Universidad Cenfotec

Maestría en Seguridad de la Información y Ciberseguridad

Documento final de Proyecto de Investigación Aplicada 1

Propuesta de evaluación de la postura de ciberseguridad y gestión de vulnerabilidades en sistemas de Tecnología Operacionales (OT) en el sector de biotecnología basado en NIST CSF 2.0/COBIT 2019

Elaborado por:

Sánchez Castro, María Paola

Junio, 2025

Resumen

La ciberseguridad en entornos de Tecnología Operacional (OT) constituye un desafío prioritario para la protección de infraestructuras críticas y procesos industriales a nivel global, ante el incremento de ciberataques dirigidos a sectores como energía, manufactura y transporte. La convergencia entre tecnologías de información (IT) y OT, impulsada por la Industria 4.0, ha generado nuevos vectores de amenaza que pueden comprometer la continuidad operativa y la seguridad física de las instalaciones. Esta investigación propone el diseño de un modelo de evaluación de gobierno y gestión para sistemas OT, fundamentado en COBIT 2019 como marco integrador, complementado con los estándares técnicos ISA/IEC 62443, NIST SP 800-82, NIST CSF 2.0 Manufacturing Profile. El modelo busca proporcionar una propuesta estructurada que permita a las organizaciones diagnosticar la madurez de sus procesos de gobierno y gestión de la seguridad OT, identificar brechas críticas y establecer prioridades de mejora. Se espera que la aplicación de este modelo contribuya a fortalecer la gobernanza, la alineación estratégica y la gestión de riesgos en sistemas industriales, ofreciendo una herramienta práctica y adaptable a distintos contextos sectoriales.

Palabras clave: Tecnología Operacional, TO, ciberseguridad industrial, COBIT 2019, gobierno de TI, evaluación de madurez, ISA/IEC 62443, NIST SP 800-82,NIST CSF 2.0, Manufacturing Profile.

Abstract

Cybersecurity in Operational Technology (OT) environments has become a critical challenge for protecting critical infrastructure and industrial processes worldwide, given the increasing number of cyberattacks targeting sectors such as energy, manufacturing, and transportation. The convergence of Information Technology (IT) and Operational Technology (OT), driven by Industry 4.0, has introduced new threat vectors that can compromise operational continuity and the physical safety of facilities. This research proposes the design of a governance and management assessment model for OT systems, based on COBIT 2019 as an integrating framework and complemented by the technical standards ISA/IEC 62443, NIST SP 800-82, and the NIST CSF 2.0 Manufacturing Profile. The model aims to provide a structured approach that enables organizations to assess the maturity of their OT security governance and management processes, identify critical gaps, and establish improvement priorities. The application of this model is expected to strengthen governance, strategic alignment, and risk management in industrial systems, offering a practical and adaptable tool for different industry sectors.

Keywords: Operational Technology, OT, industrial cybersecurity, COBIT 2019, IT governance, maturity assessment, ISA/IEC 62443, NIST SP 800-82, NIST CSF 2.0, Manufacturing Profile.

1. Introducción

1.1 Contexto y Relevancia del Problema

La ciberseguridad en entornos de Tecnología Operacional (OT) se ha convertido en un elemento crítico para la protección de infraestructuras esenciales debido a la convergencia IT/OT y la adopción de la Industria 4.0, que incrementan la exposición a amenazas cibernéticas. En este contexto, la investigación propone un modelo de evaluación de la postura de ciberseguridad y gestión de vulnerabilidades para el sector biotecnológico, utilizando COBIT 2019 como marco integrador y complementándolo con NIST CSF 2.0 Manufacturing Profile, NIST SP 800-82 e ISA/IEC 62443. El objetivo es proporcionar una metodología que permita medir la madurez de los procesos, identificar brechas de seguridad y priorizar acciones de mejora.

En Costa Rica, los ciberataques ocurridos en instituciones públicas y organizaciones estratégicas han evidenciado la vulnerabilidad de los servicios críticos y la necesidad de fortalecer la protección de los entornos OT. Aunque existe una Estrategia Nacional de Ciberseguridad, aún no se dispone de lineamientos específicos ni de modelos de evaluación y madurez adaptados a los sistemas OT. Como resultado, muchas organizaciones implementan estándares internacionales de forma parcial, generando brechas que pueden afectar la resiliencia operativa de sectores estratégicos como biotecnología, energía, manufactura, agua y transporte.

1.2 Definición del problema

El problema central de la investigación es la ausencia de un modelo estructurado que permita evaluar de forma integral la postura de ciberseguridad y la gestión de vulnerabilidades en sistemas de Tecnología Operacional (OT) del sector biotecnológico, integrando marcos como COBIT 2019, NIST CSF 2.0, NIST SP 800-82 e ISA/IEC 62443. Aunque existen estándares internacionales para la protección de entornos industriales, Costa Rica carece de metodologías adaptadas a su contexto que permitan medir la madurez de ciberseguridad, identificar brechas y orientar planes de mejora continua.

Esta situación se ve agravada por diversos desafíos, entre ellos la creciente convergencia entre los entornos TI y OT, la ausencia de modelos nacionales de evaluación de madurez, la aplicación parcial de estándares internacionales, las limitaciones en la identificación y gestión de activos OT críticos, y la falta de procesos formales de monitoreo continuo y medición de capacidades de seguridad. Como consecuencia, muchas organizaciones no cuentan con una visión clara de su postura de ciberseguridad ni de sus vulnerabilidades, incrementando el riesgo de interrupciones operativas, afectaciones a la

continuidad del negocio, incumplimientos regulatorios e impactos económicos, ambientales y reputacionales. Por ello, surge la necesidad de desarrollar un modelo de evaluación que facilite el diagnóstico, la identificación de brechas y la mejora continua de la ciberseguridad en entornos OT.

1.3 Objetivo General y Objetivos Específicos

Objetivo General

Proponer un modelo evaluación de la postura de ciberseguridad y gestión de vulnerabilidades en sistemas de Tecnología Operacionales (OT) en el sector de biotecnología, basado en COBIT 2019 e integrado con estándares como NIST CSF 2.0, que permita diagnosticar la madurez de los procesos y orientar la mejora continua.

Objetivos Específicos

1. Identificar los procesos, activos y controles de ciberseguridad presentes en los sistemas de Tecnología Operacional (OT), considerando los dominios y prácticas establecidos en COBIT 2019 y NIST CSF 2.0.
2. Analizar el estado actual de la postura de ciberseguridad y de la gestión de vulnerabilidades en los sistemas OT evaluados, mediante la aplicación de criterios de diagnóstico basados en NIST CSF 2.0 y estándares complementarios de ciberseguridad.
3. Evaluar el nivel de madurez de los procesos relacionados con la ciberseguridad y la gestión de vulnerabilidades, utilizando métricas e indicadores alineados con los principios de COBIT 2019 y NIST CSF 2.0.
4. Diseñar una propuesta de evaluación que integre los componentes de postura de ciberseguridad, gestión de vulnerabilidades y medición de madurez para entornos de Tecnología Operacional en organizaciones del sector biotecnológico.
5. Proponer un modelo de evaluación de la postura de ciberseguridad y gestión de vulnerabilidades basado en COBIT 2019 e integrado con NIST CSF 2.0, que facilite la identificación de brechas, la priorización de acciones correctivas y la mejora continua de los procesos de seguridad en entornos OT.

1.4 Pregunta de Investigación

En este contexto surge la siguiente pregunta de investigación:

¿Cómo puede desarrollarse y aplicarse una propuesta de evaluación de la postura de ciberseguridad y gestión de vulnerabilidades en sistemas de Tecnología Operacional (OT) del sector de biotecnología costarricense?

2. Metodología

2.1 Tipo de Investigación

La presente investigación es de tipo aplicada, ya que se orienta a la utilización y adaptación de conocimientos, marcos de referencia y buenas prácticas existentes para resolver una problemática específica en el ámbito de la ciberseguridad industrial. Su propósito no es generar nuevas teorías, sino desarrollar una propuesta de evaluación que permita diagnosticar la postura de ciberseguridad y la gestión de vulnerabilidades en sistemas de Tecnología Operacional (OT) del sector biotecnológico.

La propuesta resultante pretende servir como una herramienta de apoyo para la toma de decisiones en materia de ciberseguridad, permitiendo a las organizaciones del sector biotecnológico fortalecer la protección de sus sistemas OT, mejorar sus capacidades de gestión de vulnerabilidades y aumentar su resiliencia frente a amenazas cibernéticas. También busca contribuir al fortalecimiento de la seguridad de las infraestructuras industriales en Costa Rica mediante la adopción de prácticas alineadas con estándares internacionales de gobernanza y gestión de riesgos tecnológicos.

2.2 Alcance Investigativo

La investigación posee un alcance descriptivo, ya que analiza la postura actual de ciberseguridad y la gestión de vulnerabilidades en sistemas de Tecnología Operacional (OT) del sector biotecnológico costarricense, identificando los principales riesgos, amenazas y vulnerabilidades que pueden afectar los procesos industriales. Para ello, se consideran marcos y estándares internacionales como NIST CSF 2.0, COBIT 2019, NIST SP 800-82 e ISA/IEC 62443, complementados con el modelo Purdue para la clasificación de activos según su nivel de criticidad dentro del entorno OT.

A partir de este análisis, se busca identificar brechas de seguridad, evaluar el nivel de madurez de los procesos de ciberseguridad y generar una base de conocimiento que permita diseñar una propuesta de evaluación orientada a fortalecer la gestión de vulnerabilidades y apoyar la mejora continua de la seguridad en organizaciones del sector biotecnológico.

2.3 Enfoque

La investigación presenta un enfoque mixto (cualitativo-cuantitativo), ya que combina el análisis documental de marcos y estándares de ciberseguridad como NIST CSF 2.0, COBIT 2019, NIST SP 800-82 e ISA/IEC 62443, con la aplicación práctica de una propuesta de evaluación en una organización del sector biotecnológico.

El componente cuantitativo se basa en la asignación de puntuaciones y métricas para medir la madurez de los procesos, identificar brechas y evaluar la postura de ciberseguridad de los sistemas OT. La integración de ambos enfoques permite obtener una visión integral, combinando el análisis conceptual con resultados medibles que apoyan la toma de decisiones y la mejora continua.

2.4 Diseño

La investigación posee un enfoque mixto y un diseño no experimental, ya que combina la revisión documental de estándares, marcos de referencia y literatura especializada con la aplicación práctica de una propuesta de evaluación en una organización del sector biotecnológico, sin manipular variables ni intervenir sobre los entornos evaluados.

La fase cualitativa se basa en el análisis de fuentes especializadas sobre ciberseguridad OT, mientras que la fase cuantitativa utiliza escalas de madurez y criterios de valoración para medir la postura de ciberseguridad, identificar brechas y generar indicadores que apoyen la mejora continua de la gestión de vulnerabilidades en sistemas OT.

2.5 Población y Muestreo

Para este estudio se analizaron y consolidaron los estándares, normas y marcos internacionales del sector industrial mundialmente aceptadas para finalmente aplicarlas a un modelo de ciberseguridad en la población conformada por los sistemas de Tecnología Operacional (OT), procesos industriales, activos tecnológicos y personal relacionado con la gestión y operación de dichos sistemas dentro de las organizaciones del sector biotecnológico de Costa Rica.

2.6 Instrumentos de Recolección de Datos

Para la recolección de datos se utilizó una combinación de revisión documental, matrices de análisis, entrevistas semiestructuradas y cuestionarios. La revisión documental se enfocó en estándares y marcos de referencia como NIST CSF 2.0, COBIT 2019, NIST SP 800-82 Rev. 3 e ISA/IEC 62443, mientras que las matrices permitieron organizar y comparar controles, procesos y prácticas de ciberseguridad.

Adicionalmente, las entrevistas y cuestionarios aplicados al personal responsable de los sistemas OT permitieron recopilar información sobre gobernanza, gestión de riesgos, gestión de activos y vulnerabilidades. Los datos obtenidos fueron utilizados para aplicar la propuesta de evaluación, asignar puntuaciones de madurez, identificar brechas de seguridad y determinar la postura actual de ciberseguridad de la organización.

2.7 Técnicas de Análisis de Información

Una vez finalizada la recolección de datos, la información obtenida fue analizada utilizando COBIT 2019, NIST CSF 2.0 Manufacturing Profile, NIST SP 800-82 Rev. 3 e ISA/IEC 62443, permitiendo evaluar aspectos de gobernanza, gestión de riesgos, gestión de activos, gestión de vulnerabilidades y demás capacidades de ciberseguridad presentes en los entornos OT.

Posteriormente, se analizaron los activos identificados considerando su criticidad, ubicación dentro del Modelo Purdue y las zonas definidas por ISA/IEC 62443. Mediante una escala de madurez, se asignaron puntuaciones a los dominios y funciones evaluadas, lo que permitió identificar brechas de ciberseguridad, determinar el nivel de madurez de la organización y establecer acciones de mejora continua apoyadas en indicadores, matrices y gráficos de resultados.

2.8 Procedimiento Analítico en Tres Fases

Fase 1: Evaluación de la postura de ciberseguridad y madurez organizacional

La Fase 1 tiene como propósito evaluar la postura actual de ciberseguridad y el nivel de madurez de la organización en los entornos de Tecnología Operacional (OT). Para ello, se realizan entrevistas, cuestionarios y revisiones documentales con los responsables de OT, analizando políticas, procedimientos y documentación relevante.

La evaluación se basa en COBIT 2019 para medir aspectos de gobernanza, gestión de riesgos, activos, continuidad y monitoreo, y en NIST CSF 2.0 Manufacturing Profile para evaluar las funciones Govern, Identify, Protect, Detect, Respond y Recover. Como resultado, se obtiene una línea base de madurez que permite identificar fortalezas, debilidades y áreas prioritarias de mejora en la postura de ciberseguridad de la organización.

Fase 2: Identificación de sitios, activos críticos y evaluación de vulnerabilidades

La Fase 2 se enfoca en identificar los sitios operativos, validar el inventario de activos OT y analizar las vulnerabilidades presentes en la infraestructura industrial. Para ello, se realizan sesiones de trabajo con los responsables de cada instalación, identificando componentes como sistemas SCADA, PLC, DCS, servidores OT, redes industriales, sensores y demás activos críticos para la operación.

Posteriormente, los activos son clasificados según su criticidad y ubicación dentro de la arquitectura industrial, considerando las zonas y conductos definidos por ISA/IEC 62443.

La evaluación de vulnerabilidades se realiza utilizando como referencia NIST SP 800-82 Rev. 3 e ISA/IEC 62443, permitiendo identificar riesgos, niveles de exposición y áreas que requieren medidas de protección adicionales en cada sitio evaluado.

Fase 3: Análisis de resultados, monitoreo y plan de mejora

La Fase 3 consiste en consolidar los resultados obtenidos en las etapas anteriores para generar una visión integral de la postura de ciberseguridad de la organización. En esta fase se correlacionan los niveles de madurez obtenidos mediante COBIT 2019 y NIST CSF 2.0 con los activos, vulnerabilidades y riesgos identificados, permitiendo determinar las principales brechas y prioridades de atención.

Con base en este análisis, se desarrollan planes de mejora y acciones de remediación priorizadas según el nivel de riesgo y la criticidad de los activos afectados. Además, se establecen mecanismos de seguimiento, indicadores de desempeño y una hoja de ruta que define responsables, actividades y tiempos de implementación, con el objetivo de fortalecer continuamente la postura de ciberseguridad y la gestión de vulnerabilidades en los entornos OT evaluados.

3. Resultados de la revisión documental de las normas, marcos y referencias

Previamente se realizó una fase de análisis preliminar dentro del marco teórico con el objetivo de identificar los conceptos, metodologías y marcos de referencia más relevantes para el desarrollo de la investigación. Este análisis permitió delimitar los temas centrales que formarían parte del estudio, priorizando aquellos relacionados con la ciberseguridad en entornos de Tecnología Operacional (OT), la gestión de riesgos tecnológicos, la gestión de vulnerabilidades, la protección de infraestructuras industriales y los modelos de gobierno de ciberseguridad aplicables al sector biotecnológico.

Como parte de esta revisión, se analizaron marcos de referencia reconocidos internacionalmente, entre ellos COBIT 2019, NIST Cybersecurity Framework (CSF) 2.0 Manufacturing Profile, NIST SP 800-82 Rev. 3 e ISA/IEC 62443, con el propósito de identificar los objetivos, funciones, categorías y buenas prácticas más adecuadas para evaluar la postura de ciberseguridad y la gestión de vulnerabilidades en sistemas OT. La selección de estos marcos permitió establecer una base metodológica sólida para la evaluación de la gobernanza de ciberseguridad, la identificación de activos críticos, la evaluación de riesgos y el análisis de vulnerabilidades en ambientes industriales.

3.1 Marcos normativos, referencias y de trabajo

3.1.1 COBIT 2019

COBIT 2019 fue utilizado como marco de referencia para evaluar las capacidades de gobierno y gestión relacionadas con la ciberseguridad en entornos de Tecnología Operacional (OT). Para la investigación se seleccionaron objetivos enfocados en gestión de riesgos, seguridad, activos, cambios, continuidad operativa, proveedores, monitoreo y cumplimiento, por ser los más relevantes para la protección de sistemas industriales y la gestión de vulnerabilidades.

La aplicación de estos objetivos permitió analizar la postura de ciberseguridad de la organización, determinar su nivel de madurez e identificar oportunidades de mejora en áreas clave como gobernanza, gestión de riesgos, administración de activos, continuidad del negocio y cumplimiento de requisitos de seguridad en entornos OT.

3.1.2 NIST CSF 2.0 Manufacturing Profile

El NIST Cybersecurity Framework (CSF) 2.0 Manufacturing Profile proporciona un conjunto de funciones, categorías y resultados esperados orientados a fortalecer la gestión de riesgos de ciberseguridad en entornos industriales y de manufactura. Este perfil adapta las capacidades del NIST CSF a las necesidades específicas de los sistemas de Tecnología Operacional (OT), considerando aspectos como la disponibilidad de los procesos productivos, la seguridad de las personas, la continuidad operacional y la protección de los activos industriales.

Para esta investigación se seleccionaron las funciones Govern (GV), Identify (ID), Protect (PR), Detect (DE), Respond (RS) y Recover (RC), así como las categorías que presentan una relación directa con la evaluación de la postura de ciberseguridad, la identificación de activos OT, la gestión de vulnerabilidades y la determinación del riesgo asociado a los sistemas industriales.

3.1.3 NIST SP 800-82r3

NIST SP 800-82 Rev. 3 es una guía del NIST orientada a la protección de sistemas de Tecnología Operacional (OT), como ICS, SCADA, DCS y PLC. Su enfoque es principalmente técnico y operativo, proporcionando recomendaciones para gestionar los riesgos y proteger los sistemas industriales sin afectar la disponibilidad ni la continuidad de los procesos.

En esta investigación, NIST SP 800-82 Rev. 3 se utiliza como una referencia técnica complementaria a COBIT 2019 y NIST CSF 2.0, permitiendo validar que las capacidades y controles identificados durante la evaluación de la postura de ciberseguridad se encuentren alineados con las mejores prácticas específicas para entornos OT.

3.1.4 ISA/IEC 62443

La norma ISA/IEC 62443 introduce el modelo de zonas y conductos para segmentar y proteger los entornos OT. Las zonas agrupan activos con funciones y requisitos de seguridad similares, mientras que los conductos controlan la comunicación entre ellas, reduciendo la superficie de ataque y limitando la propagación de incidentes.

En esta investigación, este modelo se utiliza como referencia para clasificar activos OT según su función y criticidad, facilitando el análisis de riesgos, vulnerabilidades y niveles de protección dentro de la arquitectura industrial. Esto permite identificar las áreas con mayor exposición al riesgo y determinar dónde es necesario fortalecer los controles de seguridad.

4. Propuesta de Solución

Como resultado del análisis realizado, se identificó que las organizaciones que operan sistemas de Tecnología Operacional (OT) en el sector biotecnológico disponen de controles y prácticas de seguridad orientadas a proteger sus procesos industriales; sin embargo, en muchos casos carecen de una metodología estructurada para evaluar integralmente su postura de ciberseguridad y el nivel de madurez de sus procesos de gestión de vulnerabilidades. Esta situación dificulta la identificación de brechas de seguridad, la priorización de riesgos y la implementación de mejoras continuas, especialmente ante la creciente convergencia entre los entornos TI y OT y la adopción de tecnologías asociadas a la Industria 4.0.

Para atender esta necesidad, se propone un modelo de evaluación basado en COBIT 2019 y NIST CSF 2.0 Manufacturing Profile, complementado con NIST SP 800-82 Rev. 3 e ISA/IEC 62443. La propuesta permite evaluar tanto aspectos organizacionales como técnicos, incluyendo gobernanza, gestión de riesgos, gestión de activos, continuidad operativa, monitoreo, segmentación de redes industriales, identificación de activos OT y gestión de vulnerabilidades. Su propósito es proporcionar una herramienta adaptable que permita diagnosticar el estado actual de ciberseguridad, identificar brechas y definir planes de mejora alineados con las necesidades operativas y estratégicas de cada organización, sin pretender sustituir los estándares y marcos normativos existentes.

4.1 Estructura General de la Propuesta de Evaluación

A continuación, se describen las fases que conforman la propuesta de evaluación de la postura de ciberseguridad y gestión de vulnerabilidades en sistemas de Tecnología Operacional (OT), basada en NIST Cybersecurity Framework (CSF) 2.0 Manufacturing Profile, COBIT 2019, NIST SP 800-82 Rev. 3 e ISA/IEC 62443. Cada fase contempla actividades específicas orientadas a diagnosticar el estado actual de la organización, identificar vulnerabilidades y establecer acciones de mejora continua para fortalecer la seguridad de los entornos industriales. Ver apéndice 1 para entender el contenido de la propuesta.

4.1.1 Evaluación de la Postura de Ciberseguridad

Propósito: Determinar el nivel actual de madurez de ciberseguridad y la capacidad de la organización para gestionar riesgos asociados a los sistemas OT.

Descripción: Esta fase tiene como objetivo establecer una línea base de la postura de ciberseguridad mediante la evaluación de los procesos de gobernanza, gestión de riesgos, gestión de activos, continuidad operativa, monitoreo y seguridad. Para ello, se realizan entrevistas, cuestionarios y revisiones documentales con los responsables de TI, OT, ingeniería, automatización y ciberseguridad.

La evaluación se desarrolla utilizando COBIT 2019 para analizar los mecanismos de gobierno y gestión, y NIST CSF 2.0 Manufacturing Profile para evaluar las capacidades organizacionales relacionadas con las funciones Govern, Identify, Protect, Detect, Respond y Recover. Como resultado, se obtiene un diagnóstico inicial del nivel de madurez y de las principales brechas de ciberseguridad existentes en la organización. Ver apéndice 2 y apéndice 3 para entender la estructura.

4.1.2 Identificación de Activos y Caracterización del Entorno OT

Propósito: Obtener una visión detallada de los activos que conforman la infraestructura OT y comprender su importancia dentro de los procesos operativos.

Descripción: Una vez determinada la postura de ciberseguridad, se procede a identificar los sitios, plantas, laboratorios y áreas operativas que utilizan sistemas OT. Posteriormente, se elabora o valida el inventario de activos críticos, incluyendo sistemas SCADA, PLC, DCS, servidores OT, estaciones de ingeniería, historiadores, dispositivos de campo, redes industriales y demás componentes involucrados en la operación.

Los activos son clasificados de acuerdo con su criticidad, función operativa y nivel de impacto sobre los procesos de negocio. Como complemento, se utilizan los principios de segmentación de ISA/IEC 62443 para identificar zonas y conductos, facilitando la comprensión de la arquitectura industrial y las relaciones de comunicación entre los distintos componentes. Ver apéndice 4.

4.1.3 Evaluación de Vulnerabilidades y Riesgos

Propósito: Identificar vulnerabilidades, amenazas y riesgos que puedan afectar la disponibilidad, integridad y seguridad de los sistemas OT.

Descripción: Esta fase contempla el análisis de las vulnerabilidades presentes en los activos identificados, considerando aspectos relacionados con configuraciones inseguras, obsolescencia tecnológica, gestión de accesos, segmentación de redes, gestión de cambios y monitoreo de seguridad.

La evaluación toma como referencia los controles y recomendaciones definidos en NIST SP 800-82 Rev. 3 e ISA/IEC 62443, permitiendo identificar exposiciones de seguridad y determinar el impacto potencial sobre la operación. Los riesgos identificados son analizados considerando la criticidad de los activos, la probabilidad de ocurrencia y las consecuencias operativas para la organización. Ver apéndice 4.

4.1.4 Análisis de Brechas y Determinación de Madurez

Propósito: Comparar el estado actual de la organización con las mejores prácticas internacionales para identificar oportunidades de mejora.

Descripción: Los resultados obtenidos en las fases anteriores son consolidados y comparados con los requisitos establecidos por COBIT 2019, NIST CSF 2.0 Manufacturing Profile, NIST SP 800-82 Rev. 3 e ISA/IEC 62443. A partir de este análisis se identifican brechas de cumplimiento, deficiencias en los controles existentes y áreas que requieren fortalecimiento.

Cada dominio evaluado recibe una puntuación de madurez basada en criterios previamente definidos, permitiendo determinar el nivel de capacidad actual de la organización y establecer una línea base para futuras evaluaciones.

4.1.5 Elaboración del Plan de Mejora y Monitoreo

Propósito: Definir acciones que permitan fortalecer la postura de ciberseguridad y mejorar la gestión de vulnerabilidades en los entornos OT.

Descripción: Con base en las brechas identificadas, se desarrollan recomendaciones orientadas a mejorar los controles técnicos, procesos de gestión y mecanismos de gobernanza relacionados con la ciberseguridad industrial. Las acciones son priorizadas según el nivel de riesgo, la criticidad de los activos afectados y el impacto esperado sobre la operación.

Adicionalmente, se propone una hoja de ruta de implementación que incluye responsables, actividades, indicadores de seguimiento y tiempos estimados para la ejecución de las mejoras. Esta fase permite establecer un proceso de monitoreo continuo que facilite la evolución progresiva de la madurez de ciberseguridad y la reducción de riesgos en los sistemas OT. Ver apéndice 5.

4.1.6 Resultados de la evaluación

Los resultados evidenciaron un nivel de madurez de ciberseguridad inferior al esperado en áreas clave como gobernanza, gestión de riesgos, inventario de activos OT, gestión de vulnerabilidades, monitoreo de seguridad y respuesta ante incidentes. Se identificaron brechas significativas y diferencias en la implementación de controles, reflejando la necesidad de fortalecer la integración de la ciberseguridad dentro de los procesos operativos de la organización.

El diagnóstico permitió establecer una línea base de referencia, identificar oportunidades de mejora y justificar la implementación de una metodología estructurada para evaluar la postura de ciberseguridad y la gestión de vulnerabilidades. Esto facilitará el incremento progresivo del nivel de madurez y la alineación con las mejores prácticas definidas por COBIT 2019, NIST CSF 2.0 Manufacturing Profile, NIST SP 800-82 Rev. 3 e ISA/IEC 62443.

Referencia de algunas preguntas realizadas:

- ¿Existe un marco de gobierno que incluya explícitamente el riesgo cibernético OT?
- ¿El riesgo OT (seguridad física, continuidad) se evalúa y optimiza a nivel directivo?
- ¿Hay un marco de gestión de seguridad diferenciado para OT vs IT?
- ¿La arquitectura considera el modelo Purdue y zonas/conductos ISA 62443?

- ¿Se gestionan riesgos OT con metodología formal (probabilidad×impacto×consecuencia)?
- ¿Existe un programa de seguridad OT con controles 800-82 / 62443?
- ¿Se clasifican y protegen los datos OT (configuraciones, históricos, lab)?
- ¿Los cambios de lógica PLC/OT pasan por control de cambios con revisión de ciberseguridad?
- ¿Hay inventario validado de activos OT (manufactura y laboratorio)?
- ¿Existen líneas base de configuración segura para PLC, HMI y red OT?

Los resultados obtenidos permitieron establecer una línea base de madurez que servirá como punto de partida para la definición de acciones correctivas y planes de mejora. De igual forma, facilitaron la identificación de brechas prioritarias que deberán ser abordadas para fortalecer la postura de ciberseguridad, incrementar la resiliencia operativa y mejorar la alineación de la organización con las buenas prácticas promovidas por NIST CSF 2.0 Manufacturing Profile y los demás marcos de referencia considerados en la investigación.

Algunas preguntas de referencia:

- ¿Se identificaron las partes interesadas internas/externas (operaciones, calidad, seguridad, ingeniería, proveedores OT) y sus necesidades de ciberseguridad, y están documentadas? (800-82r3 programa OT; ISA 62443-2-1)
- ¿Se conocen y rastrean a nivel de sitio los requisitos legales, regulatorios y contractuales de ciberseguridad aplicables a OT? (800-82r3; ISA 62443-2-1)
- ¿Existen objetivos y tolerancia de riesgo de ciberseguridad OT definidos y comunicados? (800-82r3; ISA 62443-3-2)
- ¿Están asignadas formalmente las funciones y autoridades de ciberseguridad OT a nivel de sitio (p. ej. OT Site Champion)? (800-82r3; ISA 62443-2-1)
- ¿Existe una política de ciberseguridad OT establecida, comunicada y aplicada, diferenciada de IT? (800-82r3; ISA 62443-2-1)

Los hallazgos obtenidos permitieron determinar que existen activos críticos que requieren atención prioritaria dentro de la estrategia de ciberseguridad de la organización. Esta información constituye un insumo fundamental para las etapas posteriores de análisis de riesgos, priorización de acciones y definición de planes de mejora orientados al fortalecimiento de la postura de ciberseguridad y la gestión de vulnerabilidades en los entornos OT evaluados.

Durante la primera fase se aplicaron entrevistas, cuestionarios y revisiones documentales basadas en COBIT 2019 y NIST CSF 2.0 Manufacturing Profile, utilizando preguntas relacionadas con gobierno de ciberseguridad OT, gestión de riesgos, inventario de activos, arquitectura Purdue, zonas y conductos ISA/IEC 62443, gestión de cambios, continuidad operativa, monitoreo, respuesta a incidentes y cumplimiento regulatorio.

Los resultados evidenciaron un nivel de madurez inferior al esperado, identificándose brechas importantes en gobernanza, gestión de riesgos, inventario y clasificación de activos OT, monitoreo continuo, gestión de vulnerabilidades y capacidades de respuesta y recuperación. Esta evaluación permitió establecer una línea base para la mejora continua y justificó la necesidad de un modelo estructurado de evaluación.

Durante la fase 2 se identificaron diversos activos OT críticos, incluyendo sistemas de control industrial, equipos de automatización, servidores industriales, dispositivos de red y componentes esenciales para la operación.

Asimismo, se detectaron múltiples vulnerabilidades asociadas a estos activos, relacionadas con configuraciones inseguras, controles insuficientes, segmentación de red limitada y deficiencias en la gestión de seguridad. Los hallazgos permitieron determinar cuáles activos presentan mayor criticidad y requieren atención prioritaria dentro de la estrategia de ciberseguridad de la organización.

Los resultados de COBIT 2019, NIST CSF 2.0 e inventario de activos fueron consolidados en un modelo de riesgo global. La evaluación mostró que la organización presenta una postura de ciberseguridad con riesgos elevados, destacándose principalmente las funciones Protect (9.2) y Detect (9.0) con nivel Crítico, mientras que Identify (6.5), Respond (5.8) y Recover (6.0) obtuvieron niveles Altos. El riesgo global del sitio alcanzó 7.8 (Alto), cercano al nivel crítico.

Con base en estos resultados se definió un plan de mejora priorizado enfocado en segmentación de redes OT, implementación de firewalls y conductos ISA/IEC 62443, eliminación de credenciales por defecto, autenticación multifactor (MFA), hardening de activos, gestión de parches, monitoreo OT, implementación de DMZ industrial, gestión de vulnerabilidades, recuperación ante desastres y formalización de políticas y roles de ciberseguridad. La meta propuesta es reducir el riesgo global del sitio hasta aproximadamente 3.1, fortaleciendo progresivamente la madurez y resiliencia de los entornos OT.

5. Limitaciones del Estudio

- La investigación no contempla la implementación completa de los controles, procesos o recomendaciones propuestas, enfocándose únicamente en el diagnóstico, la evaluación de madurez y la identificación de oportunidades de mejora en la postura de ciberseguridad y la gestión de vulnerabilidades.
- Debido a consideraciones operativas, de confidencialidad y seguridad industrial, el acceso a configuraciones detalladas, información sensible y resultados de pruebas técnicas avanzadas puede ser limitado, por lo que parte de la evaluación depende de entrevistas, cuestionarios y documentación disponible.
- El estudio no busca crear un nuevo estándar o regulación nacional, sino adaptar e integrar marcos internacionales reconocidos como COBIT 2019, NIST CSF 2.0, NIST SP 800-82 Rev. 3 e ISA/IEC 62443 al contexto del sector biotecnológico costarricense.
- La investigación se concentra en la postura de ciberseguridad y la gestión de vulnerabilidades de los sistemas OT, sin abordar en profundidad aspectos como seguridad física, seguridad ocupacional, protección ambiental o requisitos regulatorios ajenos a la ciberseguridad.
- Los hallazgos obtenidos corresponden a una organización específica y a un momento determinado de evaluación, por lo que no representan necesariamente la realidad de todo el sector biotecnológico costarricense.
- La evolución constante de las amenazas cibernéticas, vulnerabilidades y tecnologías industriales puede afectar la vigencia de los controles y prácticas evaluadas, por lo que la propuesta debe considerarse un modelo sujeto a actualización y mejora continua.

6. Líneas de Investigación Futura

- Desarrollar un modelo automatizado de evaluación continua de la postura de ciberseguridad OT, integrando herramientas de descubrimiento de activos, monitoreo de vulnerabilidades y generación automática de indicadores de madurez.
- Adaptar metodologías de evaluación de vulnerabilidades específicas para sistemas OT, utilizando modelos complementarios a CVSS tradicional, tales como CVSS for Industrial Control Systems (ICS) o enfoques que consideren impacto operacional, seguridad física y consecuencias ambientales.
- Desarrollar un modelo cuantitativo de reducción de riesgos, que permita medir el efecto de la implementación de controles de seguridad sobre los niveles de riesgo identificados y demostrar el retorno de inversión en ciberseguridad industrial.

- Extender la aplicación del modelo a organizaciones de mayor tamaño y múltiples sitios industriales, con el propósito de validar su escalabilidad y adaptabilidad en infraestructuras OT más complejas.
- Profundizar en la evaluación técnica de arquitecturas de red industrial, considerando protocolos como Modbus/TCP, EtherNet/IP, Profinet, OPC UA y DNP3, así como mecanismos de segmentación, microsegmentación y Zero Trust para entornos OT.
- Investigar el impacto de incidentes de ciberseguridad OT desde una perspectiva operacional, ambiental y de seguridad humana, permitiendo incorporar métricas de consecuencias más allá de la disponibilidad tecnológica.
- Integrar capacidades de detección basadas en inteligencia artificial y aprendizaje automático, orientadas a la identificación temprana de anomalías en redes y activos industriales.
- Desarrollar una matriz RACI especializada para programas de ciberseguridad OT, definiendo claramente roles y responsabilidades entre áreas de ingeniería, operaciones, tecnología, ciberseguridad, calidad y alta dirección.
- Construir un modelo nacional de madurez de ciberseguridad OT para Costa Rica, alineado con la Estrategia Nacional de Ciberseguridad y adaptado a sectores críticos como biotecnología, energía, manufactura, agua y transporte.

7. Conclusiones

El desarrollo de esta investigación permitió diseñar un modelo de evaluación de la postura de ciberseguridad y gestión de vulnerabilidades para entornos de Tecnología Operacional (OT) del sector biotecnológico, integrando COBIT 2019, NIST CSF 2.0 Manufacturing Profile, NIST SP 800-82 Rev. 3 e ISA/IEC 62443. La propuesta facilitó la identificación de procesos, activos y controles de ciberseguridad presentes en la organización, así como la determinación de su nivel de madurez mediante la aplicación de métricas e indicadores alineados con las mejores prácticas internacionales. Los resultados evidenciaron la existencia de activos críticos, vulnerabilidades asociadas y diversas brechas relacionadas con gobernanza, gestión de riesgos, monitoreo continuo y gestión de vulnerabilidades.

Asimismo, el análisis realizado permitió determinar que la organización presenta un nivel de madurez inferior al deseado en varios de los dominios evaluados, lo que evidencia la necesidad de fortalecer sus capacidades de ciberseguridad industrial. La integración de COBIT 2019 y NIST CSF 2.0 demostró ser una base sólida para evaluar tanto los aspectos estratégicos como los operativos de los sistemas OT, permitiendo desarrollar un modelo estructurado, adaptable y medible que facilite la identificación de brechas, la priorización de

acciones correctivas y la definición de una hoja de ruta orientada a la mejora continua de la postura de ciberseguridad y la gestión de vulnerabilidades en organizaciones del sector biotecnológico.

8. Recomendaciones

- Fortalecer el modelo mediante la integración del NIST Risk Management Framework (RMF)
- Incorporar mecanismos de automatización para la evaluación continua
- Adaptar la metodología de valoración de vulnerabilidades al contexto OT
- Desarrollar un modelo cuantitativo de reducción de riesgos
- Ampliar la aplicación del modelo a organizaciones de mayor escala
- Incorporar un análisis técnico profundo de arquitecturas y comunicaciones industriales
- Incorporar escenarios de impacto operacional, ambiental y de seguridad
- Desarrollar una matriz RACI para la gestión de ciberseguridad OT
- Implementar monitoreo continuo de madurez
- Incorporar inteligencia de amenazas específica para OT

9. Bibliografía

Delfino. (2025). *Asegurando la infraestructura crítica en Costa Rica: por qué se requiere una defensa informada ante las amenazas*. Recuperado de https://delfino.cr/2025/08/asegurando-la-infraestructura-critica-en-costa-rica-por-que-se-requiere-una-defensa-informada-ante-las-amenazas

Cybersec Cluster. (s. f.). *Ciberseguridad en Costa Rica: panorama, retos y oportunidades*. Recuperado de https://cybersecclustercr.org/ciberseguridad-en-costa-rica-panorama/

Industrial Cyber. (2022). *NIST SP 800-82 aborda la seguridad de los sistemas OT, incluidos requisitos únicos de rendimiento, confiabilidad y seguridad.* Recuperado de https://industrialcyber-co.translate.goog/analysis/nist-sp-800-82-addresses-ot-systems-security-including-unique-performance-reliability-safety-requirements/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=sge

Forbes México. (2022). *Costa Rica sufre ciberataque que paraliza aduanas y sitios web para pago de impuestos*. Recuperado de https://forbes.com.mx/costa-rica-sufre-ciberataque-que-paraliza-aduanas-y-sitios-web-para-pago-de-impuestos/

National Institute of Standards and Technology. (2023). *Guide to Operational Technology (OT) Security.* Recuperado de https://csrc.nist.gov/pubs/sp/800/82/r3/final

National Institute of Standards and Technology. (2026). *Manufacturing Sector.* Recuperado de https://www.nist.gov/itl/smallbusinesscyber/guidance-sector/manufacturing-sector

National Institute of Standards and Technology. (2025). *Cybersecurity Framework 2.0 Manufacturing Profile*. Recuperado de https://csrc.nist.gov/pubs/ir/8183/r2/ipd

IBM. (s.f.). *¿Qué es la industria 4.0?.* Recuperado de https://www.ibm.com/es-es/think/topics/industry-4-0

ISA. (s.f.) *ISA/IEC 62443.* Recuperado de https://isagca-org.translate.goog/isa-iec-62443-standards?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Fortinet. (s.f). *Norma IEC 62443.* Recuperado de https://www.fortinet.com/lat/resources/cyberglossary/iec-62443

Gedeth Network. (2025). *Panorama económico y sectores clave de Costa Rica.* Recuperado de https://gedeth-com.translate.goog/blog/2025/04/07/costarica-economy-overview-and-key-sectors/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Lindemulder, G et al. (2024). *¿Qué es la ciberseguridad?* Recuperado de *https://www.ibm.com/es-es/think/topics/cybersecurity*

Bowman, k. (2025). *Amenaza vs Vulnerabilidad vs Riesgo: ¿Cuáles son las diferencias?* Recuperado de https://pathlock-com.translate.goog/learn/threat-vs-vulnerability-vs-risk-what-are-differences/?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Bitsight. (2025). *Tecnología Operativa (TO).* Recuperado de https://www-bitsight-com.translate.goog/glossary/operational-technology-ot?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

IT Governance. (s.f). *Estándares y marcos de ciberseguridad.* Recuperado de https://www-itgovernanceusa-com.translate.goog/cybersecurity-standards?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=tc

Gutiérrez, N. (2025). *Marcos de ciberseguridad: guía completa para empresas.* Recuperado de https://preyproject.com/es/blog/marcos-de-ciberseguridad-la-guia-definitiva

IBM. (s.f). *¿Cuál es el marco de ciberseguridad del NIST?* Recuperado de https://www.ibm.com/mx-es/think/topics/nist

Beltán, G. et al. (2021). *¿Qué es la industria 4.0? Elementos clave de la industria 4.0.* Recuperado de https://tecnotrend.lasallebajio.edu.mx/?p=104

GlobalSuite. (2023). *Estándares y normas ISO para mejorar la ciberseguridad.* Recuperado de https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/

Villamizar, C. (2023). *¿Qué es NIST Cybersecurity Framework?* Recuperado de *https://www.globalsuitesolutions.com/es/que-es-nist-cibersecurity-framework/*

Tsungmay,T. & Tanimoto, S. (2023). *A Preliminary Risk Assessment for Operational Technology Systems.* Recuperado de *http://ww.w.bncss.org/index.php/bncss/article/view/163*

Karkoszka, T. (2023). *Operational Control Model Based on Integrated Failure Analysis and Risk Assessment in Sustainable Technological Processes.* Recuperado de https://www.mdpi.com/2071-1050/15/24/16848

Stouffer, K., Pease, M., Tang, C., et al. (2023). *Guide to Operational Technology (OT) Security.* Recuperado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

Kapoor, S., Kumar, S. & Vardhan, H. (2025). *Cyber security of OT networks: A tutorial and survey.* Recuperado de https://arxiv.org/pdf/2502.14017

Solms, S. & Toit, J. (2024). *Cybersecurity Governance in the Medical Ecosystem: An Orientation Guide with Specific Reference to the Merging of IT and OT Devices.* Recuperado de https://books.google.co.cr/books?hl=es&lr=&id=fEYOEQAAQBAJ&oi=fnd&pg=PA402&dq=OT+security+governance&ots=q4gvlBXHbJ&sig=B8ZTQQaLo6bfNgdi_uG29y3NyNo&redir_esc=y#v=onepage&q=OT%20security%20governance&f=false

César, A. (2023). *¿Qué es COBIT y para qué sirve?* Recuperado de https://www.globalsuitesolutions.com/es/que-es-cobit/

Instituto nacional de Estándares y Tecnología. (2024). *El Marco de Seguridad Cibernética (CSF) 2.0 del NIST.* Recuperado de https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.spa.pdf

MiraSecIndustrial. (2025). *Modelo Purdue en redes industriales: la clave para cumplir con NIS2 y proteger tu producción.* Recuperado de Modelo Purdue en redes industriales: la clave para cumplir con NIS2 y proteger tu producción | MiraSec Industrial