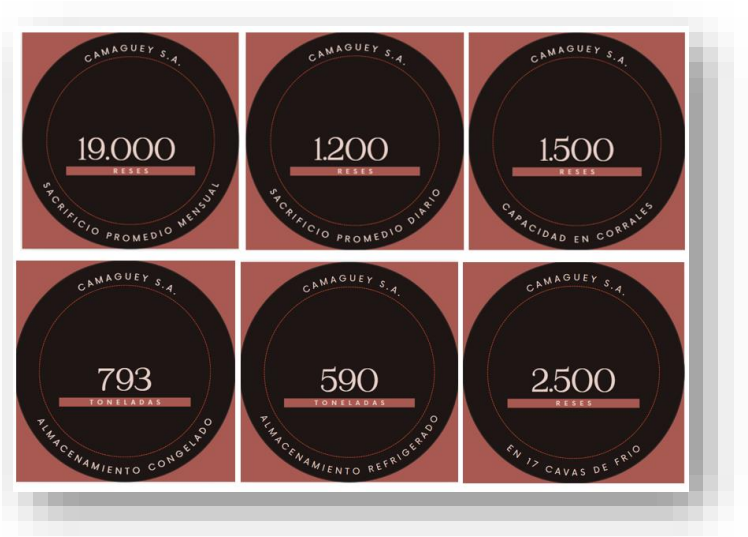
La presente investigación está orientada a las necesidades de la empresa Camagüey S.A., ubicada en la Calle 15 Cra. 19 esquina, en el municipio de Galapa, en el Departamento del Atlántico.

La organización Camagüey se define a sí misma como une empresa líder en la industria ganadera colombiana, cuyo objeto es la producción, conservación y comercialización de la carne y sus subproductos.

Esta empresa fue Fundada en 1957, y ha pasado por varios procesos de renovación que le han permitido posicionarse como el frigorífico con mayor integración y la más avanzada tecnología del país. Entre las cifras de producción más representativas de la actualidad, las cuales han sido suministradas por la organización, se encuentran las siguientes:

Figura 1.

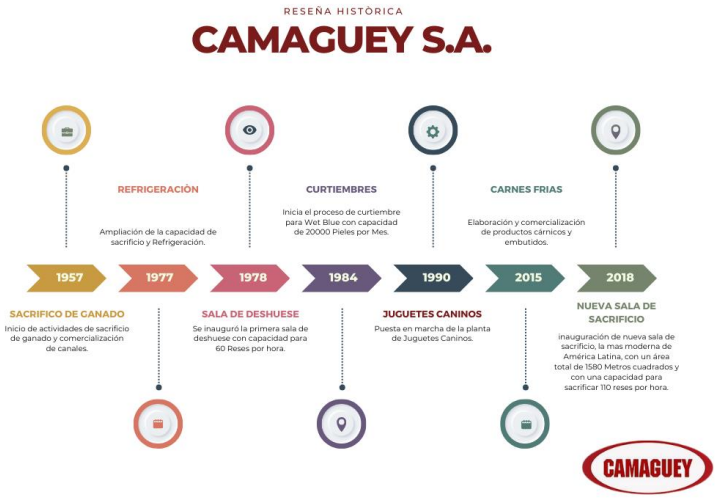
Cifras productivas Camagüey S.A. Fuente: Camagüey S.A.



La siguiente imagen presenta los hitos màs relevantes que han marcado la evoluciòn de la empresa:

Figura 2.

Trazabilidad de procesos de la empresa Camaguey S.A. Fuente: Camaguey S.A.



Misòn:

"Somos una organización empresarial del sector cárnico, subproductos y sus derivados, proveedora de soluciones de alimentación de alta calidad, fundamentadas en la eficiencia de sus procesos, tecnología distintiva, responsabilidad social y un equipo humano competente y comprometido con la inocuidad de los alimentos, destinada a satisfacer necesidades y experiencias del mercado nacional e internacional, mediante un portafolio de productos diferenciados y nutritivos de clase mundial" (*Camaguey S.A.*, s/f).

Visiòn:

"Ser la empresa líder en sacrificio y procesamiento de productos cárnicos y de sus derivados, en la comercialización de productos certificados con normas internacionales en gestión de la inocuidad alimentaria, en juguetes caninos y cueros, ser reconocida por nuestros clientes por la calidad y trazabilidad de los productos y procesos " (*Camaguey S.A.*, s/f)

Servicios:

Sacrificio: El proceso de sacrificio en las instalaciones de la empresa se desarrolla siguiendo un riguroso Proceso Operativo Estandarizado, dando especial énfasis a los aspectos sanitarios, en cumplimiento del Sistema de Análisis de Peligros y Puntos Críticos de Control, considerando en todo momento la calidad y la seguridad alimentaria es fundamental, con miras a garantizar que el producto final esté libre de contaminación y cumpla con los mas altos estándares de calidad.

La linea de sacrificio de la empresa cuenta con capacidad para procesar hasta 100 reses diarias, lo cual permite optimizar el traslado de las canales de res a la refrigeración, proceso que toma alrededor de 15 minutos, asegurando la frescura y seguridad de la carne para consumo. El comercializar más de 200,000 reses anualmente le proporciaona a la empresa una posición

destacada, ocupando el primer lugar como el mayor procesador y comercializador de carne de res en el paìs.

Deshuese: El deshuese se realiza de forma ràpida y contìnua, con una capacidad para 60 reses por hora. Los cortes en sala no superan los cinco minutos. Las canales se deshuesan a una temparatura de cero grados centígrados en un ambiente climatizado a 10° Celcius, en cumplimiento de las normas sanitarias nacionales e internacionales.

Refrigeraciòn y Congelaciòn: Camaguey tiene capacidad para:

Refrigerar 2500 canales, a cero grados Centígrados al hueso, en 30 horas.

Cuenta con 15 cuartos de refrigeración con capacidades desde 35 a 400 canales.

Posee 8 congeladores Blast Freezers con temperatura a menos 45 grados centígrados y con capacidad para 96 toneladas cada 24 horas, 5 congeladores de placas con capacidad de 2 toneladas cada 2 horas, 2 almacenes para productos congelados con capacidad para 1000 toneladas, 3 almacén para carne refrigerada empacada al vacío con capacidad para 600 toneladas.

Sacrificio y deshuese de Porcinos.

Productos:

Cortes: La empresa se especializa en ofrecer una amplia variedad de cortes de carne, acorde a las necesidades de sus clientes.

Subproductos: Camaguey convierte todos los componentes que hacen parte del sacrificio bovino y del deshuese de las canales en productos que puedan ser de utilidad en diversas industrias. De esta forma, a fin de promover el cuidado medio ambiental, evitando la contaminación de los recursos naturales en la disposición de los mismos. Algunos de los principales produtos elaborados son las harinas de carne, de sangre y de hueso calcinado; sebo fundido, cola de res, cascos secos molidos, hiel concentrada y cálculos biliares.

Curtiembre: La curtiembre Camaguey funciona a partir del sño 1985 con una capacidad de procesamiento de 25,000 pieles mensuales; las cuales son exportadas para la industria de tapiceria y calzado en sitios como Europa, Asia y resto de América.

Juguetes caninos, en este segmento de la empresa, se diseñan productos para proveer calidad y bienestar a caninos, a travès de juguetes elabordos 100% a mano, tratados naturalmente, reduciendo el uso de químicos. Se cuenta con un amplio catàlogo , integrado por mas de 60 referencias.

Carnes frìas: La elaboración de embutidos se realiza en las mismas intalaciones de la planta, a partir de materia prima cárnica producida en la planta y aprobada para exportación.

Certificaciones de calidad:

En cuanto a certificaciones que garantizan la calidad en sus operaciones y productos, la empresa cuenta con las descritas en la siguiente figura:

Figura 3.

Certificaciones de Camaguey S.A Fuente: Camaguey S.A.



Clientes:

Entre los clientes màs reconocidos de la empresa, se tienen marcas tales como almacenes Èxito, Supertiendas Olìmpica, Price Smart, Acondesa, Jerònimo Martins, entre otros.

Aseguramiento de la calidad:

La empresa cuenta con un laboratorio dentro de la planta, que cumple a cabalidad con las especificaciones contempladas por el Instituto de Vigilancia de los Medicamento y Alimentos (INVIMA). A travès de dicho laboratorio se valida el Sistema de Aseguramiento de la Calidad, mediente análisis microbiológicos diarios de los productos, materias primas, agua, insumos, superficies de trabajo, herramientas, empaques, ambiente, operarios y dotación. El talento humano de la planta priductiva se encuentra integrado por profesionales en el campo de la Ingenieria de alimentos, Microbiologìa, Veterinaria, Química, etc.

Figura 4.

Procesos de aseguramiento de la calidad.



Fuente: Camaguey S.A.

2.4 Marco teórico

Dentro de las principales teorías que dan fundamento a la presente investigación, encontramos:

Propuesta por Claude E. Shannon; la cual sin duda constituye uno de los hallazgos científicos más relevantes del siglo XX orientado a permitir la cuantificación de la información. Fue creado con la intención de descubrir los límites básicos de las tareas de procesamiento de señales, como la compresión de datos, el almacenamiento y la comunicación. Se puede encontrar su uso en una amplia gama de disciplinas, tales como la física, la química, la biología, la

inferencia estadística, la robótica, la criptografía, la computación, la lingüística, el reconocimiento de patrones y la teoría de la comunicación.

Como sucede con otras disciplinas, la alfabetización informacional usualmente se inicia con la teoría y concluye con la implementación práctica. La teoría de la información constituye un escenario amplio que incluye ideas educativas y tecnológicas. En términos generales, los programas de enseñanza de la biblioteca académica china abordan temas como las teorías de la tecnología educativa contemporánea, el diseño de la instrucción, la propagación de información, la teoría de la enseñanza moderna, la teoría de los medios, entre otros.

Desde el punto de vista general de la teoría de la información, resulta imprescindible que los bibliotecarios académicos y los expertos en información posean una serie de competencias similares; deben entender las particularidades de la educación en información y la tecnología educativa contemporánea, además de familiarizarse con los más recientes progresos en la enseñanza y el aprendizaje, identificando métodos dinámicos de propagación de información y medios de comunicación.

Es necesario investigar técnicas y formas de diseño de enseñanza para ajustarse de manera óptima a audiencias diversas, garantizando que entiendan los conceptos que se proponen. Además de la teoría general de la información, los bibliotecarios a menudo abordan aspectos de la tecnología de la información, en campos como la tecnología de sensores, la tecnología de redes, la tecnología de comunicación, la tecnología de la computación, entre otros. La tecnología de la información y las redes están particularmente en el núcleo de la tecnología de la información y, por ende, son componentes esenciales de cualquier enseñanza en torno a la interpretación y aplicación de la información. (Holik, 2016)

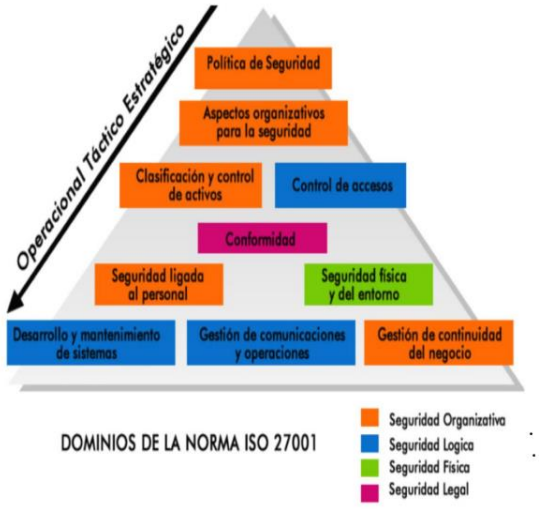
ISO 27000:

Las normas de la serie 27000 tienen sus raíces en 1995. La ISO 27001 es la única norma que se dirige a la certificación, mientras que los demás estándares ofrecen guía para la aplicación de mejores prácticas, el método adecuado para crear el SGSI; o para la implementación de procesos y controles esenciales de administración de riesgos de seguridad de la información. Las regulaciones son objeto de revisiones regulares con el objetivo de mejorar.

La Norma ISO 27000 se aplica a todas las organizaciones, especifica los requisitos para crear, poner en marcha, funcionar, realizar seguimiento, evaluar, conservar y perfeccionar un SGSI documentado en el marco de los riesgos empresariales globales de la organización. El Sistema de Administración de Seguridad de la Información, está concebido para garantizar sistemas de seguridad apropiados que aseguren la salvaguarda de los recursos de información y brinden la confianza requerida a los involucrados.

Figura 5.

Dominios de ISO 27000. Fuente: Adaptado de la Norma ISO/IEC 270001.



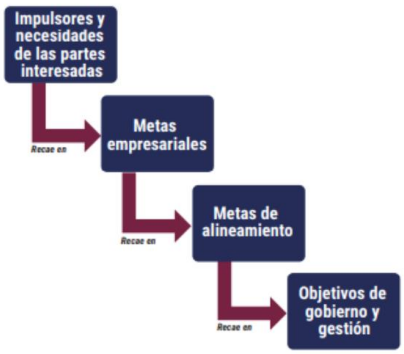
COBIT 2019:

La Asociación de auditoría y control de sistemas de información ISACA, creó un marco de referencia que ofrece un enfoque integral para la gestión y gobierno de la tecnología de la información. COBIT 2019, la actualización más reciente, es una actualización significativa que se adapta a los desafíos y cambios tecnológicos actuales. Algunas de sus principales características obedecen a la alineación entre la tecnología de la información y los objetivos estratégicos de la organización, centrándose en metas claras y medibles.

De igual manera, proporciona un marco sólido para el gobierno de TI, asegurando la toma de decisiones y la rendición de cuentas en todos los niveles, garantiza la mejora continua mediante el monitoreo y la adaptación a los cambios tecnológicos. Por otra parte, considera todas las facetas de la gestión de TI, incluida la entrega de servicios, la gestión de riesgos y el cumplimiento.

Figura 6.

Cascada de metas de COBIT 2019. Fuente: ISACA.



Este estándar se basa en 6 principios clave que van desde asegurar una cobertura total de la organización, implementar un marco estandarizado, promover un enfoque integral, separar la

gobernanza de la dirección y adaptarse al entorno empresarial, hasta mantenerse en constante evolución. Estos principios se reconocen como principios de un sistema de gobierno y a su vez, se cuenta con 3 principios del marco de gobierno.

Figura 7.

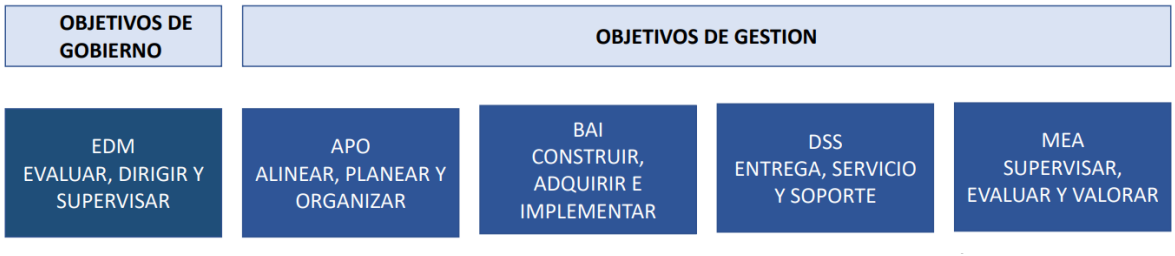
Principios de COBIT 2019. Fuente: ISACA.



La siguiente figura resume los objetivos de gobierno y de gestión de COBIT 2019, agrupados en cinco dominios que expresan el propósito de los objetivos que contienen.

Figura 8.

Dominios de COBIT 2019. Fuente: ISACA.



Los objetivos relacionados con gobierno se agrupan en el dominio Evaluar, Dirigir y Monitorizar (EDM). En este dominio, el órgano de gobierno es el encargado de evaluar las estrategias, guía al alta en la toma de decisiones sobre estrategias y monitorear su consecución.

Los objetivos de gestión se agrupan en los cuatro dominios.

Alinear, Planificar y Organizar (APO), el cual contempla la organización general, estrategia, actividades de apoyo pata las Tecnologías de la información.

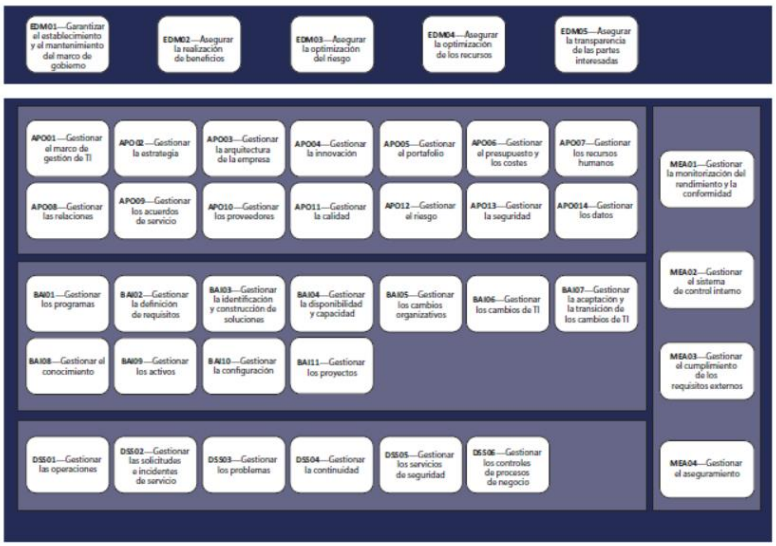
Construir, Adquirir e Implementar (BAI) se enfoca en soluciones y su integración en los procesos de negocio.

Entregar, Dar Servicio y Soporte (DSS), aborda los procesos de entrega a nivel operativo, el soporte de servicios de TI.

Monitorizar, Evaluar y Valorar (MEA), se refiere al seguimiento del rendimiento de TI y su relación con los objetivos de rendimiento internos, los objetivos de control a nivel interno y los requisitos externos.

Figura 9.

Modelo Core de COBIT 2019. Fuente: ISACA.



2.5 Marco legal

Las figuras presentadas a continuaciòn corresponden a una recopilaciòn de la normativa en materia de productos càrnicos a nivel nacional:

Tabla 1.

Marco normativo Colombia.

Tipo de norma	Nombre de norma	Descripción
DECRETO	DECRETO 1500 DE 2007	Por el cual se establece el reglamento técnico a través del cual se crea el sistema oficial de inspección, vigilancia y control de la carne, productos y derivados cárnicos, destinados para el consumo humano y los requisitos sanitarios y la inocuidad que se deben cumplir en su producción primaria, beneficio, desposte, desprese, procesamientos, almacenamiento, transporte comercialización, expendio, importación o exportación.
RESOLUCION	Resolución 4282 de 2007	por el cual se establecen los requisitos sanitarios para el funcionamiento de la planta de beneficio de las especies bovina, bufalina, y porcina, planta de desposte y almacenamiento, comercialización, expendio, transporte, importación o exportación de carnes y productos cárnicos comestibles.
DECRETO	DECRETO 2270 DE 2012	la carne y los productos cárnicos comestibles que no sean autorizados por la autoridad sanitaria competente, de acuerdo con los requisitos establecidos en el presente decreto o las normas que los modifiquen, adicionen o sustituyan, deben ser objeto de reembarque o destrucción.
RESOLUCIÓN	Resolución 4282 de 2007	por la cual se establece el reglamento técnico sobre los requisitos sanitarios y la inocuidad de la carne y los productos cárnicos comestibles de la especie porcina destinada para el consumo humano y las disposiciones para su beneficio, desposte, almacenamiento, comercialización, expendio, transporte, importación o exportación.
		por el cual se modifica el decreto 1500 de 2007 y el decreto 2270 de2012 en relación con el sistema oficial de inspección, vigilancia y control de la carne y los

DECRETO	Decreto2016 de 2013	productos cárnicos comestibles y se dictan otras disposiciones.
RESOLUCIÓN	Resolución 072 de 2007	por el cual se establece el manual de buenas prácticas de manejo para la producción y obtención de piel de ganado bovino y bufalino
RESOLUCIÓN	Resolución 2905 de 2007	por la cual se establece el reglamento técnico sobre los requisitos sanitarios y la inocuidad de la carne y los productos cárnicos comestibles de la especie bovina y bufalina destinados para el consumo humano.
RESOLUCIÓN	Resolución 18119 de 2007	por el cual se reglamentan los requisitos del plan gradual de cumplimiento para la planta de beneficio y desposte de bovinos y bufalinos.
RESOLUCIÓN	Resolución 2019055962	por el cual se adopta la guía de transporte y destino de la carne y productos cárnicos comestibles provenientes de la planta de beneficio, desposte, desprese, acondicionamiento, de establecimientos de almacenamiento y/o distribución e importadores de carne y productos cárnicos comestibles.
RESOLUCIÓN	Resolución 072 de 2007	
RESOLUCIÓN	Resolución 2905 de 2007	por la cual se establece el manual de buenas practica de manejo de producción y obtención de piel de ganado bovino y bufalino.
DESCRETO	Decreto 1282 de 2016	por el cual se establece el trámite para autorización sanitaria tradicional.
LEY	Ley 9 de 1970	por el cual se establece la clasificación de los mataderos.
DECRETO	Decreto 1036 de 1991	por el cual se establece la clasificación de los mataderos.

CONPES	Conpes 3458 de 2007	por la cual se establece la política nacional de inocuidad para la cadena de carne porcina.
CONPES	conpes 3376 de 2005	por la cual se establece la política nacional de inocuidad para la cadena de carne porcina.
RESOLUCIÓN	Resolución 2016037913	inscripción y autorización sanitaria de establecimientos acondicionadores.

Capitulo 3. Diseño metodológico

3.1 Tipo de investigación

La presente investigación adopta un enfoque **cuantitativo con alcance descriptivo**, ya que permite analizar, caracterizar y validar los elementos que conforman el modelo MSISSCF, orientado a la seguridad de la información en sistemas IoT aplicados a la supervisión de la cadena de frío en la empresa Camagüey S.A.(Fujs et al., 2019).

El enfoque cuantitativo se evidencia en el diseño y aplicación de un instrumento de validación estructurado, dirigido a un panel de expertos, cuyos resultados fueron procesados mediante técnicas estadísticas para evaluar la consistencia interna del cuestionario a través del coeficiente alfa de Cronbach. Este procedimiento permitió medir de forma objetiva la percepción de los expertos sobre aspectos clave del modelo, como su claridad, aplicabilidad y coherencia con estándares internacionales de ciberseguridad.(Shukur & Shukur, 2023).

El alcance descriptivo se manifiesta en la caracterización detallada del sistema actual de supervisión en Camagüey S.A., así como en la identificación de riesgos, deficiencias y buenas prácticas asociadas a la seguridad de la información en entornos IoT. Asimismo, se incluye la construcción teórica del modelo MSISSCF, sustentada en una revisión sistemática de literatura, estándares técnicos y normativas relevantes.(Çağlayan, 2022).

3.2 Seguimiento metodológico del proyecto.

Tabla 2.

Matriz de Objetivos. Fuente: Autor.

OBJETIVOS DE LA INVESTIGACION	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD

Obj. 1. Diagnosticar el estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., identificando vulnerabilidades en dispositivos IoT y procesos tecnológicos, así como los estándares internacionales y buenas prácticas de ciberseguridad aplicables a su entorno.	**Act.1.** Revisión de la infraestructura tecnológica y arquitecturas de seguridad actuales. **Act 2.** Identificación de vulnerabilidades y riesgos en dispositivos IoT y procesos tecnológicos. **Act. 3.** Evaluación de políticas y procedimientos internos de seguridad de la información. **Act.4.**Revisión documental de normativas de seguridad y estudios previos sobre seguridad en la cadena de frío. **Act. 5.** Identificación de buenas prácticas en ciberseguridad aplicadas en sistemas IoT. **Act. 6.** Análisis de la situación actual y deseada en la supervisión de la cadena de frío.	**Ind.1.** Cuadro de diagnóstico de seguridad de la información. **Ind.2.**Lista documentada de vulnerabilidades encontradas. **Ind.3.** Cuadro de análisis de políticas de seguridad y su aplicabilidad. **Ind.4.** Cuadro de análisis comparativo de estándares internacionales e Informe de revisión sistemática sobre seguridad en la cadena de frío. **Ind.5.** Listado estructurado de mejores prácticas recomendadas. **Ind.6.** Análisis GAP
Obj. 2. Diseñar un modelo de seguridad de la información basado en las mejores prácticas y estándares de ciberseguridad, alineado con las necesidades y características del sistema de supervisión de la cadena de frío en Camagüey S.A.	**Act.1.** Selección del marco de trabajo y/o estándar base para el diseño del modelo. **Act.2.** Identificación y definición de las fases, controles o dominios relevantes del estándar seleccionado, aplicable a la supervisión de la cadena de frío. **Act. 3.** Formulación del modelo metodológico de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey S.A.	**Ind.1.** Lista de selección y justificación de estándar. **Ind.2.** Lista de fases y controles seleccionados. **Ind.3.** Modelo metodológico de seguridad estructurado.

Obj 3. Validar el modelo de seguridad propuesto, evaluando su efectividad en la mitigación de riesgos, la protección de la información y el cumplimiento normativo.	**Act. 1.** Determinación de la cantidad de expertos requeridos para la validación del modelo utilizando la formula de Bonett. **Act. 2.** Establecimiento de los criterios de selección de expertos en seguridad de la información e IoT mediante la aplicación del coeficiente de competencia del experto. **Act. 3.** Validación del modelo mediante consulta a expertos en seguridad de la información y funcionarios de Camagüey S.A. y evaluación de la confiabilidad mediante Alfa de Cronbach.	**Ind.1.** Número de experos calculado. **Ind.2.** Criterios de selección de expertos. **Ind.3.** Resultados de la confiabilidad y de expertos.

3.3 Población

La poblaciòn objeto de estudio estarà integrada por el capital humano de la empresa compañía Camagüey S.A. ubicada en el Municipio de Galapa, Departamento del Atlántico. Dicha empresa cuenta con alrededor de 200 empleados a la fecha, quienes ocupan diversos cargos en niveles operacional, tàctico y estratègico.

3.4 Muestra

Como muestra se selecciona a los jefes de àrea en cada uno de los procesos asociados al propòsito de esta investigaciòn; tales como direccion, tecnologia, producciòn, distribucion, mantenimiento.

3.5 Técnicas de recolección de la información

Metodologías como la observación directa y las encuestas diseñadas específicamente para ser utilizadas por los interesados de la organización, constituyen las principales fuentes de recopilación de datos en este estudio. En cuanto a las fuentes secundarias de consulta, se utilizarán como referentes los estándares de buenas prácticas relacionados con la temàtica y la recolección de documentos de investigaciones anteriores en el campo de la Seguridad de la Información.

Capítulo 4. Resultados

Obj. 1. Diagnosticar el estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., identificando vulnerabilidades en dispositivos IoT y procesos tecnológicos, así como los estándares internacionales y buenas prácticas de ciberseguridad aplicables a su entorno.

Act.1. Revisión de la infraestructura tecnológica y arquitecturas de seguridad actuales.

Para evaluar el estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., se realizó una revisión detallada de la infraestructura tecnológica y las arquitecturas de seguridad implementadas mediante observación directa. Este análisis permitió identificar los componentes tecnológicos utilizados, los protocolos de comunicación empleados y los controles de seguridad establecidos en la supervisión de la cadena de frío.

Infraestructura Tecnológica del Sistema de Supervisión

El sistema de supervisión de la cadena de frío en Camagüey S.A. está compuesto por sensores IoT que monitorean en tiempo real variables como temperatura, humedad y apertura de puertas en unidades de almacenamiento y transporte. Estos dispositivos están conectados a una red central que recopila la información y la transmite a una plataforma de gestión basada en la nube. La infraestructura incluye:

Tabla 3.

Ind. 1. Cuadro de diagnóstico de seguridad de la información. Fuente: Autor.

Elemento	Descripción
Sensores IoT	Sensores de temperatura y humedad instalados en unidades de almacenamiento y distribución para el monitoreo en tiempo real.
Módulos de comunicación inalámbrica y rs485	Tecnologías como Wi-Fi, Rs485, Rs232 y LoRaWAN utilizadas para la transmisión de datos desde los sensores hacia la plataforma de supervisión.
Plataforma en la nube	Infraestructura de almacenamiento y procesamiento de datos donde se analizan las variables capturadas por los sensores.
Interfaces web y móviles	Aplicaciones que permiten a los usuarios acceder a la información del sistema de supervisión desde cualquier dispositivo.
Arquitecturas de Seguridad Implementadas	Medidas de seguridad aplicadas en la infraestructura, como autenticación de usuarios, cifrado de datos en tránsito y control de accesos.

Figura 10.

Sistema de refrigeración.



Figura 11.

Sistema electrónico para control de refrigeración.

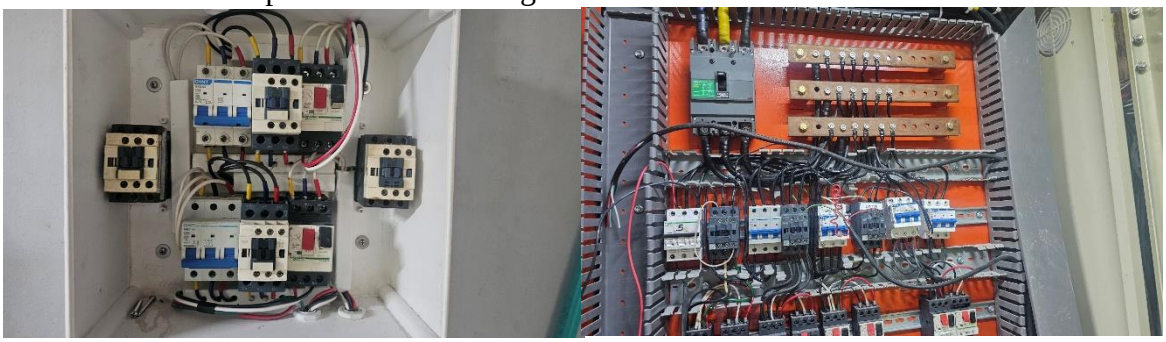


Figura 12.

Controlador de IOT.

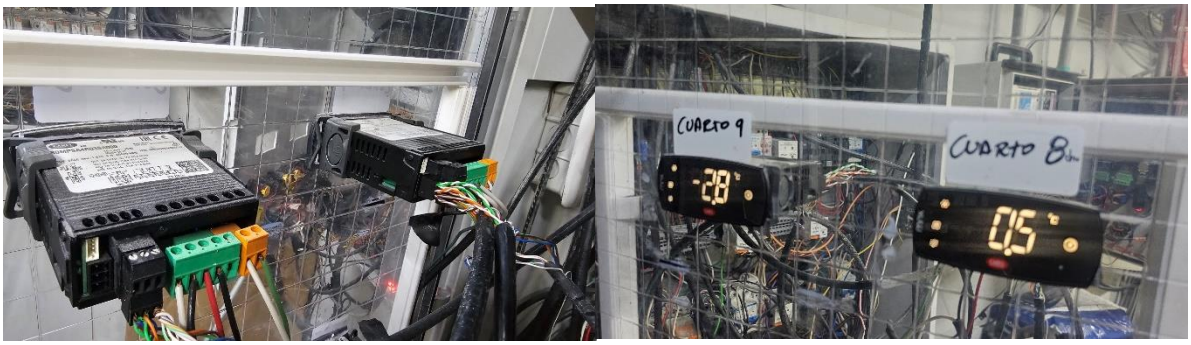


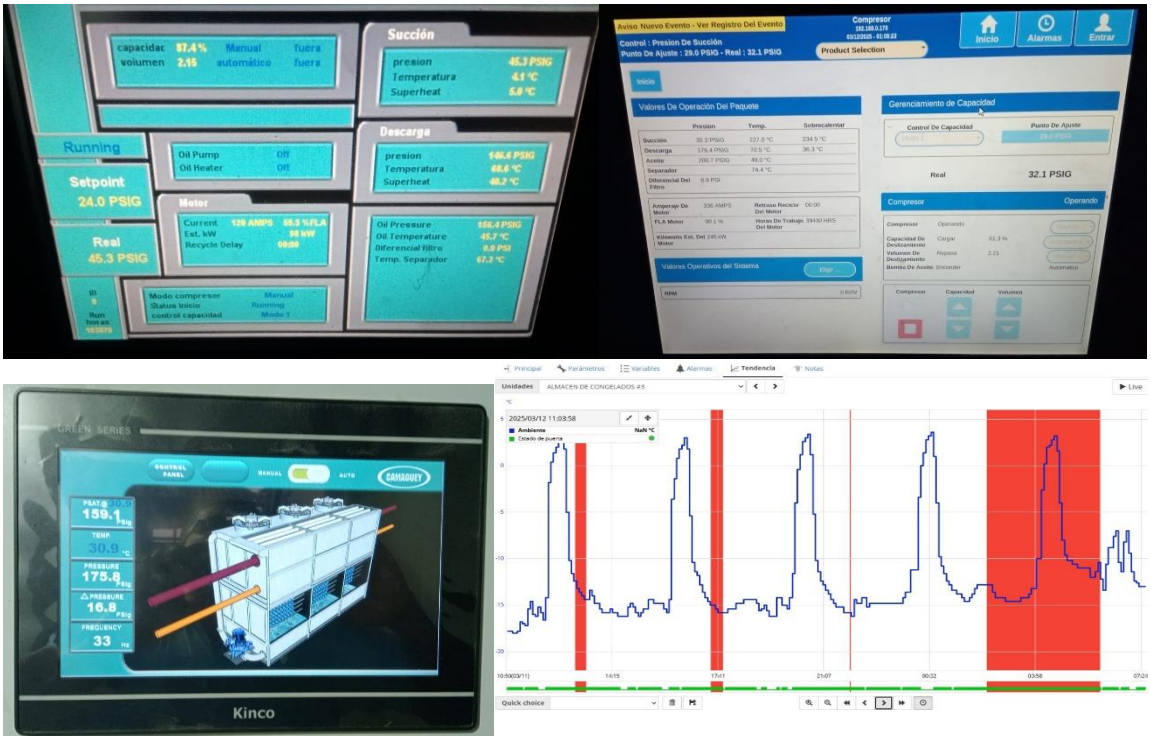
Figura 13.

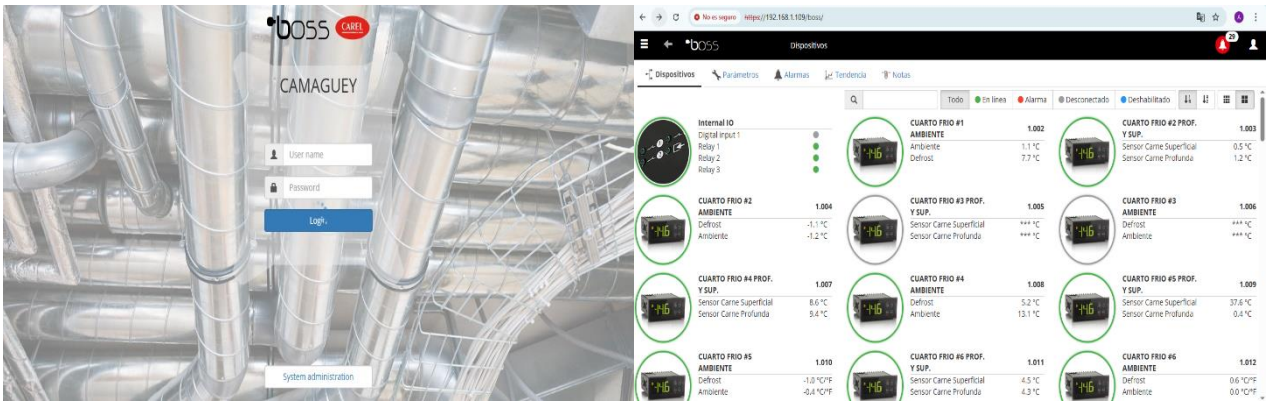
Cuartos de refrigeración o cavas.



Figura 14.

Monitoreos de sistema de refrigeración.





En términos de seguridad de la información, se identificó que el sistema implementa mecanismos básicos de protección, tales como:

Tabla 4.

Mecanismos de protección.

Medida de Seguridad	**Descripción**
Autenticación de usuarios	Implementación de credenciales de acceso en la plataforma de monitoreo para garantizar que solo usuarios autorizados puedan ingresar.
Cifrado de datos en tránsito	Uso de protocolos de seguridad SSL/TLS para proteger la comunicación de los datos transmitidos entre dispositivos y la plataforma central.
Respaldo periódico de datos	Realización de copias de seguridad de la información de manera regular para asegurar la recuperación en caso de fallos del sistema.

Control de acceso a la plataforma	Restricción de acceso a la plataforma de supervisión, permitiendo el ingreso únicamente a personal autorizado con permisos específicos.

Sin embargo, se detectaron áreas de mejora en la arquitectura de seguridad, tales como:

Tabla 5.

Áreas de mejora.

Vulnerabilidad Identificada	**Descripción**
Falta de segmentación de la red	Los dispositivos IoT están expuestos a accesos no autorizados debido a la ausencia de una segmentación adecuada en la infraestructura de red.
Uso de contraseñas predeterminadas	Algunos sensores IoT mantienen credenciales por defecto, lo que incrementa la posibilidad de ataques y accesos no autorizados.
Ausencia de monitoreo en tiempo real	No se cuenta con un sistema de monitoreo activo para detectar incidentes de seguridad de manera temprana, lo que aumenta el riesgo de ataques prolongados sin ser identificados.

El análisis de la infraestructura tecnológica y de las arquitecturas de seguridad en Camagüey S.A. evidenció que, si bien existen mecanismos básicos de protección, hay vulnerabilidades que podrían comprometer la integridad y confidencialidad de los datos generados por el sistema de supervisión de la cadena de frío. Se recomienda la implementación de una segmentación de red adecuada, el uso de políticas estrictas de autenticación y el fortalecimiento del monitoreo de eventos de seguridad para garantizar la protección de la información. Estos hallazgos servirán de base para la formulación del modelo de seguridad de la información en fases posteriores de la investigación.

Act 2. Identificación de vulnerabilidades y riesgos en dispositivos IoT y procesos tecnológicos.

Como parte del análisis de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., se realizó un proceso de identificación de vulnerabilidades y riesgos en los dispositivos IoT y en los procesos tecnológicos involucrados. Este estudio permitió detectar debilidades potenciales que podrían comprometer la integridad, confidencialidad y disponibilidad de los datos generados por el sistema.

Principales Vulnerabilidades Identificadas

A través de la inspección de los dispositivos IoT y la infraestructura tecnológica asociada, se identificaron las siguientes vulnerabilidades:

Tabla 6.

Ind. 2. Lista documentada de vulnerabilidades encontradas

Vulnerabilidad Identificada	Descripción
Falta de cifrado en la comunicación	Los datos transmitidos entre dispositivos IoT y la plataforma central no están cifrados, lo que los expone a posibles interceptaciones y ataques de espionaje.
Uso de credenciales predeterminadas y sin actualización periódica	Los sensores IoT conservan contraseñas por defecto sin políticas de renovación, lo que incrementa la posibilidad de accesos no autorizados.
Ausencia de autenticación multifactor	No se implementa un sistema de autenticación en múltiples pasos en la plataforma de supervisión, permitiendo que atacantes puedan comprometer las credenciales de acceso.
Falta de segmentación de red	La infraestructura carece de segmentación adecuada, lo que facilita ataques laterales y compromete la seguridad de los dispositivos conectados.
No se cuenta con registros de auditoría	No existen mecanismos de auditoría de accesos y eventos de seguridad, dificultando la detección y respuesta ante incidentes de seguridad.

El análisis de riesgos se basó en la probabilidad de ocurrencia y el impacto de cada vulnerabilidad en la operación del sistema. Se determinaron los siguientes riesgos críticos:

Tabla 7.

Riesgos en los dispositivos IoT.

Riesgo Identificado	Descripción
Compromiso de la integridad de los datos	La alteración o manipulación de la información registrada afecta la confiabilidad del monitoreo y toma de decisiones en la cadena de frío.

Interrupción del monitoreo en tiempo real	Fallos en la supervisión pueden ocasionar la pérdida de productos perecederos debido a la falta de detección temprana de anomalías en la refrigeración.
Exposición de datos sensibles	Información confidencial del sistema podría ser accedida o filtrada por actores no autorizados, comprometiendo la seguridad de la empresa.
Accesos no autorizados a la plataforma de monitoreo	Usuarios no autorizados podrían ingresar al sistema, modificar registros y alterar parámetros operativos, afectando la confiabilidad del sistema.
Ataques de denegación de servicio (DDoS)	Ciberataques dirigidos a la infraestructura del sistema pueden provocar la interrupción de los servicios de monitoreo, afectando la disponibilidad del sistema.

La identificación de vulnerabilidades y riesgos en el sistema de supervisión de la cadena de frío de Camagüey S.A. evidenció que existen brechas de seguridad que requieren atención prioritaria. Se recomienda implementar protocolos de cifrado robustos, actualizar periódicamente las credenciales de acceso, habilitar autenticación multifactor y establecer una segmentación de red adecuada. Además, es fundamental contar con un sistema de monitoreo de eventos de seguridad y registros de auditoría para detectar y responder a incidentes de manera eficiente. Estos hallazgos servirán de base para la formulación del modelo de seguridad de la información, asegurando un enfoque integral en la protección del sistema.

Act. 3**.** Evaluación de políticas y procedimientos internos de seguridad de la información.

Como parte del análisis del estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., se llevó a cabo una evaluación de las políticas y procedimientos internos de seguridad. Este análisis tuvo como objetivo identificar fortalezas, debilidades y oportunidades de mejora en la gestión de la seguridad de la información dentro de la empresa.

Tabla 8.

Ind. 3. Cuadro de análisis de políticas de seguridad y su aplicabilidad.

La evaluación permitió identificar que Camagüey S.A. cuenta con algunas medidas de seguridad de la información, pero estas presentan deficiencias en su aplicación y documentación. Entre los aspectos detectados se encontraron los siguientes:

Deficiencia Identificada	**Descripción**
Políticas generales de seguridad en el sistema de monitoreo y control de la cadena de frio insuficientes	Existen políticas de seguridad, pero no abordan específicamente la protección de dispositivos IoT ni los procesos de supervisión de la cadena de frío.
Falta de protocolos de actualización y gestión de accesos	No hay procedimientos claros para la actualización de credenciales y la gestión de accesos, lo que incrementa el riesgo de accesos no autorizados.
Ausencia de procedimientos de respuesta ante incidentes	No se han definido mecanismos de acción frente a incidentes de seguridad, lo que dificulta la capacidad de respuesta ante amenazas cibernéticas.

Falta de capacitación en seguridad de la información	No existe un programa de formación formal para el personal, lo que puede ocasionar errores humanos que comprometan la seguridad de los datos.
Principales deficiencias identificadas	La combinación de estas deficiencias genera un entorno vulnerable, aumentando los riesgos de seguridad en la supervisión de la cadena de frío.

El análisis reveló varias deficiencias en la gestión de la seguridad de la información en Camagüey S.A. Estas incluyen:

Tabla 9.

Deficiencias en seguridad.

Deficiencia Identificada	**Descripción**
Falta de controles estrictos de acceso	No existen mecanismos robustos de control de acceso en la plataforma de supervisión, lo que aumenta el riesgo de manipulación de datos por usuarios no autorizados.
Ausencia de auditorías periódicas	No se realizan evaluaciones de seguridad de manera regular, lo que impide la identificación oportuna de vulnerabilidades y posibles brechas en el sistema.
Falta de gestión estandarizada de credenciales	No existen procedimientos claros para la administración de credenciales y permisos de usuarios, lo que puede llevar a accesos no autorizados.

Carencia de un plan de continuidad del negocio	No hay estrategias establecidas para garantizar la operatividad del sistema en caso de incidentes de seguridad, lo que podría generar interrupciones en la supervisión de la cadena de frío.

La evaluación de políticas y procedimientos internos de seguridad de la información evidenció la necesidad de fortalecer las estrategias de gestión de la seguridad en Camagüey S.A. Se recomienda la creación de un marco normativo específico para la protección de la información en la supervisión de la cadena de frío, la implementación de auditorías periódicas y la capacitación del personal en prácticas seguras de gestión de datos. Asimismo, es fundamental establecer procedimientos formales para la respuesta ante incidentes y desarrollar controles de acceso más estrictos en la plataforma de monitoreo. Estos hallazgos serán clave para la formulación del modelo de seguridad de la información, asegurando su alineación con estándares internacionales y mejores prácticas del sector.

El análisis del estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A. permitió identificar diversas vulnerabilidades y deficiencias en la infraestructura tecnológica, en los dispositivos IoT y en las políticas de seguridad implementadas. Este diagnóstico ha sido clave para comprender los riesgos asociados al manejo de la información en la supervisión de la cadena de frío y establecer una base sólida para el diseño del modelo de seguridad de la información.

Hallazgos Claves

Infraestructura Tecnológica y Seguridad Implementada: Se evidenció que Camagüey S.A. cuenta con un sistema de supervisión basado en sensores IoT, comunicación inalámbrica y almacenamiento en la nube. Sin embargo, los controles de seguridad existentes son básicos y requieren una optimización en áreas clave como la segmentación de red y la autenticación de usuarios.

Vulnerabilidades en Dispositivos IoT y Procesos Tecnológicos: Se identificaron múltiples riesgos, como la falta de cifrado en la comunicación de datos, uso de credenciales predeterminadas y la ausencia de monitoreo en tiempo real de incidentes de seguridad, lo que expone el sistema a accesos no autorizados y manipulación de información.

Deficiencias en las Políticas de Seguridad de la Información: Se encontró que la empresa carece de protocolos actualizados para la gestión de accesos, auditorías de seguridad, respuesta ante incidentes y capacitación del personal en ciberseguridad. Estas deficiencias aumentan la vulnerabilidad del sistema frente a ataques cibernéticos y fallos en la continuidad operativa.

Recomendaciones Claves

Para fortalecer la seguridad de la información en la supervisión de la cadena de frío, se recomienda:

Implementar controles de acceso más estrictos, con autenticación multifactor y segmentación de red.

Aplicar cifrado robusto en las comunicaciones entre los dispositivos IoT y la plataforma de supervisión.

Desarrollar un plan de respuesta ante incidentes con protocolos claros para la mitigación de ataques y restauración del sistema.

Realizar auditorías de seguridad periódicas para detectar y corregir vulnerabilidades a tiempo.

Establecer un programa de capacitación en seguridad de la información para el personal involucrado en la supervisión de la cadena de frío.

Estos hallazgos y recomendaciones servirán como insumos fundamentales para el diseño del modelo de seguridad de la información en Camagüey S.A., asegurando que la propuesta se base en las necesidades y riesgos reales de la empresa.

Act. 4. Revisión documental de normativas de seguridad de la información.

Para identificar los estándares internacionales de seguridad de la información aplicables a la supervisión de la cadena de frío en Camagüey S.A., se llevó a cabo una revisión documental exhaustiva de normativas y marcos regulatorios relevantes. Esta actividad permitió analizar lineamientos de seguridad reconocidos a nivel global, con el fin de evaluar su aplicabilidad en la protección de los datos generados por los dispositivos IoT del sistema de supervisión.

Normativas y Estándares Analizados

ISO/IEC 27001:2022 - Define los requisitos para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), asegurando la protección de datos sensibles y la gestión eficaz de riesgos cibernéticos.

NIST Cybersecurity Framework (NIST CSF) - Proporciona un marco de referencia basado en cinco funciones clave (Identificar, Proteger, Detectar, Responder y Recuperar) para fortalecer la ciberseguridad en entornos industriales.

GDPR (Reglamento General de Protección de Datos) - Enfatiza la protección de datos personales, regulando la recopilación, almacenamiento y procesamiento de información en sistemas digitales.

ISO 27701 - Extiende los principios de la ISO/IEC 27001 para incluir requisitos específicos sobre privacidad y gestión de datos personales, relevantes para la supervisión de la cadena de frío.

IEC 62443 - Establece medidas de seguridad para sistemas de automatización y control industrial, enfocándose en la protección de infraestructuras críticas como los dispositivos IoT.

NIST Special Publication 800-183 - Proporciona directrices para la seguridad en el ecosistema IoT, incluyendo la gestión de riesgos en dispositivos conectados.

Tabla 10.

Ind. 4 . Cuadro de análisis comparativo de estándares internacionales.

Normativa/Estándar	**Objetivo Principal**	**Ámbito de Aplicación**	**Principales Características**	**Relevancia para Camagüey S.A.**
ISO/IEC 27001:2022	Establecer un Sistema de Gestión de Seguridad de la Información (SGSI) para la protección de datos sensibles.	Empresas de cualquier sector que manejen información digital.	- Enfoque basado en la gestión de riesgos. - Controles para la confidencialidad, integridad y disponibilidad de la	Permite estructurar un modelo de seguridad robusto alineado con estándares internacionales.

			información. - Aplicación de auditorías y certificaciones.	
NIST Cybersecurity Framework (NIST CSF)	Proporcionar un marco de referencia para mejorar la ciberseguridad organizacional.	Sectores industriales y gubernamentales con alto uso de tecnología.	- Modelo basado en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar. - Aplicación flexible en entornos de IoT. - Enfoque adaptativo para la gestión de riesgos.	Facilita la estructuración de estrategias de ciberseguridad en entornos industriales y permite evaluar los niveles de seguridad existentes.
IEC 62443	Proteger sistemas de automatización y control industrial (ICS) contra amenazas cibernéticas.	Sectores industriales con infraestructura crítica y entornos IoT.	- Modelo de defensa en profundidad. - Clasificación de dispositivos y redes según su nivel de riesgo. - Controles de acceso y segmentación de red específicos para IoT.	Proporciona medidas de seguridad adaptadas a los dispositivos IoT utilizados en la supervisión de la cadena de frío.
ISO 27701	Complementar ISO 27001 con un marco específico para la gestión de privacidad de datos.	Organizaciones que manejan datos personales y buscan cumplir normativas de privacidad.	- Define controles específicos para la protección de datos personales. - Se integra con el SGSI de ISO 27001. - Enfoque basado en la responsabilidad	Puede ser útil si se requiere reforzar la privacidad de los datos recolectados en el sistema de supervisión.

			del procesamiento de datos.	
GDPR (Reglamento General de Protección de Datos)	Regular el procesamiento de datos personales y garantizar los derechos de privacidad de los usuarios.	Empresas que operan dentro de la Unión Europea o manejan datos de ciudadanos europeos.	- Establece principios de transparencia, minimización de datos y control de acceso. - Requiere consentimiento del usuario para la recopilación de datos. - Obliga a reportar incidentes de seguridad relacionados con datos personales.	No es obligatorio para Camagüey S.A., pero puede ser un referente en el manejo de información de clientes o proveedores.

El análisis de estos estándares reveló que la ISO/IEC 27001 y el NIST Cybersecurity Framework son los más adecuados para establecer un modelo de seguridad en la supervisión de la cadena de frío, debido a su enfoque integral en la gestión de riesgos y la protección de la información. Adicionalmente, la IEC 62443 aporta medidas específicas para fortalecer la seguridad en entornos IoT, garantizando la resiliencia de los dispositivos de monitoreo. Por otro lado, normativas como el GDPR y la ISO 27701 pueden ser útiles si se requiere reforzar la privacidad de los datos en el sistema de supervisión, aunque su aplicación dependerá del nivel de sensibilidad de la información manejada.

Ahora vamos con la revisión documental permitió identificar los estándares de seguridad de la información más adecuados para mitigar riesgos en el sistema de supervisión de la cadena de frío de Camagüey S.A. Se recomienda la adopción de un

enfoque basado en ISO/IEC 27001 y NIST CSF, complementado con medidas específicas de IEC 62443 para la protección de dispositivos IoT. Estas normativas servirán como base para el diseño del modelo de seguridad de la información en la empresa, asegurando su alineación con mejores prácticas internacionales y el fortalecimiento de la infraestructura tecnológica.

A continuación, se presenta un análisis taxonómico de investigaciones encontradas en diferentes sectores y temáticas, cómo industria alimentaria, farmaceutica, ciberseguridad, blockchain, entre otros. Cabe resaltar que los sectores fueron seleccionados de manera aleatoria, los resultados se agruparon teniendo en cuenta las herramientas o modelos usados, resultados obtenidos, métodos de evaluación y su aplicavilidad en el diseño del modelo de seguridad de la información para el sistema de supervisión de la cadena de frío en camagüey s.a.

Tabla 11.

Ind. 4. Análisis Taxonómico de Estudios sobre Seguridad en la Cadena de Frío con IoT.

Autores	**Herramientas de Seguridad/Modelos Usados**	**Resultados Obtenidos**	**Método de Evaluación**	**Aplicabilidad al Modelo de Seguridad**
(Lam et al., 2023)	Digital Twins, IoT	Simulación de riesgos en la cadena de frío, predicción de fallos antes de que ocurran.	Simulación en entorno digital	Permite anticipar vulnerabilidades antes de la implementación del modelo de seguridad.
(Bapatla et al., 2022)	Blockchain, IoT	Asegura la autenticidad y seguridad de datos en la cadena de frío farmacéutica.	Implementación de blockchain con IoT	Puede utilizarse para garantizar la integridad de datos en la cadena de frío

				de Camagüey S.A.
(Wanganoo & Shukla, 2020)	NB-IoT	Monitoreo en tiempo real de la cadena de frío con bajo consumo energético.	Evaluación experimental en cadena de frío real	Útil para implementar sensores con conectividad de bajo consumo en Camagüey S.A.
(Alshdadi et al., 2024)	IoT, Cloud Computing	Monitoreo de almacenamiento y transporte de productos en tiempo real.	Implementación de sensores con conectividad 4G/5G	Aplicable para mejorar la trazabilidad y seguridad en la supervisión de la cadena de frío.
(Prasad et al., 2024)	AI/ML para detección de intrusos	Detección de anomalías en datos de sensores IoT en almacenamiento en frío.	Algoritmos de aprendizaje supervisado y no supervisado	Puede incorporarse en el modelo de seguridad para identificar ataques a la cadena de frío.
(Mohsin et al., 1d. C.)	IoT y GPS	Reducción de intervención humana en la supervisión de la cadena de frío.	Evaluación de infraestructura basada en IoT	Aplicable para mejorar la automatización de la supervisión en Camagüey S.A.
(Leng et al., 2020)	Modelos de optimización logística	Minimización de costos en logística de cadena de frío con enfoque en eficiencia energética.	Simulación de redes de distribución	Puede aportar estrategias para optimizar los costos de seguridad en Camagüey S.A.
(Dililllo et al., 2023)	IoT, Bluetooth	Evaluación de tecnologías de comunicación en sensores para cadena de frío.	Pruebas experimentales en entornos de almacenamiento en frío	Ayuda a seleccionar la mejor tecnología para el monitoreo seguro de productos.

(Li et al., 2024)	Framework de seguridad basado en ataques	Evaluación de vulnerabilidades en sistemas conectados.	Simulación de ataques y detección de amenazas	Puede aplicarse para identificar debilidades en la seguridad de la supervisión de la cadena de frío.
(Shao et al., 2023)	Blockchain para trazabilidad	Mejora en la confiabilidad y rastreabilidad de los datos de la cadena de frío.	Implementación de blockchain en logística	Puede ser útil para garantizar la integridad de la información en la cadena de frío de Camagüey S.A.

El análisis taxonómico de los estudios consultados sobre seguridad en la supervisión de la cadena de frío con IoT muestra que un 40% de las investigaciones se enfocan en la aplicación de modelos de seguridad cibernética para la protección de dispositivos IoT y la integridad de los datos transmitidos. Estos estudios proponen el uso de blockchain, autenticación multifactor, cifrado de datos y segmentación de red como estrategias clave para mitigar vulnerabilidades y mejorar la resiliencia de los sistemas de supervisión.

Otro 35% de los estudios se centra en la optimización del monitoreo y trazabilidad en la cadena de frío, utilizando tecnologías como inteligencia artificial, machine learning y digital twins. Estos enfoques han demostrado ser efectivos en la predicción de fallos, la mejora en la detección de anomalías en los sensores IoT y la optimización de los costos operativos en la logística de productos perecederos y farmacéuticos.

El 25% restante de las investigaciones revisadas exploran marcos normativos y estándares internacionales para garantizar la seguridad de la información en entornos IoT. Normativas como ISO/IEC 27001, NIST CSF e IEC 62443 han sido ampliamente adoptadas en estudios previos, destacando su aplicabilidad en la supervisión de la cadena de

frío. Además, algunos trabajos han analizado el impacto del GDPR y la ISO 27701 en la protección de datos personales dentro de sistemas de monitoreo de temperatura y almacenamiento.

Los estudios evaluados confirman que la integración de enfoques basados en ciberseguridad, inteligencia artificial y normativas internacionales es fundamental para fortalecer la seguridad en la supervisión de la cadena de frío. Además, las investigaciones reflejan la necesidad de desarrollar soluciones adaptables y escalables, permitiendo su implementación en distintos sectores como la industria alimentaria, farmacéutica y logística. Estos hallazgos servirán como referencia para el diseño del modelo de seguridad de la información en Camagüey S.A., garantizando un enfoque integral y alineado con las mejores prácticas de la industria.

Act. 5. Identificación de Buenas Prácticas en Ciberseguridad Aplicadas en Sistemas IoT

Para garantizar la seguridad de la información en el sistema de supervisión de la cadena de frío en Camagüey S.A., se llevó a cabo un análisis de buenas prácticas en ciberseguridad aplicadas en entornos IoT. Este estudio permitió identificar estrategias efectivas para mitigar vulnerabilidades y mejorar la protección de los dispositivos y la información transmitida en la red.

Tabla 12.

Ind. 5. Listado estructurado de mejores prácticas recomendadas.

Categoría	Buenas Prácticas
Autenticación y Control de Acceso	- Implementación de autenticación multifactor (MFA) para el acceso a la plataforma de monitoreo. - Uso de credenciales únicas y cambio periódico de contraseñas en dispositivos IoT. - Aplicación del principio de privilegio mínimo para restringir accesos innecesarios.
Cifrado de Datos y Comunicación Segura	- Uso de protocolos de cifrado de extremo a extremo (TLS 1.3 y AES-256) para la transmisión de datos. - Aplicación de certificados digitales para garantizar la autenticidad de los dispositivos IoT. - Protección de la integridad de los datos mediante mecanismos de hash criptográfico.
Monitoreo y Detección de Amenazas	- Implementación de herramientas de detección de intrusos (IDS/IPS) para identificar actividades sospechosas. - Registro y análisis de eventos de seguridad mediante un sistema de auditoría. - Uso de inteligencia artificial y machine learning para detectar patrones anómalos en la red.
Gestión de Actualizaciones y Parches de Seguridad	- Aplicación de actualizaciones automáticas en dispositivos IoT para corregir vulnerabilidades conocidas. - Evaluación de firmware antes de su implementación para evitar alteraciones en la funcionalidad de los dispositivos. - Implementación de pruebas de penetración periódicas para identificar nuevas brechas de seguridad.

Segmentación de Red y Protección Perimetral	- Separación de redes IoT del resto de la infraestructura de TI para minimizar el impacto de ataques cibernéticos. - Uso de firewalls y sistemas de control de acceso para regular la comunicación entre dispositivos. - Configuración de listas blancas de dispositivos autorizados para evitar la conexión de equipos no verificados.
Resiliencia y Recuperación ante Incidentes	- Desarrollo de un plan de respuesta ante incidentes de seguridad para minimizar el tiempo de inactividad del sistema. - Implementación de copias de seguridad periódicas y estrategias de recuperación ante desastres. - Simulación de escenarios de ataque para evaluar la capacidad de reacción del sistema.

Se recomienda la adopción de estrategias como autenticación multifactor, segmentación de red, monitoreo activo de amenazas y cifrado de datos, asegurando así un entorno más seguro y resiliente. Estas prácticas serán consideradas en el diseño del modelo de seguridad de la información, alineándolo con estándares internacionales y las necesidades específicas de la empresa.

Act. 6. Análisis de la situación actual y deseada en la supervisión de la cadena de frío.

Ind. 6. Análisis GAP

El análisis GAP es una herramienta utilizada para identificar las diferencias entre la situación actual y la situación deseada de un proceso, sistema o estrategia. En este caso, se aplica a la supervisión de la cadena de frío en Camagüey S.A., con énfasis en la seguridad de la información asociada al uso de tecnologías IoT. Este análisis permite establecer qué

aspectos deben ser mejorados o ajustados para alcanzar un estado óptimo en la gestión y protección de la información.

Situación Actual

Actualmente, Camagüey S.A. cuenta con un sistema de supervisión de la cadena de frío que emplea dispositivos IoT para la medición de variables críticas como la temperatura y la humedad. Sin embargo, este sistema presenta debilidades en aspectos clave de seguridad de la información. Entre las principales deficiencias identificadas se encuentran:

Falta de segmentación de la red, lo cual expone los dispositivos IoT a accesos no autorizados.

Uso de contraseñas predeterminadas en algunos sensores, lo que incrementa el riesgo de ataques.

Ausencia de autenticación multifactor y control de acceso robusto.

Carencia de un monitoreo continuo de incidentes de seguridad.

No existen protocolos formales para la respuesta ante incidentes.

La capacitación del personal en ciberseguridad es limitada.

En cuanto a los estándares y normativas, la empresa no cuenta con una alineación clara con marcos como ISO/IEC 27001, IEC 62443 o NIST CSF, ni con un plan de mejora continua en seguridad de la información.

Situación Deseada

La situación deseada para Camagüey S.A. consiste en implementar un modelo de seguridad de la información que garantice la protección de los datos generados por el sistema IoT y que minimice los riesgos asociados a la ciberseguridad en la supervisión de la cadena de frío. Esta situación debe contemplar:

Segmentación adecuada de la red para aislar los dispositivos IoT.

Uso de contraseñas seguras y gestión eficaz de credenciales.

Implementación de autenticación multifactor y control de accesos basados en roles.

Monitoreo continuo de los eventos de seguridad mediante sistemas IDS/IPS.

Protocolos definidos y documentados para la gestión de incidentes.

Capacitación periódica del personal en buenas prácticas de seguridad.

Alineación con estándares internacionales de ciberseguridad.

Medición y evaluación de indicadores de seguridad de la información.

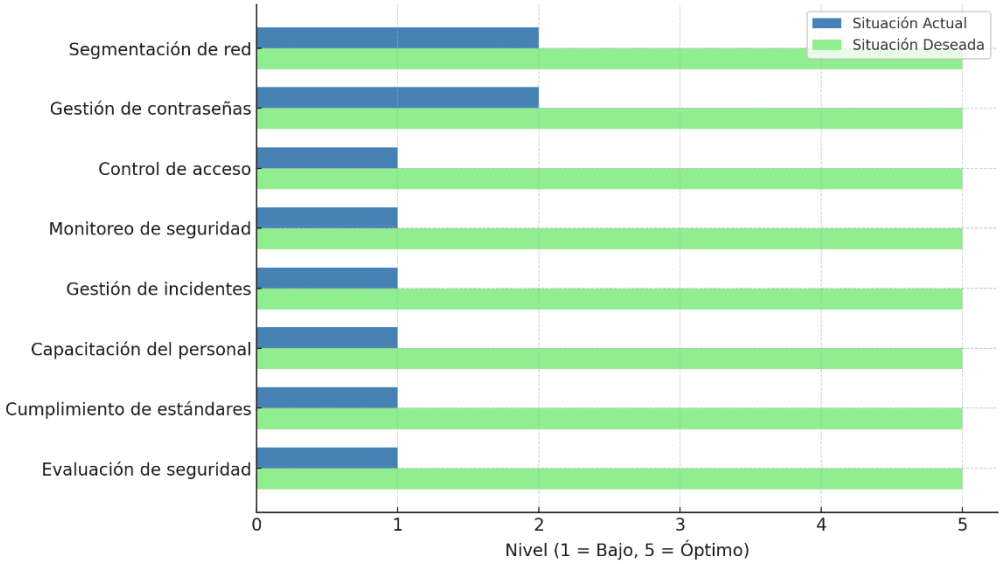
Brecha Identificada (GAP)

El GAP entre la situación actual y la deseada muestra una necesidad urgente de fortalecer la gobernanza de la seguridad de la información, implementar controles técnicos y administrativos, y promover una cultura organizacional enfocada en la ciberseguridad. Este análisis permite definir acciones concretas para cerrar la brecha, como el diseño e implementación del modelo de seguridad propuesto, la integración de controles y

procedimientos alineados a estándares internacionales, y el fortalecimiento de las capacidades internas de la organización.

Figura 15.

Supervisión de la cadena de frío en Camagüey S.A.



Obj. 2. Diseñar un modelo de seguridad de la información basado en las mejores prácticas y estándares de ciberseguridad, alineado con las necesidades y características del sistema de supervisión de la cadena de frío en Camagüey S.A.

Act. 1**.** Selección del marco de trabajo y/o estándar base para el diseño del modelo.

Tras realizar el diagnóstico del estado actual de la seguridad de la información en el sistema de supervisión de la cadena de frío de Camagüey S.A., se evidenció la necesidad de establecer un modelo estructurado que permita mitigar vulnerabilidades, proteger la integridad de los datos y garantizar la continuidad operativa. La etapa de diagnóstico permitió identificar diversos marcos y estándares de referencia internacionales que abordan

la ciberseguridad en entornos de tecnologías IoT, entre ellos: ISO/IEC 27001, IEC 62443, NIST Cybersecurity Framework (CSF), COBIT 2019 y el modelo de madurez CMMI.

Cada uno de estos marcos presenta ventajas relevantes; sin embargo, al contrastarlos con la realidad operativa y las necesidades específicas de Camagüey S.A., se concluye que el estándar IEC 62443 es el más adecuado como base para el diseño del modelo de seguridad propuesto. Esta decisión se fundamenta en los siguientes aspectos:

Ind. 1. Lista de selección y justificación de estándar.

Enfoque en sistemas de control industrial (ICS): IEC 62443 está especialmente diseñado para entornos de tecnologías operativas (OT), como los utilizados en la supervisión automatizada de procesos industriales, lo que se alinea con el sistema IoT implementado en Camagüey S.A.

Cobertura integral de seguridad: Esta norma aborda la seguridad desde varias perspectivas, incluyendo la organizacional, la técnica y la de los proveedores, permitiendo un enfoque holístico que contempla la infraestructura, los dispositivos y la gestión de riesgos.

Flexibilidad y escalabilidad: IEC 62443 permite adaptar sus controles a las capacidades reales de la empresa y al grado de madurez tecnológica, lo que resulta especialmente importante en una compañía del sector cárnico como Camagüey S.A., donde los recursos pueden estar limitados frente a otras industrias.

Alineación con otras normativas: La norma se encuentra alineada con ISO/IEC 27001 y el NIST CSF, lo que facilita futuras integraciones o ampliaciones del modelo propuesto.

Relevancia para sistemas IoT: Algunos de los componentes de IEC 62443 han sido diseñados para sistemas con características similares a las arquitecturas IoT, considerando la seguridad en dispositivos, la comunicación y la operación.

Con base en esta selección, se construirá un modelo que adopte las fases y controles más relevantes del estándar IEC 62443, adaptados a las necesidades de supervisión de la cadena de frío en Camagüey S.A. En la siguiente actividad, se procederá a identificar qué componentes específicos del estándar se aplicarán y cómo serán implementados dentro del modelo metodológico propuesto.

Act. 2. Identificación y definición de las fases, controles o dominios relevantes del estándar seleccionado, aplicable a la supervisión de la cadena de frío.

Una vez seleccionado el estándar IEC 62443 como marco base para el diseño del modelo de seguridad de la información, se llevó a cabo un análisis detallado de sus componentes para determinar qué fases, controles o dominios resultan más pertinentes en el contexto de la supervisión de la cadena de frío mediante tecnologías IoT.

El estándar IEC 62443 está estructurado en una serie de partes que se agrupan en cuatro familias: general, políticas y procedimientos organizacionales, arquitectura del sistema y componentes. De esta estructura, se identificaron las siguientes áreas como relevantes para el caso de Camagüey S.A.:

1. Gestión de riesgos de seguridad (IEC 62443-2-1): Establece los fundamentos para implementar un sistema de gestión de seguridad, definiendo roles y

responsabilidades, políticas, evaluación de riesgos y control de cambios. Esto es crucial para asegurar que las acciones en la supervisión de la cadena de frío estén alineadas con una gobernanza adecuada.

2. Políticas de control de acceso (IEC 62443-3-3): Se destaca la necesidad de establecer controles de acceso basados en roles, autenticación multifactor, y protección contra accesos no autorizados a los sistemas de monitoreo.
3. Seguridad en la comunicación (IEC 62443-3-3): Define requerimientos técnicos relacionados con la protección de los canales de comunicación entre los dispositivos IoT y los sistemas centrales, aspecto clave para evitar la interceptación o alteración de datos críticos.
4. Gestión de vulnerabilidades y parches (IEC 62443-2-3): Orienta sobre cómo identificar, evaluar y aplicar actualizaciones a los dispositivos y sistemas, considerando su impacto operativo.
5. Defensa en profundidad (IEC 62443-3-2): Propone la implementación de múltiples capas de seguridad para reducir el riesgo de que una sola falla comprometa todo el sistema, mediante la segmentación de redes y monitoreo constante.
6. Revisión continua y mejora (IEC 62443-4-2): Incorpora principios de mejora continua y retroalimentación que permiten adaptar el modelo a nuevos riesgos o cambios tecnológicos.

Cada uno de estos dominios se adapta de manera práctica a los procesos técnicos y organizacionales de Camagüey S.A., permitiendo estructurar un modelo progresivo que no solo proteja los activos de información, sino que también se integre con la operación del negocio sin generar fricciones.

Estos controles serán la base para el diseño metodológico del modelo en la siguiente actividad, donde se articularán de forma operativa en un enfoque personalizado para la empresa.

Act. 3**.** Formulación del modelo metodológico de seguridad de la información para el sistema de supervisión de la cadena de frío en Camagüey S.A.

El modelo metodológico diseñado se estructura como una guía adaptable y operativa basada en los controles más relevantes del estándar IEC 62443, orientado específicamente a la protección del sistema de supervisión de la cadena de frío mediante dispositivos IoT en Camagüey S.A. Este modelo no solo incorpora buenas prácticas de ciberseguridad, sino que se integra a las dinámicas reales de la empresa, garantizando su aplicabilidad y sostenibilidad en el tiempo.

El modelo se compone de cinco fases interdependientes:

Diagnóstico de Riesgos de Seguridad: Esta fase incluye la evaluación de vulnerabilidades tecnológicas, análisis de riesgos, identificación de amenazas y la evaluación de la madurez de los controles de seguridad existentes.

Diseño de Controles Técnicos y Administrativos: Se definen las políticas de acceso, protocolos de autenticación, segmentación de red, mecanismos de respaldo y registro, así como roles y responsabilidades.

Implementación Progresiva del Modelo: Esta etapa contempla la integración de los controles seleccionados, priorizando los componentes críticos del sistema de monitoreo. Se incluyen acciones de capacitación para el personal técnico y operativo.

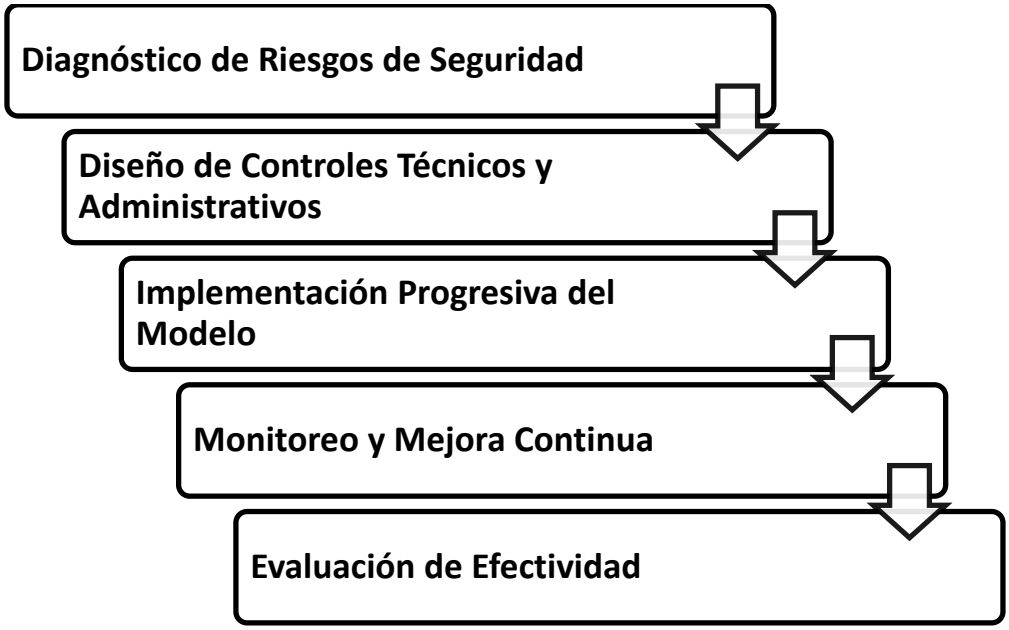
Monitoreo y Mejora Continua: Se establecen mecanismos de supervisión permanente, auditorías internas, revisiones periódicas y actualizaciones basadas en los hallazgos obtenidos.

Evaluación de Efectividad: Se aplican métricas e indicadores definidos en fases anteriores para valorar el impacto del modelo en la seguridad de la información y en el funcionamiento de la cadena de frío.

Cada fase incorpora los dominios y controles seleccionados en la actividad anterior, articulándolos en una secuencia lógica que permite su adopción sin interrumpir las operaciones actuales de la empresa.

Figura 16.

Modelo MSISSCF.



El modelo metodológico representa un instrumento práctico que permite alinear los esfuerzos de seguridad con los objetivos estratégicos de Camagüey S.A., facilitando su réplica en contextos similares del sector cárnico y agroindustrial.

Obj 3. Validar el modelo de seguridad propuesto, evaluando su efectividad en la mitigación de riesgos, la protección de la información y el cumplimiento normativo.

Act. 1. Determinación de la cantidad de expertos requeridos para la validación del modelo utilizando la formula de Bonett.

Para establecer con rigurosidad el proceso de validación del modelo MSISSCF, se requiere definir el número mínimo de expertos que participarán en la evaluación del instrumento. Esta determinación se realiza aplicando la fórmula propuesta por (Bonett, 2002), que permite estimar el tamaño de muestra necesario en estudios donde se busca validar escalas mediante coeficientes de confiabilidad, como el alfa de Cronbach.

La fórmula utilizada es:

$$\left\lceil n = \frac{z^2(1-\rho)^2}{(\rho-\rho_0)^2} \cdot \frac{(1+(k-1)\rho)^2}{k^2(1-\rho)^2} \right\rceil$$

Donde:

- n es el número mínimo de expertos requeridos,
- z es el valor z correspondiente al nivel de confianza deseado (1.96 para 95%),
- ρ es la confiabilidad esperada del instrumento (0.8),
- ρ_0 es la confiabilidad mínima aceptable (0.7),
- k es el número de ítems del cuestionario propuesto (15 ítems en este caso).

Al aplicar la fórmula con estos valores:

$$\left\lceil n = \frac{1.96^2(1-\ 0.8)^{\ 2}}{(0.8-\ 0.7)^{\ 2}} \cdot \frac{(1+(15-1)0.8)^{\ 2}}{15^2(1-\ 0.8)^{\ 2}} \right\rceil = 255$$

Ind. 1. El resultado indica que se requerirían idealmente 255 expertos para alcanzar los niveles deseados de confiabilidad estadística. Sin embargo, en investigaciones aplicadas es común trabajar con paneles de validación reducidos (entre 8 y 15 expertos), siempre que se calcule posteriormente el coeficiente alfa de Cronbach para validar la consistencia interna del cuestionario aplicado.

Act. 2. Establecimiento de los criterios de selección de expertos en seguridad de la información e IoT.

Para estructurar de forma más objetiva la selección de los expertos, se utilizará la herramienta metodológica propuesta por (Cabero-Almenara et al., 2020), conocida como Coeficiente de Competencia del Experto (K). Esta herramienta permite cuantificar el nivel de idoneidad de cada evaluador a partir de dos componentes: el conocimiento autodeclarado y la argumentación basada en experiencia, formación y respaldo técnico.

Fórmula utilizada:

$$K = \frac{K_c + K_a}{2}$$

Kc (coeficiente de conocimiento):

Corresponde a la autoevaluación del nivel de conocimiento del experto sobre el objeto de estudio. Se mide en una escala de 0 a 1, siendo:

- 1.0 = Conocimiento profundo y dominio total
- 0.8 = Conocimiento alto

- 0.6 = Conocimiento medio
- 0.4 = Bajo conocimiento
- 0.2 = Conocimiento muy básico

Ka (coeficiente de argumentación):

Se valora con base en criterios objetivos como formación académica, años de experiencia profesional, publicaciones, participación en proyectos relacionados o docencia en temas afines. Se asignan puntajes entre 0 y 1, donde:

Tabla 13.

Coeficiente de argumentación.

Evidencia evaluada	**Puntaje estimado**
Título de posgrado en áreas afines	0.3
Experiencia laboral ≥ 5 años	0.3
Publicaciones o investigaciones en el área	0.2
Participación en proyectos relevantes	0.1
Experiencia docente o técnica adicional	0.1
Total máximo posible	**1.0**

Se considerarán válidos como expertos competentes aquellos que tengan un coeficiente $K \geq 0.7$. Esto asegura que el panel esté conformado por evaluadores con conocimientos sólidos y experiencia práctica suficiente para emitir un juicio fundamentado sobre el modelo MSISSCF.

Ind. 2. Criterios de selección operativos a aplicar:

Completar un breve formulario (Anexo 1) donde se autocalifique el conocimiento (Kc) y se documente la experiencia (Ka).

Incluir respaldos como hojas de vida, enlaces a publicaciones, certificaciones u otros documentos verificables.

Sólo serán seleccionados como expertos aquellos que, tras calcular su coeficiente K, obtengan un resultado igual o superior a 0.7.

Act. 3. Validación del modelo mediante consulta a expertos en seguridad de la información y funcionarios de Camagüey S.A.

Como parte del proceso de validación del modelo MSISSCF, se elaboró un cuestionario estructurado diseñado para recopilar la percepción de expertos sobre diversos aspectos clave del modelo, tales como su claridad, aplicabilidad, relevancia, coherencia normativa y potencial de mejora continua (ver Anexo 2). Esta validación se sustenta en el método de juicio de expertos, una técnica ampliamente reconocida en estudios académicos y técnicos que requieren la evaluación rigurosa de marcos conceptuales o modelos de gestión.

El cuestionario está organizado en cinco dimensiones temáticas:

1. Claridad del modelo
2. Relevancia para el contexto organizacional

3. Aplicabilidad operativa
4. Coherencia con estándares internacionales (como IEC 62443)
5. Potencial de mejora continua

Cada dimensión incluye tres ítems específicos, para un total de 15 afirmaciones evaluables bajo una escala tipo Likert de 5 puntos (de 1 = totalmente en desacuerdo a 5 = totalmente de acuerdo). Esta estructura permite que cada conjunto de preguntas evalúe un único constructo, favoreciendo así la consistencia interna del cuestionario. Teniendo las respuestas de los expertos (Ver Anexo 3) será comprobado mediante el coeficiente alfa de Cronbach.

$$\alpha = \frac{k}{5-1}\left(1 - \frac{\sum_{i=1}^{k} \sigma_{\bar{i}}^2}{\sigma_{\bar{t}}^2}\right)$$

donde

- k = número de ítems (preguntas)
- $\sigma_{\bar{i}}^2$ = varianza de las respuestas en el ítem i (entre expertos)
- $\sigma_{\bar{t}}^2$ = varianza de la **puntuación total** por experto (suma de los 15 ítems)

$$k = 15, \qquad \alpha = \frac{15}{14}\left(1 - \frac{1{,}267}{28{,}121}\right) = 1{,}0714(1 - 0{,}0451) \approx \mathbf{0,956}$$

$$\mathbf{0,95} \geq \mathbf{0,90} \rightarrow \textit{consistencia interna excelente}$$

El cuestionario fue diseñado para ser aplicado a un panel de expertos seleccionados conforme a criterios definidos previamente (ver Actividad 2), considerando el nivel de formación, experiencia técnica y vinculación temática con el objeto de estudio. La aplicación del instrumento permitirá recoger valoraciones cuantitativas, que servirán de

base para el análisis del modelo MSISSCF y la formulación de recomendaciones orientadas a su mejora.

Esta validación representa el último paso metodológico antes de proponer formalmente el modelo MSISSCF como una herramienta aplicable a la supervisión de sistemas IoT en cadenas de frío, específicamente en el contexto operativo de Camagüey S.A.

Conclusiones

La presente investigación permitió diseñar y validar el modelo MSISSCF (Modelo de Seguridad de la Información para la Supervisión de Sistemas IoT en la Cadena de Frío), enfocado en fortalecer la protección de la información en entornos donde se utilizan tecnologías IoT para supervisar procesos críticos como la cadena de frío en la compañía Camagüey S.A. El trabajo inició con un diagnóstico integral que evidenció debilidades en las políticas de seguridad existentes, carencias en controles técnicos aplicados a los dispositivos IoT, y ausencia de protocolos específicos para la protección de la información en entornos industriales altamente conectados.

Entre los hallazgos más relevantes, se identificó la falta de segmentación de red, el uso de credenciales por defecto en algunos dispositivos, la inexistencia de registros de auditoría y una cobertura limitada de políticas adaptadas al contexto IoT. Estos vacíos representan riesgos tangibles que pueden comprometer la integridad, disponibilidad y confidencialidad de la información. Ante esta situación, el modelo MSISSCF se diseñó con base en estándares internacionales como IEC 62443, articulando fases orientadas a diagnosticar, implementar, monitorear y perfeccionar medidas de seguridad acordes a las capacidades y necesidades reales de la empresa.

La validación del modelo, realizada mediante juicio de expertos y evaluada con un cuestionario estructurado, arrojó un coeficiente alfa de Cronbach de 0.90, lo cual demuestra una consistencia interna excelente y respalda estadísticamente la confiabilidad del instrumento aplicado. Los expertos consultados valoraron de manera positiva la claridad del modelo, su aplicabilidad en el entorno industrial de Camagüey S.A., y su alineación con las buenas prácticas de seguridad de la información.

La implementación del modelo MSISSCF tiene un impacto significativo en la organización, al proporcionar un marco metodológico adaptado a sus condiciones operativas, permitiendo fortalecer los procesos de supervisión de la cadena de frío, reducir la exposición a riesgos cibernéticos y promover una cultura de mejora continua en ciberseguridad. Además, el modelo establece una base replicable para otras organizaciones con desafíos similares, lo cual amplía su aplicabilidad más allá del caso específico estudiado.

Como proyección futura, se recomienda desarrollar investigaciones orientadas a medir el desempeño del modelo en fases posteriores a su implementación, identificar indicadores de madurez en seguridad de la información en entornos IoT industriales, y explorar su aplicación en otros sectores sensibles como farmacéutica, logística alimentaria y salud, donde la supervisión en tiempo real de condiciones ambientales es igualmente crítica.

Recomendaciones

Se recomienda que Camagüey S.A. implemente progresivamente el modelo MSISSCF, comenzando por la fase de diagnóstico y priorizando los componentes más críticos detectados durante la investigación. Esta adopción inicial debe estar acompañada de un esfuerzo institucional para fortalecer la cultura de ciberseguridad, promoviendo procesos de capacitación continua al personal involucrado en la supervisión de la cadena de frío, con el objetivo de fomentar la apropiación del modelo en todos los niveles operativos.

Asimismo, es necesario establecer mecanismos de monitoreo periódico que permitan revisar y ajustar el modelo conforme a la evolución de los riesgos, las tecnologías involucradas y las condiciones del entorno productivo. La fase de perfeccionamiento del modelo debe asumirse como una práctica continua para garantizar su sostenibilidad y efectividad.

Otra recomendación importante es considerar la ampliación de la aplicación del modelo a otras áreas de la cadena de valor de la empresa, más allá del sistema de supervisión de la cadena de frío, con el fin de fortalecer un enfoque integral de seguridad de la información. Finalmente, se sugiere promover nuevas investigaciones que evalúen la aplicación del modelo MSISSCF en contextos distintos o sectores industriales similares, lo cual permitiría consolidar su validez externa y adaptabilidad como referencia metodológica para otras organizaciones.

Referencias

Aceros Orduz, D. F. (2020). Prototipo de una ruta tecnológica para el IOT, enfocada en las tecnologías de riego, para los agricultores de pequeña escala en Colombia. https://repository.unab.edu.co/handle/20.500.12749/11709

Ahmed, N., Flechas Manrique, N., & Petrović, A. (2023). Enhancing Spanish-Quechua Machine Translation with Pre-Trained Models and Diverse Data Sources: LCT-EHU at AmericasNLP Shared Task. Proceedings of the Workshop on Natural Language Processing for Indigenous Languages of the Americas (AmericasNLP), 156–162. https://doi.org/10.18653/v1/2023.americasnlp-1.16

Alshahrani, SM. (s/f). Habilitación de blockchain para la cadena de suministro de medicamentos de Arabia Saudita mediante Internet de las cosas (IoT) [PeerJ]. Recuperado el 25 de febrero de 2025, de https://peerj.com/articles/cs-2072/

Alshdadi, A., Kamel, S., Alsolami, E., Lytras, M. D., & Boubaker, S. (2024). An IoT Smart System for Cold Supply Chain Storage and Transportation Management. Engineering, Technology & Applied Science Research, 14(2), Article 2. https://doi.org/10.48084/etasr.6857

Álvarez Polo, D. A. (2021). Propuesta de optimización de los procesos de almacenamiento y transporte en Alimentos Cárnicos S.A.S. http://hdl.handle.net/10882/11144

Arriaga-Lorenzo, P., Maldonado-Simán, E., Ramírez-Valverde, R., Martínez-Hernández, P. A., Tirado-González, D. N., & Saavedra-Jiménez, L. A. (2024). Meat cold chain management in Mexican supermarkets. Theory and practice of meat processing, 9(2), 100–107. https://doi.org/10.21323/2414-438X-2024-9-2-100-107

Ashok, K., & Gopikrishnan, S. (2023). Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. IEEE

Access, 11, 2621–2651. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3234632

Asokan, D., Sunny, J., Pillai, V. M., & Nath, H. V. (2022). Blockchain technology: A troubleshooter for blood cold chains. Journal of Global Operations and Strategic Sourcing, 15(3), 316–344. https://doi.org/10.1108/JGOSS-02-2022-0010

Ávila-Camacho, F. J., & Moreno-Villalba, L. M. (2023). Internet de las Cosas (IoT) Retos para las Empresas en la era de la Industria 4.0. Pädi Boletín Científico de Ciencias Básicas e Ingenierías del ICBI, 10(20), Article 20. https://doi.org/10.29057/icbi.v10i20.9516

Azizi, N., Malekzadeh, H., Akhavan, P., Haass, O., Saremi, S., & Mirjalili, S. (2021). IoT–Blockchain: Harnessing the Power of Internet of Thing and Blockchain for Smart Supply Chain. Sensors, 21(18), Article 18. https://doi.org/10.3390/s21186048

Bapatla, A. K., Mohanty, S. P., Kougianos, E., & Puthal, D. (2022). PharmaChain 2.0: A Blockchain Framework for Secure Remote Monitoring of Drug Environmental Parameters in Pharmaceutical Cold Supply Chain. 2022 IEEE International Symposium on Smart Electronic Systems (iSES), 185–190. https://doi.org/10.1109/iSES54909.2022.00046

Benjamín Teisserenc, & Samad Sepasgozar. (s/f). Adopción de la tecnología blockchain a través de gemelos digitales en la industria de la construcción 4.0: Un enfoque PESTELS. Recuperado el 25 de febrero de 2025, de https://www.mdpi.com/2075-5309/11/12/670

Bonett, D. G. (2002). Sample Size Requirements for Testing and Estimating Coefficient Alpha. Journal of Educational and Behavioral Statistics, 27(4), 335–340. https://doi.org/10.3102/10769986027004335

Brandao, P. R. (2019). Bases, Challenges, and Main Dangers for Deploying Cybersecurity in Industry 4.0. Advances in Wireless Communications and Networks, 5(1), Article 1. https://doi.org/10.11648/j.awcn.20190501.15

Brandín, R., & Abrishami, S. (2021). Information traceability platforms for asset data lifecycle: Blockchain-based technologies. Smart and Sustainable Built Environment, 10(3), 364–386. https://doi.org/10.1108/SASBE-03-2021-0042

Cabero-Almenara, J., Romero-Tena, R., & Palacios-Rodríguez, A. (2020). Evaluation of Teacher Digital Competence Frameworks Through Expert Judgement: The Use of the Expert Competence Coefficient. Journal of New Approaches in Educational Research, 9(2), 275–293. https://doi.org/10.7821/naer.2020.7.578

Çağlayan, M. U. (2022). Review of Some Recent European Cybersecurity Research and Innovation Projects. Infocommunications journal, 14(4), 70–78. https://doi.org/10.36244/ICJ.2022.4.10

Camaguey S.A. (s/f). CAMAGUEY S.A. Recuperado el 26 de febrero de 2025, de https://www.camaguey.com.co

Castellanos, J. D. G., Hernández, V. L., & Gonzales, T. C. (2022). Tópicos de investigación de internet de las cosas en la cadena de suministro. Publicaciones e Investigación, 15(4), Article 4. https://doi.org/10.22490/25394088.5608

Cheung, K.-F., & Bell, M. G. H. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. European Journal of Operational Research, 291(2), 471–481. https://doi.org/10.1016/j.ejor.2019.10.019

Davoudi, S., Stasinopoulos, P., & Shiwakoti, N. (2024). Two Decades of Advancements in Cold Supply Chain Logistics for Reducing Food Waste: A Review with Focus on the Meat Industry. Sustainability, 16(16), 6986. https://doi.org/10.3390/su16166986

Dilillo, N., Ferrero, R., Gandino, F., & Rebaudengo, M. (2023). Investigation on Wireless Communication for Sensors in IoT Cold Chain. 2023 IEEE Conference on AgriFood Electronics (CAFE), 89–93. https://doi.org/10.1109/CAFE58535.2023.10291686

Dionicio, P. O. G., Gil, A. J. L., & Santos, A. C. M. D. L. (2023). Principales técnicas criptográficas aplicadas a la seguridad de la información en IoT: Una revisión sistemática. Ingenio Tecnológico, 5. https://portal.amelica.org/ameli/journal/266/2663842005/html/

Etemadi, N., Van Gelder, P., & Strozzi, F. (2021). An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains towards Cybersecurity. Sustainability, 13(9), Article 9. https://doi.org/10.3390/su13094672

Florrence, J. M. (2025). A Mathematical Model for Enhancing Cybersecurity in IoT Networks Using LSTM-Based Anomaly Detection and Optimization. Communications on Applied Nonlinear Analysis, 32(2), Article 2. https://doi.org/10.52783/cana.v32.1706

Fujs, D., Mihelič, A., & Vrhovec, S. L. R. (2019). The power of interpretation: Qualitative methods in cybersecurity research. Proceedings of the 14th International Conference on Availability, Reliability and Security, 1–10. https://doi.org/10.1145/3339252.3341479

Gallo, P. de, & Beatriz, H. (2022). Propuesta de una guía de actuación forense para entornos de internet de las cosas (IoT). Computación y Sistemas, 26(1), 441–460. https://doi.org/10.13053/cys-26-1-3898

Gonzalez-Amarillo, C. A., Fraga Vazquez, A., Ramirez-Gonzalez, G. A., Mendoza-Moreno, M. A., & Corrales Muñoz, J. C. (2023). BIoTS-Path: Certification Transmission of Supply Chains Based on Blockchain–Internet of Things Architectures by Validating the Information Path. Mathematics, 11(19), Article 19. https://doi.org/10.3390/math11194108

Hernández Mendoza, C. C., & Martínez Rojas, E. P. (s/f). Optimización de Cultivos de Fresas en Cundinamarca mediante la Integración de Plataformas Cloud e IoT. Recuperado el 25 de febrero de 2025, de https://repository.usta.edu.co/items/b45a0deb-9ab9-46eb-b4b9-d4881a57a04e

Herrmann, D., & Pridöhl, H. (2020). Basic Concepts and Models of Cybersecurity. En M. Christen, B. Gordijn, & M. Loi (Eds.), The Ethics of Cybersecurity (pp. 11–44). Springer International Publishing. https://doi.org/10.1007/978-3-030-29053-5_2

Huang, J., & Leong, Y. (2023). Information Traceability Management of Food Cold Chain Based on Blockchain Technology. Proceedings of the 2nd International Conference on Engineering Management and Information Science, EMIS 2023, February 24-26, 2023, Chengdu, China. Proceedings of the 2nd International Conference on Engineering Management and Information Science, EMIS 2023, February 24-26, 2023, Chengdu, China, Chengdu, People's Republic of China. https://doi.org/10.4108/eai.24-2-2023.2330665

Ibarguen Cabrera, F., & Martínez Contreras, S. A. (s/f). Desarrollo de un sistema IoT de monitoreo de temperatura, humedad relativa y estado ON/OFF de un cuarto frío de

Inversiones Medina Verbel S.A.S. Recuperado el 25 de febrero de 2025, de https://repositorio.uan.edu.co/items/157c8d82-7bcb-4217-aee0-3ac056f05fc4

ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection—Information security management systems—Requirements. (s/f). Recuperado el 25 de febrero de 2025, de https://www.iso.org/obp/ui/es/#iso:std:iso-iec:27001:ed-3:v1:en

Jaén-Barrantes, E. M. (2022). Desarrollo de un modelo de gestión de energía basado en la Norma ISO 50001 en el Ingenio La Azucarera La Estrella de Grupo Calesa, bajo concepto de Internet de las Cosas (IoT). https://repositoriotec.tec.ac.cr/handle/2238/13991

Kumar, R., & Sharma, R. (2023). Blockchain-based Model for Secure and Trusted IoT System. 2023 International Conference on Advanced Computing & Communication Technologies (ICACCTech), 743–750. https://doi.org/10.1109/ICACCTech61146.2023.00123

Lam, H. Y., Tang, V., & Ho, G. T. S. (2023). A Digital Twins Model for Analyzing and Simulating Cold Chain Risks. 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 259–263. https://doi.org/10.1109/ICAIIC57133.2023.10067025

Leng, L., Zhang, J., Zhang, C., Zhao, Y., Wang, W., & Li, G. (2020). A novel bi-objective model of cold chain logistics considering location-routing decision and environmental effects. PLOS ONE, 15(4), e0230867. https://doi.org/10.1371/journal.pone.0230867

Li, Q., Zuo, J., Cao, R., Zhang, Y., Chen, J., Liu, Q., & Wang, J. (2024). A Security Evaluation Framework for Intelligent Connected Vehicles Based on Attack Chains.

IEEE Network, 38(2), 148–155. IEEE Network. https://doi.org/10.1109/MNET.2023.3333545

Liu, H. (2024). Analysis of Blockchain-based Cold Chain Logistics Financial Business Model. Financial Engineering and Risk Management, 7(2). https://doi.org/10.23977/ferm.2024.070202

Martínez, M., & Mesías, M. (2021). Aplicación de las Tecnologías de la Información y la Comunicación (TICs) en la cadena alimentaria. Revista de Investigación en Tecnologías de la Información, 9(19), 47–57. https://doi.org/10.36825/RITI.09.19.004

Mazó Pozuelo, H. A., & Torrado Castro, D. J. (2024). Modelo de gobierno de TI para centros de servicios compartidos del sector energético. InGente Americana, 3(3). https://doi.org/10.21803/ingecana.3.3.849

Miñan Parrales, W. E. (2022). Modelo de arquitectura de gestión de la información para la cadena de suministros en empresas de consumo masivo mediante Iot y Blockchain [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/23334

Mnushka, O., & Savchenko, V. (2019). Модель безопасности информационной системы на базе технологий IoT. Вісник Національного технічного університету “ХПІ”. Серія: Інформатика і моделювання, 28 (1353), Article 28 (1353). http://pim.khpi.edu.ua/article/view/2411-0558.2019.28.09

Mohsin, A., Yellampalli, S. S., Mohsin, A., & Yellampalli, S. S. (1d. C., enero 1). IoT-Based Cold Chain Logistics Monitoring (iot-based-cold-chain-logistics-monitoring) [Chapter]. Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-7998-5354-1.Ch017; IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-5354-1.ch017

Nguyen, T. A., Min, D., & Choi, E. (2020). A Hierarchical Modeling and Analysis Framework for Availability and Security Quantification of IoT Infrastructures. Electronics, 9(1), Article 1. https://doi.org/10.3390/electronics9010155

Nyamuchiwa, K., Lei, Z., & Aranas, C. (2022). Cybersecurity Vulnerabilities in Off-Site Construction. Applied Sciences, 12(10), Article 10. https://doi.org/10.3390/app12105037

Prasad, M., Pal, P., Tripathi, S., & Dahal, K. (2024). AI/ML driven intrusion detection framework for IoT enabled cold storage monitoring system. SECURITY AND PRIVACY, 7(5), e400. https://doi.org/10.1002/spy2.400

Priya, J. S., Hemalatha, M., Porselvi, T., Thennarasu, S., Rethick, T., & Naathan, C. B. R. (2023). Cold Supply Chain Logistics with IoT to Ensure Quality and Security of the Transported Goods. 2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS), 1–4. https://doi.org/10.1109/ICCEBS58601.2023.10448521

Raj, R., & Ghosh, M. (2023). A Lightweight Blockchain Framework for secure transaction in resource constrained IoT devices. 2023 5th International Conference on Recent Advances in Information Technology (RAIT), 1–7. https://doi.org/10.1109/RAIT57693.2023.10126898

Rangel Gómez, H. Y. (2022). Modelo de integración tecnológica en la implementación de sistemas de gestión de inocuidad y seguridad alimentaria en empresas del sector Agro alimentos. http://hdl.handle.net/1992/58742

Rangel Tapia, C. A., Antequera Lasso, F. M., Otero Méndez, J. D., Bonadiez Cota, Y. M., & Riquett Márquez, M. C. (2021). El impacto de la industria 4.0 en los procesos

logísticos del sector alimentario de Barranquilla. https://hdl.handle.net/20.500.12442/9321

Ren, T., Ren, J., Mattellini, D. B., Liangrokapart, J., Weerawat, W., & Kritchanchai, D. (2023). Exploring the Utilization of a Bayesian Network-Based Risk Management System for Cold Chain Packaging. 2023 7th International Conference on Transportation Information and Safety (ICTIS), 1243–1246. https://doi.org/10.1109/ICTIS60134.2023.10243836

Santos, P. H. A., & Martins, R. A. (2020, noviembre 4). Cold Chain Management: Descriptive Bibliometric Analysis. ENEGEP 2020 - Encontro Nacional de Engenharia de Produção, Online. https://doi.org/10.14488/ENEGEP2020_TI_ST_343_1757_40700

Sargsyan, G., Castellon, N., Binnendijk, R., & Cozijnsen, P. (2019). Blockchain Security by Design Framework for Trust and Adoption in IoT Environment. 2019 IEEE World Congress on Services (SERVICES), 2642-939X, 15–20. https://doi.org/10.1109/SERVICES.2019.00018

Shao, X., Liu, Y., Tian, J., & Cheng, T. (2023). A cold chain logistics traceability system framework based on the identification and resolution system for Industrial Internet. Proceedings of the 2022 10th International Conference on Information Technology: IoT and Smart City, 242–250. https://doi.org/10.1145/3582197.3582238

Shukur, F., & Shukur, S. T. (2023). A Comprehensive Analysis of Cybersecurity Threats based IoTs. Journal of Applied Artificial Intelligence, 4(2), Article 2. https://doi.org/10.48185/jaai.v4i2.920

Sunny, J., Undralla, N., & Madhusudanan Pillai, V. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. Computers & Industrial Engineering, 150, 106895. https://doi.org/10.1016/j.cie.2020.106895

Tang, F. (2023). Application of a Cold-Chain Logistics Distribution System Based on Cloud Computing and Web Delivery Date Management: International Journal of Information Systems and Supply Chain Management, 16(1), 1–16. https://doi.org/10.4018/IJISSCM.318644

Toapanta, T. S. M., Del Pozo, D. R., Izurieta, R. R., Guamán, J. A., Orizaga, J. A., M. Arellano, R., & Baño Hifóng, M. M. (2024). Blockchain-based Security Model to Mitigate the Risks of a Database for a Public Organization. Journal of Internet Services and Information Security, 14(3), 78–98. https://doi.org/10.58346/JISIS.2024.I3.005

Torrado Castro, D. J., Suárez López, D. M., & Molina Cárdenas, M. (2023). Diseño de un modelo de gestión para proyectos de infraestructuras tecnológicas. Ingeniare, 35, 51–58.

Torres, P. A., Rodríguez, A., & Ochoa, K. (2021). Integración del internet de las cosas en la gestión de la cadena de suministro de alimentos: Una revisión sistemática de la literatura. Prisma Tecnológico, 12(1), Article 1. https://doi.org/10.33412/pri.v12.1.2448

Vargas Caballero, S. R. (2023). Sistema IoT para Monitoreo de Productos Cárnicos IoT System for Monitoring Meat Products. http://hdl.handle.net/11634/51493

Vilaginés Iglesias, M. (2023). Ciberseguridad del IoT en la industria cervecera [Master thesis, Universitat Politècnica de Catalunya]. https://upcommons.upc.edu/handle/2117/392943

Wanganoo, L., & Shukla, V. K. (2020). Real-Time Data Monitoring in Cold Supply Chain Through NB- IoT. 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1–6. https://doi.org/10.1109/ICCCNT49239.2020.9225360

Yiming, J., Rey Chen Xu, Yawei Wang, & Lang Gao. (s/f). Una solución de cadena cruzada para integrar múltiples cadenas de bloques para la gestión de datos de IoT. Recuperado el 25 de febrero de 2025, de https://www.mdpi.com/1424-8220/19/9/2042

Zhang, Y., Tang, Y., Li, C., Dong, M., Huang, M., Zhang, H., & Ota, K. (2024). Privacy-Preserving for Blockchain-Enabled Cold-Chain Logistics System With IoV and Linkable Ring Signature. IEEE Transactions on Vehicular Technology, 73(9), 12585–12596. https://doi.org/10.1109/TVT.2024.3391419

Apendice

Apéndice A.

Formulario de Evaluación de Competencia del Experto.

Este formulario tiene como objetivo calcular el Coeficiente de Competencia (K) de los expertos convocados para validar el modelo MSISSCF. Por favor, complete cada sección de manera precisa.

Sección 1: Autoevaluación del Conocimiento (Kc)

Indique su nivel de conocimiento sobre los siguientes temas, utilizando la siguiente escala:

1.0 = Conocimiento profundo y dominio total

0.8 = Conocimiento alto

0.6 = Conocimiento medio

0.4 = Bajo conocimiento

0.2 = Conocimiento muy básico

Nivel de conocimiento sobre seguridad de la información: _____

Nivel de conocimiento sobre dispositivos IoT: _____

Nivel de conocimiento sobre supervisión de cadena de frío: _____

Promedio Kc estimado (se calcula promediando las tres anteriores): _____

Sección 2: Evaluación de la Argumentación (Ka)

Marque las opciones que se aplican y adjunte soportes si es posible:

☐ Poseo título de posgrado (especialización, maestría o doctorado) en áreas afines (0.3)

☐ Tengo experiencia laboral de 5 años o más en temas relacionados con seguridad de la información, IoT o cadena de frío (0.3)

☐ He publicado investigaciones o artículos relacionados con los temas anteriores (0.2)

☐ He participado en proyectos técnicos o industriales relacionados con el tema (0.1)

☐ Tengo experiencia docente o técnica adicional en el área (0.1)

Suma de puntajes seleccionados (Ka): _____

Cálculo del Coeficiente de Competencia (K)

Utilice la siguiente fórmula para calcular su coeficiente total:

$K = (Kc + Ka) / 2$

Valor de K: _____

¿Es usted un experto competente según el criterio $K \geq 07$? ☐ Sí ☐ No

Anexo 2. Cuestionario Mejorado para la Validación del Modelo MSISSCF

Instrucciones:
Califique cada afirmación en una escala de 1 a 5, donde:

1 = Totalmente en desacuerdo
2 = En desacuerdo
3 = Neutral
4 = De acuerdo
5 = Totalmente de acuerdo

Dimensión 1: Claridad del modelo

1. Las fases del modelo MSISSCF se presentan de forma estructurada y comprensible.

❑1 ❑2 ❑3 ❑4 ❑5

2. El propósito de cada fase es claro y está bien diferenciado de las demás.

❑1 ❑2 ❑3 ❑4 ❑5

3. El lenguaje utilizado en el modelo es adecuado y facilita su interpretación.

❑1 ❑2 ❑3 ❑4 ❑5

Dimensión 2: Relevancia para el contexto organizacional

4. El modelo responde a los desafíos de seguridad de la información en empresas con supervisión IoT.

❑1 ❑2 ❑3 ❑4 ❑5

5. MSISSCF se adapta a las características operativas de empresas como Camagüey S.A.

❑1 ❑2 ❑3 ❑4 ❑5

6. Las necesidades típicas del sector cárnico son contempladas en el enfoque del modelo.

❑1 ❑2 ❑3 ❑4 ❑5

Dimensión 3: Aplicabilidad operativa

7. El modelo puede implementarse con recursos y capacidades razonables.

❑1 ❑2 ❑3 ❑4 ❑5

8. Las actividades propuestas son ejecutables dentro de la estructura de una empresa mediana.

❑1 ❑2 ❑3 ❑4 ❑5

9. Las fases del modelo son aplicables sin requerir cambios estructurales complejos.

❑1 ❑2 ❑3 ❑4 ❑5

Dimensión 4: Coherencia normativa

10. El modelo refleja principios clave del estándar IEC 62443.

❑1 ❑2 ❑3 ❑4 ❑5

11. La relación entre el modelo y los estándares aplicables está bien fundamentada.

❑1 ❑2 ❑3 ❑4 ❑5

12. El enfoque metodológico es coherente con normativas actuales de ciberseguridad.

❑1 ❑2 ❑3 ❑4 ❑5

Dimensión 5: Potencial de mejora continua

13. El modelo incluye mecanismos eficaces de seguimiento y retroalimentación.

❑1 ❑2 ❑3 ❑4 ❑5

14. MSISSCF permite adaptarse a cambios tecnológicos y operativos.

❑1 ❑2 ❑3 ❑4 ❑5

15. Las fases propuestas promueven una cultura organizacional orientada a la mejora constante.
❑1 ❑2 ❑3 ❑4 ❑5

Anexo 3. Respuestas Expertos

	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10
D1.1 Claridad fases	5	4	4	5	4	5	4	5	5	4
D1.2 Propósito fases	5	4	4	5	4	5	4	5	5	4
D1.3 Lenguaje adecuado	5	4	4	5	4	5	4	5	5	4
D2.1 Desafíos IoT	5	5	4	5	5	5	4	5	5	4
D2.2 Adaptación Camagüey	5	5	4	5	5	5	4	5	5	4
D2.3 Sector cárnico	5	5	4	5	5	5	4	5	5	4
D3.1 Recursos razonables	5	5	4	4	4	5	4	5	5	4
D3.2 Ejecutable empresa mediana	5	5	4	4	4	5	4	5	5	4
D3.3 Sin cambios complejos	5	5	4	4	4	5	4	5	5	4
D4.1 IEC 62443	5	5	4	4	4	5	4	5	4	4
D4.2 Relación estándares	5	5	4	4	4	5	4	5	4	4
D4.3 Coherencia normativa	5	5	4	4	4	5	4	5	4	4
D5.1 Seguimiento	5	5	4	4	5	5	4	5	4	4

D5.2 Adaptable cambios	5	5	4	4	5	5	4	5	4	4
D5.3 Mejora continua	5	5	4	4	5	4	4	5	4	5