



UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE
INFORMÁTICA VALPARAÍSO -
CHILE



**“GUÍA PRÁCTICA PARA ABORDAR LA
SEPARACIÓN FÍSICA, CONVERGENCIA Y
CIBERSEGURIDAD DE ENTORNOS DE
TECNOLOGÍAS DE OPERACIÓN (OT) Y
TECNOLOGÍAS DE INFORMACIÓN (TI) EN EL
RUBRO INDUSTRIAL ALIMENTICIO NACIONAL”**

REINALDO MARTINEZ BUSTAMANTE

TESINA PARA OPTAR AL GRADO
DE MAGÍSTER EN TECNOLOGÍAS
DE LA INFORMACIÓN

Profesor Guía: JORGE OLIVARES
Director de tesina: RAÚL MONGE



CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): CI Memoria o trabajo de título **X**
Tesis de Postgrado

Título del trabajo: Guía Práctica para abordar la separación física, Convergencia y Ciberseguridad de entornos de Tecnologías de Operación (OT) y Tecnologías de Información (TI) en el rubro industrial alimenticio Nacional

Nombre del candidato(a): Reinaldo Gerardo Martínez Bustamante

Carrera I Grado: Magíster en Tecnologías de la Información.

Campus: Vitacura Departamento: informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Jorge Olivares, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente DEJO CONSTANCIA que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

X El trabajo NO contiene información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

[3 El trabajo CONTIENE información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (embargo) por (marcar una opción):

C] 6 meses 12 meses C] 2 años 3 años L] 5 años C] 10 años

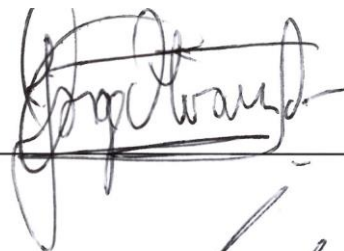
Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 08-10-2026

rma:



Estudiante o Candidato(a):

Fecha: 08-10-2026

rma:



Guía Práctica para abordar la separación física, Convergencia y Ciberseguridad de entornos de Tecnologías de Operación (OT) y Tecnologías de Información (TI) en el rubro industrial alimenticio Nacional

Reinaldo Martínez Bustamante

Empresa de Alimentos
Santa Victoria de Viluco 8c, Buin, Santiago
rmartinezb@usm.cl

Resumen: La presente investigación aborda la necesidad de mejorar la ciberseguridad en la industria alimenticia chilena, un sector donde la continuidad operativa es crítica y las plantas funcionan bajo esquemas de alta exigencia (24/6), con foco en la productividad y sin espacio para interrupciones no planificadas. En este contexto, los marcos internacionales como ISA/IEC 62443, NIST SP 800-82 o Purdue/ISA-99, aunque robustos, resultan de difícil aplicación inmediata por su complejidad, costo y orientación genérica [9]. El problema identificado radica en la falta de herramientas prácticas y localizadas que permitan aplicar estos estándares sin afectar la operación continua.

Como solución, se propone el diseño e implementación de una guía práctica de separación y convergencia tecnologías de la información (TI) y tecnologías operacionales (OT) adaptada a la realidad nacional. Esta guía tiene como objetivo facilitar progresivamente las buenas prácticas de ciberseguridad, mediante fases claras, controles aplicables, ejemplos concretos y plantillas reutilizables, permitiendo su implementación tanto por equipos de TI como de OT. La propuesta busca proteger la infraestructura crítica sin comprometer la producción, a través de mecanismos de aislamiento, contención y recuperación que aseguran la continuidad operativa ante incidentes.

La validación de la guía se llevará a cabo mediante un enfoque metodológico que incluyó un caso de uso industrial y evaluación experta. Se realizó un diagnóstico inicial del estado de madurez en infraestructura, sistemas, procesos y personas, seguido de la implementación de la guía y una evaluación posterior. Los resultados esperados muestran mejoras en indicadores clave como nivel de reducción de vulnerabilidades, aumento en la madurez organizacional y mayor capacidad de recuperación ante incidentes.

Esta propuesta de guía representa una herramienta metodológica innovadora que cierra la brecha entre teoría normativa y operación real, permitiendo a las plantas alimenticias avanzar en la separación de red TI/OT, ciberseguridad y resiliencia sin sacrificar la continuidad del negocio, contribuyendo a su competitividad y sostenibilidad a largo plazo.

Palabras Clave: Ciberseguridad, Gobernanza, Normas Nist 800-82, ISA/IEC 62443, Modelo Purdue/ISA 99, redes TI/OT.

CAPITULO 1: Introducción

1.1 Motivación

La motivación principal de la investigación es contribuir al fortalecimiento de la seguridad y resiliencia operativa en la industria alimenticia nacional, mediante la propuesta de una guía orientada a mejorar el cumplimiento de las normas de seguridad en el área de producción, a través de la separación y convergencia segura de redes TI/OT, y del establecimiento de un proceso de mejora continua. Se busca sentar las bases para que las organizaciones alcancen mayores niveles de madurez en seguridad industrial, eficiencia operativa y continuidad del negocio, asegurando así la operación ininterrumpida de sus líneas productivas frente a eventuales incidentes de ciberseguridad.

Con el propósito de facilitar su identificación y referencia a lo largo del documento, la propuesta desarrollada en esta investigación será denominada **GCTIOT (Guía de Convergencia y Ciberseguridad**

TI/OT). Esta GCTIOT integra buenas prácticas derivadas de los estándares ISA/IEC 62443, NIST Cybersecurity Framework e ISO/IEC 27001, adaptándolas al contexto operacional de la industria alimentaria mediante un enfoque práctico de evaluación y mejora continua de la convergencia entre TI/OT.

1.2 Contexto

La industria manufacturera de alimentos desempeña un rol estratégico en la economía nacional, caracterizándose por operar bajo esquemas de producción continua, generalmente 24/6, con limitadas ventanas de mantenimiento. Esta condición exige elevados niveles de disponibilidad, continuidad operacional y control de riesgos para garantizar el cumplimiento de la demanda y los objetivos del negocio.

En un mercado altamente competitivo, las empresas del sector buscan aumentar su productividad, expandir su capacidad productiva y diversificar su oferta comercial. Para ello, dependen de la integración y coordinación de múltiples áreas funcionales, donde cualquier interrupción de los procesos productivos puede generar impactos operacionales, económicos y reputacionales significativos.

En este contexto, la convergencia entre Tecnologías de la Información (TI) y Tecnologías de Operación (OT) ha adquirido un papel fundamental en la automatización y optimización de los procesos industriales. Sin embargo, la integración de sistemas como PLC, SCADA, servidores industriales y redes de control también ha incrementado la exposición a amenazas de ciberseguridad que podrían afectar la disponibilidad de las líneas productivas y la continuidad del negocio.

Frente a este escenario, la adecuada segmentación y separación de las redes TI y OT, junto con mecanismos seguros de convergencia entre ambos entornos, se convierte en una medida esencial para reducir la superficie de ataque, limitar la propagación de incidentes y fortalecer la resiliencia operacional. Asimismo, el área de informática debe asegurar la implementación de controles de ciberseguridad, planes de continuidad operacional, recuperación ante desastres y capacidades de aislamiento de incidentes que permitan minimizar los tiempos de interrupción y preservar la continuidad de los procesos productivos.

1.3 Definición del Problema

Las empresas manufactureras de alimentos nacionales operan bajo un modelo de producción continua que exige altos niveles de disponibilidad y confiabilidad de sus líneas productivas, con ventanas de mantenimiento muy limitadas, sin embargo, la creciente convergencia entre las redes TI/OT, junto con la falta de una adecuada separación y segmentación de las redes industriales, expone a estas organizaciones a riesgos cibernéticos que pueden provocar interrupciones no planificadas en los procesos productivos.

En este contexto, el problema general que se aborda en esta investigación es la insuficiente implementación de estrategias de seguridad, segmentación de redes, resiliencia operativa y gobernanza en los entornos industriales de la industria alimenticia nacional, lo que limita la capacidad de las organizaciones para prevenir, aislar y mitigar incidentes de ciberseguridad sin afectar la continuidad de la producción.

1.3.1 Problemas Específicos

Ausencia de una separación clara entre redes TI/OT. Muchas empresas del sector alimenticio no cuentan con una arquitectura de red adecuadamente segmentada, que diferencie los entornos de TI/OT, lo que facilita la propagación de incidentes cibernéticos desde la red corporativa hacia los sistemas industriales críticos.

Limitada capacidad de aislamiento de incidentes a nivel de red. La falta de mecanismos técnicos y procedimientos definidos para el aislamiento de equipos comprometidos PLC, servidores industriales, estaciones SCADA, switches y dispositivos de seguridad perimetral como firewalls, entre otros. Esta configuración representa una arquitectura de convergencia parcial que si bien puede responder a ciertos requerimientos operacionales impone serias limitaciones en términos de ciberseguridad, disponibilidad, resiliencia y continuidad operativa del negocio, ya que impide contener incidentes de seguridad sin afectar al resto de la infraestructura productiva.

Deficiencias en los planes de continuidad y recuperación ante desastres (DRP). En muchos casos, los planes de recuperación no consideran de forma específica los entornos industriales, ni contemplan tiempos de recuperación acordes a las exigencias de operación continua de las líneas productivas descritas por el negocio.

Insuficiente madurez en la gestión de ciberseguridad industrial. La inexistencia de guías y estándares internos orientados a la seguridad de los sistemas OT limita la adopción de buenas prácticas, el cumplimiento normativo y la implementación de procesos de mejora continua en seguridad industrial.

Riesgo de interrupción de la producción ante incidentes cibernéticos. La combinación de una alta dependencia tecnológica, una operación productiva ininterrumpida y una débil estrategia de seguridad incrementa la probabilidad de paradas no planificadas, afectando la productividad, los costos operacionales y la proyección de crecimiento de las empresas del sector.

1.4 Solución Propuesta

Frente a la problemática identificada en la industria alimenticia nacional, caracterizada por una operación productiva continua 24/6, una alta dependencia de sistemas industriales y una convergencia incompleta entre los entornos de TI/OT. Se propone como solución el diseño y desarrollo de una GCTIOT práctica para la separación física y lógica, y la convergencia segura de redes TI/OT, adaptada a la realidad operativa y organizacional del sector.

La solución propuesta surge como respuesta a la brecha existente entre los marcos normativos internacionales de ciberseguridad industrial —tales como ISA/IEC 62443, NIST SP 800-82 y el modelo Purdue/ISA-99— y su aplicación efectiva en plantas productivas nacionales. Donde las restricciones operacionales, las ventanas de mantenimiento limitadas y la criticidad de los procesos dificultan la adopción directa de dichos estándares. En este contexto, la GCTIOT busca operacionalizar estos lineamientos normativos en un instrumento metodológico práctico, progresivo y medible, que permita fortalecer la seguridad y resiliencia de los entornos industriales sin comprometer la continuidad de la producción.

La propuesta de solución se estructura bajo un enfoque por fases, aplicable transversalmente a cuatro ámbitos fundamentales: instalación física, hardware, software y procesos y personas. Este enfoque integral reconoce que la ciberseguridad industrial no depende únicamente de controles tecnológicos, sino también de la gobernanza, los procedimientos operativos y el factor humano.

La GCTIOT contempla mecanismos de separación efectiva de redes TI/OT, mediante el uso de segmentación física y lógica, zonas desmilitarizadas industriales, firewalls industriales y principios de mínimo privilegio, con el objetivo de reducir la propagación de incidentes y facilitar el aislamiento de eventos de seguridad a nivel de red.

En síntesis, la solución propuesta no busca reemplazar los estándares internacionales existentes, sino adaptarlos y operacionalizarlos, entregando una GCTIOT práctica y replicable que contribuya a mejorar la ciberseguridad, la continuidad operacional y la madurez tecnológica.

1.5 Hipótesis y justificación

La presente investigación tiene como objetivo evaluar la efectividad de una Guía de Convergencia Tecnológica entre Tecnologías de la Información y Tecnologías Operacionales (GCTIOT), orientada a implementar una separación y convergencia segura de entornos TI/OT en organizaciones industriales del sector alimenticio. La propuesta toma como referencia los principales marcos internacionales de ciberseguridad industrial, tales como ISA/IEC 62443, NIST SP 800-82 y el modelo Purdue/ISA-99, adaptando sus lineamientos a las necesidades operativas y de continuidad propias de plantas productivas con funcionamiento continuo.

A diferencia de la aplicación directa de estos estándares, cuya implementación suele resultar compleja debido a su amplitud y nivel de especialización, la GCTIOT propone un enfoque estructurado y práctico que facilita su adopción mediante una metodología claramente definida, orientada a la ejecución progresiva

de mejoras de seguridad, alineada con los requerimientos operacionales y las capacidades reales de las organizaciones.

En este contexto, se plantea la siguiente hipótesis de investigación:

La implementación de una Guía de Convergencia Tecnológica TI/OT (GCTIOT), caracterizada por su claridad metodológica, facilidad de uso, aplicabilidad práctica, enfoque progresivo, capacidad de medir resultados, alineación con estándares internacionales de ciberseguridad industrial y cobertura integral de personas, procesos y tecnología, permitirá incrementar el nivel de madurez en ciberseguridad industrial, reducir los riesgos asociados a la convergencia TI/OT y fortalecer la resiliencia operativa y la continuidad de las plantas productivas del sector alimenticio, sin afectar la disponibilidad de los procesos industriales.

La GCTIOT materializa los principios establecidos en los marcos normativos de referencia mediante una hoja de ruta estructurada, compuesta por fases de implementación, criterios de evaluación, indicadores de cumplimiento y mecanismos de validación asociados al nivel de madurez alcanzado. Esta aproximación permite reducir la brecha existente entre los requerimientos teóricos definidos por los estándares internacionales y su aplicación efectiva en entornos industriales reales, promoviendo una convergencia TI/OT segura, sostenible y alineada con los objetivos de continuidad operacional, resiliencia organizacional y protección de los activos críticos de producción.

1.6 Plan y diseño de investigación

El presente trabajo se enmarca en un enfoque de investigación aplicada, orientado al desarrollo de una solución práctica, medible y validable frente a un problema real identificado en la industria alimenticia nacional. En particular, se aborda la problemática asociada a la convergencia y separación segura entre las redes de TI/OT. En este contexto, el diseño del plan de investigación se estructura de manera secuencial y lógica, permitiendo abordar el problema desde un diagnóstico inicial hasta la validación de la solución propuesta.

Esta GCTIOT se estructura en 5 fases:

- FASE 1: Levantamiento de activos
- FASE 2: Definición de Controles
- FASE 3: Evaluación de madurez y análisis GAP
- FASE 4: Plan de mitigación
- FASE 5: implementación y seguimiento

Cada Fase se aborda de manera transversal a los 4 ámbitos definidos:

- Ámbito 1: Instalación Física
- Ámbito 2: Hardware
- Ámbito 3: Software
- Ámbito 4: Procesos y Personas

La GCTIOT contempla un diagnóstico inicial basado en el levantamiento y análisis del contexto actual descritos en las Fases 1, 2 y 3, mediante la revisión de la arquitectura TI/OT existente, la identificación de brechas de seguridad y la evaluación del nivel de madurez de los controles implementados. Dicho diagnóstico se sustenta en la adopción selectiva de algunos controles seleccionados a partir de los marcos normativos y modelos de referencia, los cuales permiten establecer una línea base objetiva respecto del estado de la ciberseguridad industrial.

Posteriormente, en la Fase 4, se desarrolla un plan de mitigación orientado a abordar las brechas identificadas durante el diagnóstico inicial. Este plan establece de manera estructurada las acciones necesarias, definiendo responsables, plazos y criterios de seguimiento, con el propósito de gestionar de forma controlada el cierre de las brechas detectadas y proporcionar los lineamientos para la fase de implementación.

Finalmente, en la Fase 5, se ejecuta el plan de trabajo definido y se realiza el seguimiento de las actividades comprometidas, verificando el cumplimiento de los plazos establecidos y la efectividad de las medidas implementadas. Esta etapa busca reducir progresivamente las brechas identificadas y contribuir al incremento del de madurez de la organización nivel en materia de convergencia segura TI/OT.

La validación de la hipótesis planteada contempla la aplicación de la GCTIOT propuesta en un caso de uso representativo de la industria alimentaria, con el objetivo de evaluar su viabilidad, aplicabilidad y efectividad en un entorno operativo. Para ello, se efectúa una comparación entre la situación inicial y el estado posterior a la implementación de la GCTIOT, utilizando cuestionarios de evaluación y análisis de madurez. Este proceso permite determinar el impacto de la solución en aspectos como la ciberseguridad, la resiliencia operativa, la continuidad de los procesos productivos y el nivel de madurez organizacional alcanzado.

Adicionalmente, la evaluación incorpora la participación de expertos independientes que no intervienen en el diseño de la GCTIOT ni en la evaluación piloto antes señalada. Su contribución consiste en emitir juicios técnicos y realizar una evaluación crítica de la propuesta, con el fin de determinar si esta cumple con los principios de practicidad, progresividad, medición objetiva y aplicabilidad en condiciones reales de operación industrial. De esta manera, se complementa la validación técnica de la GCTIOT mediante una perspectiva externa especializada, fortaleciendo la confiabilidad de los resultados obtenidos.

El diseño metodológico de la GCTIOT asegura una adecuada trazabilidad entre el problema identificado, los objetivos planteados y la solución propuesta. De este modo, se obtiene como resultado una GCTIOT de carácter práctico, metodológico, coherente, replicable y alineada tanto con las exigencias académicas como con las necesidades operativas del sector industrial analizado.

1.7 Organización del informe

El presente informe se estructura en nueve capítulos, organizados de forma progresiva para abordar el problema de investigación, desarrollar la solución propuesta y validar los resultados obtenidos.

El **Capítulo 1** presenta la introducción, el contexto de la industria alimenticia, la definición del problema, la solución propuesta, la hipótesis de trabajo y el diseño metodológico de la investigación.

El **Capítulo 2** desarrolla el marco teórico y el estado del arte, abordando la convergencia TI/OT, la ciberseguridad en entornos industriales, los principales estándares y modelos de referencia, y la situación actual de la convergencia TI/OT en la industria alimenticia.

El **Capítulo 3** describe la propuesta de solución, denominada GCTIOT, incluyendo su diseño metodológico, enfoque basado en fases, modelo de madurez, análisis de brechas (GAP) y métricas de evaluación.

El **Capítulo 4** presenta la aplicación y validación de la GCTIOT mediante un caso de estudio del sector alimenticio, analizando la implementación de sus fases y los resultados obtenidos.

El **Capítulo 5** expone las conclusiones y los principales aportes académicos y prácticos derivados de la investigación, como también describe las líneas de trabajo futuro y las oportunidades de mejora de la propuesta desarrollada.

El **Capítulo 6** reúne las referencias bibliográficas utilizadas en el desarrollo del estudio.

Finalmente, el **Capítulo 7** incorpora los anexos, incluyendo antecedentes complementarios, validaciones de la GCTIOT, evaluación por juicio experto y resultados detallados de las fases implementadas.

CAPITULO 2: Marco Teórico y Estado del Arte

2.1 Convergencia TI/OT en el contexto de la Industria 4.0

La Industria 4.0 representa una evolución hacia sistemas productivos altamente digitalizados, interconectados y automatizados, donde convergen tecnologías como el Internet Industrial de las Cosas (IIoT), análisis de datos, automatización avanzada e integración de sistemas empresariales.

En este contexto, la convergencia entre las TI/OT se ha consolidado como un habilitador clave para mejorar la eficiencia operativa, la trazabilidad de los procesos y la toma de decisiones en tiempo real [8].

Las TI están orientadas a la gestión de información corporativa, priorizando la confidencialidad, integridad y disponibilidad de los datos, mientras que las OT se enfocan en el control y supervisión de procesos físicos.

Donde la disponibilidad continua, la seguridad operacional y la confiabilidad de los sistemas son fundamentales [6]. La integración de ambos dominios permite aprovechar datos de planta para optimizar procesos productivos, sin embargo, cuando esta convergencia no se implementa de forma segura, se incrementa significativamente la superficie de ataque y el riesgo de interrupciones operativas [5].

En sectores industriales de alta criticidad, como la industria alimenticia, donde la producción opera bajo esquemas continuos 24/6 y las detenciones no planificadas generan impactos económicos y reputacionales relevantes, la convergencia TI/OT debe abordarse mediante arquitecturas seguras, segmentadas y resilientes [11].

2.2 Ciberseguridad en entornos industriales OT

Presenta desafíos particulares que la diferencian de la ciberseguridad tradicional en entornos TI, los sistemas OT suelen estar compuestos por dispositivos con ciclos de vida prolongados, múltiples fabricantes, protocolos industriales específicos y capacidades limitadas de actualización o parchado [10]. Muchos de estos sistemas fueron diseñados originalmente sin considerar amenazas cibernéticas, lo que incrementa su exposición frente a ataques modernos [11].

A diferencia del entorno TI, donde los sistemas pueden ser aislados o reiniciados con un impacto acotado, en OT cualquier intervención puede afectar directamente la continuidad del proceso productivo y la seguridad física de las personas [2]. Por esta razón, la ciberseguridad industrial prioriza enfoques preventivos y de contención, tales como segmentación de redes, control estricto de accesos, monitoreo pasivo del tráfico industrial y planes de recuperación ante incidentes, con el objetivo de minimizar el impacto de eventos de seguridad sin interrumpir la operación [10].

2.3 Modelos y estándares de referencia para la seguridad TI/OT

Diversos modelos y estándares internacionales han sido desarrollados para abordar la seguridad en sistemas industriales, uno de los modelos más reconocidos es el modelo Purdue/ISA-99, el cual propone una arquitectura jerárquica que segmenta los sistemas industriales en distintos niveles, desde los dispositivos de campo hasta los sistemas empresariales, facilitando la definición de zonas de seguridad y puntos de control entre capas [4].

Por su parte, la norma ISA/IEC 62443[3] constituye un marco integral de ciberseguridad para sistemas de automatización y control industrial. Este estándar introduce conceptos clave como zonas y conductos, niveles de seguridad y gestión del ciclo de vida de la seguridad, promoviendo un enfoque basado en riesgos y adaptable a la criticidad de los procesos industriales [6], [7].

Complementariamente, la guía NIST SP 800-82[2] proporciona recomendaciones específicas para la protección de sistemas de control industrial, adaptando prácticas de ciberseguridad tradicionales a las particularidades del entorno OT, este marco destaca la importancia de la segmentación, la defensa en profundidad y el monitoreo continuo como pilares para una convergencia segura [2].

Si bien estos marcos son ampliamente reconocidos y utilizados a nivel internacional, su aplicación directa suele resultar compleja en organizaciones con restricciones operativas, presupuestarias y culturales, como ocurre en gran parte de la industria alimenticia nacional [9].

Asimismo, se identificó la existencia de otros marcos complementarios, como NIST Cybersecurity Framework (CSF), ISO/IEC 27002 y C2M2 [14], orientados al gobierno de la ciberseguridad, gestión de riesgos y evaluación de madurez. Sin embargo, no se encontraron referencias que integren de manera explícita estos principios en una guía metodológica orientada a la separación y convergencia segura TI/OT para la industria alimenticia nacional.

Entre los modelos de evaluación de madurez identificados durante la revisión bibliográfica destaca el **Cybersecurity Capability Maturity Model (C2M2)**, ampliamente utilizado para medir capacidades de gestión de ciberseguridad en organizaciones de infraestructura crítica. Tanto C2M2 como **CMMI** [15] (**Capability Maturity Model Integration**) comparten una estructura basada en niveles progresivos de madurez, cuyo propósito es permitir que las organizaciones evalúen su situación actual e identifiquen

oportunidades de mejora continua. Sin embargo, ambos modelos presentan diferencias relevantes en cuanto a su enfoque y ámbito de aplicación.

C2M2 está orientado principalmente a la evaluación de capacidades organizacionales de ciberseguridad, considerando dominios relacionados con gobierno, gestión de riesgos, gestión de activos, respuesta ante incidentes y dependencia de servicios externos. Su objetivo es proporcionar una visión integral del nivel de desarrollo de las capacidades de ciberseguridad de una organización. Por su parte, CMMI constituye un modelo genérico de mejora de procesos que permite definir estados evolutivos de implementación y formalización de prácticas, facilitando su adaptación a distintos contextos organizacionales y tecnológicos.

La estructura de madurez basada en CMMI resultó más adecuada para los objetivos de la GCTIOT propuesta, al proporcionar un mecanismo simple, adaptable y alineado con la realidad operacional de las empresas de la industria alimentaria. Esta decisión busca privilegiar la evaluación del nivel de adopción de prácticas de convergencia TI/OT por sobre la medición de capacidades organizacionales generales de ciberseguridad, manteniendo un enfoque práctico y aplicable a organizaciones que se encuentran en distintas etapas de madurez dentro del sector alimenticio.

2.4 Estado del arte en la convergencia TI/OT en la industria alimenticia

El estado del arte evidencia que la convergencia TI/OT en sectores industriales críticos ha avanzado de manera desigual, estudios recientes indican que un alto porcentaje de organizaciones mantienen arquitecturas con segmentación principalmente lógica, compartiendo infraestructura física entre TI y OT, lo que limita la capacidad de aislamiento ante incidentes cibernéticos y aumenta el riesgo de propagación lateral de amenazas [11].

En el sector alimenticio, caracterizado por altos niveles de automatización, múltiples proveedores tecnológicos y operación continua, se han documentado prácticas emergentes orientadas a fortalecer la seguridad industrial, tales como el uso de zonas desmilitarizadas industriales (iDMZ), firewalls específicos para OT, monitoreo pasivo del tráfico industrial y planes de continuidad operacional integrados [10][11]. No obstante, estas prácticas suelen implementarse de forma parcial o reactiva, sin un modelo metodológico que permita su adopción progresiva y sostenible.

Diversos estudios destacan además la existencia de una brecha entre los enfoques normativos y su aplicación práctica en entornos productivos reales, especialmente en contextos latinoamericanos, donde factores culturales, organizacionales y presupuestarios dificultan la implementación de arquitecturas de convergencia segura [12][13], a partir de la revisión del estado del arte, no fue posible identificar publicaciones que propongan una metodología integral de convergencia TI/OT específicamente diseñada para la industria alimenticia.

La literatura encontrada se concentra principalmente en la aplicación de estándares como ISA/IEC 62443 en entornos industriales de carácter general, sin abordar de manera explícita las particularidades operacionales, regulatorias y productivas propias de este sector. Este hallazgo permite identificar una brecha de investigación y de aplicación práctica, la cual sustenta el aporte de la presente tesis al desarrollar una GCTIOT de implementación adaptada al contexto de la industria alimentaria.

La revisión de la literatura y las experiencias observadas en el ámbito industrial evidencia una tendencia creciente hacia la utilización conjunta de los marcos ISA/IEC 62443, NIST SP 800-82 y el modelo Purdue como base para la protección de entornos OT. Estas iniciativas han sido adoptadas principalmente en sectores como minería y energía, donde la segmentación de redes, la definición de zonas y conduits y la implementación de arquitecturas seguras constituyen prácticas ampliamente recomendadas. No obstante, la evidencia disponible muestra una limitada adaptación de estos marcos al contexto particular de la industria alimenticia nacional, especialmente bajo un enfoque que integre controles técnicos, organizacionales y operacionales.

2.5 Síntesis del marco teórico y estado del arte

En síntesis, el marco teórico y el estado del arte evidencian que la convergencia TI/OT es un componente esencial para la evolución hacia la Industria 4.0, pero también un desafío significativo en términos de

ciberseguridad y continuidad operativa. Si bien existen modelos y estándares internacionales robustos para abordar esta problemática, persiste una brecha entre la teoría normativa y su aplicación práctica en industrias con operación continua y alta criticidad.

Esta brecha justifica la necesidad de desarrollar una GCTIOT práctica de convergencia TI/OT, adaptada al contexto de la industria alimenticia nacional, que permita operacionalizar los estándares internacionales en acciones concretas, progresivas y medibles, alineadas con las exigencias operativas reales de las plantas productivas.

CAPITULO 3: Desarrollo de Propuesta de Solución

3.1 Diseño metodológico de la GCTIOT

El diseño metodológico de la solución propuesta se fundamenta en un enfoque estructurado, progresivo y adaptable, orientado a facilitar la implementación de controles de ciberseguridad en entornos industriales caracterizados por la coexistencia de redes de Tecnologías de la Información (TI) y Tecnologías de la Operación (OT).

Este diseño tiene como propósito principal operacionalizar algunos de los lineamientos contenidos en marcos normativos internacionales, tales como ISA/IEC 62443, NIST SP 800-82 y el modelo Purdue/ISA-99, mediante una GCTIOT práctica que permita su aplicación efectiva en el contexto de la industria alimenticia nacional.

La estrategia de implementación se basará en un enfoque incremental, el cual permitirá introducir cambios de manera gradual, evitando impactos significativos sobre los procesos productivos. Este enfoque considerará la aplicación de medidas de seguridad priorizando aquellos activos, sistemas o zonas que presenten mayor criticidad o exposición al riesgo.

En una primera etapa, se abordarán componentes de bajo impacto operacional, tales como la documentación de activos, la formalización de accesos, la implementación de controles básicos y la mejora de la visibilidad del entorno. Posteriormente, se avanzará hacia la incorporación de mecanismos más complejos, tales como, por ejemplo, segmentación de red, la implementación de firewalls industriales, la habilitación de un servidor pivote en una zona intermedia mediante una iDMZ, entre otros.

Este enfoque progresivo permite validar cada intervención para que en un futuro se pueda realizar su masificación y así reducir la probabilidad de errores y generar capacidades internas en la organización, tanto a nivel técnico como operativo. Asimismo, facilitará la alineación con las áreas productivas, evitando interrupciones no planificadas o efectos adversos sobre la continuidad del negocio.

La GCTIOT se articula sobre la base de un modelo metodológico compuesto por fases secuenciales, complementado por una aplicación transversal en distintos ámbitos organizacionales, junto con la definición de mecanismos de evaluación de madurez y métricas de seguimiento. Este enfoque permite abordar de manera integral las dimensiones técnicas, organizacionales y operativas asociadas a la ciberseguridad industrial.

3.2 Enfoque metodológico basado en fases

La GCTIOT propuesta se estructura en un modelo de cinco fases, cuyo desarrollo progresivo permite a la organización avanzar de manera controlada en la adopción de medidas de seguridad, minimizando el impacto sobre la continuidad operacional.

- **FASE 1: Levantamiento de activos**

Consiste en la identificación y clasificación de los activos TI y OT, incluyendo infraestructura, sistemas, aplicaciones, redes, capacitaciones y dispositivos industriales. Esta fase permite establecer una visión clara del entorno, identificando elementos críticos para la operación productiva.

Esta fase se aplica transversalmente sobre los cuatro ámbitos de la GCTIOT. A diferencia de las fases siguientes, el levantamiento fija los activos y estos permanecen estables, salvo que se incorporen nuevas tecnologías —en cuyo caso el activo debe recorrer nuevamente todas las fases—. Por ello, el aumento del nivel de madurez se obtiene iterando sobre las Fases 2 a 5, mientras la Fase 1 permanece como referencia.

- **FASE 2: Definición de Controles**

En esta fase se determinan los controles de ciberseguridad aplicables a cada activo o entorno identificado, en función de su criticidad y nivel de exposición. Se consideran algunos lineamientos derivados de estándares internacionales, adaptados al contexto particular de la organización.

A diferencia de la Fase 1, que fija los activos, la Fase 2 establece el «qué» de la seguridad: define los controles objetivo que posteriormente se evalúan (Fase 3), se priorizan (Fase 4) y se implementan (Fase 5). Su ejecución no modifica todavía el entorno productivo, sino que produce el marco de control formal sobre el cual se mide la brecha.

La selección de los controles se fundamenta en la necesidad de abordar los principales riesgos asociados a la convergencia entre entornos de TI/OT en la industria, considerando tanto las amenazas de ciberseguridad como los requerimientos de continuidad operacional propios de procesos productivos de alta disponibilidad.

La decisión de utilizar algunos de los controles provenientes de los marcos ISA/IEC 62443 y NIST SP 800-82 responde a que ambos constituyen referencias ampliamente reconocidas a nivel internacional para la protección de sistemas industriales y entornos OT.

Sin embargo, dado que dichos marcos contienen un número considerable de controles, la GCTIOT se enfoca en aquellos controles que presentan una relación directa con las problemáticas que se identificarán durante la Fase 1 de levantamiento de activos y que posean una aplicación práctica dentro de organizaciones que se encuentran en etapas iniciales en ciberseguridad industrial.

Asimismo, la selección de los controles que se ejecutarán será considerando su capacidad para generar mejoras progresivas y medibles en los cuatro ámbitos definidos en el capítulo siguiente que son: instalación física, hardware, software y procesos y personas.

- **FASE 3: evaluación de madurez y análisis GAP**

La tercera fase de la GCTIOT tiene como objetivo determinar el nivel de madurez de la organización en ciberseguridad industrial y convergencia TI/OT, además de identificar las brechas existentes entre la situación actual y el estado objetivo definido. Para ello, se establece una línea base cuantificable que permite evaluar el grado de implementación, formalización y efectividad de los controles identificados en las fases anteriores.

La evaluación se realiza mediante un instrumento de diagnóstico compuesto por 27 preguntas (Anexo 2: Análisis de Madurez Inicial), desarrollado a partir de los resultados obtenidos en las Fases 1 y 2. El cuestionario se basa en buenas prácticas y requisitos provenientes de ISA/IEC 62443, NIST SP 800-82 y los principios de segmentación y defensa en profundidad del modelo Purdue/ISA-99, permitiendo una valoración práctica de la ciberseguridad en entornos industriales.

Las preguntas abarcan los cuatro ámbitos definidos por la metodología: instalación física, hardware, software y procesos y personas. Cada una evalúa la existencia de controles de seguridad relevantes para el entorno operativo. Las respuestas positivas evidencian mecanismos formalizados de protección y gestión, mientras que las negativas reflejan oportunidades de mejora o carencias de control frente a riesgos identificados.

El cuestionario fue diseñado para ser simple, objetivo y aplicable en organizaciones industriales con distintos niveles de desarrollo en ciberseguridad OT. Además, permite realizar evaluaciones periódicas y comparar resultados en el tiempo para medir avances y verificar la efectividad de las acciones implementadas.

La determinación del nivel de madurez utiliza una adaptación del modelo CMMI (Capability Maturity Model Integration), descrito en el Capítulo 3.2.2, el cual clasifica el desarrollo de los procesos en cinco niveles progresivos, desde prácticas iniciales y reactivas hasta procesos optimizados y orientados a la mejora continua. Esta adaptación considera las características propias de los entornos industriales y de las organizaciones de manufactura, con foco en la convergencia segura entre las redes TI y OT.

Los resultados permiten evaluar el grado de implementación y efectividad de controles relacionados con seguridad física, segmentación de redes, gestión de accesos, protección de infraestructura tecnológica, monitoreo, continuidad operacional, respaldo y recuperación, gestión de vulnerabilidades y gobierno de la ciberseguridad.

Posteriormente, se realiza un análisis GAP que compara el nivel de madurez actual con el nivel objetivo definido para cada ámbito evaluado. Este análisis permite identificar y cuantificar las brechas existentes, determinando las áreas donde es necesario fortalecer capacidades, incorporar nuevos controles o mejorar los mecanismos ya implementados.

Asimismo, las brechas se priorizan considerando el impacto operacional, la criticidad de los activos, el nivel de riesgo asociado y la dependencia de los procesos productivos, permitiendo orientar los recursos hacia las iniciativas con mayor contribución a la reducción del riesgo y a la continuidad operacional.

Como resultado, esta fase entrega una visión integral del estado de madurez de la organización, identificando fortalezas, debilidades y oportunidades de mejora. La información obtenida constituye la línea base para la elaboración del plan de mitigación de brechas, incluyendo iniciativas de mejora, responsables, plazos e indicadores de seguimiento.

De este modo, la evaluación de madurez y el análisis GAP se convierten en el principal mecanismo para orientar la evolución progresiva hacia un modelo de convergencia TI/OT más seguro, resiliente, medible y alineado con las mejores prácticas internacionales de ciberseguridad industrial.

- **FASE 4: Plan de mitigación**

A partir de las brechas detectadas, se diseña un plan de acción orientado a la implementación de medidas correctivas, estableciendo prioridades, responsables, plazos y recursos necesarios.

El plan de mitigación constituirá el principal instrumento para la implementación de la solución, ya que transformó los resultados del análisis de brechas en un conjunto concreto de acciones. Este plan se establece a partir del contraste entre el estado actual de la organización y el nivel de madurez objetivo definido, permitiendo identificar desviaciones, riesgos asociados y oportunidades de mejora.

Cada acción de mitigación fue definida considerando los siguientes elementos:

- Descripción de la medida.
- Activo o proceso afectado
- Nivel de prioridad
- Responsables de ejecución
- Recursos requeridos.
- Plazos estimados.

La priorización ayudará a definir los criterios de criticidad operacional, impacto potencial en la seguridad y factibilidad de implementación.

Adicionalmente, el plan será coherente con la arquitectura definida, asegurando que las medidas propuestas contribuyan a fortalecer la segmentación de red, la protección de zonas críticas y el control de accesos entre dominios TI y OT. Este instrumento, además, debe tener un seguimiento estructurado del avance de la implementación y facilitar la toma de decisiones a nivel organizacional.

- **FASE 5: Implementación y seguimiento**

Se ejecutan las acciones definidas en el plan de mitigación, incorporando mecanismos de monitoreo y control que permitan evaluar el avance y asegurar la sostenibilidad de las medidas adoptadas.

La implementación técnica de la GCTIOT debe seguir procedimientos controlados, considerando buenas prácticas de gestión de cambios en entornos críticos. Cada intervención es planificada, documentada y validada previamente a su ejecución con el comité de cambio e incorporando instancias de prueba que permitan verificar su correcto funcionamiento en condiciones similares al entorno productivo.

En este contexto, resulta fundamental coordinar ventanas de intervención con las áreas operacionales, especialmente en sistemas que no pueden ser detenidos sin afectar la producción. Asimismo, se deben utilizar entornos de prueba o simulación cuando sea posible, con el fin de reducir la incertidumbre asociada a los cambios.

Una vez implementadas las medidas, es fundamental que se realice una validación técnica que considere aspectos como la conectividad, el rendimiento, la compatibilidad de sistemas y la correcta aplicación de las políticas de seguridad. Esta validación tendrá que ser documentada, dejando evidencia que respalden la efectividad de la intervención.

Un aspecto central de la implementación es considerar permanentemente la continuidad operacional. En este sentido, cada acción de mejora es evaluada en función de su impacto potencial sobre la operación productiva, asegurando que los beneficios en términos de seguridad no generaran riesgos adicionales para el negocio.

Para ello, se definen mecanismos de gestión de riesgos que permitan anticipar posibles efectos adversos de la implementación, tales como fallas en la comunicación entre sistemas, incompatibilidades tecnológicas o interrupciones de servicios críticos. En aquellos casos en que fuera necesario, se establecen planes de contingencia y rollback que permitan restaurar el estado previo ante incidentes durante el despliegue.

Asimismo, se considera tener respaldo, monitoreo continuo y planes de recuperación ante desastres, lo cual fortalece la resiliencia del entorno industrial, asegurando que la organización pudiera responder adecuadamente frente a eventos de seguridad o fallas operacionales. La implementación se complementa con un enfoque de seguimiento periódico y mejora continua, el cual asegura la vigencia y efectividad de las medidas adoptadas en el tiempo.

Este enfoque metodológico permite transitar desde un diagnóstico inicial hacia un modelo de mejora continua, alineado con los principios de gestión de la seguridad de la información y ciberseguridad industrial.

3.2.1 Ámbitos de aplicación

Cada Fase descrita anteriormente se aplica de manera transversal a cuatro ámbitos fundamentales, reconociendo que la ciberseguridad en entornos TI/OT no depende exclusivamente de componentes tecnológicos, sino que involucra aspectos físicos, organizacionales y humanos.

- **ÁMBITO 1: Instalación física**

Considera la seguridad perimetral, control de accesos físicos, segregación de áreas y protección de infraestructura crítica.

- **ÁMBITO 2: Hardware**

Incluye la gestión de dispositivos, control de acceso a equipos, segmentación de redes y protección de activos industriales.

- **ÁMBITO 3: Software**

Abarca la gestión de sistemas operativos, aplicaciones, parches de seguridad, control de accesos lógicos y monitoreo de actividades.

- **ÁMBITO 4: Procesos y personas**

Considera la definición de políticas, procedimientos, capacitación, gestión de roles y responsabilidades, y cultura organizacional en ciberseguridad.

Algunos niveles de aplicabilidad de los ÁMBITOS se muestran en la figura 1.



Figura 1: Ámbitos y sus niveles de aplicabilidad.

Este enfoque integral permite asegurar que las medidas implementadas sean coherentes y efectivas en todos los niveles de la organización.

Cada FASE se aplica transversalmente sobre los 4 ÁMBITOS, como lo muestra la figura 2.



Figura 2: Enfoque metodológico de la GCTIOT con sus fases y ámbitos

3.2.2 Modelo de madurez y análisis de brechas (GAP)

El modelo de madurez constituye un elemento central del diseño metodológico que está plasmado en la Fase 3, ya que permite evaluar de manera sistemática el estado de implementación de los controles de ciberseguridad. Para ello, se consideran distintos niveles de madurez, que reflejan el grado de formalización, control y optimización de las prácticas implementadas.

Para evaluar la madurez de la organización y el impacto esperado de la GCTIOT propuesta, se empleó un modelo de Madurez TI/OT de cinco niveles basado en CMMI. Permitiendo medir el grado de formalización, gestión y optimización de los controles de ciberseguridad industrial.

La priorización de acciones dentro del análisis GAP se realiza considerando tanto la magnitud de la brecha detectada como el nivel de riesgo que dicha brecha representa para la organización. En términos prácticos, no todas las desviaciones identificadas tienen el mismo impacto sobre la ciberseguridad, la continuidad operacional o la resiliencia de los procesos productivos. Por esta razón, una vez identificadas las diferencias entre el estado actual y el nivel de madurez objetivo, es necesario establecer un orden de implementación que permita abordar primero aquellas brechas que generan una mayor exposición al riesgo.

Para ello, cada brecha puede ser evaluada considerando criterios como el impacto potencial sobre la operación, la probabilidad de ocurrencia de incidentes de seguridad, el nivel de exposición de los activos críticos, los requisitos normativos asociados y la complejidad de implementación de los controles. Aquellas brechas que afectan la disponibilidad de los sistemas industriales, la seguridad de los procesos productivos o la protección de los dispositivos críticos deben recibir una prioridad alta, mientras que las brechas de menor impacto pueden ser abordadas en etapas posteriores.

Como resultado de este proceso, las acciones de mitigación se clasifican y ordenan en un plan de trabajo progresivo, permitiendo asignar recursos, responsables y plazos de forma eficiente. De esta manera, el análisis GAP no solo identifica las diferencias existentes entre el nivel de madurez actual y el objetivo, sino que también proporciona una base objetiva para la toma de decisiones y la planificación de las iniciativas de mejora. Este enfoque facilita una evolución controlada hacia niveles superiores de madurez, asegurando que las inversiones y esfuerzos se orienten prioritariamente a la reducción de los riesgos más significativos para la organización.

Criterios de priorización

La priorización considera tres variables: **Prioridad = Impacto × Riesgo × Complejidad**

Donde:

- **Impacto:** Consecuencia sobre la producción, seguridad operacional o continuidad del negocio.

- **Riesgo:** Probabilidad de que la brecha sea explotada o genere un incidente.
- **Complejidad:** Esfuerzo requerido para implementar la mejora.

Esta metodología permite enfocar los esfuerzos iniciales en los controles que entregan una mayor reducción del riesgo y contribuyen al avance de madurez de la organización.

De forma referencial, se establecen niveles progresivos que van desde un estado inicial, caracterizado por la ausencia de controles formales, hasta un estado optimizado, en el cual los procesos se encuentran plenamente integrados, monitoreados y sujetos a mejora continua.

Niveles de madurez (1–5), que se muestran en figura 3:

- **Nivel 1 – Inicial:** Corresponde a un estado en el cual no existen controles formales ni prácticas definidas. Las acciones son reactivas y dependen de iniciativas individuales, sin una estrategia estructurada de ciberseguridad.
- **Nivel 2 – Parcial:** Se identifican ciertas prácticas o controles implementados de manera aislada, sin una estandarización ni documentación formal. La gestión es incipiente y no existe una visión integrada del entorno TI/OT.
- **Nivel 3 – Funcional:** Los controles son implementados de forma consistente en áreas específicas y comienzan a alinearse con procesos definidos. Existe cierta documentación y repetibilidad, aunque aún con limitaciones en integración y cobertura.
- **Nivel 4 – Gestionado:** Los controles se encuentran formalizados, documentados y gestionados de manera sistemática. Se dispone de métricas, monitoreo y mecanismos de control que permiten evaluar su desempeño y asegurar su cumplimiento.
- **Nivel 5 – Optimizado:** Corresponde al nivel más avanzado, donde los procesos están plenamente integrados, automatizados y sujetos a mejora continua. La organización adopta un enfoque proactivo, basado en análisis de datos, gestión de riesgos y optimización permanente de la ciberseguridad.

Modelo de madurez y posición inicial de la organización

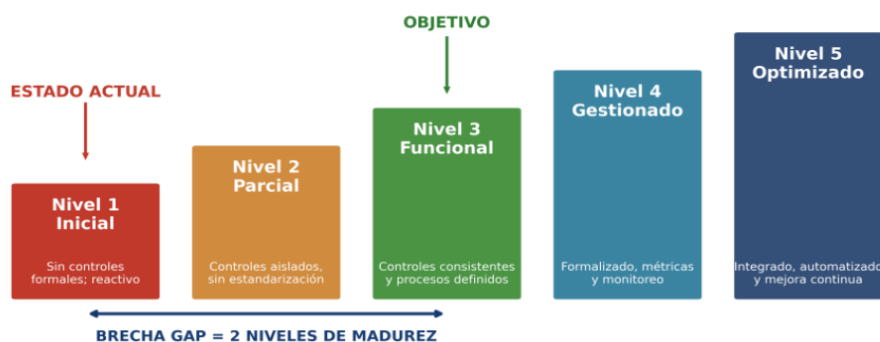


Figura 3: Modelo de madurez basado en CMMI

El análisis de brechas (GAP) se realiza comparando el estado actual de la organización con el nivel objetivo definido, permitiendo identificar desviaciones y priorizar acciones de mejora. Este análisis se alinea con los requerimientos de estándares como ISA/IEC 62443, facilitando la trazabilidad y el cumplimiento normativo.

3.3 Métricas e indicadores de evaluación

Con el propósito de evaluar de manera objetiva la efectividad de la GCTIOT propuesta y determinar su contribución a la mejora de la seguridad en entornos de convergencia TI/OT, se establece un conjunto de métricas e indicadores de desempeño que permiten medir tanto los aspectos técnicos como organizacionales

asociados a la implementación de los controles definidos. Estos indicadores constituyen una herramienta fundamental para verificar el cumplimiento de los objetivos planteados, cuantificar la reducción de brechas identificadas durante el diagnóstico y determinar el avance de la organización hacia el nivel de madurez objetivo.

Desde la perspectiva técnica, los indicadores están orientados a medir el grado de implementación y efectividad de los controles de seguridad incorporados en la infraestructura tecnológica e industrial. Entre ellos se consideran aspectos como el nivel de segmentación entre redes TI y OT, la gestión y control de accesos a sistemas críticos, la cobertura de monitoreo de eventos de seguridad, la protección de activos industriales, la existencia de mecanismos de respaldo y recuperación, y la capacidad para detectar y responder oportunamente ante incidentes de ciberseguridad. Estos indicadores permiten evaluar la reducción de la superficie de ataque, el fortalecimiento de los mecanismos de defensa y el aumento de la resiliencia operativa de la organización.

Por otra parte, los indicadores organizacionales tienen como finalidad medir el grado de institucionalización de los controles y procesos asociados a la ciberseguridad industrial. Dentro de esta categoría se consideran variables tales como el cumplimiento de políticas y estándares internos, la formalización y documentación de procedimientos, la definición de roles y responsabilidades, el nivel de capacitación y concientización del personal, así como la incorporación de prácticas de gestión de riesgos y continuidad operacional. Estos elementos permiten determinar en qué medida la organización ha integrado la ciberseguridad dentro de sus procesos de gestión y gobernanza.

Adicionalmente, se incorporan métricas asociadas al modelo de madurez utilizado en la investigación, permitiendo comparar el estado inicial de la organización con la situación posterior a la implementación de la GCTIOT. De esta forma, es posible medir el avance alcanzado en cada uno de los ámbitos evaluados — instalación física, hardware y redes, software y sistemas, y procesos y personas— identificando las brechas que han sido mitigadas y aquellas que requieren nuevas acciones de mejora.

La definición y seguimiento periódico de estos indicadores proporciona un marco de evaluación estructurado y verificable, facilitando la toma de decisiones basada en evidencia, la asignación eficiente de recursos y la priorización de iniciativas de seguridad. Asimismo, permite monitorear el progreso de la implementación, evaluar el impacto real de los controles adoptados y establecer un proceso de mejora continua que contribuya a incrementar progresivamente el nivel de madurez de la organización en materia de convergencia segura TI/OT.

Indicadores considerados:

Categoría	Indicador	Objetivo
Técnico	Porcentaje de activos TI/OT inventariados	Asegurar visibilidad de la infraestructura
Técnico	Porcentaje de segmentación de redes implementada	Reducir la exposición entre entornos TI y OT
Técnico	Cobertura de monitoreo de activos críticos	Mejorar la detección temprana de incidentes
Técnico	Tiempo de detección y respuesta a incidentes	Incrementar la resiliencia operativa
Organizacional	Cumplimiento de políticas y procedimientos	Asegurar la adopción de controles definidos
Organizacional	Personal capacitado en ciberseguridad TI/OT	Fortalecer la cultura de seguridad
Organizacional	Procedimientos formalizados y documentados	Mejorar la gobernanza y trazabilidad
Madurez	Nivel de madurez alcanzado por ámbito	Medir el avance hacia el Nivel deseado
GAP	Porcentaje de brechas mitigadas	Evaluar la efectividad de la GCTIOT propuesta

De esta manera, las métricas e indicadores definidos permiten no solo validar la hipótesis de investigación, sino también demostrar cuantitativamente el impacto de la GCTIOT sobre la ciberseguridad, la continuidad operacional y el incremento del nivel de madurez de la organización.

CAPITULO 4: Aplicación de la GCTIOT

4.1 Implementación y validación

La implementación y validación de la GCTIOT tuvo por objetivo definir el conjunto de directrices, estrategias y actividades necesarias para llevar a la práctica el diseño metodológico y arquitectónico descrito en las secciones anteriores. Este modelo buscó asegurar una transición controlada desde el estado actual de la organización (Inicial=1) hacia un estado objetivo de mayor nivel de seguridad (Funcional=3), manteniendo en todo momento la continuidad operacional y minimizando los riesgos asociados a la intervención sobre entornos productivos.

Dado el carácter crítico de los sistemas industriales y las exigencias de operación continua propias de la industria, el modelo de implementación se estructuró bajo un enfoque progresivo, basado en la priorización de riesgos, la segmentación de las intervenciones y la validación continua de los cambios realizados. En este contexto, la implementación no se concibió como un proceso único o estático, sino como un ciclo iterativo de mejora continua, alineado con los resultados obtenidos en el análisis de madurez y brechas.

4.2 Caso de Estudio

La implementación de la GCTIOT de separación física y convergencia segura entre entornos de TI/OT se desarrolló en una planta productiva del sector alimenticio nacional. Como unidad de análisis se seleccionó una línea de producción representativa, caracterizada por una operación continua bajo régimen 24/6, altos niveles de automatización y una dependencia crítica de sistemas de control industrial para la continuidad del proceso productivo.

Desde el punto de vista técnico, el entorno analizado correspondía a una arquitectura industrial con un alto grado de intercambio de información sin una convergencia segura entre redes TI y OT, desarrollada de forma progresiva y sin un modelo de referencia formal. Esta evolución derivó en una infraestructura heterogénea, caracterizada por la existencia de múltiples interconexiones directas entre ambos entornos, baja segmentación de red, escasa visibilidad del tráfico industrial y una limitada capacidad de control sobre las comunicaciones.

En el ámbito organizacional, se evidenciaron brechas relevantes en la gestión de ciberseguridad, incluyendo la ausencia de procesos formales, debilidades en la gestión de accesos —particularmente en entornos OT—, baja capacitación del personal y una dependencia significativa de proveedores externos que acceden de forma remota a la red de control sin controles robustos. Estas condiciones configuraban un escenario de riesgo elevado, incrementando la superficie de ataque y dificultando la detección y contención de incidentes.

Como consecuencia, el entorno presentaba una alta exposición a amenazas capaces de propagarse desde redes corporativas (niveles superiores del modelo Purdue) hacia niveles críticos de operación (niveles 1 y 2), donde residen los sistemas de supervisión y control, generando un impacto potencial directo sobre la disponibilidad y continuidad operacional.

En este contexto, el caso de estudio se centra en la ausencia de un modelo estructurado que permita gestionar de forma segura la convergencia TI/OT, asegurando la segmentación de redes, el control de accesos y la protección de los activos críticos sin afectar la operación industrial.

La intervención consistió en la aplicación de la GCTIOT, la cual propone un enfoque estructurado basado en la incorporación de algunos controles técnicos, arquitectónicos y organizacionales, alineados a los marcos de referencia como ISA/IEC 62443 y NIST SP 800-82, junto con la adopción del modelo Purdue como base para la segmentación del entorno.

El objetivo fue evaluar la aplicabilidad y efectividad de la GCTIOT en un entorno industrial, mediante el análisis del estado inicial y su evolución posterior a la intervención, considerando su impacto en la seguridad, visibilidad y continuidad operacional. La validación tuvo como propósito demostrar que la GCTIOT propuesta permite operacionalizar los controles de marcos internacionales en una metodología

sencilla, práctica, progresiva, medible y aplicable a entornos industriales reales. Se evaluó su capacidad para reducir brechas de seguridad, priorizar acciones según el riesgo, mejorar la resiliencia operativa y aumentar el nivel de madurez organizacional.

Los resultados permitieron verificar que la GCTIOT proporciona una hoja de ruta clara y realista para implementar controles de ciberseguridad de forma gradual, adaptándose a las restricciones operativas de la industria y facilitando la adopción efectiva de buenas prácticas de convergencia segura TI/OT.

4.3 Implementación de Fases y Ámbitos

A.- FASE 1: Levantamiento de activos por ámbito

Estado de la fase: Completada-Entregable: inventario de activos TI/OT identificado y clasificado, establecido como línea base, ver Anexo 6.

La Fase 1 fue ejecutada con el propósito de levantar los activos del entorno. Durante su desarrollo se llevó a cabo la identificación y clasificación de los activos de TI/OT, incluyendo redes, infraestructura, aplicaciones, dispositivos industriales y capacitaciones. Como resultado, se obtuvo una visión clara del entorno, se identificaron los elementos críticos para la operación productiva y se estableció la línea base sobre la cual se aplican las fases posteriores. A diferencia de las fases siguientes, el levantamiento fija los activos y estos permanecen estables.

A.1 Ejecución por ámbito

- **Ámbito 1 — Instalación física**

El levantamiento abarcó las instalaciones, salas y racks, la ubicación de los equipos y el perímetro físico que aloja los activos TI y OT. El diagnóstico evidenció racks compartidos entre TI y OT, condición que incumple los requisitos de seguridad física de ISA/IEC 62443 al no existir separación entre ambos dominios. Esta situación permitió dimensionar la exposición física de los activos críticos.

- **Ámbito 2 — Hardware / Red**

Se identificaron los dispositivos de hardware y red: PLC, switches, servidores, dispositivos industriales y la topología de red. El levantamiento reveló dispositivos no gestionados, es decir, activos sin control formal de configuración ni de altas y bajas, lo que incumple NIST CM-8 (inventario de componentes del sistema). Este inventario constituyó la base para la posterior segmentación por niveles Purdue.

- **Ámbito 3 — Software / Lógico**

El levantamiento del software cubrió los sistemas operativos, las aplicaciones, los servicios y el SCADA, junto con sus versiones y estado de parches. Se constató la existencia de versiones sin control, sin una gestión formal de actualizaciones, situación que incumple NIST SI-2 (gestión de fallas y parches). La identificación de versiones expuso la deuda técnica y el riesgo asociado a componentes desactualizados.

- **Ámbito 4 — Procesos y personas**

En el plano organizacional se levantaron las políticas, los procedimientos, los roles y responsabilidades y los registros de capacitación. El resultado mostró que estos elementos eran inexistentes o no formalizados, incumpliendo NIST PL-2 (plan de seguridad del sistema). La ausencia de documentación formal confirmó la falta de gobierno de la ciberseguridad OT.

Síntesis del levantamiento por ámbito, se muestran en Tabla 1:

Tabla 1: Resultados del levantamiento de activos (Fase 1) por ámbito.

Ámbito	Activos levantados	Hallazgo	Control incumplido
Instalación física	Instalaciones, salas, racks; ubicación de equipos; perímetro físico	Racks compartidos entre TI y OT	ISA/IEC 62443 (seg. física)
Hardware / Red	PLC, switches, servidores; dispositivos industriales; topología de red	Dispositivos no gestionados	NIST CM-8

Ámbito	Activos levantados	Hallazgo	Control incumplido
Software / Lógico	Sistemas operativos, aplicaciones, SCADA; versiones y parches	Versiones sin control	NIST SI-2
Procesos y personas	Políticas, procedimientos, roles; registros de capacitación	Inexistentes / no formalizados	NIST PL-2

Una vez concluida la Fase 1, se logró visibilidad del entorno, eliminando una de las principales debilidades del Nivel 1: la falta de conocimiento sobre los activos existentes y su estado. Al ser un componente de bajo impacto operacional, el levantamiento se abordó en la primera etapa junto con la documentación de activos y la mejora de la visibilidad.

Con los activos identificados y clasificados como línea base, la organización quedó en condiciones de aplicar las fases siguientes sobre un entorno conocido, condición indispensable para avanzar de forma controlada hacia el Nivel 3 de madurez (Funcional) que es el deseado por la organización. Los resultados de la Fase 1 en los cuatro ámbitos se pueden ver en el Anexo 7.

B. FASE 2: Definición de controles

Estado de la fase: Completada-**Entregable:** conjunto de controles de ciberseguridad definidos por ámbito y mapeados a NIST e ISA/IEC 62443, como control objetivo ver Anexo 6.

La Fase 2 fue ejecutada para determinar los controles de ciberseguridad aplicables a cada ámbito, en función de la criticidad y el nivel de exposición de los activos identificados en la Fase 1. Los controles se derivaron de estándares internacionales y se adaptaron al contexto particular de la organización. Se definieron los controles objetivo que posteriormente se evalúan (Fase 3).

B.1 Ejecución por ámbito

- **Ámbito 1 — Instalación física**

Sobre la base del levantamiento de la Fase 1, se definió el control de acceso físico como medida base para las instalaciones, salas y racks que alojan activos TI y OT. Este control responde directamente a una de las debilidades del estado inicial —los racks compartidos y el acceso físico no controlado— y se orienta a separar y proteger la infraestructura crítica. Su definición se alinea con la familia de control de acceso de NIST aplicada al plano físico.

- **Ámbito 2 — Hardware / Red**

Se definió la segmentación de la red según el modelo Purdue como control estructural del ámbito de hardware y red. Esta medida ataca la raíz del riesgo del Nivel 1 —la convergencia TI/OT no gobernada y la interconexión directa entre niveles— y establece la base para el posterior aislamiento por zonas. Se fundamenta en ISA/IEC 62443 SR 5 (restricción de flujo) y en las familias NIST SC.

- **Ámbito 3 — Software / Lógico**

En el ámbito de software se definieron dos controles complementarios: el hardening de los sistemas operativos y aplicaciones, y el control de acceso lógico. En conjunto, buscan cerrar brechas del estado inicial como el SCADA accesible desde TI sin control intermedio y el uso de credenciales compartidas. Estos controles se alinean con las familias NIST AC (control de acceso) e IA (identificación y autenticación).

- **Ámbito 4 — Procesos y personas**

Para el ámbito de procesos y personas se definió la formalización de procedimientos como control organizacional base. Esta medida responde a la ausencia de procedimientos formales y de gobierno de ciberseguridad detectada en el estado inicial, y sienta las condiciones para la posterior definición de roles y la capacitación del personal. Se fundamenta en ISA/IEC 62443 SR 1.

Síntesis por ámbito, se muestran en Tabla 2:

Tabla 2: Controles definidos en la Fase 2 por ámbito, con la debilidad del Nivel 1 que mitigan y su referencia.

Ámbito	Control definido	Qué mitiga (Nivel 1)	Referencia
Instalación física	Control de acceso físico	Racks compartidos; acceso físico no controlado	NIST AC
Hardware / Red	Segmentación Purdue	Convergencia TI/OT no gobernada	ISA/IEC 62443 SR 5
Software / Lógico	Hardening + control de acceso lógico	SCADA accesible; credenciales compartidas	NIST AC · IA
Procesos y personas	Procedimientos formales	Ausencia de procesos y gobierno	ISA/IEC 62443 SR 1

Con la Fase 2 concluida, se establecieron los controles base en los cuatro ámbitos. Al pasar de un entorno sin controles definidos a uno con un marco de control formalizado, la organización logró la transición del Nivel 1 (inicial) al Nivel 2 (parcial).

Estos controles constituyen la referencia contra la cual la Fase 3 realiza el análisis de madurez y de brechas (GAP), permitiendo cuantificar qué tan lejos se encuentra la implementación real respecto del marco definido y priorizar, con enfoque de riesgo, las acciones de mitigación de las fases siguientes. Los resultados de la Fase 2 en los cuatro ámbitos se pueden ver en el Anexo 7.

C. FASE 3: Evaluación de madurez y análisis de brechas (GAP)

Estado de la fase: Completada-**Entregable:** análisis de brechas (GAP) con los incumplimientos, el riesgo asociado y su priorización, como insumo del plan de mitigación, ver Anexo 6.

La Fase 3 fue ejecutada para evaluar el grado de implementación de los controles definidos en la Fase 2 y detectar las brechas existentes. La evaluación se realizó contrastando el marco de control con la situación real del entorno, lo que permitió identificar las desviaciones y su criticidad.

El análisis de brechas (GAP) se orientó a la priorización de acciones en función del riesgo asociado, alineándose con los requerimientos de ISA/IEC 62443 para facilitar la trazabilidad y el cumplimiento normativo.

C.1 Ejecución por ámbito

- **Ámbito 1 — Instalación física**

La evaluación evidenció la ausencia de un control de acceso físico formal sobre las áreas y racks que alojan activos OT. Esta brecha implica un riesgo de acceso físico no autorizado a la infraestructura crítica y mantiene la exposición identificada en el estado inicial. Constituye un incumplimiento de los requisitos de seguridad física de ISA/IEC 62443.

- **Ámbito 2 — Hardware / Red**

Se detectó la ausencia de firewalls que controlaran el tráfico entre TI y OT. Esta brecha es una de las más críticas, ya que habilita el movimiento lateral y la propagación de amenazas desde las redes corporativas hacia la capa de control industrial. Corresponde a un incumplimiento de NIST SC-7 (protección de frontera).

- **Ámbito 3 — Software / Lógico**

La evaluación reveló dos brechas relevantes: la falta de autenticación en el acceso a los sistemas industriales y la ausencia de monitoreo del tráfico OT. La primera facilita accesos no controlados y el escalamiento de privilegios; la segunda impide la detección de anomalías y la contención temprana de incidentes. Estas brechas incumplen NIST IA-2 (autenticación) e ISA/IEC 62443 SR 7 (logging y monitoreo).

- **Ámbito 4 — Procesos y personas**

Se detectó la ausencia de capacidad de respuesta ante incidentes, sin procesos documentados que orienten la actuación frente a un evento de seguridad. Esta brecha reduce la capacidad de contención y recuperación de la organización, e incumple NIST IR-4 (respuesta a incidentes), como también la falta de capacitación.

Síntesis por ámbito, se muestran en Tabla 3:

Tabla 3: Brechas detectadas en la Fase 3 por ámbito, con su riesgo asociado y el control incumplido.

Ámbito	Brecha detectada	Riesgo asociado	Incumple
Instalación física	Sin control de acceso físico	Acceso físico no autorizado a OT	ISA/IEC 62443 (física)
Hardware / Red	Sin firewalls entre TI y OT	Movimiento lateral TI → OT	NIST SC-7
Software / Lógico	Sin autenticación ni monitoreo	Accesos no controlados; sin detección	NIST IA-2 · SR 7
Procesos y personas	Sin respuesta a incidentes / Falta de capacitación	Baja contención ante eventos / poco conocimiento	NIST IR-4

Resultado de la Fase 3:

Con la Fase 3 concluida, las brechas quedaron identificadas y priorizadas con enfoque de riesgo. Los incumplimientos críticos concentran el mayor impacto potencial sobre la seguridad y la continuidad, por lo que encabezan la priorización.

Este análisis constituye el insumo directo del plan de mitigación (Fase 4): interpreta el estado de madurez en un conjunto ordenado de brechas con su riesgo asociado, sobre el cual se definen las medidas correctivas, sus responsables, sus recursos y sus plazos. Los resultados de la Fase 3 en los cuatro ámbitos se pueden ver en el Anexo 7.

D. FASE 4: Plan de mitigación de brechas

Estado de la fase: Completada-**Entregable:** plan de mitigación con las medidas de alto impacto, cada una asociada a la brecha, con su prioridad, responsables, recursos y plazos, ver Anexo 6.

La Fase 4 fue ejecutada para transformar las brechas detectadas en la Fase 3 en un conjunto concreto de medidas correctivas. Cada medida se definió con su descripción, el activo o proceso afectado, el nivel de prioridad, los responsables, los recursos requeridos y los plazos estimados.

La priorización se basó en tres criterios: la criticidad operacional, el impacto potencial en la producción y la factibilidad técnica de implementación.

D.1 Ejecución por ámbito

- **Ámbito 1 — Instalación física**

Se planificaron el control de acceso físico y la separación de racks entre TI y OT, medidas orientadas a cerrar la brecha de acceso físico no controlado detectada en la Fase 3.

- **Ámbito 2 — Hardware / Red**

Se priorizaron, con prioridad alta, la segmentación TI/OT, la implementación de una iDMZ y la incorporación de firewalls para contener el movimiento lateral hacia la capa de control.

- **Ámbito 3 — Software / Lógico**

Se planificaron, con prioridad alta, el control de accesos y la implementación de monitoreo del tráfico industrial, con el fin de cerrar las brechas de autenticación y de visibilidad.

- **Ámbito 4 — Procesos y personas**

Se planificaron la formalización de procedimientos y la capacitación del personal OT, medidas que atienden la ausencia de respuesta a incidentes (NIST IR-4) y de gobierno.

Síntesis por ámbito, se muestran en Tabla 4:

Tabla 4: Medidas del plan de mitigación (Fase 4) por ámbito, con la brecha que atienden y su prioridad.

Ámbito	Medida priorizada	Atiende brecha	Prioridad
Instalación física	Control de acceso físico y separación de racks	Acceso físico no controlado	Media

Ámbito	Medida priorizada	Atiende brecha	Prioridad
Hardware / Red	Segmentación TI/OT, iDMZ y firewalls	Sin firewalls (SC-7)	Alta
Software / Lógico	Control de accesos y monitoreo	Sin autenticación ni monitoreo	Alta
Procesos y personas	Procedimientos y capacitación	Sin respuesta a incidentes	Media

Resultado de la Fase 4:

Con la Fase 4 concluida, se dispuso de un plan de mitigación priorizado por riesgo operacional, impacto en producción y factibilidad técnica. El plan estableció el orden de intervención, comenzando por las medidas de alto impacto que reducen la superficie de ataque entre TI y OT.

Este plan es coherente con la arquitectura objetivo (segmentación, iDMZ y control de accesos) y constituye la hoja de ruta directa de la Fase 5, en la que las medidas se implementan y validan mediante procedimientos controlados de gestión de cambios. Los resultados de la Fase 4 en los cuatro ámbitos se pueden ver en el Anexo 7.

E. FASE 5: Implementación y seguimiento

Estado de la fase: Completada-Entregable: controles implementados y validados por ámbito, con arquitectura segmentada operativa; se alcanza el Nivel 3 Funcional ver Anexo 6.

La Fase 5 fue ejecutada para implementar las medidas del plan de mitigación mediante procedimientos controlados de gestión de cambios. Cada intervención fue planificada, documentada y validada previamente con el comité de cambios, incorporando instancias de prueba en condiciones similares a las de producción. La implementación consideró en todo momento la continuidad operacional.

E.1 Ejecución por ámbito

- **Ámbito 1 — Instalación física**

Se implementaron la separación de racks y el control de acceso físico a las áreas OT, cerrando la brecha de acceso físico no controlado. Con ello, la infraestructura crítica quedó protegida y segregada de la red corporativa, conforme a los requisitos de seguridad física.

- **Ámbito 2 — Hardware / Red**

Se implementaron los firewalls industriales y la segmentación según el modelo Purdue, habilitando una iDMZ entre los niveles 3, 4 y conduits controlados. Esta intervención cierra la brecha de ausencia de firewalls y desacopla funcionalmente TI de OT, conteniendo el movimiento lateral hacia la capa de control (ISA/IEC 62443 SR 5).

- **Ámbito 3 — Software / Lógico**

Se implementaron el hardening de los sistemas y la autenticación de accesos, junto con un monitoreo parcial del tráfico industrial. La autenticación cierra la brecha de credenciales y accesos no controlados.

- **Ámbito 4 — Procesos y personas**

Se implementaron los procedimientos formales y la capacitación del personal OT, cerrando la brecha organizacional y fortaleciendo la respuesta ante incidentes.

Síntesis por ámbito, se muestran en Tabla 5:

Tabla 5: Controles implementados en la Fase 5 por ámbito, con la brecha cerrada y el control aplicado.

Ámbito	Implementado	Brecha cerrada	Control aplicado
Instalación física	Separación de racks; control de acceso	Acceso físico no controlado	ISA/IEC 62443 (física)
Hardware / Red	Firewalls; segmentación Purdue; Idmz	Sin firewalls (SC-7)	NIST SC-7 · ISA SR 5

Ámbito	Implementado	Brecha cerrada	Control aplicado
Software / Lógico	Hardening; autenticación; monitoreo parcial	Sin autenticación (monitoreo parcial)	NIST IA-2 · SR 1
Procesos y personas	Procedimientos; capacitación	Sin respuesta a incidentes	ISA/IEC 62443-2-1

Resultado de la Fase 5:

Con la Fase 5 concluida, se implementó y validó los controles en los 4 ámbitos, logrando una arquitectura segmentada, control de accesos, monitoreo operativo, procesos definidos y personal capacitado. Esto materializó la transición del Nivel 1 (inicial) al Nivel 3 (Funcional).

Como parte del seguimiento, la reevaluación periódica de la madurez y la actualización del análisis de brechas permitirán sostener y elevar el nivel alcanzado mediante la mejora continua. Los resultados de la Fase 5 en los cuatro ámbitos se pueden ver en el Anexo 7.

4.4 Análisis de los resultados obtenidos

La aplicación de la GCTIOT en un entorno industrial real permitió transformar los lineamientos de ISA/IEC 62443, NIST SP 800-82 y el modelo Purdue en acciones concretas y aplicables. La metodología abordó progresivamente las brechas iniciales de segmentación, gestión de accesos, visibilidad de activos y formalización de procesos, manteniendo la continuidad operacional.

Los resultados evidenciaron mejoras en los ámbitos físico, tecnológico y organizacional. Se implementó una arquitectura segmentada basada en Purdue, con zonas, conduits, firewalls e iDMZ; se fortalecieron la autenticación, el control de acceso y el monitoreo; y se formalizaron procedimientos, roles y responsabilidades. Estas medidas permitieron reducir la exposición de los sistemas OT y mejorar la capacidad de gestión y respuesta ante incidentes.

Como resultado, la organización avanzó desde el Nivel 1, Inicial, al Nivel 3, Funcional, según muestran las figuras 4 y 5. Este avance confirma que la GCTIOT proporciona una hoja de ruta sencilla, práctica, progresiva, medible y adaptable, capaz de priorizar riesgos e implementar controles de ciberseguridad industrial sin afectar la continuidad de los procesos productivos.

El análisis posterior evidenció una madurez promedio de 2,8, con avances en instalación física, hardware y red, software y procesos y personas. Los resultados obtenidos validan la hipótesis planteada y demuestran la aplicabilidad de la GCTIOT en condiciones reales de operación.

Indicador	Cuestionario Nivel 1
Total de preguntas	27
Respuestas "Si"	0
Respuestas "Parcial"	0
Respuestas "No"	27
Madurez promedio	1.0
Nivel de madurez resultante	Nivel 1 — Inicial

Madurez promedio por ámbito

Ámbito	Nivel 1 (inicial)
Instalación física	1.0
Hardware / Red	1.0
Software / Lógico	1.0
Procesos y personas	1.0

Figura 4: Resumen de resultado del cuestionario, que indica nivel de madurez = 1 (Inicial).

Indicador	Cuestionario Nivel 1	Cuestionario Nivel
Total de preguntas	27	20
Respuestas "Si"	0	16
Respuestas "Parcial"	0	4
Respuestas "No"	27	0
Madurez promedio	1.0	2.8
Nivel de madurez resultante	Nivel 1 — Inicial	Nivel 3 — Funcional

Madurez promedio por ámbito

Ámbito	Nivel 1 (inicial)	Nivel 3 (funcional)
Instalación física	1.0	3.0
Hardware / Red	1.0	2.8
Software / Lógico	1.0	2.7
Procesos y personas	1.0	2.8

Figura 5: Resumen de resultado del cuestionario, que indica nivel de madurez = 3 (Funcional).

El Nivel 3 (Funcional) se logró tras completar las 5 Fases y volver a evaluar las Fases 2 a 5, esto tuvo un real impacto ya que la organización tomando esta hoja de ruta pudo llegar a un nivel de Madurez 3 (Funcional) que era el deseado por la organización, como también se volvió a realizar el cuestionario obteniendo mejores resultados tal como lo muestra la figura 6 y el Anexo 2.1.



Figura 6: Madurez promedio por ámbito.

Como resultado de la investigación y con el propósito de validar de manera explícita la hipótesis de investigación, la Tabla 6 sintetiza la relación entre los atributos declarados para la GCTIOT propuesta y la evidencia obtenida durante su diseño, aplicación y evaluación. Esta consolidación permite verificar el grado de cumplimiento de cada atributo, aportando trazabilidad metodológica y fortaleciendo la auditabilidad de los resultados alcanzados.

Tabla 6: Matriz de Validación de la Hipótesis de Investigación

Atributo	Definición en la hipótesis	Evidencia de validación	Resultado observado
Sencilla	La GCTIOT debe ser fácil de comprender y utilizar por organizaciones que inician procesos de convergencia TI/OT.	Estructura organizada en fases, ámbitos y actividades claramente definidas. Los expertos destacaron positivamente la claridad metodológica y facilidad de uso.	La implementación no requirió conocimientos especializados adicionales para comprender la metodología propuesta.
Práctica	La GCTIOT debe entregar recomendaciones aplicables en entornos industriales reales.	Las acciones propuestas se implementaron utilizando recursos existentes y considerando restricciones operacionales propias de la industria alimentaria.	Se ejecutaron mejoras concretas sin afectar la continuidad operacional de la organización.

Progresiva	La adopción debe realizarse de forma gradual y controlada.	La metodología establece fases secuenciales de diagnóstico, planificación, implementación y seguimiento.	Se observó una evolución ordenada del nivel de madurez inicial hacia estados superiores de desarrollo.
Medible	Los avances deben poder cuantificarse objetivamente.	Se utilizaron cuestionarios, métricas e indicadores para determinar niveles de madurez antes y después de la aplicación de la GCTIOT.	Fue posible comparar estados iniciales y finales mediante resultados cuantificables y trazables.
Aplicable	La GCTIOT debe adaptarse a las condiciones reales de una organización industrial.	La metodología fue validada mediante un caso práctico en una empresa del sector alimentario y evaluada por especialistas del área.	La GCTIOT demostró ser utilizable bajo condiciones reales de operación y gestión.

Los antecedentes recopilados permiten concluir que los cinco atributos definidos en la hipótesis fueron evidenciados durante el proceso de implementación y validación de la GCTIOT. La existencia de evidencia empírica, junto con la evaluación realizada por especialistas, respalda un nivel de cumplimiento alto para cada uno de los atributos analizados, fortaleciendo la validez de la propuesta desarrollada.

CAPITULO 5: Conclusiones

Los resultados obtenidos permiten concluir que el objetivo general de la investigación fue cumplido satisfactoriamente. La aplicación de la GCTIOT en una planta del sector alimentario demostró que es posible implementar un proceso estructurado para identificar activos críticos, evaluar niveles de madurez, detectar brechas, priorizar riesgos y aplicar medidas de mitigación de forma gradual, sin afectar la continuidad operacional.

Asimismo, se validó la hipótesis de investigación, demostrando que marcos internacionales como ISA/IEC 62443 y NIST SP 800-82 pueden transformarse en una metodología práctica, progresiva, medible, sencilla, aplicable y de fácil utilización adaptada a las condiciones reales de la industria. La GCTIOT permite operacionalizar requisitos técnicos complejos en acciones concretas, facilitando su adopción por organizaciones con distintos niveles de madurez en ciberseguridad OT.

La validación evidenció además una mejora en la postura de seguridad de la organización analizada, permitiendo avanzar desde un escenario con controles limitados hacia un entorno con procesos definidos, controles implementados, capacidades de monitoreo y una arquitectura más segura. Complementariamente, la evaluación realizada por especialistas destacó la claridad metodológica, facilidad de aplicación y utilidad práctica de la propuesta para reducir brechas de ciberseguridad y fortalecer la convergencia TI/OT.

En conclusión, la GCTIOT constituye una herramienta práctica y contextualizada que combina estándares internacionales, evaluación objetiva y un enfoque operativo realista, proporcionando una hoja de ruta efectiva para mejorar la ciberseguridad industrial y apoyar una convergencia TI/OT segura y sostenible.

Como trabajos futuros, el presente trabajo constituye una base sólida para la convergencia segura entre entornos TI y OT en la industria alimenticia con separación física y lógica de redes TI/OT, no obstante, se puede validar en distintos contextos industriales y replicar la GCTIOT en diversas plantas productivas y en sectores críticos (energía, farmacéutica, minería) con el fin de evaluar su aplicabilidad, escalabilidad y capacidad de adaptación.

Agradecimientos:

Agradezco primeramente a mi familia por darme el espacio y paciencia de invertir en mi futuro con este magister tan importante de la Universidad Federico Santa María, en segundo lugar, a mi profesor guía Jorge Olivares por ser tan gentil en darme los tiempos y su juicio experto en estas materias con el cual aprendí muchas cosas y a los profesores con los cuales tuve variadas clases y que siempre estuvieron dispuestos a aclarar mis dudas y entregar su experiencia, agradezco también a los colegas del rubro que bajo su juicio experto evaluaron la GCTIOT entregando un feedback oportuno.

CAPITULO 6: Referencias

- [1] 802.1Q – Standard for Local and Metropolitan Area Networks—Bridges and Bridged Networks.
- [2] NIST SP 800-82 Revision 3 (2024) – Guide to Industrial Control Systems (ICS) Security.
- [3] ISA/IEC 62443-3-2:2020 – Security Risk Assessment for System Design.
- [4] Williams, T.J., The Purdue enterprise reference architecture, Purdue University, 1992.
- [5] J. Weiss, Protecting Industrial Control Systems from Electronic Threats, Momentum Press, 2010.
- [6] ISA/IEC 62443-1-1, 2018. Security for Industrial Automation and Control Systems - Part 1: Terminology, Concepts and Models.
- [7] ISA/IEC 62443-3-3, 2019. System Security Requirements and Security Levels.
- [8] Kumar, R. et al., 2022. "Industrial IoT Security Challenges in the Context of Industry4.0".
- [9] Gartner, 2023. "Market Guide for Operational Technology Security".
- [10] SANS ICS, 2021. "Case Study: Cyber Resilience in Food & Beverage Sector".
- [11] McKinsey, 2022. "Cybersecurity in the Food Industry: Building Resilience through Segmentation and Monitoring".
- [12] M. García, Ruiz, y J. Fernández, "Implementación de ISA 62443 en una planta de alimentos con producción continua", Revista Latinoamericana de Ciberseguridad Industrial, vol. 5, pp. 35-49, 2020.
- [13] A. Pereira et al., "Estudio de convergencia TI/OT en industrias brasileñas", Revista Iberoamericana de Seguridad Industrial, vol. 3, no. 2, pp. 14-27, 2019.
- [14] <https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2>
- [15] <https://www.6sigma.us/process-improvement/capability-maturity-model-integration-cmmi/>



CAPITULO 9: ANEXOS

Anexo 1: Controles Normativos

Controles de ISA/IEC 62443

La GCTIOT utilizará principalmente los requerimientos fundamentales definidos en la norma ISA/IEC 62443-3-3.

Código	Control	Aplicación en la GCTIOT
SR 1	Identification and Authentication Control (IAC)	Gestión de identidades, autenticación y control de accesos a sistemas TI/OT
SR 2	Use Control (UC)	Gestión de privilegios y acceso basado en roles
SR 3	System Integrity (SI)	Hardening, gestión de configuraciones y protección contra modificaciones no autorizadas
SR 4	Data Confidentiality (DC)	Protección de información crítica y comunicaciones
SR 5	Restricted Data Flow (RDF)	Segmentación de redes, zonas, conduits e implementación de iDMZ
SR 6	Timely Response to Events (TRE)	Gestión y respuesta ante incidentes de ciberseguridad
SR 7	Resource Availability (RA)	Resiliencia operacional, respaldos y continuidad operacional

Controles de NIST SP 800-82

La GCTIOT adopta controles asociados a la protección de sistemas de control industrial (ICS).

Familia NIST	Control	Aplicación en la GCTIOT
AC	Access Control	Control de acceso lógico y remoto
AT	Awareness and Training	Capacitación y concientización del personal
AU	Audit and Accountability	Auditoría, registros y trazabilidad
CM	Configuration Management	Inventario y gestión de configuraciones
CP	Contingency Planning	Planes de recuperación y continuidad
IA	Identification and Authentication	Gestión de identidades y autenticación
IR	Incident Response	Gestión de incidentes
MA	Maintenance	Gestión segura de mantenimiento y soporte remoto
PS	Personnel Security	Roles, responsabilidades y segregación de funciones



RA	Risk Assessment	Evaluación de riesgos y análisis GAP
SC	System and Communications Protection	Segmentación de red y protección de comunicaciones
SI	System and Information Integrity	Gestión de vulnerabilidades, monitoreo y actualizaciones

Mapeo de controles por ámbito

Ámbito 1: Instalación física

ISA/IEC 62443

- SR 1 - SR 5 - SR 7

NIST

- PE (Protección física y ambiental) – AC - CP

Controles aplicados

- Control de acceso a salas técnicas
- Separación física de infraestructura TI y OT
- Protección ambiental
- Control de visitas
- Registro de accesos

Ámbito 2: Hardware

ISA/IEC 62443

- SR 2 - SR 3 - SR 5 - SR 7

NIST

- CM – SC - SI

Controles aplicados

- Inventario de activos
- Segmentación por niveles Purdue
- Firewalls industriales
- Control de puertos físicos
- Gestión de cambios de hardware

Ámbito 3: Software

ISA/IEC 62443

- SR 1 - SR 2 - SR 3 - SR 6

NIST



- IA – SI – AU - CM

Controles aplicados

- Hardening
- Gestión de parches
- Control de versiones
- Gestión de cuentas
- Registro de eventos
- Monitoreo de seguridad

Ámbito 4: Procesos y Personas

ISA/IEC 62443-2-1

- Programa de gestión de ciberseguridad
- Roles y responsabilidades
- Gestión de incidentes
- Capacitación

NIST

- AT – IR – PS - RA

Explicación de cada control

1. Control de identificación y autenticación (ISA/IEC 62443 SR1 – NIST IA)

Este control fue seleccionado debido a que uno de los hallazgos más recurrentes en entornos industriales corresponde al uso compartido de credenciales, cuentas genéricas y mecanismos débiles de autenticación.

Su incorporación permite:

- Identificar de manera inequívoca a cada usuario.
- Mejorar la trazabilidad de las acciones realizadas sobre sistemas críticos.
- Reducir el riesgo de accesos no autorizados.
- Facilitar auditorías y análisis forenses.

La correcta gestión de identidades constituye uno de los pilares fundamentales para proteger sistemas SCADA, estaciones de ingeniería y plataformas administrativas que interactúan con el entorno OT.

2. Control de uso y gestión de privilegios (ISA/IEC 62443 SR2 – NIST AC)

La selección de este control responde a la necesidad de aplicar el principio de mínimo privilegio, limitando el acceso de los usuarios únicamente a los recursos necesarios para el desempeño de sus funciones.

Su implementación permite:



- Reducir el riesgo de errores operacionales.
- Minimizar la superficie de ataque interna.
- Prevenir modificaciones accidentales o maliciosas en sistemas de control.
- Mejorar la segregación de funciones entre personal TI, OT y proveedores.

Este control resulta especialmente relevante en plantas industriales donde múltiples actores interactúan sobre una misma infraestructura tecnológica.

3. Control de integridad de sistemas (ISA/IEC 62443 SR3 – NIST SI y CM)

La integridad de los sistemas industriales constituye un factor crítico para garantizar una operación segura y confiable. Este control fue seleccionado debido a las brechas identificadas en la gestión de configuraciones, actualizaciones y mantenimiento de equipos OT.

Su aplicación permite:

- Gestionar de forma controlada cambios de configuración.
- Implementar procesos de hardening.
- Mantener versiones actualizadas de sistemas y aplicaciones.
- Reducir vulnerabilidades asociadas a configuraciones inseguras.

La integridad de los sistemas es especialmente relevante en entornos donde fallas o modificaciones indebidas pueden afectar directamente la producción.

4. Control de flujo restringido de información (ISA/IEC 62443 SR5 – NIST SC)

Este control constituye uno de los elementos centrales de la GCTIOT, debido a que la problemática principal de la investigación está asociada a la convergencia entre redes TI y OT.

Su incorporación permite:

- Implementar segmentación de redes.
- Definir zonas y conduits conforme a ISA/IEC 62443.
- Establecer zonas desmilitarizadas industriales (iDMZ).
- Controlar y monitorear el tráfico entre dominios.

La implementación de este control reduce significativamente la posibilidad de movimiento lateral de amenazas y la propagación de incidentes hacia sistemas industriales críticos.

5. Control de monitoreo y respuesta a eventos (ISA/IEC 62443 SR6 y SR7 – NIST SI e IR)

Los incidentes de ciberseguridad en entornos industriales suelen detectarse de forma tardía debido a la ausencia de monitoreo especializado. Por esta razón, se seleccionaron controles relacionados con la detección, registro y respuesta ante eventos.

Los beneficios asociados incluyen:

- Mayor visibilidad del entorno TI/OT.
- Detección temprana de actividades anómalas.
- Reducción de los tiempos de respuesta.
- Disponibilidad de evidencia para auditorías e investigaciones.

Este control permite avanzar desde un enfoque reactivo hacia un enfoque proactivo de gestión de amenazas.



6. Control de disponibilidad y continuidad operacional (ISA/IEC 62443 SR7 – NIST CP)

La industria alimenticia depende de procesos altamente automatizados que operan bajo esquemas continuos de producción. En consecuencia, cualquier interrupción puede generar impactos económicos significativos.

Por este motivo, la GCTIOT incorpora controles destinados a:

- Asegurar la disponibilidad de servicios críticos.
- Gestionar respaldos de sistemas industriales.
- Implementar planes de recuperación ante desastres (DRP).
- Definir procedimientos de continuidad operacional.

La incorporación de estos controles permite aumentar la resiliencia operativa de la organización frente a eventos de ciberseguridad o fallas tecnológicas.

7. Controles asociados a procesos y personas (ISA/IEC 62443-2-1 – NIST AT, PS e IR)

La experiencia obtenida durante el diagnóstico evidenció que una gran parte de las brechas identificadas no estaban relacionadas exclusivamente con la tecnología, sino con aspectos organizacionales.

Por este motivo, la GCTIOT incorpora controles orientados a:

- Definir roles y responsabilidades.
- Implementar programas de capacitación y concientización.
- Formalizar procedimientos de operación segura.
- Establecer procesos de gestión de incidentes.
- Gestionar adecuadamente proveedores y terceros.

Estos controles permiten reducir la dependencia del conocimiento individual, fortalecer la cultura de seguridad y asegurar la sostenibilidad de las medidas implementadas en el tiempo.

Anexo 2: Análisis de Madurez inicial

Cuestionarios de evaluación de madurez — Ciberseguridad TI/OT

Caso de estudio: planta del sector alimenticio · Marcos: ISA/IEC 62443 · NIST SP 800-82 · Modelo Purdue/ISA-99

1. Propósito y uso

Este documento reúne instrumentos de evaluación aplicados sobre los mismos dominios de control. El Cuestionario Nivel 1 (inicial) identifica por qué la organización se clasifica en el estado inicial. Cada pregunta está mapeada a un control de ISA/IEC 62443, NIST SP 800-82 y/o al nivel Purdue.

Escala de madurez (1–5)

Nivel	Estado	Descripción
1	Inicial	Sin controles formales; acciones reactivas.
2	Parcial	Controles aislados, sin estandarización.
3	Funcional	Controles consistentes en áreas, con procesos definidos.
4	Gestionado	Formalizado, con métricas y monitoreo.
5	Optimizado	Integrado, automatizado y con mejora continua.

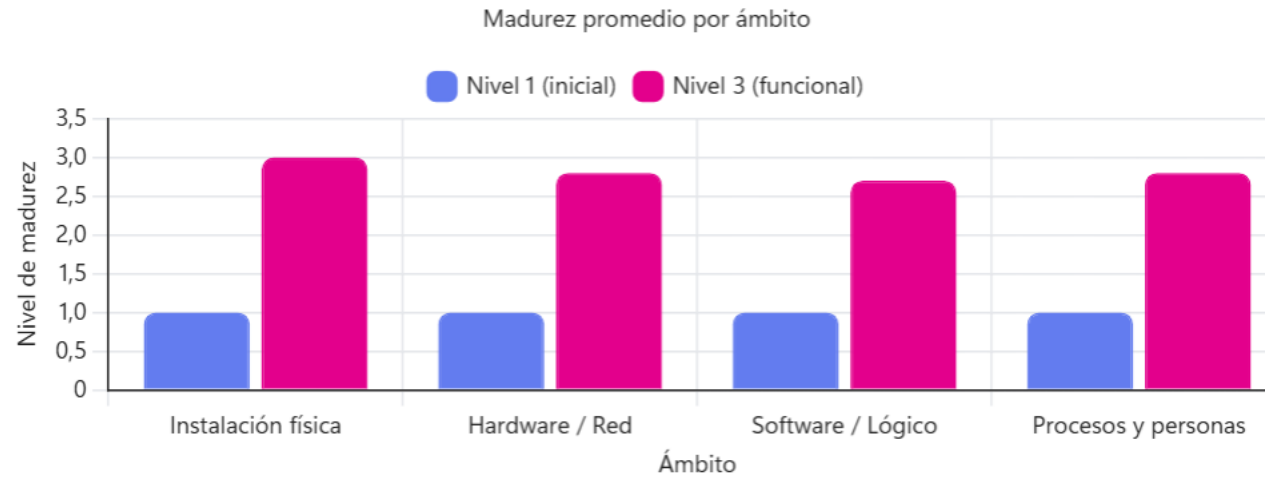
Leyenda de respuestas: *Sí* = control implementado (valor 3) · *Parcial* = implementado de forma incompleta o en consolidación (valor 2) · *No* = ausente (valor 0).

2. Resumen y puntuación de madurez

Indicador	Cuestionario Nivel 1	Cuestionario Nivel
Total de preguntas	27	27
Respuestas "Sí"	0	22
Respuestas "Parcial"	0	5
Respuestas "No"	27	0
Madurez promedio	1.0	2.8
Nivel de madurez resultante	Nivel 1 — Inicial	Nivel 3 — Funcional

Madurez promedio por ámbito

Ámbito	Nivel 1 (inicial)	Nivel 3 (funcional)
Instalación física	1.0	3.0
Hardware / Red	1.0	2.8
Software / Lógico	1.0	2.7
Procesos y personas	1.0	2.8



3. Cuestionario Nivel 1 — Diagnóstico del estado inicial (¿por qué Nivel 1?)

Las respuestas evidencian la ausencia de controles que sitúa a la organización en el Nivel 1 (Inicial).

Nº	Ámbito	Dominio / Control	Referencia (ISA/NIST/Purdue)	Purdue	Pregunta de evaluación	Resp.	Mad.	Hallazgo / Evidencia
1	Instalación física	Separación física	ISA 62443-3-2 (seg. física)	Transversal	¿Existe separación física (racks/gabinets) entre activos TI y OT?	No	1	Racks compartidos entre TI y OT.
2	Instalación física	Acceso físico	ISA 62443-2-1	N0–N2	¿Se controla el acceso físico a las áreas y racks que alojan PLC/SCADA?	No	1	Acceso físico no controlado a activos críticos.
3	Instalación física	Segregación de áreas	ISA 62443 (seg. física)	N0–N1	¿Están segregadas físicamente las áreas críticas de operación?	No	1	Sin segregación de áreas críticas.
4	Hardware / Red	Inventario de activos	NIST CM-8	N1–N3	¿Existe un inventario formal y actualizado de activos OT?	No	1	Falta de inventario de activos OT.
5	Hardware / Red	Segmentación de red	ISA 62443-3-2 · NIST SC-32	Transversal	¿La red está segmentada según niveles Purdue (zonas y conduits)?	No	1	Segmentación inexistente o débil; sin zonas ni conduits.
6	Hardware / Red	Zona intermedia	NIST SC-7 · Purdue	N3–N4	¿Existe una iDMZ entre los niveles 3 y 4?	No	1	Ausencia de iDMZ; sin desacoplamiento funcional.
7	Hardware / Red	Aislamiento de PLC	ISA 62443-3-2	N1	¿Los PLC están aislados de la red compartida?	No	1	PLC expuestos en red compartida sin aislamiento.
8	Hardware / Red	Firewall industrial	NIST SC-7 · AC-4	N3–N4	¿Se emplean firewalls industriales para controlar el tráfico TI/OT?	No	1	Sin firewalls; comunicación directa TI-OT.
9	Hardware / Red	Mecanismo de aislamiento	NIST SC-32	Transversal	¿El aislamiento se apoya en mecanismos adicionales a las VLANs?	No	1	VLANs como único mecanismo (insuficiente).
10	Hardware / Red	Gestión de dispositivos	NIST CM-8	N1–N2	¿Los dispositivos industriales están gestionados (configuración, altas/bajas)?	No	1	Dispositivos industriales no gestionados.
11	Software / Lógico	Gestión de parches	NIST SI-2	N2–N3	¿Existe gestión de parches para sistemas OT/SCADA?	No	1	Falta de gestión de parches.
12	Software / Lógico	Credenciales	NIST IA-5	N2–N3	¿El acceso a OT usa credenciales individuales (no compartidas)?	No	1	Credenciales compartidas.
13	Software / Lógico	Autenticación	NIST IA-2 · ISA SR 1	N2–N3	¿Existe autenticación para el acceso a sistemas industriales?	No	1	Sin autenticación robusta en OT.
14	Software / Lógico	Control de acceso lógico	NIST SC-7 · AC-4	N2–N3	¿El acceso al SCADA desde TI pasa por un control intermedio?	No	1	SCADA accesible desde TI sin control intermedio.
15	Software / Lógico	Control de flujo	ISA 62443 SR 5 · NIST AC-4	N3–N4	¿Se restringe y controla el flujo de datos entre TI y OT?	No	1	Flujo no restringido; incumple SR 5.



16	Software / Lógico	Visibilidad OT	NIST SI-4 · ISA SR 7	Transversal	¿Existe visibilidad y monitoreo del tráfico OT?	No	1	Tráfico OT no monitoreado.
17	Software / Lógico	Logging	ISA 62443 SR 7	Transversal	¿Se generan registros auditable (logging) de eventos OT?	No	1	Falta de registros auditable.
18	Software / Lógico	Monitoreo / SIEM	NIST SI-4	Transversal	¿Existe un SIEM o solución de monitoreo industrial?	No	1	Ausencia de SIEM / monitoreo industrial.
19	Software / Lógico	Hardening	ISA 62443 SR 1 · NIST CM	N2–N3	¿Se aplica hardening a los sistemas operativos y aplicaciones?	No	1	Sistemas sin hardening.
20	Procesos y personas	Roles de seguridad OT	ISA 62443-2-1	Transversal	¿Existen roles y responsabilidades formales de seguridad OT?	No	1	Sin roles de seguridad OT.
21	Procesos y personas	Políticas y procedimientos	NIST PL-2	Transversal	¿Existen políticas y procedimientos formales de ciberseguridad?	No	1	Ausencia de procedimientos formales.
22	Procesos y personas	Gestión de incidentes	NIST IR-1	Transversal	¿Están documentados los procesos de gestión de incidentes?	No	1	Procesos de incidentes no documentados.
23	Procesos y personas	Respuesta a incidentes	NIST IR-4	Transversal	¿Existe capacidad de respuesta ante incidentes?	No	1	Sin capacidad de respuesta a incidentes.
24	Procesos y personas	Coordinación TI-OT	ISA 62443-2-1	Transversal	¿Existe coordinación formal entre TI y Operaciones?	No	1	Falta de coordinación TI-Operación.
25	Procesos y personas	Capacitación	ISA 62443-2-1	Transversal	¿El personal recibe capacitación en ciberseguridad OT?	No	1	Bajo nivel de capacitación técnica.
26	Procesos y personas	Gobierno e indicadores	ISA 62443-2-1 · NIST PM	Transversal	¿Existe gobierno de ciberseguridad con indicadores de desempeño?	No	1	Sin gobierno ni indicadores de desempeño.
27	Procesos y personas	Gestión de terceros	ISA 62443-2-1	Transversal	¿Se aplican controles de ciberseguridad a proveedores/terceros?	No	1	Alta dependencia de terceros sin controles robustos.

Resultado = respuestas NO = 1, la suma es 27 del puntaje total / cantidad de preguntas (27), el resultado del nivel de madurez es 1.

El resultado de madurez inicial (Nivel 1) y la obtención de un 100% de respuestas negativas se explican porque el cuestionario fue construido a partir de las brechas previamente identificadas durante las fases de levantamiento de activos y diagnóstico inicial. Las preguntas no tuvieron un carácter exploratorio, sino que buscaron verificar de manera objetiva la existencia de controles específicos asociados a los marcos ISA/IEC 62443 y NIST SP 800-82. Por esta razón, los resultados obtenidos son consistentes con la evidencia recopilada previamente y constituyen una validación cuantitativa de las brechas observadas. En consecuencia, la madurez promedio de 1,0 representa una línea base realista y trazable del estado inicial de la organización, sobre la cual posteriormente se evaluó la mejora alcanzada mediante la aplicación de la GCTIOT.

Anexo 2.1: Evaluación posterior a la implementación de la GCTIOT.

El siguiente cuestionario muestra el estado de madurez hacia la transición del Nivel 3 (verificación) registra los controles implementados que permitieron alcanzar el estado Funcional. Cada pregunta está mapeada a un control de ISA/IEC 62443, NIST SP 800-82 y/o al nivel Purdue.

Cuestionario Nivel 3 — Verificación del estado funcional (¿cómo se alcanzó Nivel 3?)

Las respuestas registran los controles implementados que permitieron la transición al Nivel 3 (Funcional).

Nº	Ámbito	Dominio / Control	Referencia (ISA/NIST/Purdue)	Purdue	Pregunta de evaluación	Resp.	Mad.	Hallazgo / Evidencia
1	Instalación física	Separación física	ISA 62443-3-2 (seg. física)	Transversal	¿Existe separación física (racks/gabinetes) entre activos TI y OT?	SI	3	Separación de racks ejecutada
2	Instalación física	Acceso físico	ISA 62443-2-1	N0–N2	¿Se controla el acceso físico a las áreas y racks que alojan PLC/SCADA?	SI	3	Control de acceso físico implementado.
3	Instalación física	Segregación de áreas	ISA 62443 (seg. física)	N0–N1	¿Están segregadas físicamente las áreas críticas de operación?	SI	3	Existe segregación de áreas críticas.
4	Hardware / Red	Inventario de activos	NIST CM-8	N1–N3	¿Existe un inventario formal y actualizado de activos OT?	SI	3	Inventario logrado; se eliminó una debilidad clave del Nivel 1.
5	Hardware / Red	Segmentación de red	ISA 62443-3-2 · NIST SC-32	Transversal	¿La red está segmentada según niveles Purdue (zonas y conduits)?	SI	3	Segmentación por niveles implementada en la línea piloto.
6	Hardware / Red	Zona intermedia	NIST SC-7 · Purdue	N3–N4	¿Existe una iDMZ entre los niveles 3 y 4?	SI	3	iDMZ con servidor pivote habilitada.
7	Hardware / Red	Aislamiento de PLC	ISA 62443-3-2	N1	¿Los PLC están aislados de la red compartida?	Parcial	2	Aislamiento vía segmentación de la línea (piloto).
8	Hardware / Red	Firewall industrial	NIST SC-7 · AC-4	N3–N4	¿Se emplean firewalls industriales para controlar el tráfico TI/OT?	SI	3	Firewall industrial y conduits definidos.
9	Hardware / Red	Mecanismo de aislamiento	NIST SC-32	Transversal	¿El aislamiento se apoya en mecanismos adicionales a las VLANs?	SI	3	Se implemento firewall y software de separacion
10	Hardware / Red	Gestión de dispositivos	NIST CM-8	N1–N2	¿Los dispositivos industriales están gestionados (configuración, altas/bajas)?	SI	3	Dispositivos industriales gestionados.
11	Software / Lógico	Gestión de parches	NIST SI-2	N2–N3	¿Existe gestión de parches para sistemas OT/SCADA?	SI	3	Gestión de parches calendarizado.
12	Software / Lógico	Credenciales	NIST IA-5	N2–N3	¿El acceso a OT usa credenciales individuales (no compartidas)?	SI	3	Credenciales individuales

13	Software / Lógico	Autenticación	NIST IA-2 · ISA SR 1	N2–N3	¿Existe autenticación para el acceso a sistemas industriales?	SI	3	Autenticación de accesos implementados.
14	Software / Lógico	Control de acceso lógico	NIST SC-7 · AC-4	N2–N3	¿El acceso al SCADA desde TI pasa por un control intermedio?	SI	3	Control de accesos implementados.
15	Software / Lógico	Control de flujo	ISA 62443 SR 5 · NIST AC-4	N3–N4	¿Se restringe y controla el flujo de datos entre TI y OT?	SI	3	Flujo de datos controlado por conduits/firewall.
16	Software / Lógico	Visibilidad OT	NIST SI-4 · ISA SR 7	Transversal	¿Existe visibilidad y monitoreo del tráfico OT?	Parcial	2	Monitoreo parcial operativo (área en consolidación).
17	Software / Lógico	Logging	ISA 62443 SR 7	Transversal	¿Se generan registros auditables (logging) de eventos OT?	Parcial	2	Logging parcial habilitado.
18	Software / Lógico	Monitoreo / SIEM	NIST SI-4	Transversal	¿Existe un SIEM o solución de monitoreo industrial?	Parcial	2	Monitoreo parcial operativo (área en consolidación).
19	Software / Lógico	Hardening	ISA 62443 SR 1 · NIST CM	N2–N3	¿Se aplica hardening a los sistemas operativos y aplicaciones?	SI	3	Hardening aplicado
20	Procesos y personas	Roles de seguridad OT	ISA 62443-2-1	Transversal	¿Existen roles y responsabilidades formales de seguridad OT?	SI	3	Roles y responsabilidades definidos.
21	Procesos y personas	Políticas y procedimientos	NIST PL-2	Transversal	¿Existen políticas y procedimientos formales de ciberseguridad?	SI	3	Procedimientos formalizados.
22	Procesos y personas	Gestión de incidentes	NIST IR-1	Transversal	¿Están documentados los procesos de gestión de incidentes?	Parcial	2	Procesos de incidentes en definición.
23	Procesos y personas	Respuesta a incidentes	NIST IR-4	Transversal	¿Existe capacidad de respuesta ante incidentes?	SI	3	Capacitación del personal OT realizada y DRP..
24	Procesos y personas	Coordinación TI-OT	ISA 62443-2-1	Transversal	¿Existe coordinación formal entre TI y Operaciones?	SI	3	Coordinación mediante comité de cambios.
25	Procesos y personas	Capacitación	ISA 62443-2-1	Transversal	¿El personal recibe capacitación en ciberseguridad OT?	SI	3	Capacitación del personal OT realizada.
26	Procesos y personas	Gobierno e indicadores	ISA 62443-2-1 · NIST PM	Transversal	¿Existe gobierno de ciberseguridad con indicadores de desempeño?	SI	3	Existe gobierno e indicadores de desempeño.
27	Procesos y personas	Gestión de terceros	ISA 62443-2-1	Transversal	¿Se aplican controles de ciberseguridad a proveedores/terceros?	SI	3	Alta dependencia de terceros con controles y evaluaciones robustas.

Resultado = respuestas SI = 3, la suma es 66

respuestas parciales = 2, la suma es 10

puntaje total (76) / cantidad de preguntas (27), el resultado del nivel de madurez es 3.



Anexo 3: Informe estado actual

INFORME DE ESTADO INICIAL (NIVEL 1)

Ciberseguridad industrial — Convergencia y separación de entornos TI/OT

Caso de estudio: planta productiva del sector alimenticio nacional (operación continua 24/6, línea automatizada).

Marcos de referencia: ISA/IEC 62443 · NIST SP 800-82 · Modelo Purdue / ISA-99.

Estado de madurez evaluado: **Nivel 1 – Inicial** | Estado objetivo: **Nivel 3 – Funcional**

1. Resumen ejecutivo

El presente informe documenta el estado inicial (Nivel 1 – Inicial) de una planta productiva del sector alimenticio nacional, caracterizada por una operación continua bajo régimen 24/6, un alto nivel de automatización y una dependencia crítica de sistemas de control industrial para la continuidad del proceso productivo.

El entorno analizado corresponde a una arquitectura industrial con un alto grado de convergencia entre redes TI y OT, desarrollada de forma progresiva y sin un modelo de referencia formal. Esta evolución derivó en una infraestructura heterogénea, con múltiples interconexiones directas entre ambos dominios, baja segmentación de red, escasa visibilidad del tráfico industrial y una limitada capacidad de control sobre las comunicaciones.

En el plano organizacional se evidencian brechas relevantes: ausencia de procesos formales, debilidades en la gestión de accesos —particularmente en OT—, baja capacitación del personal y una dependencia significativa de proveedores externos sin controles robustos. En conjunto, estas condiciones configuran un escenario de riesgo elevado, con una amplia superficie de ataque y una limitada capacidad de detección y contención de incidentes.

Clasificación de madurez: el entorno se clasifica como Nivel 1 – Inicial, caracterizado por la ausencia de controles estructurados, operación reactiva, ausencia de gobierno de ciberseguridad y ausencia de indicadores de desempeño. El objetivo de la intervención es transitar de forma controlada hacia el Nivel 3 – Funcional, preservando en todo momento la continuidad operacional.

2. Alcance y marco metodológico

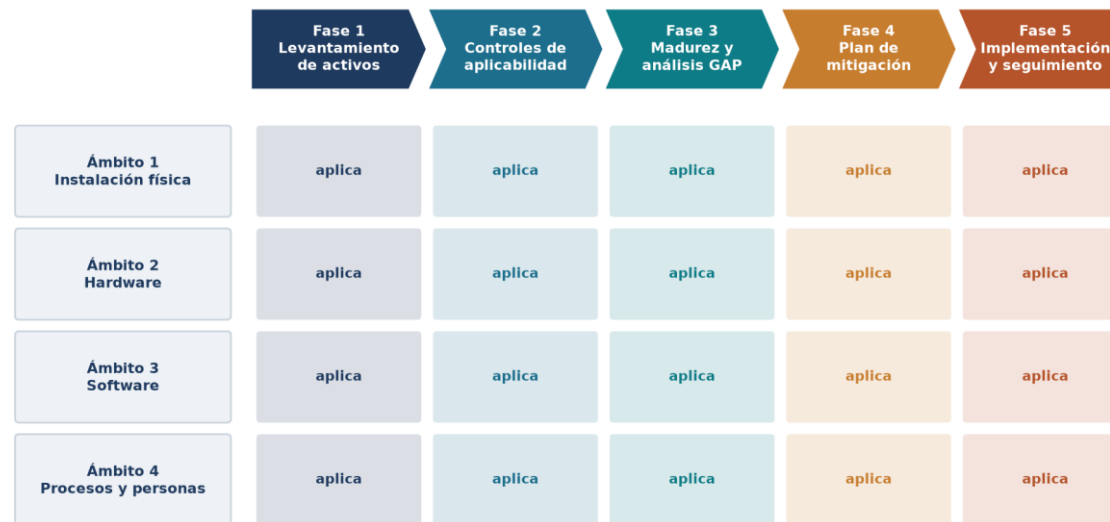
El diagnóstico se enmarca en una GCTIOT metodológica estructurada en cinco fases secuenciales, aplicadas transversalmente sobre cuatro ámbitos, y complementada por un modelo de madurez que permite evaluar de forma sistemática el grado de implementación de los controles.

2.1 Fases y ámbitos

- **Fase 1 – Levantamiento de activos:** identificación y clasificación de activos TI y OT (infraestructura, sistemas, aplicaciones, redes, dispositivos industriales).
- **Fase 2 – Controles de aplicabilidad:** determinación de los controles aplicables según criticidad y exposición.
- **Fase 3 – Evaluación de madurez y análisis GAP:** medición del grado de implementación e identificación de brechas respecto al estado objetivo.
- **Fase 4 – Plan de mitigación:** definición de medidas correctivas con prioridades, responsables, plazos y recursos.
- **Fase 5 – Implementación y seguimiento:** ejecución de las acciones con monitoreo y control para asegurar su sostenibilidad.

Cada fase se aplica sobre cuatro ámbitos: Instalación física, Hardware, Software y Procesos y personas, reconociendo que la ciberseguridad TI/OT no depende solo de la tecnología, sino también de factores físicos, organizacionales y humanos.

Enfoque metodológico: 5 Fases aplicadas transversalmente sobre 4 Ámbitos



Cada fase se ejecuta sobre los cuatro ámbitos → diagnóstico integral (técnico, físico, lógico y humano)

Figura 1: Enfoque metodológico — 5 fases aplicadas transversalmente sobre 4 ámbitos.

2.2 Modelo de madurez (1–5)

- **Nivel 1 – Inicial:** sin controles formales; acciones reactivas y dependientes de iniciativas individuales.
- **Nivel 2 – Parcial:** controles aislados, sin estandarización ni documentación formal.
- **Nivel 3 – Funcional:** controles consistentes en áreas específicas, alineados con procesos definidos.
- **Nivel 4 – Gestionado:** controles formalizados, documentados y gestionados con métricas y monitoreo.
- **Nivel 5 – Optimizado:** procesos integrados, automatizados y sujetos a mejora continua.

El análisis de brechas (GAP) compara el estado actual con el nivel objetivo, permitiendo identificar desviaciones y priorizar acciones. La organización se ubica en el Nivel 1 y define como meta el Nivel 3.



Figura 2: Modelo de madurez y posición inicial de la organización (actual: Nivel 1; objetivo: Nivel 3).

3. Caracterización del entorno

La Tabla 1 resume las principales características del entorno analizado en el estado inicial.

Categoría	Descripción
Industria	Alimenticia
Tipo de operación	Continua (24/6)
Unidad de análisis	Línea de producción automatizada
Nivel de automatización	Alto (SCADA, PLC, sistemas de supervisión)
Dependencia tecnológica	Crítica para la continuidad operacional
Arquitectura TI/OT	Convergencia no gobernada
Segmentación de red	Limitada
Visibilidad del tráfico OT	Baja
Gestión de accesos	Parcial y no estandarizada
Participación de terceros	Alta

Tabla 1: Caracterización del entorno del caso de estudio.

4. Arquitectura del estado inicial

El entorno presenta una convergencia TI/OT no gobernada sobre el modelo Purdue: existe comunicación directa entre los niveles corporativos (Nivel 4 – TI) y los niveles de operación y control (Niveles 3, 2 y 1 – OT), sin una zona intermedia (iDMZ) que permita desacoplar funcionalmente ambos dominios.

Arquitectura del Estado Inicial (Nivel 0)

Convergencia TI/OT no gobernada · Modelo Purdue sin segmentación

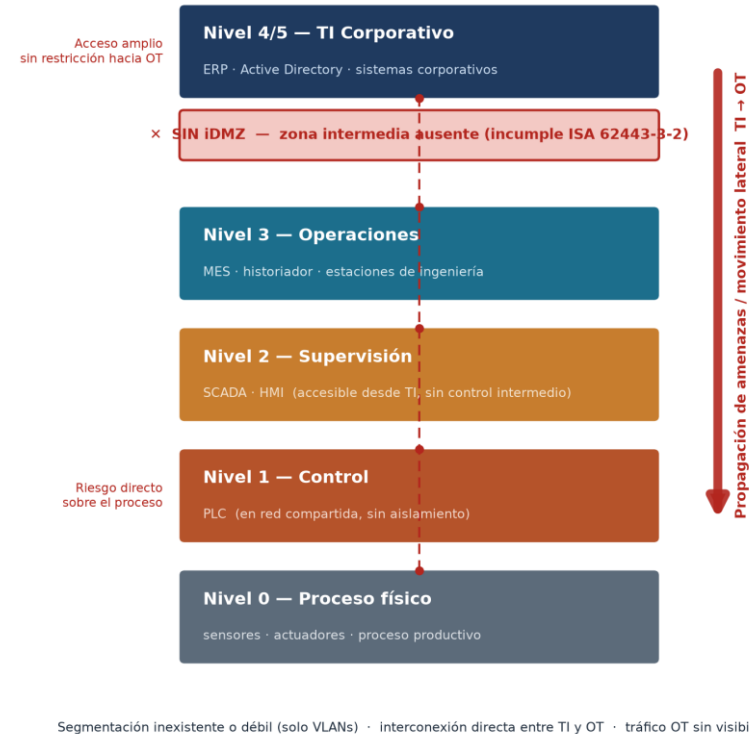


Figura 3: Arquitectura del estado inicial — modelo Purdue sin gobierno de la convergencia TI/OT.

Análisis del problema por nivel:



- **Nivel 5–4 (TI):** acceso amplio, sin restricciones hacia OT.
- **Nivel 3:** SCADA expuesto a TI sin filtros.
- **Nivel 2:** PLC accesible indirectamente desde TI.
- **Nivel 1–0:** sin aislamiento; riesgo directo sobre el proceso físico.

Esta configuración permite el paso de amenazas desde TI hacia OT, la interrupción de procesos productivos y la alteración directa de variables industriales.

5. Hallazgos del estado inicial

El diagnóstico permitió identificar un conjunto amplio de brechas, clasificadas en dimensiones arquitectónicas, técnicas, de monitoreo y organizacionales.

5.1 Hallazgos arquitectónicos

- Arquitectura de red con segmentación inexistente o débil.
- Comunicación directa entre niveles Purdue 4 (TI) y 2–3 (OT).
- Ausencia de iDMZ, que impide el desacoplamiento funcional.
- No definición de zonas ni conduits (incumple ISA 62443-3-2).
- Uso de VLANs como único mecanismo de aislamiento (insuficiente).

Controles no cumplidos: ISA/IEC 62443 SR 5 (restricción de flujo) · NIST SC-7 (protección de frontera) · NIST SC-32 (separación de redes).

5.2 Hallazgos técnicos

- Falta de inventario de activos OT (NIST CM-8).
- PLCs expuestos en red compartida, sin aislamiento.
- SCADA accesible desde la red TI, sin control intermedio.
- Falta de gestión de parches (NIST SI-2).
- Credenciales compartidas (NIST IA-5 no cumplido).

Implicaciones: riesgo de movimiento lateral, escalamiento de privilegios y acceso directo a la capa de control industrial.

5.3 Hallazgos de monitoreo

- No existe visibilidad del tráfico OT.
- Falta de registros auditable.

- No se detectan anomalías de comportamiento.
- Ausencia de SIEM o monitoreo industrial.

Controles no cumplidos: NIST SI-4 (monitoreo continuo) · ISA 62443 SR 7 (logging y monitoreo).

5.4 Hallazgos organizacionales

- Falta de roles de seguridad OT (ISA 62443-2-1).
- Procesos de gestión de incidentes no documentados (NIST IR-1).
- Falta de coordinación entre TI y Operación.
- Bajo nivel de capacitación técnica.

5.5 Síntesis de hallazgos e impacto

La Tabla 2 resume los hallazgos y el impacto potencial en caso de no ser tratados de forma efectiva.

Análisis	Hallazgo	Impacto
Arquitectura	Interconexión directa entre TI y OT	Alta propagación de amenazas
Segmentación	Ausencia de zonificación basada en Purdue	Falta de aislamiento de activos críticos
Visibilidad	Tráfico OT no monitoreado	Dificultad de detección de incidentes
Accesos	Accesos no controlados a sistemas industriales	Riesgo de accesos no autorizados
Procesos	Ausencia de procedimientos formales	Baja capacidad de gestión
Personas	Baja capacitación en ciberseguridad OT	Mayor probabilidad de error humano

Tabla 2: Hallazgos del estado inicial y su impacto.

6. Modelo de riesgo observado

El análisis del entorno permitió identificar un patrón de riesgo asociado a la convergencia no controlada entre TI y OT, particularmente en relación con el modelo Purdue. La exposición se incrementa a medida que las amenazas descienden desde los niveles corporativos hacia la capa de control y el proceso físico.

Mapa de exposición de riesgo por nivel Purdue (estado inicial)			
Nivel Purdue	Activos asociados	Riesgo identificado	Severidad
Nivel 4 (TI)	ERP, AD, sistemas corporativos	Punto de origen de amenazas	Alto
Nivel 3	Sistemas de operación	Falta de control de tráfico	Alto
Nivel 2	SCADA / HMI	Exposición a accesos externos	Alto
Nivel 1	PLC	Riesgo crítico de manipulación	Crítico
Nivel 0	Proceso físico	Impacto directo en producción	Crítico

Figura 4: Mapa de exposición de riesgo por nivel Purdue (estado inicial).

Nivel Purdue	Activos asociados	Riesgo identificado
Nivel 4 (TI)	ERP, AD, sistemas corporativos	Punto de origen de amenazas
Nivel 3	Sistemas de operación	Falta de control de tráfico
Nivel 2	SCADA	Exposición a accesos externos
Nivel 1	PLC	Riesgo crítico de manipulación

Nivel Purdue	Activos asociados	Riesgo identificado
Nivel 0	Proceso físico	Impacto directo en producción

Tabla 3: Exposición de riesgos según niveles Purdue.

7. Evaluación de madurez inicial y análisis GAP

El entorno fue clasificado como Nivel 1 – Inicial, caracterizado por:

- Ausencia de controles estructurados.
- Operación reactiva.
- Sin gobierno de ciberseguridad.
- Sin indicadores de desempeño.

La Tabla 4 contrasta el estado actual con el estado objetivo por dominio de control, base para la priorización del plan de mitigación.

Dominio de control	Referencia	Estado actual	Estado objetivo (Nivel 3)
Segmentación / zonas y conduits	ISA 62443-3-2; NIST SC-7, SC-32	No cumple	iDMZ y segmentación estricta por niveles Purdue
Restricción / control de flujo	ISA SR 5; NIST AC-4	No cumple	Flujo controlado mediante conduits definidos
Inventario de activos OT	NIST CM-8	No cumple	Inventario formal y mantenido
Gestión de parches	NIST SI-2	No cumple	Proceso de actualización controlado
Autenticación y credenciales	NIST IA-2, IA-5	No cumple	Autenticación individual, sin credenciales compartidas
Monitoreo y logging	NIST SI-4; ISA SR 7	No cumple	Monitoreo industrial y registros auditables
Respuesta a incidentes	NIST IR-1, IR-4	No cumple	Procesos documentados de respuesta

Dominio de control	Referencia	Estado actual	Estado objetivo (Nivel 3)
Roles de seguridad OT	ISA 62443-2-1	No cumple	Roles y responsabilidades definidos
Seguridad física	ISA 62443 (seguridad física)	Racks compartidos	Separación de racks y control de acceso físico

Tabla 4: Análisis GAP — brechas del estado inicial frente al estado objetivo.

8. Síntesis y priorización hacia el plan de mitigación

El estado inicial corresponde a un entorno sin gobierno de ciberseguridad, con convergencia TI/OT no controlada y sin capacidades de visibilidad ni respuesta. Los hallazgos evidencian que la principal debilidad del Nivel 1 es la falta de aislamiento entre dominios, que habilita la propagación de amenazas hacia la capa de control industrial.

A partir de este diagnóstico, las medidas de mayor impacto para iniciar la transición hacia el Nivel 3 (Funcional) son:

- Segmentación TI/OT e implementación de una IDMZ entre los niveles 3 y 4.
- Definición de zonas y conduits controlados, con firewalls industriales.
- Control de accesos y autenticación individual en OT.
- Implementación de visibilidad y monitoreo del tráfico industrial.
- Formalización de procesos, roles y capacitación del personal OT.

Estas acciones se priorizan según criticidad operacional, impacto potencial en la seguridad y factibilidad técnica, asegurando que las mejoras de seguridad no introduzcan riesgos adicionales para la continuidad del negocio. El levantamiento de activos (Fase 1) queda fijado como línea base; la elevación del nivel de madurez se logra iterando sobre las Fases 2 a 5.

Anexo 4: Resultados del plan de mitigación de los hallazgos

A partir del levantamiento inicial, se identificaron los principales hallazgos críticos que caracterizan la situación base del entorno.

Aplicación del modelo por fases y ámbitos

A. Fase 1: Levantamiento de activos

Hallazgos por ámbito:

- **Ámbito Físico:** racks compartidos → incumple ISA 62443 physical security

- **Ámbito Hardware:** dispositivos no gestionados → incumple CM-8
- **Ámbito Software:** versiones sin control → incumple SI-2
- **Ámbito Procesos/Personas:** inexistentes → incumple NIST PL-2

Resultado: Se logró visibilidad, eliminando una de las principales debilidades del Nivel 1.

B. Fase 2: Definición de controles

Controles definidos:

Ámbito	Control
Física	control de acceso físico
Hardware	segmentación Purdue
Software	hardening + control acceso
Procesos	procedimientos formales

Basado en:

- NIST AC, SC, IA
- ISA 62443 SR 1, SR 5

Resultado: Se establecen controles base → transición a Nivel 1 parcial.

C. Fase 3: GAP (incumplimientos detectados)

Ejemplos críticos:

- No cumplimiento SC-7 (sin firewalls)
- No cumplimiento IA-2 (sin autenticación)
- No cumplimiento SR-7 (sin monitoreo)
- No cumplimiento IR-4 (sin respuesta a incidentes)

Esto permitió priorizar mitigación con enfoque de riesgo.

D. Fase 4: Plan de mitigación

Medidas con alto impacto:

- Segmentación TI/OT
- Implementación iDMZ
- Control de accesos

- Implementación monitoreo

Priorizadas según:

- riesgo operacional
- impacto en producción
- factibilidad técnica

E. Fase 5: Implementación

Resultados por ámbito:

Ámbito Físico

- separación de racks
- control acceso

Ámbito Hardware

- implementación de firewalls
- segmentación Purdue

Ámbito Software

- hardening
- autenticación

Ámbito Procesos/Personas

- procedimientos
- capacitación

Resultados y evolución de madurez

Se logró transición: Nivel 1 → Nivel 3 (Funcional)

Cambios clave:

- arquitectura segmentada
- control de accesos implementado
- monitoreo parcial operativo
- procesos definidos
- capacitación personal OT

Validación contra marcos

NIST SP 800-82

- AC → control acceso ✓
- SC → protección red ✓
- IA → autenticación ✓
- SI → monitoreo ✓

ISA/IEC 62443

- zonas ✓
- conduits ✓
- control acceso ✓
- monitoreo ✓

Análisis profundo de resultados

Beneficios técnicos:

- reducción de superficie de ataque
- segmentación efectiva
- control tráfico industrial

Beneficios operacionales:

- continuidad protegida
- menor riesgo de interrupción

Limitaciones:

- sistemas legacy
- madurez parcial en monitoreo
- dependencia de proveedores

Anexo 5: Plan de mitigación

Cuadro de acciones de mitigación (Fase 4 — Plan de mitigación)

Ciberseguridad industrial TI/OT · ISA/IEC 62443 · NIST SP 800-82 · Modelo Purdue/ISA-99

Cada acción de mitigación fue definida considerando su descripción, el activo o proceso afectado, el nivel de prioridad, los responsables de ejecución, los recursos requeridos y los plazos estimados. La priorización se basó en la criticidad operacional, el impacto potencial en la producción y la factibilidad técnica.

Nº	Descripción de la medida	Activo o proceso afectado	Prioridad	Responsables de ejecución	Recursos requeridos	Plazo estimado
1	Segmentación de la red TI/OT según el modelo Purdue	Red industrial; niveles Purdue 2–4	Alta	Infraestructura TI · Redes	Rediseño de subredes/VLAN, equipamiento de red, HH de ingeniería	Corto plazo (0–3 meses)
2	Implementación de una iDMZ entre los niveles 3 y 4	Frontera TI/OT; servidor pivote	Alta	Redes y Ciberseguridad OT	Servidor pivote, reglas de firewall, HH de ingeniería	Corto plazo (0–3 meses)
3	Implementación de firewalls industriales y conduits controlados	Tráfico TI↔OT; perímetro de zona	Alta	Redes y Ciberseguridad OT	Firewall industrial, licencias, configuración	Corto plazo (0–3 meses)
4	Control de accesos y autenticación en entornos OT	SCADA, HMI, estaciones; cuentas de usuario	Alta	Seguridad de la Información	Gestión de identidades, políticas de acceso, HH	Mediano plazo (3–6 meses)
5	Implementación de monitoreo del tráfico industrial	Red OT; eventos y registros (logs)	Alta	Ciberseguridad OT · Monitoreo	Sonda/monitoreo industrial, almacenamiento de logs	Mediano plazo (3–6 meses)
6	Hardening de sistemas operativos y aplicaciones	Servidores, SCADA y estaciones	Media	Administración de Plataformas	Guías de hardening, ventanas de mantenimiento, HH	Mediano plazo (3–6 meses)
7	Control de acceso físico y separación de racks TI/OT	Salas técnicas y racks	Media	Infraestructura TI · Facilities	Gabinets, control de acceso físico, obra menor	Mediano plazo (3–6 meses)
8	Formalización de procedimientos de ciberseguridad e incidentes	Procesos de gestión y de incidentes	Media	Seguridad de la Información	Documentación, definición de roles	Mediano plazo (3–6 meses)
9	Capacitación y concientización del personal OT	Personal técnico y operativo	Media	RRHH · Ciberseguridad	Programa de capacitación, material, HH	Continuo (desde el inicio)

Nota: la descripción, el activo afectado y la prioridad se derivan del análisis de brechas (Fase 3). Los responsables, recursos y plazos son referenciales —expresados por rol funcional y horizonte temporal— y deben ajustarse a la estructura, la disponibilidad y la planificación de la organización.

Anexo 6: Entregables

Entregable de la Fase 1 — Inventario de activos TI/OT (línea base)

Levantamiento de activos · ISA/IEC 62443 · NIST SP 800-82 · Modelo Purdue/ISA-99

La Fase 1 estableció como entregable el inventario de activos TI y OT, identificados y clasificados por ámbito, dominio (TI/OT), nivel Purdue y criticidad. Este inventario constituye la línea base del entorno sobre la cual se aplican las fases posteriores y permanece fijo salvo la incorporación de nuevas tecnologías.

Nº	Activo	Ámbito	Dominio (TI/OT)	Nivel Purdue	Criticidad	Estado inicial (Fase 1)
1	ERP y sistemas corporativos	Software	TI	Nivel 4	Alta	Punto de origen de amenazas; acceso amplio hacia OT
2	Active Directory (directorio corporativo)	Software	TI	Nivel 4	Alta	Autenticación corporativa; sin control sobre OT
3	Servidores y estaciones corporativas	Hardware	TI	Nivel 4	Alta	Alojados en racks compartidos con OT
4	Sistemas de operación (MES, historiador)	Software	OT	Nivel 3	Alta	Sin control de tráfico hacia niveles inferiores
5	SCADA (supervisión y control)	Software	OT	Nivel 2	Alta	Accesible desde la red TI sin control intermedio
6	HMI (estaciones de supervisión)	Hardware	OT	Nivel 2	Alta	Sin autenticación robusta
7	PLC (controladores lógicos)	Hardware	OT	Nivel 1	Crítica	Expuestos en red compartida, sin aislamiento
8	Sensores, actuadores y proceso físico	Hardware	OT	Nivel 0	Crítica	Impacto directo en la producción
9	Red industrial (switches, VLAN, enlaces)	Hardware / Red	TI / OT	Transversal	Alta	Segmentación débil (solo VLAN); sin zonas ni conduits
10	Racks y salas técnicas	Instalación física	TI / OT	Transversal	Alta	Racks compartidos; acceso físico no controlado
11	Sistemas operativos y aplicaciones	Software	TI / OT	Transversal	Media	Versiones sin control; sin gestión de parches
12	Cuentas y credenciales de acceso	Software	TI / OT	Transversal	Alta	Credenciales compartidas; sin autenticación individual
13	Políticas y procedimientos	Procesos y personas	Transversal	—	Media	Inexistentes o no formalizados

Nº	Activo	Ámbito	Dominio (TI/OT)	Nivel Purdue	Críticidad	Estado inicial (Fase 1)
14	Roles y responsabilidades de seguridad OT	Procesos y personas	Transversal	—	Media	No definidos
15	Capacitación del personal OT	Procesos y personas	Transversal	—	Media	Bajo nivel de capacitación técnica

Nota: el inventario clasifica las categorías de activos identificadas en el levantamiento. La criticidad se deriva de la exposición por nivel Purdue (Tabla de riesgo del estado inicial) y el estado inicial corresponde a los hallazgos de la Fase 1. El detalle específico de cada activo (identificador, cantidad, ubicación, responsable) se completa en el registro operativo de la organización.

Entregable de la Fase 2 — Marco de control objetivo (controles por ámbito)

Controles mapeados a NIST SP 800-82/800-53 e ISA/IEC 62443 · Modelo Purdue/ISA-99

La Fase 2 estableció como entregable el conjunto de controles de ciberseguridad definidos por ámbito y mapeados a los estándares NIST SP 800-82/800-53 e ISA/IEC 62443. Este marco de control objetivo constituye la referencia contra la cual se evalúan las brechas (Fase 3) y se priorizan e implementan las medidas (Fases 4 y 5).

Nº	Ámbito	Control definido	Referencia NIST	Referencia ISA/IEC 62443	Objetivo del control
1	Instalación física	Control de acceso físico a áreas y racks OT	PE-3 / AC	Seguridad física	Restringir el acceso físico a los activos críticos
2	Instalación física	Separación física entre TI y OT (racks/salas)	SC-32	Parte 3-2	Segregar físicamente los dominios
3	Hardware / Red	Segmentación de red por niveles (modelo Purdue)	SC-32	Parte 3-2	Aislar los niveles de operación y control
4	Hardware / Red	Definición de zonas y conduits	SC-7	Parte 3-2	Gobernar la convergencia TI/OT
5	Hardware / Red	Protección de frontera (firewall industrial / iDMZ)	SC-7	SR 5	Controlar el tráfico entre TI y OT
6	Hardware / Red	Control de flujo de datos TI↔OT	AC-4	SR 5	Restringir los flujos de datos permitidos
7	Hardware / Red	Inventario y gestión de activos	CM-8	Parte 2-1	Mantener el control de configuración

Nº	Ámbito	Control definido	Referencia NIST	Referencia ISA/IEC 62443	Objetivo del control
8	Software / Lógico	Hardening de sistemas y aplicaciones	CM-6	SR 1	Reducir la superficie de ataque
9	Software / Lógico	Autenticación de accesos (individual)	IA-2	SR 1	Identificar y autenticar a los usuarios OT
10	Software / Lógico	Gestión de credenciales	IA-5	SR 1	Eliminar las credenciales compartidas
11	Software / Lógico	Gestión de parches	SI-2	Parte 2-1	Mantener los sistemas actualizados
12	Software / Lógico	Monitoreo del tráfico y registros	SI-4	SR 7	Detectar anomalías y registrar eventos
13	Procesos y personas	Formalización de procedimientos	PL-2	Parte 2-1	Establecer procesos formales de seguridad
14	Procesos y personas	Roles y responsabilidades de seguridad OT	PM-2	Parte 2-1	Definir el gobierno de la seguridad
15	Procesos y personas	Gestión de incidentes	IR-1 / IR-4	SR 7	Documentar y responder ante incidentes
16	Procesos y personas	Capacitación y concientización	AT-2	Parte 2-1	Fortalecer las competencias del personal OT

Nota: la referencia indica la familia de control de NIST y el requisito o parte de ISA/IEC 62443 aplicable a cada control (SR = System Requirement; Parte = documento de la serie 62443). Los controles se derivan de los ámbitos y estándares del modelo; su parametrización específica se define en la política de seguridad de la organización.

Entregable de la Fase 3 — Análisis de brechas (GAP)

Incumplimientos detectados, riesgo asociado y priorización · insumo del plan de mitigación

La Fase 3 estableció como entregable el análisis de brechas (GAP): la comparación del marco de control objetivo (Fase 2) con el estado real del entorno, identificando los incumplimientos, el riesgo asociado a cada uno y su priorización con enfoque de riesgo. Este análisis constituye el insumo directo del plan de mitigación (Fase 4).

Nº	Ámbito	Brecha / incumplimiento detectado	Control incumplido (NIST · ISA)	Riesgo asociado	Prioridad
1	Instalación física	Sin control de acceso físico a áreas y racks OT	ISA 62443 (física)	Acceso físico no autorizado a activos críticos	Media

Nº	Ámbito	Brecha / incumplimiento detectado	Control incumplido (NIST · ISA)	Riesgo asociado	Prioridad
2	Instalación física	Racks compartidos TI/OT (sin separación física)	SC-32 · 62443-3-2	Exposición cruzada entre dominios	Media
3	Hardware / Red	Segmentación inexistente o débil (sin zonas ni conduits)	SC-32 · 62443-3-2	Falta de aislamiento de activos críticos	Alta
4	Hardware / Red	Sin iDMZ ni protección de frontera (sin firewalls)	SC-7 · ISA SR 5	Movimiento lateral / propagación TI→OT	Alta
5	Hardware / Red	Sin control de flujo de datos TI↔OT	AC-4 · ISA SR 5	Flujos no restringidos entre dominios	Alta
6	Hardware / Red	Sin inventario ni gestión de activos OT	CM-8 · 62443-2-1	Activos no gestionados; superficie desconocida	Media
7	Software / Lógico	Sin autenticación en sistemas industriales	IA-2 · ISA SR 1	Accesos no controlados; escalamiento de privilegios	Alta
8	Software / Lógico	Credenciales compartidas	IA-5 · ISA SR 1	Trazabilidad nula; accesos no atribuibles	Media
9	Software / Lógico	Sin gestión de parches	SI-2	Explotación de vulnerabilidades conocidas	Media
10	Software / Lógico	Sistemas sin hardening	CM-6 · ISA SR 1	Mayor superficie de ataque	Media
11	Software / Lógico	Sin visibilidad ni monitoreo del tráfico OT	SI-4 · ISA SR 7	Sin detección de anomalías ni de incidentes	Alta
12	Procesos y personas	Sin roles ni gobierno de seguridad OT	62443-2-1	Baja capacidad de gestión de la seguridad	Media
13	Procesos y personas	Procesos de incidentes no documentados / sin respuesta	IR-1 / IR-4 · SR 7	Baja contención y recuperación ante eventos	Alta
14	Procesos y personas	Ausencia de procedimientos formales	PL-2	Gestión reactiva; sin trazabilidad	Media
15	Procesos y personas	Bajo nivel de capacitación del personal OT	AT-2 · 62443-2-1	Mayor probabilidad de error humano	Media

Nota: el control incumplido indica la familia de NIST y el requisito o parte de ISA/IEC 62443 no satisfecho (SR = System Requirement). La priorización se basa en la criticidad operacional, el impacto potencial y la factibilidad técnica, y ordena las medidas del plan de mitigación (Fase 4).

Entregable de la Fase 4 — Plan de mitigación de brechas

Medidas asociadas a la brecha que atienden, con prioridad, responsables, recursos y plazos

La Fase 4 estableció como entregable el plan de mitigación: cada medida se definió asociada a la brecha que atiende (Fase 3) y con su nivel de prioridad, responsables de ejecución, recursos requeridos y plazos estimados. La priorización se basó en la criticidad operacional, el impacto potencial en la producción y la factibilidad técnica.

Nº	Medida de mitigación	Brecha que atiende	Prioridad	Responsables de ejecución	Recursos requeridos	Plazo estimado
1	Segmentación de la red TI/OT (modelo Purdue)	Segmentación inexistente (SC-32, 62443-3-2)	Alta	Infraestructura TI · Redes	Rediseño de subredes/VLAN, equipamiento de red, HH de ingeniería	Corto plazo (0–3 meses)
2	Implementación de una iDMZ entre los niveles 3 y 4	Sin iDMZ ni frontera (SC-7, SR 5)	Alta	Redes y Ciberseguridad OT	Servidor pivote, reglas de firewall, HH de ingeniería	Corto plazo (0–3 meses)
3	Firewalls industriales y conduits controlados	Sin firewalls; sin control de flujo (SC-7, AC-4)	Alta	Redes y Ciberseguridad OT	Firewall industrial, licencias, configuración	Corto plazo (0–3 meses)
4	Control de accesos y autenticación en OT	Sin autenticación; credenciales compartidas (IA-2, IA-5)	Alta	Seguridad de la Información	Gestión de identidades, políticas de acceso, HH	Mediano plazo (3–6 meses)
5	Implementación de monitoreo del tráfico industrial	Sin visibilidad ni monitoreo (SI-4, SR 7)	Alta	Ciberseguridad OT · Monitoreo	Sonda/monitoreo industrial, almacenamiento de logs	Mediano plazo (3–6 meses)
6	Hardening de sistemas operativos y aplicaciones	Sistemas sin hardening (CM-6, SR 1)	Media	Administración de Plataformas	Guías de hardening, ventanas de mantenimiento, HH	Mediano plazo (3–6 meses)
7	Control de acceso físico y separación de racks	Racks compartidos; acceso físico no controlado	Media	Infraestructura TI · Facilities	Gabinetes, control de acceso físico, obra menor	Mediano plazo (3–6 meses)
8	Formalización de procedimientos e incidentes	Sin procedimientos; sin respuesta (PL-2, IR-1/IR-4)	Media	Seguridad de la Información	Documentación, definición de roles	Mediano plazo (3–6 meses)
9	Capacitación y concientización del personal OT	Baja capacitación (AT-2, 62443-2-1)	Media	RRHH · Ciberseguridad	Programa de capacitación, material, HH	Continuo (desde el inicio)

Nota: la medida, la brecha que atiende y la prioridad se derivan del análisis de brechas (Fase 3). Los responsables, recursos y plazos —expresados por rol funcional y horizonte temporal— y deben ajustarse a la estructura, la disponibilidad y la planificación de la organización.

Entregable de la Fase 5 — Controles implementados y validados por ámbito

Arquitectura segmentada operativa · validación NIST SP 800-82 e ISA/IEC 62443 · la organización alcanza el Nivel 3 (Funcional)

La Fase 5 estableció como entregable los controles implementados y validados por ámbito, con la arquitectura segmentada operativa. Cada control se validó contra los marcos NIST SP 800-82 e ISA/IEC 62443 mediante procedimientos controlados de gestión de cambios. Con ello, la organización materializó la transición del Nivel 1 al Nivel 3 (Funcional).

Nº	Ámbito	Control implementado	Brecha cerrada	Estado	Validación (NIST · ISA/IEC 62443)
1	Instalación física	Control de acceso físico a áreas y racks OT	Acceso físico no controlado	Implementado	ISA 62443 (seg. física)
2	Instalación física	Separación física TI/OT (racks/salas)	Racks compartidos	Implementado	NIST SC-32 · ISA 62443-3-2
3	Hardware / Red	Segmentación de red por niveles (modelo Purdue)	Segmentación inexistente	Implementado	NIST SC-32 · ISA 62443-3-2
4	Hardware / Red	Zonas y conduits controlados	Sin zonas ni conduits	Implementado	ISA 62443-3-2
5	Hardware / Red	iDMZ y protección de frontera (firewall industrial)	Sin iDMZ ni firewalls	Implementado	NIST SC-7 · ISA 62443 SR 5
6	Hardware / Red	Control de flujo de datos TI↔OT	Sin control de flujo	Implementado	NIST AC-4 · ISA 62443 SR 5
7	Software / Lógico	Hardening de sistemas y aplicaciones	Sistemas sin hardening	Implementado	NIST CM-6 · ISA 62443 SR 1
8	Software / Lógico	Autenticación de accesos (individual)	Sin autenticación; credenciales compartidas	Implementado	NIST IA-2 · ISA 62443 SR 1
9	Software / Lógico	Monitoreo del tráfico industrial	Sin visibilidad ni monitoreo	Parcial	NIST SI-4 · ISA 62443 SR 7
10	Procesos y personas	Formalización de procedimientos	Sin procedimientos formales	Implementado	NIST PL-2 · ISA 62443-2-1
11	Procesos y personas	Roles y gobierno de seguridad OT	Sin roles de seguridad OT	Implementado	ISA 62443-2-1
12	Procesos y personas	Gestión y respuesta a incidentes	Sin respuesta a incidentes	Parcial	NIST IR-1/IR-4 · ISA 62443 SR 7



Nº	Ámbito	Control implementado	Brecha cerrada	Estado	Validación (NIST · ISA/IEC 62443)
13	Procesos y personas	Capacitación del personal OT	Baja capacitación	Implementado	ISA 62443-2-1

Resultado global: controles implementados y validados; arquitectura segmentada operativa. La organización alcanza el Nivel 3 – Funcional (monitoreo y respuesta a incidentes en consolidación).

Nota: el estado indica si el control quedó plenamente implementado o de forma parcial (en consolidación). La validación referencia la familia de NIST y el requisito o parte de ISA/IEC 62443 verificados. El monitoreo del tráfico y la gestión de incidentes quedaron operativos de forma parcial, coherente con un estado Funcional con áreas en consolidación.

Anexo 7: Revisión por expertos

Objetivo de la revisión

Con el propósito de complementar la validación práctica de la GCTIOT, se realizó una revisión por juicio de expertos orientada a evaluar su pertinencia, claridad metodológica, aplicabilidad y alineación con los marcos de referencia utilizados en la GCTIOT. Esta revisión permitió obtener una evaluación independiente de la propuesta desde la perspectiva de profesionales con experiencia en ciberseguridad industrial, convergencia TI/OT y gestión de riesgos.

Participantes

La revisión fue realizada por **cuatro evaluadores externos**, conformados por profesionales del ámbito industrial, especialistas en ciberseguridad y tecnologías de la información y operación. La participación de perfiles diversos permitió obtener observaciones desde perspectivas tanto técnicas como organizacionales.

Instrumento utilizado

Se aplicó una pauta estructurada de evaluación compuesta por los siguientes criterios:

Criterio evaluado	Descripción
Claridad metodológica	Comprensión de las fases y secuencia propuesta.
Facilidad de uso	Nivel de simplicidad para aplicar la GCTIOT en entornos industriales.
Aplicabilidad práctica	Factibilidad de implementación en organizaciones productivas.



Enfoque progresivo	Capacidad de implementar controles de forma gradual.
Medibilidad	Posibilidad de evaluar resultados mediante indicadores y niveles de madurez.
Alineación normativa	Coherencia con ISA/IEC 62443, NIST SP 800-82 y Purdue.
Cobertura integral	Consideración equilibrada de personas, procesos y tecnología.

Formato de respuesta

Cada criterio fue evaluado utilizando una escala ordinal de cuatro niveles:

- Excelente
- Bueno
- Aceptable
- Requiere mejora

Adicionalmente, la pauta contempló observaciones abiertas para recoger sugerencias, oportunidades de mejora y comentarios técnicos complementarios.

Síntesis de resultados

Los resultados obtenidos mostraron una valoración favorable de la GCTIOT en todos los criterios evaluados. Los expertos destacaron especialmente:

- La claridad y facilidad de comprensión de la metodología propuesta.
- El carácter práctico y progresivo de la GCTIOT para entornos industriales.
- La adecuada integración de aspectos tecnológicos, organizacionales y procedimentales.
- La alineación con estándares reconocidos de ciberseguridad industrial.
- La utilidad del enfoque de madurez para medir el avance de la organización.

Entre las recomendaciones de mejora se identificó la conveniencia de reforzar algunas orientaciones asociadas a capacitación, gestión del cambio y seguimiento continuo de las medidas implementadas, aspectos que posteriormente fueron incorporados en el refinamiento de la GCTIOT.

Tabla 1. Resultados agregados de la evaluación por expertos

Escala utilizada: 4 = Excelente, 3 = Bueno, 2 = Aceptable, 1 = Requiere mejora.

Criterio evaluado	Promedio obtenido	Valoración
Claridad metodológica	3,8	Excelente
Facilidad de uso	3,8	Excelente
Aplicabilidad práctica	4,0	Excelente
Enfoque progresivo	3,8	Excelente
Medibilidad de los resultados	3,5	Bueno
Alineación con ISA/IEC 62443, NIST SP 800-82 y Purdue	4,0	Excelente
Cobertura de personas, procesos y tecnología	3,8	Excelente
Promedio general	3,81	Excelente

Tabla 1: Resultados agregados de la evaluación realizada por cuatro expertos independientes.

Los resultados obtenidos evidencian una valoración altamente favorable de la GCTIOT propuesta, alcanzando un promedio general de 3,81 sobre 4,0. Los criterios mejor evaluados fueron la aplicabilidad práctica y la alineación con los marcos de referencia ISA/IEC 62443, NIST SP 800-82 y el modelo Purdue, obteniendo la máxima valoración promedio. Estos resultados refuerzan la capacidad de la propuesta para transformar requisitos normativos en actividades concretas y aplicables a entornos industriales reales. La revisión también destacó la claridad metodológica, la facilidad de uso y el enfoque progresivo de implementación, aspectos que fueron identificados como elementos diferenciadores para facilitar la adopción de controles de ciberseguridad industrial en organizaciones con distintos niveles de madurez. Las observaciones realizadas se concentraron principalmente en oportunidades de fortalecimiento relacionadas con la capacitación, la gestión del cambio y el seguimiento continuo de las medidas implementadas, elementos que fueron considerados en la mejora final de la GCTIOT. En conjunto, la evaluación de expertos complementa los resultados obtenidos mediante el cuestionario de madurez y aporta evidencia adicional de la validez, aplicabilidad y utilidad práctica de la GCTIOT desarrollada.

Resultado	Frecuencia	Porcentaje
Excelente	18	64,3 %
Bueno	9	32,1 %
Aceptable	1	3,6 %
Requiere mejora	0	0,0 %
Total respuestas	28	100 %

(4 evaluadores $\times$ 7 criterios = 28 evaluaciones).

Conclusión de la revisión experta

La revisión independiente realizada por especialistas permitió corroborar que la GCTIOT constituye una metodología práctica, progresiva y aplicable para apoyar la convergencia segura entre entornos TI y OT. Las observaciones recibidas respaldan la validez de la propuesta y complementan los resultados obtenidos mediante la evaluación de madurez, reforzando la evidencia de que la GCTIOT facilita la implementación gradual de controles de ciberseguridad industrial en organizaciones del sector productivo.

Anexo 7: Resultado de Implementación



Figura 1: Levantamiento de activos aplicado a los cuatro ámbitos, con el hallazgo y control asociado en cada uno.

Resultado de la Fase 2 en los cuatro ámbitos según figura 5:



Figura 2: Control definido en cada ámbito, la debilidad del Nivel 1 que mitiga y su estándar de referencia.



Figura 3: Brecha detectada en cada ámbito, su riesgo asociado y el control incumplido.



Figura 4: Medida priorizada en cada ámbito, la brecha que atiende y su nivel de prioridad.



Figura 5: Controles implementados en cada ámbito, la brecha que cierran y el control aplicado.