Riesgos de Ciberataques y Protección de Activos Críticos en Redes OT del Sector Cervecero Mediante un SOC en Colombia

Helmer Arturo Montealegre Garzón

Asesor

Edgar Roberto Dulce Villarreal

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2025

Agradecimientos

Primero que nada, quiero expresar mi más profundo agradecimiento a todas las personas que me han acompañado a lo largo de este enriquecedor viaje académico. Sin el apoyo, amor y confianza de las personas que mencionaré a continuación, no habría sido posible llegar a este Éxito. Cada uno de ustedes ha jugado un papel fundamental en mi vida, y es un honor dedicarles este espacio.

Arturo, estoy supremamente orgulloso de este significativo paso, me llena de alegría superarme y sobre todo cumplir metas, hoy me agradezco cada esfuerzo, cada reto, cada proyecto y cada paso que he dado para hoy poder estar escribiendo estas palabras; hoy miro hacia atrás y debo reconocer que he avanzado significativamente y aunque no estoy donde quiero, estoy dando los pasos indicados en el camino correcto, un logro más que comprueba que las metas si son alcanzables si te lo propones, un logro que comprueba que el amor por lo que te gusta y apasiona, siempre te llevará lejos.

Mis padres, Alfonso y Matha, les agradezco todo. Ustedes son mi mayor fuente de inspiración y motivación desde que tengo uso de razón; gracias por su incansable esfuerzo para brindarme educación, por sus esfuerzos, por su paciencia infinita y por enseñarme que, con esfuerzo y dedicación, todo es posible.

Sus palabras de aliento y sus ejemplos de vida me han motivado para continuar cuando las dificultades o los retos parecían insuperables. Hoy que estoy aquí, con este proyecto en mis manos, es gracias a su amor, y a su confianza incondicional en mí, incluso en los momentos en los que yo llegué a dudar de mis capacidades; cada paso que doy es, en parte, un reflejo del ejemplo que me han dado. Los amo profundamente y me siento afortunado de ser su hijo Este logro es también es de ustedes

Samantha, quiero dedicarte estas palabras con todo mi amor. Eres mi mayor fuente de alegría e inspiración, la razón por la que siempre me esfuerzo por ser mejor a diario. Aunque este camino me haya llevado mucho tiempo y esfuerzo, cada minuto lejos de ti ha sido compensado por tu sonrisa, tus miradas, tus abrazos y la forma en que iluminas mi vida con tu presencia. Gracias por ser tan comprensiva y empática cuando los estudios y otras obligaciones me exigían tiempo y por darme tu apoyo incondicional; siempre recordaré esos momentos en los que, con tu ternura e inocencia, me recordabas lo importante que es disfrutar de la vida, incluso en medio de los desafíos. Este logro es de los dos, me siento profundamente agradecido y orgulloso por tenerte como mi hija. Te amo con mi vida y este trabajo es un reflejo del amor que compartimos.

Finalmente, quiero dedicar unas palabras especiales a una de las redes de apoyo más significativas en mi vida: mi familia Netmask. En este recorrido académico, he tenido el privilegio de ser parte de un grupo de personas que no solo comparten intereses profesionales, sino también valores, respeto, compañerismo mutuo y, sobre todo, una amistad genuina. A cada miembro de esta "familia" que me ha apoyado quiero expresarles mi más sincero agradecimiento.

A todos ustedes, mis padres, mi hija, y Netmask, les dedico este trabajo con el corazón lleno de gratitud y alegría. Sin ustedes, este proyecto no habría sido posible, y la vida misma que se vuelve una marea espesa como el mar, sería mucho más compleja de navegar. Gracias por ser mi motivación, mi familia, mi refugio y mi fuente de energía. Este logro, sin duda, es el reflejo de la fuerza, el amor, la comprensión y compañía que me brindan a diario.

Dedicatoria

Al concluir esta especialización, no puedo dejar de reflexionar sobre el arduo camino que he recorrido, lleno de desafíos, aprendizajes y momentos de superación. Este logro no sería posible sin mi tenacidad, mi resiliencia, mis ganas de superarme y sin el apoyo incondicional de mis seres queridos, quienes me han acompañado a lo largo de este proceso y han sido apoyo fundamentales para que hoy pueda decir con orgullo que he alcanzado este objetivo.

En este tipo de escritos siempre solemos agradecer y dedicar nuestro esfuerzo a nuestro entorno y a terceras personas que si bien, son supremamente importantes en nuestras vidas juegan un papel tercero en este, el mayor y gran esfuerzo que realizamos al querer superarnos cómo personas; cómo seres humanos y por supuesto como profesionales.

Hoy quiero dedicarme este espléndido proyecto que es un triunfo más, quiero agradecerme por las veces que lo intenté aún sin tener ganas de hacerlo, por las madrugadas, por las trasnochadas, por las veces que dejé todo de lado para cumplirme con este, mi proyecto más grande, me doy las gracias por mi esfuerzo y dedicación a este arduo trabajo y esta larga siembra que hoy está dando frutos, me agradezco por mi esfuerzo y superación y primordial por mantener mi foco.

Mi entorno en este proceso ha sido muy importante, por eso quiero dedicar este triunfo a mi persona favorita, ¡mi hija Samantha! Ella es el motor que impulsa este gran sueño, la inspiración que tiene mi ser y la motivación que me levanta a diario para querer ser mejor ser humano, gracias por comprender las veces que he tenido que estudiar o trabajar, sacrificando nuestros espacios y nuestro tiempo juntos, gracias por tu comprensión y por tu compañía. Aquí está el resultado de esos espacios que me partían en dos por cumplir con mi responsabilidad y mi

sueño, solo deseo con mi alma y mi corazón; estés muy orgullosa de mí, cómo yo lo estoy de ti, te dedico este y cada uno de mis logros mi Samy.

Mis padres Alfonso y Martha, son una pieza fundamental de todo este proceso, han sido motivación e inspiración hoy quiero que se sientan orgulloso de su hijo, de éste que lejos de casa está dando su cien y más, para superarse a diario, quiero llenarles de orgullo por mi logro y quiero que sepan que estoy inmensamente agradecido por su esfuerzo y dedicación con los pilares de mi educación, los que me han traído a querer y lograr escalar esta montaña, que si bien no ha sido fácil está siendo muy satisfactorio el querer escalar la sima, gracias papá, gracias mamá por apoyarme y por sobre todo, darme ánimo cuando lo necesité.

Mi dedicatoria es por mi esfuerzo y por superarme al querer y poder lograrlo.

Resumen

Este proyecto aborda el diseño e implementación de un Centro de Operaciones de Seguridad (SOC) especializado en redes de tecnología operacional (OT) para la industria cervecera en Colombia, con el objetivo de mejorar la detección, análisis y respuesta ante ciberataques dirigidos a activos críticos industriales. Dado el incremento de amenazas cibernéticas en infraestructuras industriales, particularmente en ambientes convergentes TI-OT, se realiza un análisis profundo de vulnerabilidades en redes OT, utilizando el modelo Purdue para la segmentación y clasificación de niveles de control industrial.

Se evalúa el impacto potencial de ataques cibernéticos sobre sistemas SCADA, PLC y HMI, componentes esenciales para la operación de procesos productivos en plantas cerveceras, mediante metodologías de análisis de riesgo reconocidas. Con base en estos resultados, se diseña una propuesta de SOC que integra soluciones tecnológicas Fortinet especializadas en seguridad OT, que incluyen segmentación avanzada, sistemas de detección de intrusos (IDS), autenticación multifactor y monitoreo continuo.

La propuesta contempla además aspectos organizacionales, como la definición de roles y procesos para la gestión efectiva de incidentes, y métricas para medir el tiempo de respuesta y efectividad del SOC. Se emplean estándares internacionales como el NIST Cybersecurity Framework 2.0 para asegurar la alineación con mejores prácticas y normativas vigentes.

Los resultados demuestran que la implementación del SOC especializado incrementa significativamente la resiliencia frente a ciberataques, minimizando el riesgo de interrupciones operativas y pérdidas económicas en la industria cervecera colombiana. Esta investigación contribuye a cerrar la brecha de seguridad en redes OT del sector, proporcionando una guía práctica y escalable para la protección de infraestructuras críticas en entornos industriales.

Palabras Clave: Ciberseguridad, Redes OT, Operaciones, Industria, cervecera

Abstract

This thesis addresses the design and implementation of a Security Operations Center (SOC) specialized in Operational Technology (OT) networks for the Colombian brewing industry. Its aim is to enhance the detection, analysis, and response to cyberattacks targeting critical industrial assets. Given the increasing cyber threats to industrial infrastructures, particularly in converged IT-OT environments, a deep vulnerability analysis of OT networks is conducted, utilizing the Purdue model for the segmentation and classification of industrial control levels.

The potential impact of cyberattacks on SCADA, PLC, and HMI systems—essential components for the operation of production processes in brewing plants—is evaluated using recognized risk analysis methodologies. Based on these findings, an SOC proposal is designed, integrating Fortinet technological solutions specialized in OT security. These solutions include advanced segmentation, intrusion detection systems (IDS), multifactor authentication, and continuous monitoring.

The proposal also considers organizational aspects, such as the definition of roles and processes for effective incident management, and metrics to measure the SOC's response time and effectiveness. International standards like the NIST Cybersecurity Framework 2.0 are employed to ensure alignment with best practices and current regulations.

The results demonstrate that the implementation of the specialized SOC significantly increases resilience against cyberattacks, minimizing the risk of operational disruptions and economic losses in the Colombian brewing industry. This research contributes to closing the security gap in the sector's OT networks, providing a practical and scalable guide for protecting critical infrastructures in industrial environments.

Tabla de Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

La importancia de la seguridad de redes operacionales en las industrias productoras en Colombia es esencial y especialmente crítica con la llegada de la cuarta revolución industrial, donde la tecnología de la información y la automatización de procesos tiene una sólida base en la infraestructura de las empresas y las industrias, y a su vez el desarrollo de las soluciones tecnológicas para este fin presenta complicaciones al momento de normativas regulatorias en este sentido a nivel global. Adicionalmente, no se evidencian estudios en el país referentes al desarrollo comercial tecnológico y a los problemas funcionales generados por la inseguridad de las redes.

Debido a lo anterior, se justifica la importancia de implementar redes seguras en OT dentro de los objetivos principales de las industrias productoras en el país, mediante el desarrollo de la presente investigación, con el fin de tener un referente en Colombia de la realidad de la seguridad de redes OT. La seguridad de las redes es aún un problema difícil incluso después de varias décadas de investigación; en última instancia, la dificultad al abordar el problema viene dada por el hecho que la seguridad es un concepto difuso y la diferenciación entre seguridad perfecta e inseguridad total es muy tenue. Adicionalmente, se considera un entorno muy avanzado en los protocolos de esta tecnología, lo cual no lo hace menos frágil frente a los riesgos que representa estar expuesto, íntimamente relacionado el origen de esto con la ciberdelincuencia, puesto que los ciberdelincuentes aprovechan las vulnerabilidades de los sistemas de control industriales para provocar incidentes cibernéticos, o bien, explotarlas o generar actividades malintencionadas u otros ilícitos.

Planteamiento del Problema

¿Cómo puede la implementación de un SOC mejorar la protección de activos críticos frente a ciberataques en redes OT del sector cervecero colombiano?

A pesar del avance tecnológico en el sector cervecero colombiano, se ha identificado una falta de preparación frente a amenazas cibernéticas que afectan redes OT. Las empresas del sector suelen centrar sus esfuerzos en proteger redes de TI (Tecnología de la Información), descuidando la protección de sistemas industriales que operan procesos críticos como fermentación, embotellado o control de calidad.

Esta situación se agrava por la ausencia de SOCs adaptados al entorno OT, que permitan monitorear de forma continua los eventos y vulnerabilidades específicas de estos sistemas. Como resultado, las cerveceras quedan expuestas a posibles ciberataques que podrían interrumpir su producción, alterar fórmulas de productos o generar fallas en la cadena de suministro.

Estudios como los de Dragoni et al. (2021) muestran que más del 60% de incidentes en entornos industriales no son detectados a tiempo, y el sector de alimentos y bebidas figura entre los más vulnerables. En Colombia, los reportes de la CRC (2023) indican un crecimiento sostenido en ataques dirigidos a infraestructuras críticas, sin que exista una estrategia clara de defensa cibernética en la industria cervecera.

Justificación

La ciberseguridad industrial se ha convertido en una prioridad estratégica para garantizar la continuidad operativa y la resiliencia de las organizaciones frente a amenazas digitales (National Institute of Standards and Technology, 2024). En el sector cervecero colombiano, la digitalización de procesos ha expuesto a las empresas a nuevas vulnerabilidades que requieren medidas proactivas de mitigación (López & Santoyo, 2022).

Este estudio es relevante porque aborda una problemática poco explorada en el contexto nacional: la protección de redes OT en la industria cervecera mediante un SOC. A diferencia de los sistemas tradicionales de monitoreo, un SOC adaptado a OT ofrece capacidades especializadas para detectar intrusiones, comportamientos anómalos y ataques dirigidos a sistemas industriales (ISA, 2020).

Además, la Comisión de Regulación de Comunicaciones (CRC, 2023) ha señalado un incremento sostenido en ciberataques a infraestructuras críticas en Colombia, lo cual resalta la necesidad de estrategias especializadas de defensa. La implementación de un SOC no solo mejora la capacidad de respuesta ante incidentes, sino que permite una gestión integral del riesgo tecnológico.

Este proyecto, por tanto, aporta a la sostenibilidad tecnológica de un sector clave para la economía nacional, alineándose con las buenas prácticas promovidas por entidades internacionales como el NIST y la ISA/IEC 62443.

Objetivos

Objetivo General

Analizar los riesgos de ciberataques en redes OT del sector cervecero colombiano ante el panorama de amenazas actual, identificando y evaluando críticamente sus vulnerabilidades, con el fin de fortalecer su ciberseguridad y proponer un Centro de Operaciones de Seguridad (SOC) como estrategia integral para la protección de sus activos operativos.

Objetivos Específicos

Analizar las vulnerabilidades de seguridad cibernética más prevalentes en las redes de Tecnología Operacional (OT) de empresas del sector cervecero en Colombia, durante el período 2024-2025, con el fin de proponer estrategias de mitigación.

Evaluar el impacto potencial de ciberataques sobre activos críticos (SCADA, PLC, HMI) en procesos de producción de plantas cerveceras colombianas, aplicando metodologías de análisis de riesgo, durante año 2025, para establecer prioridades de protección.

Diseñar una propuesta de SOC especializado en OT, integrando soluciones Fortinet, para la industria cervecera colombiana, a ser presentada a finales del año 2025, con el fin de mejorar la detección y respuesta a ciberataques.

Marco Referencial

Antecedentes

La creciente digitalización de procesos industriales ha expuesto a múltiples sectores, incluyendo el cervecero, a riesgos cibernéticos cada vez más sofisticados. Las redes de Tecnología Operativa (OT), tradicionalmente aisladas, han sido integradas con sistemas de Tecnología de la Información (TI), generando nuevos vectores de ataque (Piggin, 2013). Esta convergencia ha generado preocupación por la protección de los activos críticos que sostienen los procesos de producción y distribución de las empresas manufactureras, incluyendo las del sector cervecero.

Diversos estudios han abordado el diseño e implementación de Centros de Operaciones de Ciberseguridad (SOC) como mecanismos clave para la detección y respuesta ante amenazas en entornos industriales. Bernal Mora (2024) desarrolló una propuesta de SOC basada en la norma ISO/IEC 27001, aplicada en el sector salud, resaltando su capacidad para mitigar riesgos relacionados con la confidencialidad, integridad y disponibilidad de los datos. Por su parte, Fole de Navia de la Cruz (2024) exploró un enfoque automatizado para el despliegue y escalado de un SOC, lo que resulta particularmente relevante para empresas con infraestructura crítica distribuida, como es el caso de muchas cerveceras con plantas, centros logísticos y canales de venta interconectados.

A nivel de gestión del riesgo, (Cordero-Robles, 2021) propuso un conjunto de herramientas basado en el NIST Cybersecurity Framework para mejorar las evaluaciones de riesgo cibernético, enfatizando la necesidad de metodologías adaptables a contextos específicos. Cruz Villón (2023), por su parte, aplicó la norma ISO 31000:2018 para formular planes de

acción en empresas de seguridad física, lo cual resulta extrapolable a empresas industriales que requieren planes robustos para enfrentar amenazas cibernéticas.

Pese al avance en este tipo de investigaciones, se identifica una escasa documentación sobre la implementación de SOC en industrias alimentarias específicas como la cervecera en el contexto colombiano. Esta ausencia justifica el desarrollo del presente trabajo, que busca fortalecer la seguridad de las redes OT en este tipo de entornos mediante el diseño estratégico de un SOC.

Marco Conceptual

Redes OT (Operational Technology)

Las redes OT son aquellas que controlan dispositivos físicos en entornos industriales, como sensores, actuadores, sistemas SCADA, PLCs y HMIs. Su función es permitir el monitoreo y control de procesos productivos en tiempo real (Piggin, 2013).A diferencia de las redes TI, que se enfocan en el procesamiento y almacenamiento de información, las OT están diseñadas para garantizar continuidad operativa y seguridad física.

Ciberseguridad Industrial

La ciberseguridad industrial comprende el conjunto de políticas, tecnologías y prácticas orientadas a proteger la integridad de los sistemas industriales frente a amenazas digitales. Esta disciplina ha ganado relevancia ante la digitalización de procesos industriales y la creciente convergencia TI/OT. El estándar IEC 62443, propuesto por (Piggin, 2013), establece lineamientos específicos para asegurar infraestructuras críticas en entornos como plantas de producción.

Centro de Operaciones de Ciberseguridad (SOC)

Un SOC es una unidad encargada de la monitorización, detección, análisis y respuesta a incidentes de ciberseguridad dentro de una organización. Según Bernal Mora (2024), su diseño debe alinearse a marcos normativos como ISO/IEC 27001 y debe incorporar capacidades de automatización, correlación de eventos y personal especializado. Fole de Navia de la Cruz (2024) complementa que el uso de herramientas escalables permite gestionar ambientes con alta demanda como los industriales.

Gestión de Riesgos Cibernéticos

La gestión de riesgos cibernéticos es el proceso mediante el cual se identifican, evalúan y tratan amenazas que pueden afectar los activos tecnológicos de una organización. (Cordero-Robles, 2021) destaca el uso del NIST Cybersecurity Framework como herramienta eficaz para evaluar madurez y priorizar controles de seguridad. En el mismo sentido, Cruz Villón (2023) resalta la aplicación de la norma ISO 31000:2018 como base para elaborar planes de acción frente a riesgos identificados.

Activos Críticos

Son aquellos recursos cuya pérdida, alteración o indisponibilidad puede comprometer la continuidad operativa o generar impactos financieros, legales o reputacionales. En el sector cervecero, los activos críticos incluyen sistemas de control de calidad, plantas de producción automatizadas, y plataformas de distribución digital.

Transformación Digital en la Industria Cervecera

La transformación digital ha impulsado al sector cervecero a integrar tecnologías como IoT, sistemas ERP y plataformas cloud en sus procesos de producción y distribución (Castellanos Reyes, 2018). Esta evolución, aunque eficiente, ha incrementado los riesgos de exposición a amenazas cibernéticas que requieren estrategias de defensa más robustas, como un SOC especializado en entornos OT.

Marco Teórico

La creciente digitalización y automatización de procesos industriales ha generado un entorno de vulnerabilidad en las redes de tecnología operacional (OT), particularmente en sectores críticos como el cervecero. Las redes OT, que tradicionalmente eran sistemas aislados y específicos, hoy están cada vez más interconectadas con redes de tecnología de la información (TI), exponiéndolas a ciber amenazas similares a las de cualquier infraestructura informática convencional (Piggin, 2013) .

Uno de los elementos fundamentales para abordar estos riesgos es la implementación de un Centro de Operaciones de Ciberseguridad (SOC). Un SOC actúa como un núcleo centralizado donde se supervisan, detectan, analizan y responden a incidentes de seguridad cibernética, proporcionando una vigilancia constante sobre la infraestructura crítica de una organización (Bernal Mora, 2024).

La literatura especializada destaca que los ataques cibernéticos en redes OT pueden tener consecuencias devastadoras, desde la interrupción de operaciones hasta el daño físico de equipos, pérdidas económicas y afectaciones reputacionales Cordero-Robles, (2021). En particular, el sector cervecero, al depender de procesos automatizados para producción, envasado y distribución, requiere una estrategia robusta de ciberseguridad.

La integración de un SOC en entornos OT implica diversos desafíos. En primer lugar, la necesidad de contar con personal capacitado para interpretar los datos de seguridad generados por sistemas industriales. En segundo lugar, se debe considerar la compatibilidad entre herramientas TI y protocolos OT, como Modbus, DNP3 o OPC-UA, lo que dificulta la implementación de soluciones estándar (Fole de Navia de la Cruz, 2024).

Además, marcos de trabajo como el NIST Cybersecurity Framework ofrecen una guía estructurada para la gestión de riesgos cibernéticos en infraestructuras críticas, apoyando tanto el diagnóstico como el diseño de planes de acción que involucren un SOC (NIST, 2018). La norma IEC 62443 también proporciona estándares específicos para proteger los sistemas de control industrial, siendo una referencia clave para los profesionales de ciberseguridad OT (Piggin, 2013).

Finalmente, autores como Castellanos Reyes (2018) y Cruz Villón (2023) coinciden en que la planificación estratégica de la seguridad cibernética debe alinearse con los objetivos de transformación digital de las organizaciones, especialmente cuando estas dependen de activos críticos automatizados para su operación y competitividad.

Marco Legal

La protección de infraestructuras críticas en Colombia, especialmente en sectores industriales como el cervecero, ha adquirido un papel fundamental dentro de las políticas de seguridad nacional. La regulación legal relacionada con la ciberseguridad en entornos industriales se fundamenta en diversas leyes, decretos y normas internacionales que establecen los principios para garantizar la confidencialidad, integridad y disponibilidad de los activos digitales y operacionales.

Una de las normativas más relevantes es la Ley 1273 de 2009, mediante la cual se modifica el Código Penal Colombiano para tipificar los delitos informáticos y proteger la información y los datos. Esta ley representa un paso importante hacia el reconocimiento jurídico de la ciberseguridad como un componente esencial para la estabilidad operativa en sectores económicos críticos como el alimentario y cervecero (*Ley 1273 de 2009 - Gestor Normativo*, s. f.).

Adicionalmente, la Ley 1581 de 2012 establece disposiciones generales para la protección de datos personales, lo cual es clave para garantizar que la información sensible manejada por sistemas SCADA y OT sea tratada de forma adecuada.

En el plano internacional, la serie de normas IEC 62443 resulta fundamental para la protección de sistemas de control industrial. Esta normativa define requisitos de seguridad para todo el ciclo de vida de los sistemas de automatización, incluyendo la segmentación de redes, control de accesos y gestión de incidentes (Piggin, 2013). Su aplicación en la industria cervecera garantiza estándares mínimos para mitigar riesgos de ciberataques que afecten los procesos de producción y distribución.

A nivel de gestión de riesgos, la ISO/IEC 27001 y la ISO 31000:2018 son normas ampliamente aceptadas que permiten establecer políticas y procedimientos para proteger la infraestructura tecnológica mediante un enfoque sistemático de mejora continua (Cruz Villón, 2023; Bernal Mora, 2024). La implementación de un Centro de Operaciones de Seguridad (SOC) bajo estas normas facilita una vigilancia constante de los eventos de seguridad y permite la toma de decisiones informadas ante amenazas potenciales.

De esta manera, el marco legal vigente proporciona tanto las herramientas como los lineamientos para que organizaciones del sector cervecero desarrollen políticas de ciberseguridad robustas, alineadas con estándares nacionales e internacionales, asegurando así la continuidad operativa de sus redes OT.

Marco Contextual

Este trabajo se enmarca en la realidad del sector cervecero colombiano, un segmento industrial de gran dinamismo económico y con alto grado de tecnificación en sus procesos. En los últimos años, esta industria ha adoptado de forma progresiva tecnologías operacionales (OT) para automatizar y optimizar su cadena productiva, integrando sistemas de control industrial como SCADA, PLCs y DCS. Esta evolución ha mejorado la eficiencia y trazabilidad de la producción, pero también ha introducido nuevos desafíos en términos de seguridad cibernética.

La transformación digital impulsada por la Industria 4.0 ha potenciado la interconectividad entre sistemas, facilitando la recolección y análisis de datos en tiempo real, el monitoreo remoto y la toma de decisiones automatizadas. En el caso del sector cervecero, empresas colombianas han comenzado a implementar tecnologías como sensores inteligentes, controladores remotos y plataformas digitales para gestionar procesos críticos, desde la fermentación hasta la logística de distribución (Impacto TIC, 2024). No obstante, esta integración entre sistemas de tecnología de la información (IT) y tecnología operacional (OT) ha generado una superficie de ataque más amplia para amenazas cibernéticas, incrementando el riesgo de incidentes que podrían afectar no solo la información corporativa, sino también la continuidad del servicio, la calidad del producto y la seguridad física de los operarios (Cordero-Robles, 2021; Fole de Navia de la Cruz, 2024).

Aunque en Colombia existen esfuerzos gubernamentales e institucionales para fortalecer la ciberseguridad en infraestructuras críticas, la protección de entornos industriales como el cervecero aún presenta brechas importantes. En particular, se observa una limitada implementación de Centros de Operaciones de Seguridad (SOC) con capacidad para monitorear, detectar y responder a amenazas en entornos OT. Este vacío representa un riesgo considerable,

ya que los ciberataques a infraestructuras industriales no solo buscan acceso a la información, sino que pueden tener impactos físicos directos, incluyendo la paralización de procesos o la alteración de parámetros operativos clave (Piggin, 2013).

Frente a este panorama, la presente investigación busca analizar los riesgos de ciberataques en entornos OT del sector cervecero y proponer una estrategia de protección mediante la implementación de un SOC adaptado a las particularidades de este tipo de infraestructura. Esta propuesta se apoya en marcos normativos y arquitecturas reconocidas internacionalmente, como el NIST, la norma ISA/IEC 62443 y el Modelo Purdue, el cual establece una estructura jerárquica para dividir los procesos industriales en niveles funcionales, facilitando la implementación de controles de seguridad específicos para cada capa del sistema (Instituto Nacional de Ciberseguridad de España [INCIBE], 2019). (Instituto Nacional de Ciberseguridad de España, 2019)

Diseño Metodológico

La presente investigación es de tipo descriptivo con enfoque cualitativo, ya que busca caracterizar los riesgos cibernéticos en las redes OT del sector cervecero colombiano y proponer estrategias de mitigación mediante la implementación de un Centro de Operaciones de Seguridad (SOC). La metodología utilizada se fundamenta en la recolección, análisis e interpretación de información documental especializada y normativa vigente.

Para el logro de los objetivos propuestos, se realizó una revisión bibliográfica y documental sistemática, utilizando bases de datos académicas como Scopus, IEEE Xplore, Scielo y Google Scholar, así como informes técnicos de entidades como NIST, ISA y la Comisión de Regulación de Comunicaciones (CRC). Esta etapa permitió identificar riesgos frecuentes en entornos OT, tipos de ciberataques, buenas prácticas de seguridad industrial y el diseño funcional de un SOC orientado a infraestructuras críticas.

A continuación, se desarrolló un análisis comparativo de casos documentados de ciberseguridad industrial aplicados a sectores productivos similares, enfocándose especialmente en el sector cervecero y de bebidas a nivel regional y nacional (González & Torres, 2021). Se identificaron puntos comunes en las amenazas, niveles de madurez en ciberdefensa y herramientas tecnológicas empleadas.

Finalmente, se propuso un modelo de SOC adaptado a las particularidades de las redes OT en la industria cervecera colombiana. Esta propuesta fue estructurada con base en los lineamientos del marco NIST CSF y los estándares ISA/IEC 62443, adaptándolos a un contexto empresarial con recursos limitados pero alto impacto operativo.

La metodología empleada permite cumplir con los objetivos específicos de manera estructurada y coherente, contribuyendo a la comprensión de la problemática y proponiendo soluciones aplicables al entorno real del sector cervecero.

Analizar las Vulnerabilidades de Seguridad Cibernética más Prevalentes en las Redes de Tecnología Operacional (OT) de Empresas del Sector Cervecero en Colombia, Durante el Período 2024-2025, con el Fin de Proponer Estrategias de Mitigación

El sector cervecero en Colombia se encuentra en una etapa de profunda transformación digital, donde la adopción de la Tecnología Operacional (OT) es crucial para optimizar la eficiencia de la producción, la calidad del producto y la competitividad en un mercado globalizado (Industria de Alimentos y Bebidas, 2023). Desde la automatización de la maltería y el proceso de cocción hasta el envasado y la logística de distribución, las redes OT se han convertido en el corazón de estas operaciones. Sin embargo, esta modernización introduce una superficie de ataque significativamente mayor, exponiendo a las empresas cerveceras a vulnerabilidades de ciberseguridad que podrían tener consecuencias devastadoras, como interrupciones en la producción, pérdida de propiedad intelectual (recetas), daños a la reputación, riesgos para la seguridad de los trabajadores e incluso impactos económicos a nivel nacional (Díaz, 2022).

Este proyecto de grado se centra en analizar las vulnerabilidades de seguridad cibernética más prevalentes en las redes de Tecnología Operacional (OT) de empresas del sector cervecero en Colombia, durante el período 2024-2025, con el propósito fundamental de proponer estrategias de mitigación efectivas. El enfoque temporal (2024-2025) asegura la relevancia de la investigación frente a las amenazas cibernéticas en constante evolución y el actual panorama tecnológico del sector. La identificación de estas vulnerabilidades permitirá a las cervecerías colombianas anticipar y fortalecer sus defensas contra ataques dirigidos a sus procesos críticos.

Para la identificación y clasificación estructurada de las vulnerabilidades en las redes OT del sector cervecero colombiano, esta investigación adopta el Modelo Purdue para el Control

Industrial como su base metodológica. Este modelo, reconocido por su capacidad para jerarquizar la infraestructura industrial, organiza los sistemas en niveles que van desde la interacción física con el proceso (Nivel 0) hasta la planificación de recursos empresariales (Nivel 4). Sin embargo, la creciente convergencia IT/OT en la industria moderna, donde las redes de información corporativas se interconectan cada vez más con los sistemas de control industrial, demanda una visión más amplia (Ciberseguridad en el modelo de Purdue, s. f.).

Por esta razón, la investigación extiende el Modelo Purdue para incluir un "Nivel 5", que corresponde a los sistemas empresariales o IT corporativa (ISA-S95 y IIoT: La potencia sin control, no sirve de nada – ISA Sección Española, s. f.). Esta extensión permite un análisis integral de cómo las vulnerabilidades pueden propagarse desde el entorno IT hacia los sistemas OT, reconociendo que un compromiso en un sistema de correo electrónico (Nivel 5) podría, por ejemplo, facilitar un ataque de phishing dirigido al personal de operaciones, comprometiendo posteriormente un PLC (Nivel 1). Esta segmentación lógica es crucial, ya que facilita la localización de debilidades específicas en cada capa del sistema y una evaluación precisa de los riesgos cibernéticos asociados a cada interacción y componente (National Institute of Standards and Technology, 2024).

La clasificación de las vulnerabilidades a través de este modelo extendido posibilita un análisis sistemático de cómo diversas amenazas cibernéticas desde malware diseñado para ICS hasta accesos no autorizados o errores de configuración pueden afectar los distintos componentes de una red industrial. Esto abarca desde la capa física del proceso (Nivel 0), donde un ataque podría manipular sensores de temperatura en un fermentador, hasta los sistemas corporativos empresariales (Nivel 5), donde un ransomware podría detener las operaciones de facturación y

logística, impactando indirectamente la producción (National Institute of Standards and Technology, 2024).

Adicionalmente, el Modelo Purdue se complementa con la integración de estándares internacionales clave que proporcionan directrices sólidas para la seguridad de infraestructuras críticas industriales, asegurando que las estrategias de mitigación propuestas sean robustas y estén alineadas con las mejores prácticas globales:

ISA-95 (IEC 62264): Este estándar se enfoca en la integración entre los sistemas de control de producción y los sistemas de gestión empresarial (ISA-S95 y IIoT: La potencia sin control, no sirve de nada – ISA Sección Española, s. f.). Para el sector cervecero, es fundamental para comprender cómo los datos fluyen entre la planificación de la producción (Nivel 4), la ejecución de la manufactura (Nivel 3) y los sistemas de control (Nivel 2, 1, 0). Su aplicación en la investigación permitirá identificar vulnerabilidades en las interfaces y protocolos de comunicación que conectan la cadena de suministro con el piso de planta, como por ejemplo, la forma en que las órdenes de producción se traducen en comandos de control.

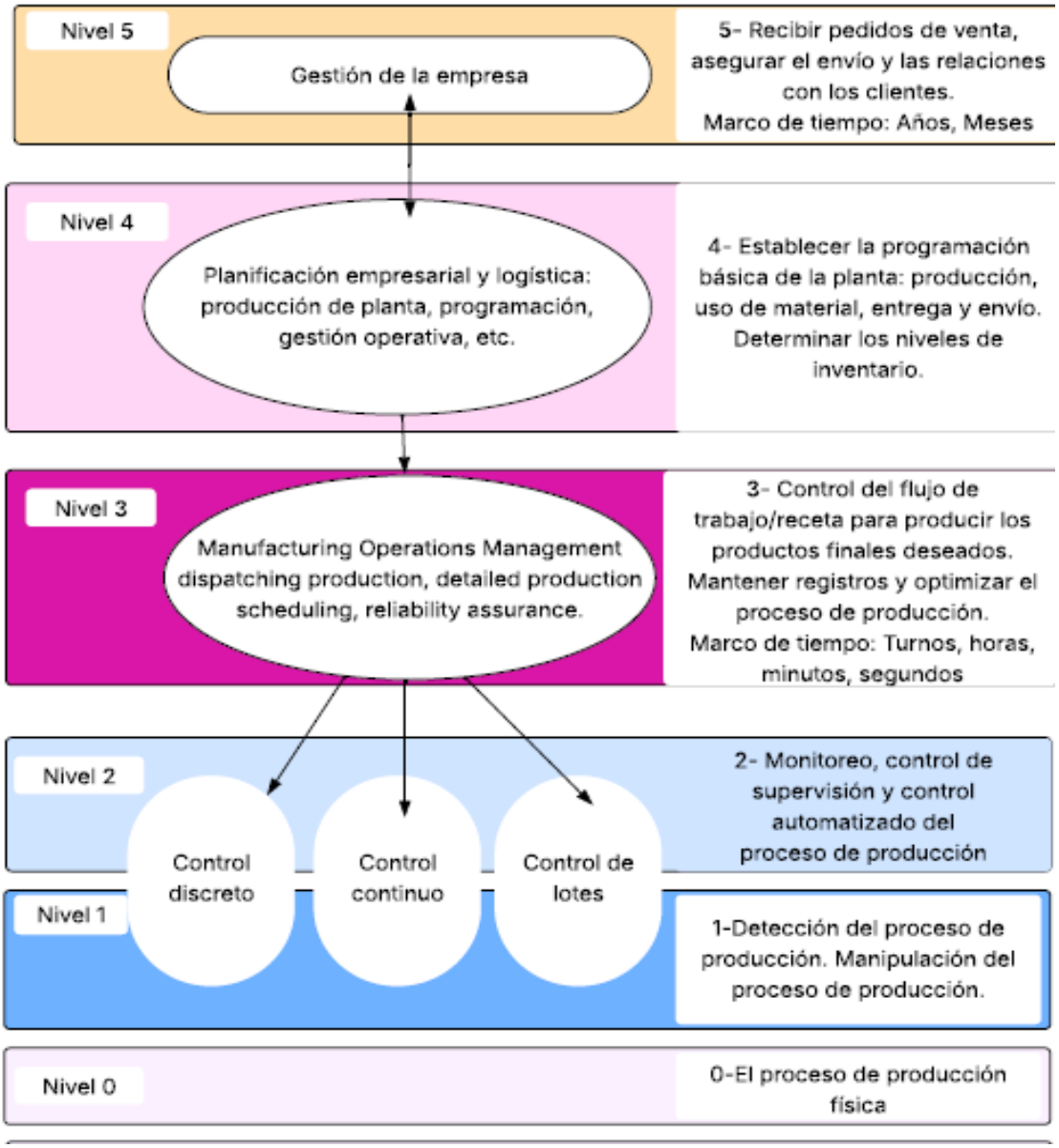
ISA/IEC 62443 (anteriormente ISA99): Esta serie de estándares es un pilar para la ciberseguridad en sistemas de automatización industrial y sistemas de control (IACS) (ISA99, Industrial Automation&Control Sys Security- ISA, s. f.). Proporciona un marco robusto para la evaluación de riesgos, la implementación de contramedidas y el diseño de arquitecturas seguras para los entornos OT. Es vital para definir los niveles de seguridad (SL) necesarios para proteger los equipos críticos de las cervecerías, tales como PLCs y SCADA, asegurando que se implementen controles como la segmentación de red (zonas y conductos) y la gestión de acceso para prevenir la propagación de ataques dentro de la red de producción.

NIST SP 800-82 (Guía de Ciberseguridad para Sistemas de Control Industrial): Publicada por el National Institute of Standards and Technology, esta guía ofrece recomendaciones detalladas y prácticas para la seguridad de los ICS, adaptando los principios de ciberseguridad a las particularidades de los entornos OT (National Institute of Standards and Technology, 2024). Para las empresas cerveceras, esta guía es esencial para implementar controles operativos como la gestión de parches en equipos heredados, la creación de políticas de acceso privilegiado para ingenieros de control y la planificación de la respuesta a incidentes específicos para sistemas OT, asegurando la continuidad de las operaciones frente a las ciberamenazas.

La combinación estratégica del Modelo Purdue extendido con la guía de estos estándares internacionales permitirá a la investigación no solo identificar las vulnerabilidades actuales y emergentes, sino también construir un marco sólido para la formulación de estrategias de mitigación proactivas y sostenibles, específicamente adaptadas a las características operativas y los desafíos de ciberseguridad del dinámico sector cervecero en Colombia (Beyond the Pyramid, s. f.).

Figura 1

El Modelo Funcional ISA95



Nota. La imagen muestra la jerarquía funcional de los sistemas de automatización industrial, siguiendo el modelo Purdue (también conocido como el modelo ISA-95). Este modelo estructura las operaciones industriales en seis niveles (del 0 al 5), diferenciando claramente las responsabilidades de cada uno y su temporalidad operativa. Tomado de. (ISA95, s. f.).

Tabla 1

Correspondencia entre Niveles del Modelo Purdue e ISA

Principales Vulnerabilidades por Nivel

Nivel Purdue	Descripción Funcional	Correspondencia ISA 95 / IT-OT	Vulnerabilidades / Riesgos Comunes
Nivel 5	Gestión empresarial (ERP, CRM, correo, Internet)	Nivel empresarial	Falta de segmentación entre IT/OT, malware (ej. NotPetya), software desactualizado, accesos inseguros
Nivel 4	Sistemas MES (producción, calidad, trazabilidad)	Nivel de gestión de operaciones	Interfaces web expuestas, credenciales débiles, escalamiento lateral, falta de control de accesos
Nivel 3 / 3.5	Zona desmilitarizada y controladores de dominio	Red perimetral (DMZ)	Falsos positivos en IDS, exposición de datos históricos, configuraciones inseguras
Nivel 2	Supervisión de procesos (SCADA, HMI, estaciones)	Nivel de supervisión	Protocolos inseguros (Modbus, DNP3), falta de autenticación, replay attacks, ausencia de IDS/IPS
Nivel 1	Control del proceso (PLCs, RTUs)	Nivel de control	Firmware desactualizado, contraseñas por defecto, comandos maliciosos, hardening ausente
Nivel 0	Proceso físico (sensores, actuadores, maquinaria)	Nivel de proceso físico	Manipulación directa, señales falsas, ausencia de redundancia, sabotaje físico

Nota. Esta tabla sintetiza la relación entre el modelo Purdue tradicional y la interpretación moderna utilizada en arquitecturas IT/OT, complementada con vulnerabilidades comunes en cada nivel. La clasificación permite realizar un análisis estructurado de seguridad cibernética en infraestructuras industriales, especialmente en sectores como el cervecero, facilitando la implementación de medidas de defensa en profundidad. Adaptado de. (*Ciberseguridad en el modelo de Purdue*, s. f.; *ISA99, Industrial Automation&Control Sys Security- ISA*, s. f.; García Núñez, 2024, National Institute of Standards and Technology, 2024).

Nivel 5: Red Empresarial (Corporate Network)

Representa la capa superior y más amplia en la arquitectura extendida del Modelo Purdue, abarcando los sistemas de Tecnología de la Información (IT) que sustentan las operaciones corporativas de una empresa cervecera. En este nivel se concentran activos IT tradicionales de vital importancia, como servidores de aplicaciones, sistemas de correo electrónico, plataformas de planificación de recursos empresariales (ERP) y las conexiones a Internet (National Institute of Standards and Technology, 2024). Estos sistemas son indispensables para la gestión administrativa, financiera, de recursos humanos y logística de la organización. Sin embargo, su interconexión inherente con los niveles inferiores de Tecnología Operacional (OT) los convierte en un punto de entrada crítico y un vector de riesgo significativo para la ciberseguridad industrial.

La principal vulnerabilidad en el Nivel 5 radica en la falta de segmentación efectiva entre las redes IT y OT (García Núñez, 2024). Históricamente, las redes IT y OT operaban de forma aislada, creando una "brecha de aire" (air gap) que impedía la propagación directa de amenazas. No obstante, la evolución hacia la Industria 4.0 y la necesidad de optimizar procesos, compartir datos en tiempo real y habilitar el monitoreo remoto han forzado la convergencia de estos dos mundos (ISA Sección Española, n.d.). Cuando esta convergencia no se gestiona con controles de seguridad adecuados, se crea un canal bidireccional que permite la propagación de amenazas desde los sistemas administrativos hacia los entornos de control industrial, lo que representa un riesgo inminente para la continuidad y seguridad de la producción cervecera. Un ataque exitoso en la red corporativa, aparentemente inofensivo para los procesos industriales, puede convertirse en una catástrofe operativa si logra cruzar la frontera IT/OT.

Un ejemplo paradigmático de esta debilidad es el ataque del ransomware NotPetya en 2017. Este malware, inicialmente diseñado para atacar sistemas IT, logró propagarse globalmente explotando vulnerabilidades en redes corporativas, incluyendo las de grandes empresas manufactureras. A través de estas brechas en los sistemas administrativos, NotPetya consiguió cruzar hacia los entornos de control industrial, causando interrupciones masivas de operación y pérdidas económicas millonarias al afectar directamente los sistemas OT y paralizar líneas de producción (García Núñez, 2024). Este incidente sirve como una clara advertencia para el sector cervecero colombiano: una vulnerabilidad en un servidor de correo electrónico o un sistema ERP aparentemente alejado del proceso de fermentación puede, en realidad, ser el punto de partida de un ataque que paralice toda la planta de producción. La lección es clara: la seguridad de la red corporativa es intrínsecamente la seguridad de la red operacional cuando no hay una segmentación robusta.

Más allá de la segmentación deficiente, el Nivel 5 presenta una serie de vulnerabilidades específicas que amplían la superficie de ataque para las empresas cerveceras en Colombia. Estas incluyen la persistencia de sistemas sin parches de seguridad y el uso de protocolos de comunicación no cifrados, entre otros (Rodrigo Díaz, 2024). Abordar estas debilidades es crucial para mitigar el riesgo de que la red corporativa se convierta en la puerta de entrada para ataques dirigidos a la producción.

Una de las vulnerabilidades más comunes y persistentes es la falta de una gestión de parches rigurosa y oportuna en los servidores, estaciones de trabajo y aplicaciones del Nivel 5. Los atacantes explotan con frecuencia vulnerabilidades conocidas para las que ya existen parches, pero que no han sido aplicados debido a la complejidad de las infraestructuras, la falta de recursos o la priorización de la disponibilidad (García Núñez, 2024). En una empresa

cervecera, un servidor ERP sin parches podría ser el blanco de un ataque que, una vez exitoso, se utilice como trampolín para acceder a la red OT, manipular recetas o detener operaciones. La ventana de oportunidad que estas vulnerabilidades no parcheadas ofrecen a los atacantes es considerable, especialmente cuando se trata de vulnerabilidades "día cero" o recién descubiertas.

Otro punto débil significativo es el uso de protocolos de comunicación no cifrados o débilmente autenticados dentro de la red corporativa o en sus interconexiones con redes externas. Por ejemplo, si los sistemas de correo electrónico no utilizan cifrado de extremo a extremo, la información sensible puede ser interceptada. De igual manera, las transferencias de archivos o las conexiones remotas que no emplean protocolos seguros pueden ser blanco de ataques de "man-in-the-middle" (hombre en el medio) o de escucha (eavesdropping), permitiendo a los atacantes capturar credenciales o datos críticos que podrían ser utilizados posteriormente para acceder a la red OT (National Institute of Standards and Technology, 2024). Esto es particularmente riesgoso en las empresas cerveceras que pueden tener oficinas remotas o personal trabajando fuera de la red corporativa, que se conectan a los recursos de la empresa sin las debidas precauciones de seguridad.

Además de estas vulnerabilidades técnicas, el Nivel 5 es el principal objetivo de ataques de ingeniería social, como el phishing y el spear-phishing. Los empleados de la red corporativa son a menudo el eslabón más débil, y los atacantes buscan explotar su confianza o falta de concienciación en ciberseguridad para obtener acceso a la red. Un correo electrónico malicioso que simula ser de un proveedor de lúpulo o cebada, por ejemplo, podría engañar a un empleado para que revele credenciales o descargue malware, comprometiendo así la red corporativa y, potencialmente, abriendo una puerta a la red OT (Díaz, 2022). La educación y el entrenamiento constante en ciberseguridad para todos los empleados son, por lo tanto, una defensa esencial.

Finalmente, la exposición indebida a Internet de servicios y aplicaciones corporativas, sin la debida fortificación o monitoreo, también amplía la superficie de ataque. Un servidor web corporativo mal configurado o una aplicación empresarial accesible públicamente sin las protecciones adecuadas pueden ser explotados como puntos de entrada iniciales para un ataque que luego se expanda internamente, buscando la forma de alcanzar los sistemas de control de producción (National Institute of Standards and Technology, 2024). La visibilidad limitada sobre estos activos expuestos y la falta de gestión de vulnerabilidades externas son riesgos latentes para las cervecerías.

Nivel 4: Sistemas de Gestión Industrial (MES).

Este nivel alberga los Sistemas de Gestión Industrial, específicamente los Manufacturing Execution Systems (MES), juega un papel pivote en la arquitectura extendida del Modelo Purdue. Este nivel actúa como la interfaz crítica entre la capa empresarial (Nivel 5) y las operaciones directas en planta (Niveles 0-3) (International Society of Automation, n.d.). Los MES son esenciales para la eficiencia y la visibilidad en las empresas cerveceras colombianas, ya que permiten gestionar en tiempo real aspectos fundamentales como las órdenes de producción, el control de calidad, la gestión de inventario de materias primas y productos terminados, y la trazabilidad completa de cada lote de cerveza desde la maltería hasta el embotellado (Siemens Software, n.d.). Esta capacidad de orquestación y monitoreo de la producción los convierte en activos de altísimo valor estratégico y operativo.

Sin embargo, precisamente por su rol de interfaz y su inherente exposición a redes IT, los sistemas MES se han convertido en blancos frecuentes de ataques cibernéticos (Vilaginés Iglesias, 2023). La interconexión necesaria para intercambiar datos con los sistemas ERP (Nivel 5) y para recibir información de los sistemas SCADA/HMI (Nivel 2) crea una superficie de

ataque significativa. Las vulnerabilidades más comunes en este nivel surgen de prácticas de seguridad deficientes. Por ejemplo, la ausencia de políticas de autenticación robustas es un riesgo recurrente, donde credenciales débiles o compartidas facilitan el acceso no autorizado (Vilaginés Iglesias, 2023). Un atacante que logre comprometer un sistema MES con credenciales predeterminadas o fácilmente adivinables podría manipular registros de producción, alterar recetas, modificar datos de calidad o incluso detener la producción.

Además, la presencia de interfaces web expuestas sin las protecciones adecuadas, o el uso de credenciales predeterminadas de fábrica que no han sido cambiadas, amplifica estas vulnerabilidades (Vilaginés Iglesias, 2023). Un panel de control MES accesible desde Internet sin autenticación robusta, o con credenciales bien conocidas, podría ser el punto de entrada para un atacante que busca sabotear la producción o exfiltrar propiedad intelectual, como las formulaciones de productos (Díaz, 2022). La integración del MES con otros sistemas, si no se asegura correctamente, también puede crear puntos débiles. Por ejemplo, una API (Interfaz de Programación de Aplicaciones) mal configurada entre el MES y el ERP podría permitir la inyección de comandos maliciosos o el acceso no autorizado a datos críticos.

Los riesgos asociados a la vulnerabilidad de los sistemas MES son de gran magnitud para el sector cervecero. Un ataque exitoso en este nivel puede llevar a manipulaciones de órdenes de producción, lo que podría resultar en la fabricación de lotes de cerveza defectuosos, el desperdicio de materias primas o la interrupción de las cadenas de suministro (García Núñez, 2024). El sabotaje digital es una preocupación real, donde un atacante podría alterar los parámetros del proceso de fermentación, causar un sobrellenado en el embotellado o incluso activar secuencias de limpieza en momentos inapropiados, comprometiendo la calidad del producto y la seguridad de la planta (Rodrigo Díaz, 2024).

La falta de seguridad en los sistemas MES también puede tener implicaciones en la trazabilidad y la confianza del consumidor. Si los registros de producción son alterados, la empresa podría no cumplir con las normativas de seguridad alimentaria o no poder identificar rápidamente el origen de un problema en un lote de producto. Esto no solo genera pérdidas económicas, sino que también daña la reputación de la marca, algo vital en la competitiva industria cervecera colombiana.

Nivel 3: Supervisión y Control (SCADA, HMI)

Aquí residen los sistemas SCADA (Supervisory Control and Data Acquisition) y HMI (Human-Machine Interface), elementos indispensables en cada etapa de la producción cervecera (International Society of Automation, n.d.). Estos sistemas son el cerebro que permite a los operadores monitorear y ajustar parámetros críticos en líneas de producción como la fermentación, el envasado y el control de temperatura en tanques y calderas. Cualquier alteración o compromiso en este nivel puede tener consecuencias directas y devastadoras en la calidad del producto, la seguridad del personal y la continuidad operativa de la planta.

La vitalidad de los sistemas SCADA y HMI contrasta con una de sus vulnerabilidades más críticas: la persistencia en el uso de protocolos de comunicación inseguros. Históricamente, protocolos como Modbus, DNP3 o Profibus fueron diseñados para la eficiencia y la simplicidad en entornos aislados, sin incorporar funcionalidades de cifrado ni mecanismos robustos de autenticación (Serna & Ortiz, 2011; Corrales Paucar, 2007). Esta carencia inherente de seguridad los convierte en un punto débil significativo. Un atacante con acceso a la red de control podría interceptar fácilmente el tráfico, leer los datos de los sensores o incluso inyectar comandos maliciosos sin ser detectado o verificado.

Las debilidades de estos protocolos heredados abren la puerta a una variedad de ataques cibernéticos altamente peligrosos para el sector cervecero:

Ataques de Tipo Replay: Un atacante puede interceptar y grabar comandos legítimos de un HMI o SCADA, para luego "reproducirlos" en un momento posterior, engañando al sistema para que ejecute acciones no deseadas, como abrir una válvula o detener una bomba (Corrales Paucar, 2007). Imagina que se repite un comando de drenaje de un tanque de fermentación, causando la pérdida de un lote completo de cerveza.

Ataques de Spoofing (Suplantación de Identidad): Dada la falta de autenticación, un atacante puede hacerse pasar por un dispositivo o sistema legítimo, enviando comandos falsos o datos erróneos a los controladores. Esto podría llevar a la manipulación de temperaturas de fermentación, presiones en el proceso de carbonatación o niveles de llenado en la línea de envasado, afectando directamente la calidad y el volumen de producción (Serna & Ortiz, 2011).

Inyección Directa de Comandos Maliciosos: Sin cifrado ni verificación de integridad, un atacante puede inyectar comandos arbitrarios directamente en el flujo de comunicación, forzando a los equipos a realizar acciones peligrosas o perjudiciales. Esto podría incluir la sobrepresurización de equipos, el uso incorrecto de agentes de limpieza o incluso la detención total de una línea de producción crítica.

La gravedad de estas vulnerabilidades es confirmada por investigaciones recientes. Según Andrade-Logroño y Cobos-Torres (2025), la mayoría de los ataques documentados contra infraestructuras SCADA han aprovechado precisamente esta carencia de autenticación y monitoreo. Un ejemplo notorio fue el ataque a la infraestructura eléctrica de Ucrania en 2015, donde la falta de autenticación robusta y la capacidad de los atacantes para interactuar directamente con los sistemas de control a través de sus protocolos nativos, fueron clave para

causar apagones masivos (National Institute of Standards and Technology, 2024). Para una cervecería, un ataque similar podría traducirse en el control remoto de los procesos de pasteurización o la alteración de la dosificación de aditivos, poniendo en riesgo la salud pública y la continuidad del negocio.

Nivel 2: Control de Procesos (PLCs, RTUs)

En este nivel se ejecuta el control directo y local de los procesos industriales, siendo el corazón de la automatización en cualquier cervecería moderna. Aquí residen los Controladores Lógicos Programables (PLC), las Unidades Terminales Remotas (RTU) y los Dispositivos Electrónicos Inteligentes (IED) (International Society of Automation, n.d.). Estos dispositivos son los "músculos" de la planta, responsables de ejecutar las instrucciones recibidas del Nivel 3 (SCADA/HMI) y de interactuar directamente con el Nivel 1 (sensores y actuadores) para controlar cada etapa de la producción de cerveza. Esto incluye desde la apertura y cierre de válvulas en los fermentadores, el control de bombas para el trasiego de líquidos, la regulación de la temperatura en las calderas de cocción, hasta la coordinación de la maquinaria de embotellado y etiquetado. Cualquier falla o compromiso en este nivel puede tener un impacto inmediato y catastrófico en la integridad del proceso, la calidad del producto y la seguridad de los operarios.

A pesar de su criticidad, los dispositivos en el Nivel 2 presentan vulnerabilidades inherentes debido a su diseño original, que priorizaba la fiabilidad y la funcionalidad en entornos aislados, sin considerar las amenazas cibernéticas modernas. Una de las principales debilidades es la falta de autenticación en las comunicaciones y en la programación. Muchos PLCs y RTUs permiten la conexión y modificación de su lógica de control sin requerir una autenticación robusta, o incluso sin autenticación alguna (National Institute of Standards and Technology, 2024). Esto significa que un atacante con acceso a la red de control podría modificar la lógica de

un PLC para alterar los parámetros de un proceso de fermentación, cambiar las secuencias de llenado en las embotelladoras o incluso deshabilitar dispositivos de seguridad, sin necesidad de credenciales legítimas.

Además, la ausencia de cifrado en el tráfico de red para protocolos industriales como EtherNet/IP o PROFINET, aunque más modernos que Modbus o DNP3, sigue siendo una vulnerabilidad significativa. Si un atacante logra posicionarse en la red de control, podría interceptar datos sensibles o inyectar comandos maliciosos sin que la comunicación esté protegida contra la escucha o la alteración (Claroty, 2024). Esto es particularmente riesgoso en entornos donde la información sobre el estado del proceso o los comandos de control se transmiten sin cifrar. La vida útil prolongada de estos equipos, sumado a la dificultad de aplicar parches, exacerba estas vulnerabilidades al mantener en operación firmware obsoleto con fallas de seguridad conocidas.

El ejemplo paradigmático es Stuxnet, que logró alterar procesos físicos sin ser detectado gracias a vulnerabilidades en los PLCs, lo que evidencia la necesidad de aplicar técnicas de hardening, actualización de firmware y aislamiento físico o lógico (Andrade-Logroño & Cobos-Torres, 2025).

ISA/IEC 62443-4-2 propone la validación estricta de firmware, autenticación de dispositivos y la eliminación de servicios innecesarios como medidas prioritarias de defensa (*Cybersecurity Certificates - ISA*, 2025).

Nivel 1: Dispositivos de Campo (Sensores y Actuadores)

El Nivel 1 representa la capa más fundamental de la Tecnología Operacional (OT), donde la interacción entre los sistemas de control y la maquinaria industrial se materializa a través de los dispositivos de campo. En una cervecería, este nivel está poblado por sensores y actuadores

que son la columna vertebral de la automatización (International Society of Automation, n.d.). Los sensores recogen datos vitales del proceso físico, como la temperatura precisa en los tanques de fermentación, el caudal de agua o malta, el nivel de llenado en los depósitos, o la presión en las líneas de embotellado. Por su parte, los actuadores traducen las señales de control de los niveles superiores en acciones físicas, como la apertura o cierre de válvulas, la activación o desactivación de bombas, el ajuste de la velocidad de los motores en las máquinas de llenado, o el control de los elementos calefactores en la caldera. Son, en esencia, los "ojos y manos" del sistema automatizado, esenciales para la calidad, eficiencia y seguridad de la producción cervecera.

A pesar de su rol crítico, los dispositivos de campo en el Nivel 1 son intrínsecamente vulnerables, tanto física como lógicamente. Su diseño histórico priorizó la robustez y la simplicidad operacional, a menudo sin incorporar mecanismos de protección cibernética intrínsecos como cifrado, autenticación robusta o validación de señales (INCIBE-CERT, n.d.; National Institute of Standards and Technology, 2024). Muchos de estos dispositivos están expuestos en el piso de planta, lo que los hace accesibles a la manipulación física si la seguridad perimetral es deficiente. La ausencia de validación de señales significa que una lectura alterada o un comando inyectado pueden ser aceptados por el sistema de control como legítimos, sin una verificación cruzada adecuada.

La dificultad de actualizar o "parchar" el *firmware* de muchos de estos dispositivos de campo, a menudo legacy, exacerba estos riesgos al mantener vulnerabilidades conocidas y explotables en el sistema por años (Rodrigo Díaz, 2024).

Esto puede dar lugar a situaciones de falsificación de datos de temperatura, presión o caudal, con impactos directos en la producción cervecera, afectando la calidad o seguridad del

producto final. ISA/IEC 62443-2-1 recomienda implementar mecanismos de validación cruzada (redundancia), cifrado a nivel de campo y protección física de acceso como parte de una estrategia de defensa en profundidad (ISA99, s.f.)

Nivel 0: Proceso Físico

El Nivel 0 es la base de la Pirámide de Automatización, representando la realidad física del proceso productivo en sí mismo. Aquí no hay sistemas informáticos o dispositivos electrónicos complejos, sino la maquinaria, los fluidos, las temperaturas y presiones que definen la fabricación de la cerveza (International Society of Automation, n.d.). Este nivel incluye operaciones como la carbonatación, el embotellado, la pasteurización, la fermentación, la maceración, la cocción y el enfriamiento. Aunque no es una "capa cibernética" en el sentido tradicional, las amenazas cibernéticas en los niveles superiores pueden manifestarse aquí con consecuencias catastróficas (National Institute of Standards and Technology, 2024).

Las amenazas en el Nivel 0 son críticas porque un ciberataque exitoso que se propague a través de los niveles superiores puede alterar directamente la materia prima o el producto final, ocasionando fallas físicas en los equipos, paros no planificados en la producción o, lo que es más grave, poner en riesgo la vida de los operarios (Rodrigo Díaz, 2024). Los sistemas de seguridad que operan en este nivel, como las paradas de emergencia físicas o los interlocks de seguridad, son los últimos baluartes contra un incidente catastrófico.

El incidente de Triton/Trisis en 2017 es un claro ejemplo de cómo un ciberataque puede impactar directamente el Nivel 0 y sus consecuencias (Claroty, 2024). Este malware fue diseñado específicamente para atacar los controladores de seguridad (SIS - Safety Instrumented Systems) de un sistema de control industrial en una instalación de infraestructura crítica. Al manipular estos controladores, el malware logró desactivar los sistemas de protección de

seguridad, lo que puede derivar en fallas catastróficas al permitir que el proceso opere en condiciones inseguras. En el contexto de una cervecería, un ataque similar podría:

Desactivar una parada de emergencia que evitaría la sobrepresurización de un tanque de fermentación, con riesgo de explosión.

Neutralizar los interlocks de seguridad en una línea de embotellado, lo que podría resultar en colisiones de maquinaria o atrapamiento de personal.

Permitir que las temperaturas de pasteurización excedan los límites seguros, comprometiendo la calidad del producto y su inocuidad.

Tales incidentes pueden causar no solo pérdidas materiales millonarias por daño a la infraestructura, sino también lesiones graves o fatales al personal, y un impacto ambiental por derrames de producto o efluentes (National Institute of Standards and Technology, 2024).

Tabla 2

Ciberataques en Entornos Industriales

Casos Representativos de Ciberataques en Entornos Industriales

Año	Nombre del ataque	Sector afectado	Tipo de ataque	Consecuencias principales
2000	Maroochy Shire	Saneamiento (agua)	Acceso remoto no autorizado	Vertido de 800,000 litros de aguas residuales en Queensland (Australia)
2010	Stuxnet	Energía nuclear	Malware (gusano informático)	Sabotaje de centrifugadoras en Irán, primer ciberataque OT de impacto físico documentado
2014	Havex/Trojanized SCADA	Manufactura / SCADA	APT (software espía)	Robo de información en equipos SCADA mediante infección de instaladores legítimos
2015	BlackEnergy	Energía eléctrica	Malware (backdoor + KillDisk)	Apagón eléctrico masivo en Ucrania, afectando a más de 230,000 personas
2017	Triton/Trisis	Petroquímica	Malware (SIS sabotage)	Manipulación de controladores de seguridad; riesgo de explosión en planta industrial
2017	NotPetya	Transporte / Logística	Ransomware (worm)	Caída de operaciones globales; Maersk, FedEx y otros afectados; impacto de 10.000 M USD

Año	Nombre del ataque	Sector afectado	Tipo de ataque	Consecuencias principales
2021	Colonial Pipeline	Energía / oleoducto	Ransomware	Paralización del suministro de combustible en EE. UU.; declaración de emergencia nacional
2021	Oldsmar, Florida	Agua potable	Control remoto no autorizado	Intento de envenenamiento del suministro de agua modificando niveles de soda cáustica

Nota. La tabla es elaborada con base en fuentes de análisis sobre ciber incidentes industriales publicados en los sitios web por Álvarez, (s. f.), (*Riesgos de no proteger un proceso industrial con ciberseguridad | IMEPI México*, s. f.) y por Pachón (2022).

Se seleccionaron casos representativos que evidencian vulnerabilidades comunes en sistemas OT tales como el acceso remoto inseguro, uso de software sin validar, conexiones IT-OT sin segmentación y ausencia de monitoreo continuo. Estos eventos ilustran el impacto real y creciente de los ciberataques en infraestructuras críticas a nivel global, reforzando la necesidad de implementar controles como los propuestos por la norma ISA/IEC 62443 y el modelo de defensa en profundidad. Esta información complementa el análisis de riesgos descrito previamente en este proyecto y justifica la implementación de un SOC especializado en entornos OT industriales. *Fuente*. (Álvarez, s. f.; Pachón, 2022; *Riesgos de no proteger un proceso industrial con ciberseguridad | IMEPI México*, s. f.).

A partir del análisis de las vulnerabilidades identificadas en los distintos niveles del modelo Purdue, se concluye que la adopción de tecnologías emergentes vinculadas a la Industria 4.0 constituye una estrategia eficaz para fortalecer la seguridad cibernética en entornos OT del sector cervecero colombiano.

La Industria 4.0 promueve la convergencia entre tecnologías digitales avanzadas, como el Internet Industrial de las Cosas (IoT), analítica avanzada, inteligencia artificial, aprendizaje automático y computación en la nube, las cuales permiten incrementar tanto la visibilidad como la capacidad de respuesta ante incidentes cibernéticos (Vilaginés Iglesias, 2023; Pinto Rojas, 2023).

Estas tecnologías pueden integrarse en los distintos niveles de la arquitectura Purdue para mejorar el monitoreo en tiempo real, la detección de amenazas y la toma de decisiones automatizada. Su implementación fortalece los sistemas de control industrial mediante capacidades como:

Monitoreo continúo basado en inteligencia artificial,

Sistemas de detección de intrusos adaptativos,

Segmentación de red lógica avanzada,

Políticas de acceso dinámicas y contextuales,

Orquestación automática de respuestas a incidentes.

Asimismo, marcos normativos como ISA-95 y NIST CSF 2.0, junto con las directrices de la serie ISA/IEC 62443, proporcionan una base sólida para integrar estos avances tecnológicos de forma segura, garantizando la interoperabilidad sin comprometer la integridad de los procesos industriales (ISA95, s. f.; National Institute of Standards and Technology, 2024).

Tabla 3

Estrategias de Mitigación Estrategias de Mitigación por Nivel del Modelo Purdue en Plantas Cerveceras Colombianas

Nivel Purdue	Activos principales	Riesgos comunes	Estrategias de mitigación recomendadas
Nivel 0	Sensores, actuadores, dispositivos finales	Manipulación física, sabotaje local, malware transmitido desde controladores	Se recomienda aplicar controles estrictos de acceso físico al entorno industrial, mediante credenciales, vigilancia o sistemas biométricos. Además, debe implementarse segmentación de red a nivel de celda utilizando VLANs industriales que limiten el tráfico entre procesos. También es recomendable realizar inspecciones periódicas para verificar la integridad de señales y correlacionarlas con el estado real del proceso.
Nivel 1	PLC, controladores de campo	Inyección de comandos maliciosos, modificación de lógica, uso de protocolos inseguros	Se deben instalar firewalls industriales entre los niveles 1 y superiores, para filtrar el tráfico hacia los PLC. Es esencial establecer listas blancas de comunicación, autorizando solo dispositivos y protocolos confiables. Se debe mantener el firmware actualizado y monitorear accesos al controlador. En sistemas heredados, es aconsejable aislar los controladores mediante data diodes o zonas DMZ.
Nivel 2	HMI, estaciones de operación	Manipulación de visualización, ransomware,	La segmentación lógica de red es clave, así como el control de sesiones con autenticación multifactor o al menos contraseñas robustas. Deben aplicarse políticas estrictas de

Nivel Purdue	Activos principales	Riesgos comunes	Estrategias de mitigación recomendadas
		accesos no autorizados	actualización de software, preferiblemente con entornos de prueba. Se recomienda la instalación de antivirus industrial y el bloqueo de puertos USB para prevenir la infección por dispositivos externos.
Nivel 3	SCADA, servidores de automatización, historiadores	DoS, manipulación de datos, acceso persistente (APT)	Es fundamental contar con soluciones de monitoreo continuo como IDS/IPS industriales para detectar comportamientos anómalos. Las actualizaciones deben realizarse en ventanas controladas y con respaldo completo previo. Se recomienda mantener copias de seguridad periódicas en sistemas fuera de línea. También se debe implementar control de accesos basado en roles y registros de auditoría.
Nivel 4	MES, ERP, servidores corporativos de producción	Movimiento lateral desde IT a OT, fuga de información	La comunicación entre IT y OT debe estar protegida mediante firewalls dedicados, segmentación de red y políticas de acceso basado en roles. También se recomienda implementar soluciones de análisis de comportamiento del usuario (UBA) y sistemas de prevención de fuga de datos (DLP). Las interfaces entre sistemas deben ser monitoreadas en tiempo real.
Nivel 5	Aplicaciones empresariales, BI, servicios en la nube	Exposición remota, accesos privilegiados	Se debe implementar una estrategia sólida de gestión de identidades (IAM), incluyendo autenticación multifactor para accesos remotos. Toda comunicación debe cifrarse y verificarse mediante certificados digitales.

Nivel Purdue	Activos principales	Riesgos comunes	Estrategias de mitigación recomendadas
		mal gestionados	Además, se deben realizar auditorías regulares de seguridad en los servicios en la nube y definir políticas claras para proveedores externos.

Nota. Este cuadro sintetiza las estrategias más relevantes para mitigar los riesgos en cada nivel jerárquico de la arquitectura industrial, según el modelo Purdue. Su implementación escalonada favorece la aplicación del principio de defensa en profundidad, protegiendo los activos más críticos y minimizando las posibilidades de propagación lateral de amenazas en entornos OT.

En línea con el enfoque adoptado en esta investigación, el trabajo desarrollado por Boretto, Brusa, Margheim, Martín y Rotela (2024), titulado "Análisis de la amenaza cibernética en el sector eléctrico argentino", representa una contribución relevante para la comprensión de las vulnerabilidades que emergen en entornos industriales híbridos donde convergen tecnologías OT e IT. Aunque el estudio se enfoca específicamente en infraestructuras críticas del sector energético, sus hallazgos resultan transferibles y altamente pertinentes para otros sectores industriales, como el cervecero, que comparten dinámicas similares de automatización avanzada, dependencia de sistemas de control industrial, y exposición creciente a amenazas cibernéticas sofisticadas.

Particularmente, este trabajo destaca la importancia de abordar la ciberseguridad desde una perspectiva integral que no solo contemple la tecnología, sino también los factores humanos, la organización y los procesos. Elementos como la segmentación de redes, la identificación y priorización de activos críticos, el fortalecimiento de capacidades internas y la adopción de marcos tácticos como la Kill Chain y MITRE ATT&CK para entornos industriales, son considerados pilares estratégicos para mitigar los riesgos. La experiencia analizada en el sector

eléctrico, al igual que en la industria cervecera, evidencia una evolución tecnológica que ha desdibujado las fronteras entre los sistemas tradicionalmente aislados de producción y las infraestructuras TI corporativas, generando nuevas superficies de ataque que requieren ser abordadas con metodologías especializadas y visión estratégica.

Por ello, se propone incorporar a esta investigación ciertos componentes clave del enfoque metodológico de Boretto et al. (2024), con el fin de enriquecer la base conceptual de la evaluación proyectada de riesgos, asegurando una mayor robustez en la identificación de amenazas, el diseño de controles y la planificación de medidas preventivas y reactivas en el entorno industrial cervecero.

Tabla 4

Elementos Clave para el Análisis de Riesgo

Elementos Clave para el Análisis de Riesgo en Entornos OT–TI Industriales (Adaptado de Boretto Et Al., 2024)

Componente Estratégico	Aplicación Relevante en el Sector Cervecero
Segmentación de redes	Separación lógica y física entre redes OT y TI para reducir la superficie de ataque. Aplicación directa sobre arquitecturas basadas en el modelo Purdue.
Identificación de activos críticos	Clasificación sistemática de componentes industriales sensibles (sensores, PLC, estaciones SCADA) para priorizar su protección.
Capacitación y concienciación	Formación continua del personal operativo y técnico en protocolos de ciberseguridad industrial y respuesta ante incidentes.

Modelos de ataque (Kill Chain / MITRE ATT&CK)	Uso de marcos tácticos para modelar posibles vectores de ataque en ambientes híbridos OT–TI, desde la intrusión hasta la persistencia y el impacto operativo.
Vulnerabilidades OT–TI comunes	Identificación de brechas como conexiones inseguras, software desactualizado, accesos no autorizados y fallas en protocolos industriales.
Amenazas avanzadas persistentes (APT)	Consideración del riesgo generado por actores sofisticados con motivaciones políticas o económicas, capaces de atacar infraestructuras críticas con técnicas dirigidas y prolongadas.

Nota. La tabla presenta una síntesis de componentes estratégicos identificados por Boretto et al. (2024) para fortalecer la ciberseguridad en entornos industriales críticos. Aunque el estudio original se enfoca en el sector eléctrico, los elementos han sido adaptados al contexto de la industria cervecera colombiana, considerando su creciente exposición a riesgos cibernéticos derivados de la convergencia OT–TI.

Evaluar el Impacto Potencial de Ciberataques sobre Activos Críticos (SCADA, PLC, HMI) en Procesos de Producción de Plantas Cerveceras Colombianas, Aplicando Metodologías de Análisis de Riesgo, Durante Año 2025, para Establecer Prioridades de Protección

Como se expuso en el capítulo anterior, los entornos industriales cerveceros presentan una estructura jerárquica según el modelo Purdue, en la cual se identifican distintos niveles de activos tecnológicos que van desde los sistemas corporativos (nivel 5) hasta el proceso físico (nivel 0). Dentro de esta arquitectura, los componentes SCADA, PLC y HMI desempeñan un papel crucial en los niveles operacionales (niveles 3, 2 y 1), siendo responsables de la supervisión, control y visualización de los procesos productivos.

Estos activos constituyen lo que se denomina infraestructura crítica operativa, y su compromiso por parte de actores maliciosos puede generar consecuencias severas, tales como paros de producción, alteración de la calidad del producto, daños a los equipos o incluso

afectación a la salud de los consumidores y trabajadores (García Núñez, 2024; Rodrigo Díaz, 2024).

En este capítulo se desarrolla un análisis teórico del impacto potencial que podrían generar ciberataques dirigidos específicamente contra activos críticos de tecnología operacional (OT), tales como los sistemas SCADA, los controladores lógicos programables (PLC) y las interfaces hombre-máquina (HMI), en el contexto particular de las plantas cerveceras colombianas. Estos activos representan elementos esenciales para la continuidad operativa, la calidad del producto y la seguridad industrial. Su vulnerabilidad frente a amenazas cibernéticas emergentes plantea un riesgo significativo para la disponibilidad, integridad y confiabilidad de los procesos productivos (Cordero-Robles, 2021; Pinto Rojas, 2023).

El enfoque adoptado en esta investigación se basa en la aplicación proyectada de metodologías internacionalmente reconocidas para el análisis de riesgos en infraestructuras críticas. Se consideran como pilares teóricos la norma ISO/IEC 27005:2018, que ofrece una guía sistemática para la gestión de riesgos de seguridad de la información en el marco de un SGSI, y que resulta adaptable a los entornos OT mediante una adecuada interpretación de activos, amenazas y vulnerabilidades (Hernández, Fernández & Baptista, 2014).

Asimismo, se toma como referencia el marco metodológico del NIST SP 800-30 revisión 1, el cual permite estructurar la evaluación de riesgos desde una perspectiva cuantitativa y cualitativa, considerando la probabilidad de ocurrencia de incidentes de ciberseguridad y su impacto sobre activos críticos. Este marco ha demostrado ser aplicable a entornos industriales, especialmente en sectores que integran tecnología de automatización avanzada, como es el caso del sector cervecero (Castellanos Reyes, 2018).

De forma complementaria, se incluye en el planteamiento investigativo la serie de normas ISA/IEC 62443, reconocida por su enfoque especializado en sistemas de control industrial y su capacidad para abordar tanto aspectos técnicos como organizacionales de la ciberseguridad. Esta familia normativa establece conceptos clave como zonas y conduits de seguridad, niveles de madurez de defensa y segmentación lógica, todos ellos esenciales para comprender y modelar riesgos en infraestructuras OT (Fole de Navia de la Cruz, 2024).

La aplicación futura de estas metodologías, en el marco del presente estudio, permitirá estimar con mayor precisión la probabilidad e impacto de ciberataques sobre los activos mencionados, así como proponer un orden de priorización técnica para su protección. Aunque aún no se ha ejecutado un análisis práctico en planta, este capítulo sienta las bases teóricas necesarias para la etapa de evaluación de riesgos, proyectada para desarrollarse durante el año 2025. Este enfoque anticipado busca establecer criterios racionales y fundamentados que orienten la toma de decisiones en materia de ciberseguridad industrial para el sector cervecero Colombiano (Bernal Mora et al., 2024).

Además del análisis proyectado basado en normas y marcos metodológicos especializados, es imprescindible considerar el entorno tecnológico actual donde se desarrollan los procesos industriales. En este sentido, la convergencia entre tecnologías operativas (OT) y tecnologías de la información (TI) ha transformado de manera sustancial la dinámica de producción en las plantas cerveceras colombianas. Este fenómeno, propio de la Industria 4.0, ha traído consigo avances relevantes en eficiencia y automatización, pero también ha ampliado significativamente la superficie de exposición a ciberataques. Esta expansión se debe, principalmente, a la conectividad creciente entre sistemas de automatización industrial y las redes corporativas, eliminando las barreras que antes aislaban entornos críticos. Como resultado,

equipos fundamentales para el control de los procesos, que anteriormente operaban en redes segregadas, ahora están expuestos a vectores de amenaza externos, lo que aumenta la complejidad del análisis de riesgo y demanda medidas de protección más integrales (Sañicela & Xavier, 2023).

En este contexto, los dispositivos OT, diseñados históricamente para operar en entornos cerrados y sin conectividad externa, se encuentran ahora expuestos a vectores de ataque propios del ecosistema digital. Diversos estudios muestran que esta situación ha generado brechas críticas de seguridad en sectores industriales latinoamericanos, incluyendo el Colombiano, donde muchas plantas aún no han adoptado marcos robustos de ciberseguridad (Solarte et al., 2015).

La industria cervecera colombiana no es ajena a esta realidad. A pesar de los avances en automatización e integración digital, muchas de sus plantas aún operan bajo esquemas tecnológicos híbridos, donde conviven sistemas modernos con plataformas heredadas de difícil actualización. Esta coexistencia tecnológica introduce complejidades adicionales al momento de aplicar esquemas de protección integral, ya que impide la implementación homogénea de controles de seguridad y segmentación lógica (Cabrera González & Arango Cárdenas, 2023). En consecuencia, la gestión del riesgo cibernético en estos entornos debe trascender el diagnóstico técnico, integrando una comprensión sistémica de los procesos industriales, de las jerarquías de comunicación tecnológica como las representadas en el modelo Purdue y de la criticidad operativa de los activos implicados.

En este ecosistema industrial, los sistemas SCADA, PLC y HMI desempeñan funciones esenciales en la operación y automatización de los procesos de producción. Estos componentes, al formar parte de la infraestructura crítica de control, se convierten en vectores privilegiados para los actores maliciosos que buscan comprometer la disponibilidad, integridad o trazabilidad

del proceso productivo. Su vulnerabilidad no se limita a aspectos técnicos: también tienen un alto valor estratégico desde el punto de vista del impacto financiero, reputacional y regulatorio ante un eventual incidente de ciberseguridad.

Los SCADA (Supervisory Control and Data Acquisition), al centralizar datos operativos de sensores distribuidos, permiten la supervisión y control remoto de diversas unidades funcionales dentro de la planta. Esta capacidad, aunque estratégica, representa un riesgo considerable, especialmente cuando se expone a redes IP no segmentadas, accesos remotos inseguros o protocolos obsoletos. Entre los vectores de ataque más comunes a SCADA se encuentran los ataques de denegación de servicio (DoS), la manipulación de parámetros críticos de operación y los accesos persistentes avanzados (APT) que permanecen ocultos en la red, alterando la operación sin ser detectados (Boretto et al., 2024). Casos documentados en sectores industriales latinoamericanos muestran cómo estas plataformas han sido utilizadas como puntos de entrada para comprometer procesos completos y alterar parámetros de calidad o seguridad.

Los PLC (Controladores Lógicos Programables), por su parte, se encuentran en los niveles más bajos del modelo Purdue (0 y 1) y son los encargados de ejecutar acciones físicas críticas dentro de la planta, como apertura de válvulas, arranque de motores o regulación térmica de tanques. Un ataque dirigido a estos dispositivos puede tener consecuencias inmediatas sobre la receta cervecera, causando pérdida de materia prima, desbalance en las líneas de producción o incluso daños mecánicos irreversibles. Dado que muchos de estos controladores fueron diseñados sin funciones de autenticación, cifrado o trazabilidad, su exposición a redes abiertas los convierte en puntos de alto riesgo (Kleinmann & Wool, s. f.). Además, el uso de protocolos industriales como Siemens S7 o Modbus, en versiones sin cifrado, amplifica aún más la vulnerabilidad del entorno OT.

Las HMI (Interfaces Hombre-Máquina) constituyen el nexo directo entre el operador humano y el sistema de control automatizado. Una alteración en estas interfaces puede inducir a errores de operación, modificar visualizaciones o impedir acciones críticas durante eventos no deseados. Estudios aplicados en redes industriales de Latinoamérica muestran que estas interfaces son frecuentemente blanco de ataques cuando operan sobre sistemas operativos desactualizados, carecen de autenticación robusta o están expuestas sin restricciones en segmentos de red mal protegidos (Cabrera González & Arango Cárdenas, 2023). Su manipulación puede tener un impacto no solo técnico, sino también humano, afectando directamente la capacidad de respuesta ante una anomalía o contingencia.

Ante este panorama, se vuelve imprescindible no solo evaluar la función técnica de cada activo, sino también su nivel de exposición, impacto y valor dentro del proceso industrial. El modelo Purdue resulta particularmente útil para esta tarea, al ofrecer una representación jerárquica que permite mapear los activos según su función, ubicación y criticidad. Esta visión estructurada facilita el diseño de defensas en profundidad, la segmentación de zonas industriales, y la priorización de controles en aquellos niveles donde una intrusión podría tener consecuencias más graves (Solarte et al., 2015).

En este contexto, la identificación, valoración y gestión de los riesgos que enfrentan estos activos críticos debe realizarse bajo marcos metodológicos sólidos, que integren aspectos técnicos, organizacionales y estratégicos. Una de las metodologías destacadas en este sentido es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), desarrollada por el Gobierno de España. MAGERIT permite un enfoque sistemático que parte de la identificación de activos, análisis de amenazas y vulnerabilidades, valoración del impacto y establecimiento de controles de seguridad proporcionales. Su flexibilidad la hace aplicable tanto

en entornos IT como OT, lo que la convierte en una herramienta útil para abordar escenarios híbridos como los que presenta la industria cervecera(*Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método*, s. f.).

Aplicar MAGERIT en una planta de producción implica considerar no solo los SCADA, PLC y HMI, sino también los servidores de automatización, redes industriales, estaciones de ingeniería, bases de datos de control y otros activos digitales. Cada uno de estos componentes puede ser valorado según criterios de confidencialidad, integridad, disponibilidad y trazabilidad, lo que permite establecer un perfil de riesgo y orientar la asignación de recursos de seguridad.(Sañicela & Xavier, 2023).

Complementariamente, el modelo Purdue permite clasificar los activos por niveles jerárquicos, lo que facilita la definición de zonas seguras, conduits de comunicación controlada y mecanismos de defensa escalonada. Así, los dispositivos ubicados en los niveles 0 y 1 (sensores, actuadores, PLC) deben protegerse contra accesos físicos no autorizados y comandos externos manipulados, mientras que los componentes de los niveles 2 y 3, como los SCADA y HMI, requieren segmentación de red, autenticación de usuarios, y monitoreo continuo de eventos. En tanto, los elementos del nivel 4 (servidores, bases de datos de producción) deben estar alineados con políticas corporativas de ciberseguridad y mecanismos de control de acceso basados en roles.

En síntesis, para evaluar adecuadamente el impacto potencial de ciberataques sobre activos críticos en plantas cerveceras, es necesario adoptar un enfoque metodológico integral que combine la clasificación funcional de los activos (modelo Purdue), con el análisis sistemático de amenazas y controles (MAGERIT). Esta estrategia permitirá establecer una base priorizada de protección, en función de la exposición, criticidad y consecuencias operacionales ante un evento de ciberseguridad, y servirá como insumo fundamental para las decisiones técnicas y estratégicas

que se deriven en el diseño de soluciones de defensa, como la implementación de un SOC especializado en entornos OT.

La siguiente tabla sintetiza una propuesta de priorización de protección basada en el Modelo Purdue, adaptada al entorno cervecero colombiano:

Tabla 5

Prioridades de Protección según el Modelo Purdue

Nivel Purdue	Activo Principal	Prioridad de Protección	Justificación
Nivel 0	Sensores y Actuadores	Alta	Son la base de la operación física; su compromiso puede causar daños inmediatos.
Nivel 1	PLC	Muy Alta	Controlan procesos críticos; vulnerables a ataques que pueden alterar la producción.
Nivel 2	HMI	Alta	Interfaz directa con el operador; su manipulación puede inducir errores humanos.
Nivel 3	SCADA	Muy Alta	Supervisión y control centralizado; su compromiso afecta múltiples procesos.
Nivel 4	Sistemas Empresariales	Media	Aunque menos críticos para la operación inmediata, pueden ser vectores de ataque hacia niveles inferiores.

Nota. Esta priorización responde a criterios de impacto operativo, facilidad de explotación y consecuencias para la continuidad del proceso cervecero. Su aplicación requiere un análisis contextualizado en cada planta, considerando su infraestructura, automatización y nivel de conectividad.

A partir de este diagnóstico, se propone la adopción de una serie de recomendaciones estratégicas para ser aplicadas progresivamente durante el año 2025, con el objetivo de mitigar los riesgos asociados a los activos más vulnerables. Estas recomendaciones, además de responder

a criterios técnicos, buscan establecer las bases para un modelo sostenible de gestión de la ciberseguridad en el sector cervecero colombiano.

En primer lugar, se recomienda realizar una evaluación integral del inventario de activos industriales, identificando no solo los dispositivos físicos (SCADA, PLC, HMI), sino también los sistemas auxiliares que los soportan, como estaciones de ingeniería, gateways industriales, switches administrables y servidores de historización. Esta evaluación debe incorporar criterios de criticidad funcional, trazabilidad de datos y dependencia de red (Cordero-Robles, 2021; García Núñez, 2024).

En segundo lugar, se debe aplicar un modelo de segmentación de red industrial basado en zonas y conduits, en coherencia con el modelo Purdue y las prácticas recomendadas por la norma ISA/IEC 62443. Esta segmentación permitirá aislar los dispositivos de control más sensibles, restringir la propagación de malware y limitar la escalabilidad de los ataques (*Ciberseguridad en el modelo de Purdue*, s. f.; Piggin, 2013). Además, favorece la implementación de políticas de acceso más estrictas, como la autenticación multifactor, listas de control de acceso (ACLs) y firewalls industriales.

Una tercera medida clave es el fortalecimiento de las capacidades de detección temprana y respuesta a incidentes en entornos OT. Esto implica integrar soluciones de monitoreo continuo, como sistemas IDS/IPS industriales, y plataformas de análisis de tráfico especializado, que sean capaces de identificar comportamientos anómalos, cambios en patrones de comunicación y accesos no autorizados (Kleinmann & Wool, s. f.). Estas capacidades deben estar alineadas con un centro de operaciones de seguridad (SOC) o al menos con un equipo de respuesta industrial con formación específica en redes OT.

También se recomienda adoptar una política de parches y actualizaciones segura para sistemas industriales, priorizando las actualizaciones críticas en componentes expuestos, sin comprometer la continuidad operativa. En este punto es clave diseñar ventanas de mantenimiento industrial, validar compatibilidad en entornos de prueba, y generar respaldos completos antes de la intervención (Boretto et al., 2024).

Desde una perspectiva organizacional, se sugiere la implementación de planes de formación y concienciación para operadores, ingenieros y técnicos de planta, orientados a fortalecer la cultura de ciberseguridad industrial. Esta formación debe incluir aspectos como manejo seguro de dispositivos USB, identificación de correos sospechosos, políticas de contraseñas y protocolos de actuación frente a eventos anómalos (Cabrera González & Arango Cárdenas, 2023).

Finalmente, se recomienda documentar y mantener actualizado un plan de continuidad operativa y recuperación ante incidentes, que contemple escenarios específicos de ciberataques a los activos SCADA, PLC y HMI. Este plan debe estar alineado con los análisis de riesgo realizados, y contar con responsables definidos, rutas de escalamiento, y procedimientos de recuperación validados (Andrade-Logroño & Cobos-Torres, 2025).

Estas medidas proyectadas para 2025 no solo buscan mitigar el impacto de potenciales ciberataques, sino también establecer una hoja de ruta técnica y organizacional que permita al sector cervecero colombiano avanzar hacia un modelo de producción resiliente, seguro y alineado con los estándares internacionales de protección de infraestructuras críticas.

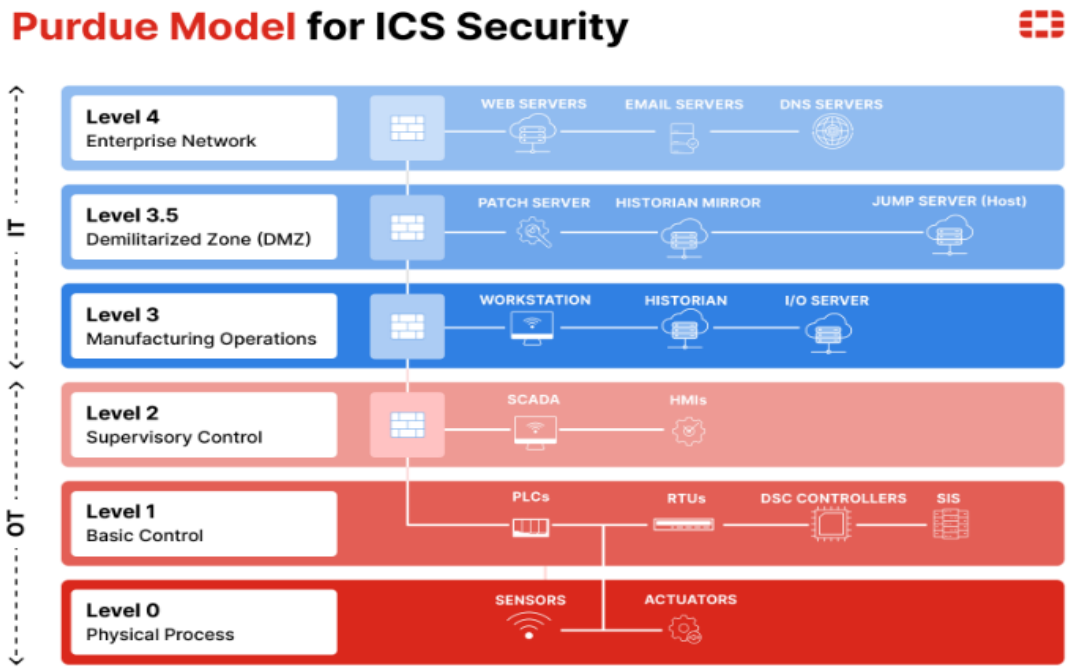
Diseñar una Propuesta de SOC Especializado en OT, Integrando Soluciones Fortinet, para la Industria Cervecera Colombiana, a Ser Presentada a Finales del Año 2025, con el Fin De Mejorar la Detección y Respuesta a Ciberataques.

El presente capítulo desarrolla una propuesta concreta para el diseño de un Centro de Operaciones de Seguridad (SOC) especializado en entornos de Tecnologías Operativas (OT), debe partir del entendimiento del modelo tradicional de SOC en entornos IT. El trabajo de (Román-Torres, 2019) ofrece una guía sólida para este propósito, ya que desglosa funciones críticas del SOC como la prevención, detección y respuesta ante incidentes, además de un enfoque metodológico integral que puede ser adaptado a las particularidades del entorno industrial.

A diferencia de un SOC convencional enfocado en la protección de sistemas administrativos, la presente propuesta está diseñada para abordar los desafíos específicos de los entornos OT, tales como la disponibilidad continua, la baja tolerancia a interrupciones y la necesidad de monitoreo en tiempo real de redes industriales. En este contexto, (Fortinet, s. f.-a, p. Fortinet) define un SOC como una unidad dedicada al análisis de seguridad continua que permite a las organizaciones prevenir, detectar, evaluar y responder eficazmente ante amenazas que afecten tanto infraestructura como procesos de negocio. Esta definición es reforzada por la visión planteada por Román Torres (2019), quien argumenta que un SOC debe ser capaz de adaptarse al tipo de organización y a los riesgos específicos de su operación.

Figura 2

Modelo Purdue Aplicado por Fortinet para Protección OT/IT



*Nota***.** La figura ilustra el Modelo Purdue para la Seguridad de Sistemas de Control Industrial (ICS), una arquitectura de referencia fundamental para la segmentación y protección de entornos operativos críticos. Este modelo estratifica una organización industrial en distintos niveles funcionales, estableciendo una clara demarcación entre los dominios de Tecnología Operacional (OT) y Tecnología de la Información (IT). Fuente. (*What Is the Purdue Model for ICS Security?* s. f.) (Fortinet, 2025).

Para el caso colombiano, la industria cervecera enfrenta una serie de retos técnicos y organizacionales que limitan su capacidad de respuesta ante incidentes. Pérez Fernández, (2022) destaca que muchas empresas carecen de una estructura mínima de gestión de ciberseguridad y que los sistemas de monitoreo existentes no están diseñados para correlacionar eventos en

tiempo real, lo cual impide una acción efectiva frente a ataques dirigidos. En consecuencia, se propone un modelo de SOC que se apoye en la arquitectura Security Fabric de Fortinet y que adopte una estructura organizativa escalable, con personal capacitado en normas como IEC 62443, NIST CSF y la ISO/IEC 27001.

Vilcarromero Zubiate & Vilchez Linares (2018) plantean, en su estudio sobre telecomunicaciones, que el establecimiento de un SOC debe partir de una evaluación de madurez en ciberseguridad, la identificación de activos críticos, y una política clara de escalamiento ante incidentes. Estos mismos principios resultan aplicables al entorno cervecero, donde las redes industriales como SCADA, PLCs y HMIs deben ser monitoreadas con herramientas adaptadas a sus protocolos de comunicación (Modbus, OPC UA, entre otros) y donde el impacto de una interrupción puede afectar directamente la productividad, calidad y reputación de la planta.

Fortinet, por su parte, propone una arquitectura modular de SOC que incluye tecnologías como FortiSIEM para correlación de eventos, FortiSOAR para automatización de respuestas, FortiNDR para detección basada en inteligencia artificial, y FortiAnalyzer para centralización de logs (Fortinet, 2025). Este ecosistema puede adaptarse a las condiciones operativas de las plantas cerveceras, permitiendo implementar un SOC escalable desde una fase piloto hasta un entorno 24/7 con capacidad de respuesta distribuida.

Por tanto, el diseño de este SOC OT especializado no solo debe contemplar la dimensión técnica, sino también la organizativa y normativa, integrando procesos definidos, personal capacitado, herramientas especializadas y marcos de gestión alineados a estándares internacionales. Las siguientes secciones desarrollarán en detalle estos componentes.

Estructura Organizativa del SOC Industrial Cervecero

El diseño funcional de un SOC especializado en entornos OT exige una estructura organizativa clara, escalable y con roles definidos que permitan operar en turnos continuos, alineados con los procesos de producción industrial. En este modelo propuesto para la industria cervecera colombiana, se contempla una estructura de tipo mediana, con la capacidad de operar 24/7 y responder a eventos en tiempo real que afecten tanto a las redes OT como IT.

Según el modelo propuesto por Román Torres (2019), un SOC debe conformarse por al menos tres niveles de analistas (Nivel 1, 2 y 3), además de un coordinador de incidentes y un jefe de operaciones que funcione como enlace entre el área técnica y la alta dirección. Para entornos OT, esta estructura requiere ser ampliada con roles adicionales, como un ingeniero de automatización OT, capaz de interpretar eventos en redes industriales, y un oficial de cumplimiento normativo enfocado en estándares como IEC 62443 y NIST CSF.

Vilcarromero Zubiate y Vilchez Linares (2018) insisten en la necesidad de contar con una gobernanza clara dentro del SOC, definiendo responsabilidades desde la planificación de la seguridad hasta la supervisión de su efectividad. Este principio cobra especial importancia en una planta cervecera, donde el área de tecnología debe coordinarse estrechamente con mantenimiento, control de calidad y producción.

Adicionalmente, Pérez Fernández (2022) recomienda la asignación de perfiles técnicos con experiencia en herramientas específicas de seguridad, incluyendo SIEMs, IDS/IPS, correladores y sistemas de respaldo. En su diseño de SOC para una empresa de servicios, el autor destaca que la capacitación técnica inicial, el conocimiento del entorno y la gestión del conocimiento a través de la documentación de casos, son elementos críticos para el éxito operativo del centro.

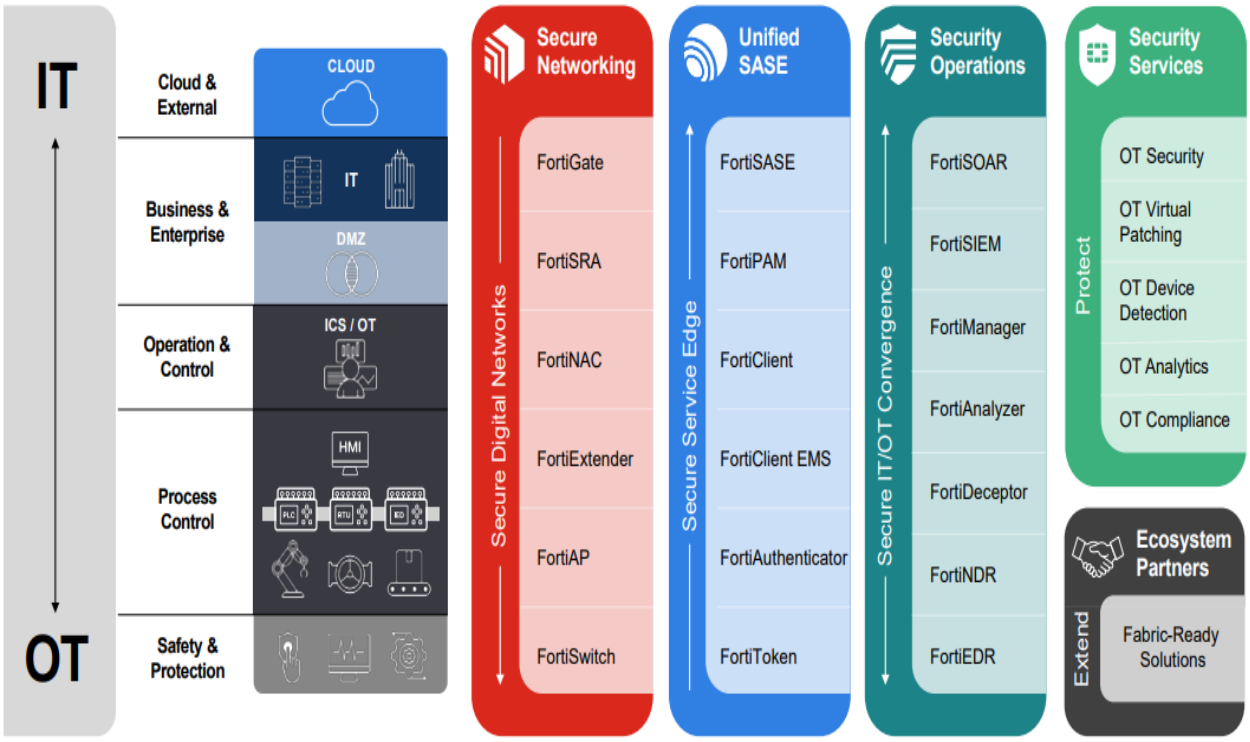
El personal debe ser seleccionado y formado bajo un enfoque dual: conocimiento técnico en ciberseguridad y comprensión del entorno industrial. Esto implica entrenamientos continuos en análisis de tráfico OT, gestión de vulnerabilidades en PLCs, lectura de protocolos industriales y comprensión de los procesos de producción cervecera. El SOC no debe verse como una entidad ajena a la operación, sino como un componente transversal al negocio.

Arquitectura Tecnológica del SOC con Soluciones Fortinet

La propuesta tecnológica para este SOC OT toma como base la plataforma de Operaciones de Seguridad de Fortinet, cuyo enfoque modular y escalable permite adaptarse tanto a grandes corporaciones como a plantas industriales de mediana escala. (Fortinet, s. f.-a, s. f.-b, 2025) establece que una arquitectura de SOC efectiva debe integrar elementos para supervisión continua, correlación, inteligencia artificial, orquestación y automatización de respuestas, todo ello orquestado desde una plataforma de comando centralizada.

Figura 3

Arquitectura de referencia para SOC industrial con herramientas Fortinet



Nota. La figura ilustra la Plataforma de Seguridad de Fortinet, diseñada para proteger entornos complejos que abarcan tanto la Tecnología de la Información (IT) como la Tecnología Operacional (OT). La arquitectura presentada detalla cómo las soluciones de Fortinet se integran en las diferentes capas de una infraestructura industrial moderna, desde la nube empresarial hasta el control de procesos físicos, gestionando la creciente convergencia IT/OT. Fuente. (*What Is the Purdue Model for ICS Security?*, s. f.)

En este sentido, se propone una arquitectura que incluya las siguientes herramientas Fortinet:

FortiSIEM: como plataforma de correlación y análisis de eventos en tiempo real, compatible con más de 500 dispositivos y protocolos, incluyendo los usados en entornos OT.

FortiAnalyzer: para la centralización de logs, visualización gráfica de eventos y generación de informes regulatorios.

FortiSOAR: para la automatización de flujos de trabajo ante incidentes, integrando playbooks adaptados a entornos industriales.

FortiNDR: como sistema de detección de amenazas avanzadas, con capacidades de inteligencia artificial para identificar comportamientos anómalos en redes OT.

FortiGate Rugged y FortiSwitch Industrial: para la segmentación de redes industriales bajo el modelo Purdue, con capacidades de inspección profunda de protocolos como Modbus, DNP3 y OPC UA.

Tal como señala Fortinet (2025), estas herramientas se integran mediante su arquitectura Security Fabric, que facilita la interoperabilidad entre dispositivos de red, plataformas SIEM, entornos cloud, y sistemas SCADA. La visibilidad unificada que ofrece esta integración permite detectar comportamientos sospechosos en zonas críticas como la fermentación, el envasado o la calibración de válvulas automatizadas, mitigando riesgos antes de que se conviertan en incidentes operacionales graves.

En el diseño de referencia propuesto por Pérez Fernández (2022), se plantea una arquitectura virtualizada sobre servidores internos, integrando herramientas como Nagios o PRTG, GLPI, Wazuh y SNORT. Esta estructura puede funcionar como laboratorio o entorno de pruebas, pero para una operación en planta se recomienda un entorno híbrido que combine software libre con licencias Fortinet, priorizando la estabilidad, soporte técnico y actualizaciones automáticas.

Por su parte, Román Torres (2019) establece que la arquitectura lógica de un SOC debe contemplar múltiples capas de seguridad, desde el borde hasta el core de red, incluyendo zonas

de desmilitarización (DMZ), segmentación de tráfico y monitoreo pasivo para evitar interferencias en redes críticas. Esta arquitectura se replica en el modelo Fortinet con dispositivos especializados que permiten aplicar microsegmentación y control granular sobre flujos OT/IT.

La arquitectura tecnológica propuesta permite un monitoreo continuo y contextual de los procesos cerveceros, habilitas respuestas automatizadas en función de la criticidad de los activos afectados y proporciona una base sólida para escalar hacia un SOC regional o multisede en el futuro.

Procesos Operativos y Flujos de Respuesta Automatizada.

La eficacia de un SOC no depende exclusivamente de la tecnología empleada, sino también de la definición clara y sistemática de sus procesos operativos. Estos procesos deben estar orientados a garantizar la detección oportuna de anomalías, la respuesta eficiente a los incidentes y la recuperación controlada de la operación industrial. En el entorno OT de la industria cervecera, donde los procesos son continuos y altamente sensibles a interrupciones, es esencial implementar flujos de trabajo automatizados que minimicen la intervención humana, pero sin perder control estratégico.

Román Torres (2019) propone un modelo funcional basado en seis fases: preparación, identificación, análisis, contención, erradicación y recuperación. Este modelo, alineado con el NIST SP 800-61r2, se complementa con una fase final de aprendizaje organizacional, denominada “lecciones aprendidas”, orientada a documentar el incidente y reforzar la capacidad de respuesta futura.

En el caso del SOC propuesto, cada fase está soportada por herramientas de la plataforma Fortinet. La identificación y análisis se realizan mediante FortiSIEM y FortiNDR, que recolectan y correlacionan eventos de múltiples fuentes. La contención y erradicación son gestionadas a

través de FortiSOAR, que automatiza tareas como aislamiento de segmentos de red, bloqueo de IPs maliciosas y ejecución de scripts de control en dispositivos OT. La recuperación, por su parte, se apoya en sistemas de respaldo y políticas de configuración segura que pueden ser gestionadas mediante FortiManager.

Fortinet (s.f.) destaca que la automatización de procesos mediante playbooks estructurados permite reducir el tiempo de respuesta de horas a minutos, eliminando tareas repetitivas y optimizando la asignación de recursos humanos. Esta automatización también permite mantener la trazabilidad de las acciones ejecutadas, facilitando auditorías internas o externas, y fortaleciendo el cumplimiento regulatorio.

La automatización también se extiende al análisis proactivo mediante inteligencia artificial. Con FortiAI y FortiNDR, el SOC puede analizar patrones de comportamiento anómalos en redes industriales, incluso cuando no existe una firma de ataque conocida. Esto resulta fundamental para detectar amenazas avanzadas persistentes (APT), que suelen camuflarse como tráfico legítimo en entornos OT.

los procesos operativos del SOC propuesto se apoyan en una lógica automatizada y orquestada, donde cada evento genera una cadena de acciones correctivas predefinidas, validadas previamente por el equipo de analistas y adaptadas a los activos críticos de la planta.

Nivel de Servicio (SLA) para el SOC OT Cervecero.

Los Acuerdos de Nivel de Servicio (SLA) son instrumentos fundamentales para definir expectativas claras entre el SOC y sus usuarios internos o externos, estableciendo tiempos, métricas de calidad y responsabilidades. En entornos OT industriales, donde la continuidad operativa es crítica, la implementación de SLAs permite formalizar compromisos sobre

respuesta, monitoreo y resolución de incidentes, asegurando una operación confiable y alineada con las necesidades del negocio**.**

De acuerdo con un análisis especializado sobre SOC realizado por Scitum (2021), los SLA dentro de un SOC deben especificar los niveles de desempeño esperados, los criterios de tiempo de respuesta, la cobertura del servicio y los procesos de escalamiento definidos. Estos acuerdos son gestionados junto con los Acuerdos de Nivel Operativo (OLA), que definen responsabilidades internas entre equipos técnicos (SCITUM, 2021).

En el contexto de la planta cervecera colombiana, se propone que el SOC defina SLAs para aspectos como:

Tiempo máximo de respuesta para incidentes OT críticos, por ejemplo, menos de 15 minutos para incidentes que afecten SCADA o controladores.

Disponibilidad del monitoreo 24/7, garantizando cobertura permanente.

Tasa máxima aceptable de falsos positivos, por ejemplo, menos del 5% por semana.

Tiempo de resolución o contención efectiva, medido desde la detección hasta el restablecimiento del servicio primario.

Estos parámetros deben alinearse con los objetivos estratégicos de la planta y su política de continuidad de negocio.

Implementar SLA implica también establecer mecanismos de monitoreo y reporte. El SOC debe generar informes periódicos que reflejen indicadores de cumplimiento, desviaciones y acciones correctivas realizadas. Estos reportes deben presentarse trimestralmente ante el comité técnico y la gerencia de planta para sustentar la mejora continua.

Además, dentro del marco de gestión de proveedores, ISO/IEC 27036 promueve la inclusión de cláusulas de seguridad en los contratos y SLA con terceros, especialmente cuando el

SOC interactúa con proveedores externos o opera mediante modelos como SOC-as-a-Service (*ISO/IEC 27036-4*, 2016). Esto es particularmente relevante si se externaliza parte de la operación, ya que permite establecer penalizaciones, responsabilidades y mecanismos de escalamiento contractual claros.

La definición correcta de SLA también contribuye a la gobernanza del SOC: como afirman Román Torres (2019) y Vilcarromero Zubiate (2018), una estructura de servicio formal permite ordenar procesos, definir roles y garantizar que los niveles de servicio técnico estén alineados con las metas corporativas y normativas (Román Torres, 2019; Vilcarromero Zubiate & Vilchez Linares, 2018).

Tabla 6

Estructura y Tiempos de Respuesta SLA

Área de Servicio	Métrica Clave	Objetivo del SLA
Detección de Incidentes	Tiempo Promedio de Detección (MTTD - Mean Time To Detect)	Reducir el MTTD a menos de 30 minutos para incidentes críticos.
Respuesta a Incidentes	Tiempo Promedio de Respuesta (MTTR - Mean Time To Respond)	Iniciar la respuesta a incidentes críticos en menos de 15 minutos.
Contención de Incidentes	Tiempo Promedio de Contención (MTTC - Mean Time To Contain)	Contener incidentes críticos en menos de 2 horas.
Resolución de Incidentes	Tiempo Promedio de Resolución (MTTR - Mean Time To Resolve)	Resolver incidentes críticos en menos de 24 horas.
Disponibilidad de Herramientas SOC	Porcentaje de tiempo de actividad de las herramientas de seguridad del SOC	Mantener la disponibilidad de las herramientas clave del SOC en >= 99.5%.
Generación de Informes	Tiempo de entrega de informes de incidentes y análisis de vulnerabilidades	Entregar informes en 4 horas desde la finalización del análisis.
Gestión de Amenazas	Porcentaje de amenazas conocidas bloqueadas	Bloquear >= 99.8% de las amenazas conocidas.
Actualización de Inteligencia	Frecuencia de actualización de fuentes de inteligencia de amenazas (TI)	Actualizar fuentes de TI cada 60 minutos.

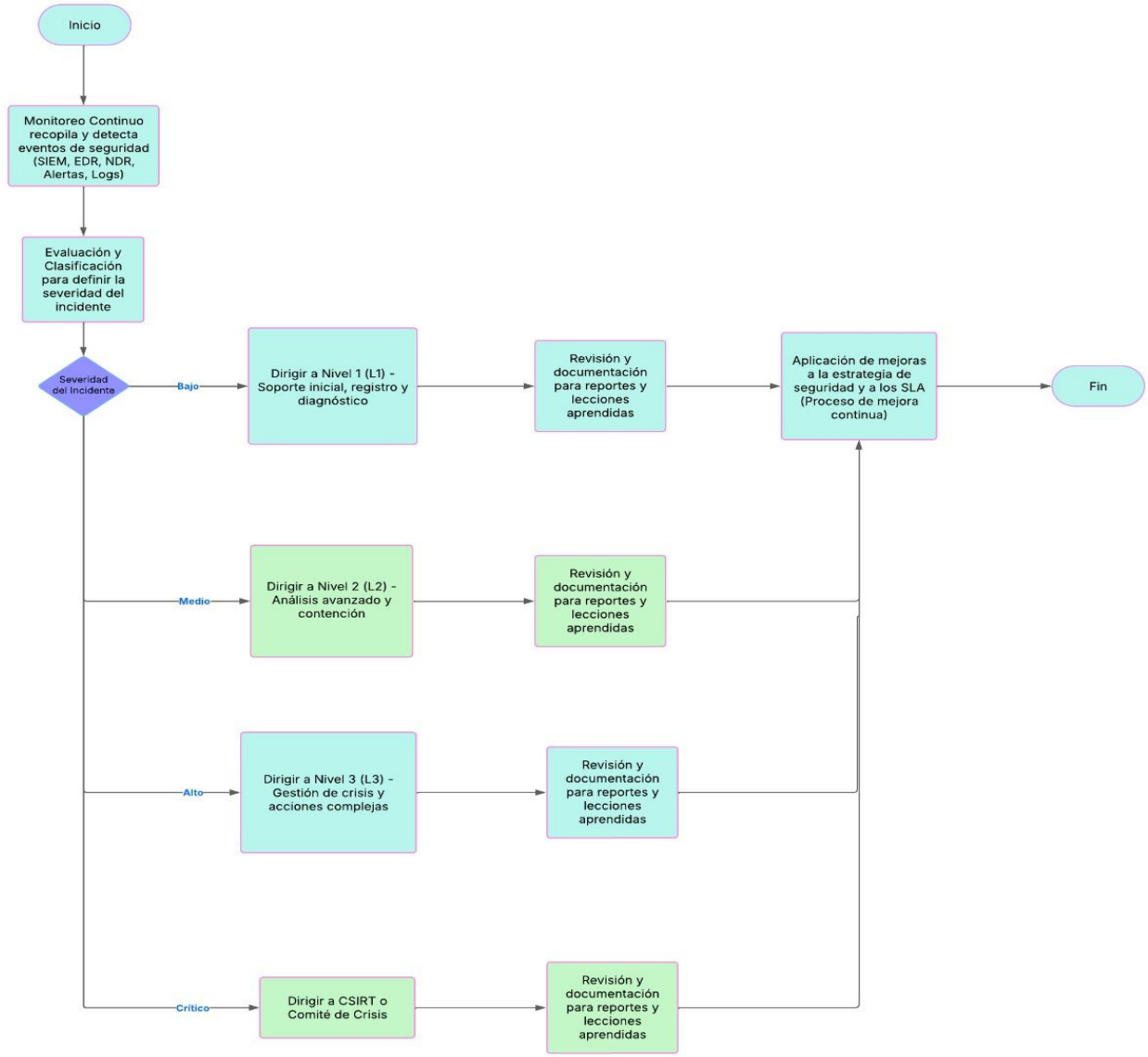
Nota. Basado en el fuente (SCITUM, 2021)

La operación del SOC especializado debe estar respaldada por flujos de trabajo estructurados que aseguren una respuesta eficiente y escalonada ante los distintos niveles de severidad de los incidentes. La Figura 3 presenta un diagrama de flujo que ilustra el proceso de monitoreo, clasificación y escalamiento de incidentes dentro del SOC. Este modelo se apoya en

la lógica de niveles de atención técnica (L1, L2, L3) y en la activación del CSIRT para eventos críticos. Cada ruta contempla la documentación de lecciones aprendidas y retroalimentación para aplicar mejoras continuas, en línea con los SLA establecidos. Este enfoque permite no solo responder eficazmente, sino también mejorar progresivamente las capacidades del SOC (Román Torres, 2019; Fortinet, s.f.; Scitum, 2021).

Figura 4

Diagrama de Flujo SLA



Indicadores clave de desempeño (KPIs) en entornos OT

Medir el rendimiento del SOC es esencial para validar su efectividad, justificar su inversión y aplicar mejoras continuas. Para ello, se deben establecer indicadores de desempeño específicos que reflejen tanto la eficiencia operativa como el impacto real en la producción cervecera.

Román Torres (2019) propone indicadores como el Tiempo Medio de Detección (MTTD), el Tiempo Medio de Respuesta (MTTR) y el porcentaje de incidentes correctamente escalados. En entornos industriales, estos indicadores deben complementarse con otros más específicos, como el tiempo de indisponibilidad de sistemas SCADA, la cantidad de falsos positivos que afectan procesos de producción, y el número de intervenciones exitosas sin detención de líneas productivas.

Vilcarromero Zubiate y Vilchez Linares (2018) destacan la importancia de aplicar un modelo de madurez que evalúe la evolución del SOC no solo en cuanto a capacidades tecnológicas, sino también a nivel de procesos, personal y cultura organizacional. Para ello, proponen un enfoque gradual que permita escalar la capacidad del SOC desde una operación parcial a una gestión estratégica integrada.

Fortinet (2024.) recomienda utilizar dashboards visuales e indicadores en tiempo real para facilitar la toma de decisiones del equipo SOC, y mejorar la comunicación con los responsables de tecnología y operaciones. Herramientas como FortiAnalyzer y FortiSIEM ofrecen tableros personalizables que muestran tendencias, alertas críticas, fuentes más frecuentes de incidentes y nivel de exposición general de la organización.

A continuación, se presenta una lista de KPIs sugeridos para el SOC OT cervecero:

MTTD (Mean Time to Detect): Tiempo promedio entre la ocurrencia y detección de un incidente.

MTTR (Mean Time to Respond): Tiempo promedio entre la detección y la contención o mitigación del incidente.

Tasa de falsos positivos: Porcentaje de alertas que no corresponden a incidentes reales.

Porcentaje de incidentes OT impactando procesos: Relación entre incidentes detectados y los que afectan directamente la operación.

Número de alertas críticas resueltas automáticamente: Indicador del grado de madurez de la automatización.

Disponibilidad mensual del sistema SCADA/PLC supervisado: Refleja el impacto indirecto del SOC en la continuidad operativa.

Estos indicadores no solo deben medirse, sino reportarse regularmente a la dirección técnica y al comité de riesgos de la planta, permitiendo una retroalimentación efectiva y la asignación adecuada de recursos para mejorar la postura de seguridad industrial.

Alineación Normativa y Cumplimiento Regulatorio.

La eficacia del SOC especializado en entornos OT no solo depende de la tecnología y el personal que lo conforman, sino también de su alineación con marcos normativos reconocidos a nivel internacional. Estas normativas aportan lineamientos esenciales para la gestión de riesgos, la implementación de controles y la mejora continua de la postura de ciberseguridad industrial.

En primer lugar, la norma IEC 62443, desarrollada por la ISA (International Society of Automation), proporciona un enfoque estructurado para proteger sistemas de control industrial (ICS) mediante la definición de zonas y conduits, modelos de madurez y requisitos de seguridad técnica. Esta norma resulta fundamental para segmentar redes OT e implementar controles

específicos por niveles, permitiendo una arquitectura segura desde sensores hasta aplicaciones de monitoreo (Piggin, 2013).

En segundo lugar, el marco NIST Cybersecurity Framework (CSF) permite establecer capacidades de identificación, protección, detección, respuesta y recuperación ante ciberincidentes. Este modelo es especialmente útil para organizaciones en proceso de madurez, ya que propone una autoevaluación de capacidades que puede ser aplicada directamente al SOC, mediante controles adaptables al nivel de criticidad de la planta (NIST, 2018).(National Institute of Standards and Technology, 2024, 2024; Sañicela & Xavier, 2023).

Finalmente, la norma ISO/IEC 27001:2022 aporta un Sistema de Gestión de Seguridad de la Información (SGSI) que articula las políticas del SOC con los objetivos del negocio, facilitando auditorías y cumplimiento con estándares internacionales. Esta norma es útil para definir procesos formales de gestión de activos, tratamiento de riesgos, controles técnicos y medidas de continuidad del servicio, incluyendo lo relacionado con proveedores y acuerdos de nivel de servicio (Solarte et al., 2015).

Como señalan Vilcarromero Zubiate y Vilchez Linares (2018), los marcos normativos no deben ser vistos como requisitos regulatorios aislados, sino como herramientas para estructurar una operación eficiente del SOC y elevar su madurez operacional. Alinearse con estas normativas permite también optar a certificaciones internacionales, aumentar la confianza de socios comerciales y fortalecer la reputación organizacional.

Fases de Implementación y Cronograma Estimado.

La puesta en marcha del SOC especializado en OT requiere una planificación progresiva que asegure la viabilidad técnica, organizativa y financiera. Se proponen cinco fases principales

de implementación, cuya ejecución puede desarrollarse en un período estimado de 10 a 12 meses, conforme a los recursos disponibles y el tamaño de la planta cervecera:

Fase 1: Diagnóstico inicial y evaluación de riesgos (Meses 1–2).

Levantamiento de arquitectura OT existente.

Identificación de activos críticos.

Evaluación del nivel de madurez en ciberseguridad (NIST CSF).

Fase 2: Diseño del SOC (Meses 3–4).

Definición de estructura organizativa.

Selección de herramientas Fortinet.

Diseño de arquitectura bajo modelo Purdue e IEC 62443.

Fase 3: Implementación piloto (Meses 5–7).

Instalación de sensores OT, FortiSIEM, FortiAnalyzer y FortiGate Rugged.

Capacitación del personal SOC y producción.

Configuración de flujos de trabajo en FortiSOAR.

Fase 4: Integración y operación formal (Meses 8–10).

Validación del modelo de operación 24/7.

Afinación de SLA internos.

Inicio del monitoreo real de procesos críticos.

Fase 5: Evaluación y mejora continua (Meses 11–12).

Medición de KPIs operativos.

Auditoría interna de cumplimiento normativo.

Revisión de SLA y retroalimentación organizacional.

Este cronograma puede adaptarse a contextos multicentro si se desea escalar el SOC a más de una planta industrial. Asimismo, el modelo es compatible con la externalización parcial mediante SOC-as-a-Service (SOCaaS), en casos donde los recursos locales son limitados.

El diseño del SOC propuesto para la industria cervecera colombiana ofrece una solución integral, escalable y alineada a estándares internacionales, capaz de responder de forma efectiva a las amenazas cibernéticas que enfrentan los entornos OT. Mediante el uso de soluciones Fortinet y un enfoque normativo estructurado, se garantiza no solo la protección de los activos críticos, sino también la continuidad del negocio y la resiliencia operativa de las plantas de producción.

Conclusiones

La presente investigación, desarrollada bajo un enfoque cualitativo-descriptivo, permitió realizar un análisis exhaustivo de los riesgos vinculados a la ciberseguridad en redes OT dentro de la industria cervecera colombiana. A partir de una rigurosa revisión documental y un profundo análisis del contexto sectorial, se identificaron las particularidades operativas, tecnológicas y organizacionales que condicionan la vulnerabilidad de las plantas cerveceras, lo que condujo a la propuesta de implementación de un Centro de Operaciones de Seguridad (SOC) especializado como solución integral.

Los resultados evidencian que la creciente integración entre tecnologías IT y OT ha incrementado exponencialmente las superficies de ataque, exponiendo activos críticos como sistemas SCADA, PLC, sensores industriales y servidores de automatización. Esta situación se agrava debido a la insuficiencia de medidas específicas de ciberseguridad industrial y a un bajo nivel de madurez digital en algunas plantas, lo cual convierte a la industria cervecera en un blanco vulnerable para ataques dirigidos que pueden comprometer la seguridad alimentaria, la continuidad operativa y la reputación empresarial.

En este sentido, la implementación de un SOC especializado en entornos OT constituye no solo una solución tecnológica, sino una estrategia organizacional fundamental para fortalecer la resiliencia cibernética. La propuesta integra tecnologías como SIEM, EDR, IDS y plataformas basadas en inteligencia artificial para la detección temprana de anomalías, alineadas con marcos normativos internacionales como ISO/IEC 27001, IEC 62443 y el NIST Cybersecurity Framework. Asimismo, se fundamenta en arquitecturas robustas, como el Modelo Purdue, que posibilita una segmentación eficiente de la red industrial y la aplicación de una defensa en profundidad.

El componente humano también resulta crucial para el éxito de esta estrategia, destacando la necesidad de equipos capacitados en respuesta a incidentes, análisis forense y monitoreo continuo, capaces de actuar de manera efectiva frente a amenazas avanzadas en tiempo real.

Este trabajo no solo aporta un marco técnico para la implementación de un SOC en plantas cerveceras, sino que también sienta las bases para la formulación de políticas de ciberseguridad industrial, la adopción de estándares internacionales y el fortalecimiento de una cultura organizacional orientada a la protección de infraestructuras críticas. Con ello, se contribuye a garantizar la sostenibilidad, competitividad y confianza del sector cervecero colombiano en la era digital.

El análisis detallado de los sistemas SCADA, PLC y HMI en el contexto de las plantas cerveceras colombianas confirma la creciente vulnerabilidad de estos activos críticos frente a ciberataques. La convergencia entre tecnologías OT y TI ha ampliado la superficie de ataque, exponiendo infraestructuras esenciales a amenazas que ponen en riesgo la continuidad operativa y la calidad del producto final.

La aplicación de metodologías de análisis de riesgos, como MAGERIT y NIST SP 800-30, facilita la identificación y evaluación precisa de las amenazas específicas que enfrentan estos sistemas, permitiendo priorizar adecuadamente las medidas de protección. La implementación de estas metodologías en el entorno cervecero Colombiano subraya la necesidad de una estrategia de ciberseguridad integral que considere las particularidades de cada planta, tales como el nivel de automatización, conectividad y recursos disponibles.

Recomendaciones

A partir de los hallazgos obtenidos en esta investigación, se proponen a continuación una serie de recomendaciones estratégicas orientadas a robustecer la ciberseguridad en redes OT dentro de la industria cervecera colombiana. Estas sugerencias están enfocadas en la implementación de un Centro de Operaciones de Seguridad (SOC) especializado, considerando tanto los marcos normativos aplicables como las particularidades operativas del sector productivo.

Es aconsejable que las organizaciones del sector mantengan un proceso continuo de identificación y evaluación de vulnerabilidades en sus infraestructuras OT. Esta tarea debe centrarse en detectar configuraciones inseguras, dispositivos desactualizados y el uso de protocolos industriales sin mecanismos de cifrado. Para llevarlo a cabo, es recomendable apoyarse en marcos técnicos como la norma IEC 62443, el modelo Purdue y metodologías como Margerit, ya que permiten ubicar correctamente los activos críticos dentro de una jerarquía funcional. Complementar este análisis con esquemas actualizados de red facilitará la toma de decisiones y la priorización de medidas correctivas.

También se sugiere aplicar metodologías formales de análisis de riesgo que permitan valorar el impacto potencial de ciberataques sobre sistemas industriales esenciales, como SCADA, PLC y HMI. Herramientas como el marco NIST SP 800-30, combinadas con matrices de impacto y probabilidad, permitirán establecer prioridades en la protección de activos. Estos análisis deben incluir escenarios realistas, basados en incidentes reportados en la industria, con el fin de justificar decisiones técnicas y orientar futuras inversiones en ciberseguridad industrial.

En cuanto a la implementación de un SOC, se propone diseñar una solución adaptada a las características operativas de las plantas cerveceras. Se recomienda integrar tecnologías

Fortinet, tales como FortiGate Rugged para proteger el perímetro industrial, FortiSIEM para la correlación de eventos, FortiAnalyzer para el análisis forense y FortiNAC para el control de accesos. Esta arquitectura debe contemplar sensores distribuidos, gestión centralizada de registros, y procedimientos claros para la generación de alertas y la respuesta a incidentes. Es fundamental definir tiempos máximos de detección y reacción, sustentados en acuerdos de nivel de servicio (SLA) que reflejen la criticidad de los procesos industriales.

Para facilitar su adopción, se plantea implementar el SOC por fases. Inicialmente, se sugiere comenzar con capacidades básicas de monitoreo y alertamiento; posteriormente, incorporar automatización en la respuesta; y en una tercera etapa, integrar inteligencia de amenazas y capacidades de orquestación de incidentes. Este enfoque gradual permitirá una implementación viable en términos técnicos y presupuestales. Además, es necesario definir un equipo mínimo de operación, con funciones específicas para analistas de seguridad, especialistas en redes OT y personal de soporte, garantizando una cobertura adecuada y continua.

Es imprescindible mantener una segmentación estricta entre las redes IT y OT. Esta separación debe estar respaldada por controles como firewalls industriales, zonas de desmilitarización (DMZ), políticas de acceso restringido y sistemas de inspección profunda. Más que buscar una integración entre ambos entornos, lo recomendable es establecer mecanismos de interoperabilidad controlada, que permitan el monitoreo y análisis sin comprometer la estabilidad de los sistemas industriales. Este enfoque contribuye a prevenir la propagación de amenazas entre dominios y refuerza la capacidad del SOC para responder de forma efectiva ante cualquier incidente.

Bibliografía

Álvarez, J. R. (s. f.). *Consecuencias de un ciberataque en entornos industriales*. Telefónica Tech. 28 de mayo de 2025, de https://telefonicatech.com/blog/consecuencias-de-un-ciberataque-en-entornos-industriales

Andrade-Logroño, F., & Cobos-Torres, J. C. (2025). Vulnerabilidades y ciberseguridad en sistemas SCADA: Análisis de riesgos y estrategias de protección en infraestructuras críticas. *MQRInvestigar*, *9*(1), Article 1. https://doi.org/10.56048/MQR20225.9.1.2025.e289

Bernal Mora, Y. N., Noguera Bocachica, J. A., & Santos Suárez, J. W. (2024). *Diseño de un centro de operaciones de ciberseguridad (SOC) basado en la norma ISO 27001 para el centro médico Oasis Colombia*. https://repository.ucc.edu.co/entities/publication/repository.ucc.edu.co

Boretto, M., Martín, C., & Margheim, D. (2024). *Análisis de la amenaza cibernética en el sector eléctrico argentino: Implicancias*. https://cefadigital.edu.ar/handle/1847939/3026

Ciberseguridad en el modelo de Purdue: Dispositivos de nivel 1 | INCIBE-CERT | INCIBE. (s. f.). Recuperado 25 de mayo de 2025, de https://www.incibe.es/incibe-cert/blog/ciberseguridad-el-modelo-purdue-dispositivos-nivel-1

Cordero-Robles, H. Y. (2021). *Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework, para el mejoramiento y estandarización de las evaluaciones tecnológicas del área de auditoría de TI que apoya las auditorías financieras de los clientes de HCR*. https://repositoriotec.tec.ac.cr/handle/2238/13508

Cybersecurity Certificates—ISA. (2025). Isa.Org. https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program

Fole de Navia de la Cruz, A. (2024). *Centro de operaciones de seguridad con despliegue y escalado automatizado*. https://riunet.upv.es/entities/publication/8785a15b-d613-400e-8aa7-49a6743dde0c

Fortinet. (s. f.-a). *¿Qué es un Centro de operaciones de seguridad (SOC)?* Fortinet. 27 de julio de 2025, de https://www.fortinet.com/lat/resources/cyberglossary/what-is-soc.html

Fortinet. (s. f.-b). *Servicio de seguridad para OT de FortiGuard*. Fortinet. Recuperado 29 de mayo de 2025, de https://www.fortinet.com/lat/support/support-services/fortiguard-security-subscriptions/industrial-security.html

Fortinet. (2025). *SIEM, SOAR, and XDR in a SOC | Security Operations Concept Guide*. https://docs.fortinet.com/document/fortianalyzer/7.6.0/security-operations-concept-guide/545849/docs.fortinet.com/document/fortianalyzer/7.6.0/security-operations-concept-guide/545849/siem-soar-and-xdr-in-a-soc

García Núñez, N. (2024). *Análisis, explotación y refuerzo de vulnerabilidades en entornos de convergencia IT/OT*. https://uvadoc.uva.es/handle/10324/71360

ISA95. (s. f.). *Beyond the Pyramid: Using ISA95 for Industry 4.0 and Smart Manufacturing*. ISA.ORG. Recuperado 25 de mayo de 2025, de https://www.isa.org/intech-home/2021/october-2021/features/beyond-the-pyramid-using-isa95-for-industry-4-0-an

ISA99, Industrial Automation&Control Sys Security- ISA. (s. f.). Isa.Org. Recuperado 25 de mayo de 2025, de https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99

ISO/IEC 27036-4:2016. (2016). ISO. https://www.iso.org/standard/59689.html

Ley 1273 de 2009—Gestor Normativo. (s. f.). Recuperado 29 de mayo de 2025, de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. (s. f.).

National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (No. NIST CSWP 29; p. NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pachón, C. (2022, octubre 19). 4 ataques importantes que han interrumpido la producción de sistemas industriales en el mundo. *NSIT*. https://www.nsit.com.co/4-ataques-importantes-que-han-interrumpido-la-produccion-de-sistemas-industriales-en-el-mundo/

Pérez Fernández, M. (2022). *Diseño de un centro de operación de seguridad – SOC para la Empresa Platino Sistema*. http://repository.unad.edu.co/handle/10596/50119

Piggin, R. S. H. (2013). Development of industrial cyber security standards: IEC 62443 for SCADA and Industrial Control System security. *IET Conference on Control and Automation 2013: Uniting Problems and Solutions*, 1-6. https://doi.org/10.1049/cp.2013.0001

Riesgos de no proteger un proceso industrial con ciberseguridad | IMEPI México. (s. f.). Recuperado 28 de mayo de 2025, de https://imepi.com.mx/riesgos-de-no-proteger-un-proceso-industrial-con-ciberseguridad/

Román-Torres, M. J. (2019). *Proceso para Definir y Establecer un Centro de Operaciones de Seguridad (SOC) en una Organización Financiera* [masterThesis]. https://reunir.unir.net/handle/123456789/8169

Sañicela, R., & Xavier, S. (2023). *Análisis comparativo de metodologías de análisis de riesgos (MAGERIT vs. NIST SP 800-30)*.

SCITUM. (2021). *CENTRO DE OPERACIONES DE CIBERSEGURIDAD*.

Serna, C. A. S., & Ortiz, L. C. C. (2011). Buses de campo y protocolos en redes industriales. *Ventana Informática*, *25*, Article 25. https://doi.org/10.30554/ventanainform.25.126.2011

Solarte, F. N. S., Rosero, E. R. E., & Benavides, M. del C. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica - ESPOL*, *28*(5), Article 5. https://rte.espol.edu.ec

Vilcarromero Zubiate, L. L., & Vilchez Linares, E. (2018). Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones. *Universidad Peruana de Ciencias Aplicadas (UPC)*. https://repositorioacademico.upc.edu.pe/handle/10757/624832

What Is the Purdue Model for ICS Security? (s. f.). Fortinet. 25 de mayo de 2025, de https://www.fortinet.com/resources/cyberglossary/purdue-model

Apéndices

Apéndice A

Glosario

Cadena de Suministro y Riesgos Externos	Evaluación y gestión de los riesgos derivados de los proveedores y actores externos que interactúan con la infraestructura tecnológica de la empresa.
Ciber amenazas	Actos intencionales para comprometer la seguridad de los sistemas informáticos o industriales, como malware, ransomware y ataques DDoS.
Ciberseguridad Industrial	Disciplina centrada en proteger los sistemas de control industrial de amenazas cibernéticas, incluyendo ataques a SCADA, PLCs y dispositivos IoT.
Controles de Seguridad	Políticas, procedimientos y tecnologías implementadas para proteger los sistemas y datos de amenazas cibernéticas.
Evaluación de Riesgos	Proceso de identificación, análisis y evaluación de riesgos cibernéticos en la infraestructura tecnológica, tanto OT como IT.
IEC 62443	Estándar internacional para la seguridad de sistemas de control industrial (como SCADA y PLCs), con enfoque en la protección de infraestructuras críticas.
IoT (Internet de las Cosas)	Conexión de dispositivos físicos a través de internet para recopilar y compartir datos, especialmente en entornos industriales.
ISO 27001	Norma internacional que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI).
Marcos de Ciberseguridad	Conjunto de directrices para la gestión de riesgos cibernéticos. Ejemplos incluyen NIST-Cybersecurity Framework, ISO 27001, y IEC 62443.
NIST-Cybersecurity Framework	Conjunto de directrices del NIST (Instituto Nacional de Estándares y Tecnología) para gestionar los riesgos cibernéticos, enfocado en cinco funciones: identificar, proteger, detectar, responder y recuperar.

Norma ISO 31000:2018	Estándar internacional que proporciona directrices para la gestión de riesgos en una organización, incluyendo riesgos operacionales y externos.
PLC (Controlador Lógico Programable)	Dispositivo de automatización industrial utilizado para controlar procesos y máquinas mediante programación, como sensores y actuadores.
Riesgos Cibernéticos	Amenazas que afectan la integridad, confidencialidad y disponibilidad de los sistemas tecnológicos.
SCADA (Supervisión y Control de Adquisición de Datos)	Sistema para monitorear y controlar procesos industriales a distancia, utilizado en plantas de energía, agua y telecomunicaciones.
SOC OT (Centro de Operaciones de Seguridad para Tecnología Operativa)	Centro encargado de monitorear, detectar, prevenir y responder a incidentes de seguridad en sistemas industriales críticos como SCADA, PLC, y IoT.
Tecnologías de la Información (IT)	Sistemas y aplicaciones utilizados para procesar, almacenar y gestionar datos en una organización, como servidores, bases de datos, y redes.
Tecnologías Operacionales (OT)	Sistemas utilizados para controlar y monitorear procesos industriales. Incluye sistemas SCADA, PLC, y dispositivos IoT.