Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE INVESTIGACIÓN DEL PLAN METODOLÓGICO PARA REDUCIR LOS PAROS DE PRODUCCIÓN DEBIDO A LA ALTA VULNERABILIDAD DE ATAQUES CIBERNÉTICOS EN UNA EMPRESA DE MANUFACTURA EN GUATEMALA, UTILIZANDO LA METODOLOGÍA DE LEAN SIX SIGMA

Héctor Alfredo Orozco Toralla
Asesorado por el Ing. Julio César Rodas

Guatemala, enero 2025

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE INVESTIGACIÓN DEL PLAN METODOLÓGICO PARA REDUCIR LOS PAROS DE PRODUCCIÓN DEBIDO A LA ALTA VULNERABILIDAD DE ATAQUES CIBERNÉTICOS EN UNA EMPRESA DE MANUFACTURA EN GUATEMALA, UTILIZANDO LA METODOLOGÍA DE LEAN SIX SIGMA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA
DE LA FACULTAD DE INGENIERÍA
POR

HÉCTOR ALFREDO OROZCO TORALLA
ASESORADO POR EL ING. JULIO CÉSAR RODAS

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO ELECTRÓNICO

GUATEMALA, ENERO DE 2025

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. José Francisco Gómez Rivera (a. i.)
VOCAL II	Ing. Mario Renato Escobedo Martínez
VOCAL III	Ing. José Milton De León Bran
VOCAL IV	Ing. Kevin Vladimir Armando Cruz Lorente
VOCAL V	Ing. Fernando José Paz González
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Julio I. González Podszueck
EXAMINADOR	Ing. Edwin Solares
EXAMINADOR	Ing. Walter Guillén
EXAMINADOR	Ing. Marlene de Hidalgo
SECRETARIO	Ing. Francisco J. González López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE INVESTIGACIÓN DEL PLAN METODOLÓGICO PARA REDUCIR LOS PAROS DE PRODUCCIÓN DEBIDO A LA ALTA VULNERABILIDAD DE ATAQUES CIBERNÉTICOS EN UNA EMPRESA DE MANUFACTURA EN GUATEMALA, UTILIZANDO LA METODOLOGÍA DE LEAN SIX SIGMA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica de la Facultad de Ingeniería, con fecha 28 de septiembre de 2024.

Héctor Alfredo Orozco Toralla

EEPFI-PP-5300-2024
Guatemala, 28 de septiembre de 2024

Director
Armando Alonso Rivera Carrillo
Escuela De Ingenieria Mecanica Electrica
Presente.

Estimado Armando Alonso Rivera Carrillo

Reciba un cordial saludo de la Escuela de Estudios de Postgrado de la Facultad de Ingeniería.

El propósito de la presente es para informarle que se ha revisado y aprobado el Diseño de Investigación titulado: **DISEÑO DE INVESTIGACIÓN DEL PLAN METODOLÓGICO PARA REDUCIR LOS PAROS DE PRODUCCIÓN DEBIDO A LA ALTA VULNERABILIDAD DE ATAQUES CIBERNÉTICOS EN UNA EMPRESA DE MANUFACTURA EN GUATEMALA, UTILIZANDO LA METODOLOGÍA DE LEAN SIX SIGMA**, el cual se enmarca en la línea de investigación: **Área de Operaciones - Análisis de riesgos**, presentado por el estudiante **Héctor Alfredo Orozco Toralla** carné número **008811804**, quien optó por la modalidad del "PROCESO DE GRADUACIÓN DE LOS ESTUDIANTES DE LA FACULTAD DE INGENIERÍA OPCIÓN ESTUDIOS DE POSTGRADO". Previo a culminar sus estudios en la Maestría en Artes en Gestion Industrial.

Y habiendo cumplido y aprobado con los requisitos establecidos en el normativo de este Proceso de Graduación en el Punto 6.2, aprobado por la Junta Directiva de la Facultad de Ingeniería en el Punto Décimo, Inciso 10.2 del Acta 28-2011 de fecha 19 de septiembre de 2011, firmo y sello la presente para el trámite correspondiente de graduación de Pregrado.

Atentamente,

"Id y Enseñad a Todos"

Mtro. Julio Cesar Rodas
Asesor(a)

JULIO CESAR RODAS
Ingeniero Electricista
COL. No.3843

UNIVERSIDAD DE SAN CARLOS
ESCUELA DE POSTGRADO
FACULTAD DE INGENIERIA
DE GUATEMALA

Mtro. Carlos Humberto Aroche Sandoval
Coordinador(a) de Maestría

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECTORA
POSTGRADO

Mtra. Aurelia Anabela Cordova Estrada
Directora
Escuela de Estudios de Postgrado
Facultad de Ingeniería

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

EEP-EIME-5162-2024

El Director de la Escuela De Ingenieria Mecanica Electrica de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del Asesor, el visto bueno del Coordinador y Director de la Escuela de Estudios de Postgrado, del Diseño de Investigación en la modalidad Estudios de Pregrado y Postgrado titulado: **DISEÑO DE INVESTIGACIÓN DEL PLAN METODOLÓGICO PARA REDUCIR LOS PAROS DE PRODUCCIÓN DEBIDO A LA ALTA VULNERABILIDAD DE ATAQUES CIBERNÉTICOS EN UNA EMPRESA DE MANUFACTURA EN GUATEMALA, UTILIZANDO LA METODOLOGÍA DE LEAN SIX SIGMA**, presentado por el estudiante universitario **Héctor Alfredo Orozco Toralla**, procedo con el Aval del mismo, ya que cumple con los requisitos normados por la Facultad de Ingeniería en esta modalidad.

ID Y ENSEÑAD A TODOS

Mtro. Armando Alonso Rivera Carrillo
Director
Escuela De Ingenieria Mecanica Electrica

Guatemala, septiembre de 2024

Decanato
Facultad e Ingeniería

24189101- 24189102

LNG.DECANATO.OIE.5.2025

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE INVESTIGACIÓN DEL PLAN METODOLÓGICO PARA REDUCIR LOS PAROS DE PRODUCCIÓN DEBIDO A LA ALTA VULNERABILIDAD DE ATAQUES CIBERNÉTICOS EN UNA EMPRESA DE MANUFACTURA EN GUATEMALA, UTILIZANDO LA METODOLOGÍA DE LEAN SIX SIGMA**, presentado por: **Hector Alfredo Orozco Toralla** después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Firmado electrónicamente por: José Francisco Gómez Rivera
Motivo: Informe final PREGRADOPOSTGRADO
Fecha: 11/01/2025 19:11:40
Lugar: Facultad de Ingeniería, USAC.

Ing. José Francisco Gómez Rivera
Decano a.i.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO a.i.
Facultad de Ingeniería

Guatemala, enero de 2025

ACTO QUE DEDICO A:

Dios	Por estar conmigo y darme la vida para cumplir esta importante etapa de mi vida.
Mis padres	Héctor Orozco y Marta Toralla (q. e. p. d.), por su apoyo, ejemplo y motivación.
Mi esposa	Lucía Paiz, por su amor, apoyo incondicional y por estar siempre a mi lado.
Mis hijos	Rodrigo y Sofía Orozco, por ser mi motivación a diario y por inspirarme a seguir adelante.
Mis hermanas	Lucky, Ligia, Karla y Mariela Orozco, por su amor y motivación.
Mi suegra	Ana María Ruiz, por su amor, amistad y por darme ánimo en cada momento.

AGRADECIMIENTOS A:

Universidad de San Carlos de Guatemala	Por ser la principal cuna de aprendizaje de mi formación profesional.
Ingenieros	MBA Julio Rodas y MSc. Jeanette Orozco por su apoyo para completar esta importante etapa estudiantil de mi vida.
Mis amigos	Miguel Escobar, Julio Sandoval, Carlos Zamora, Alvaro Monzón y Rafael Cuyán, por su amistad y apoyo en toda la etapa universitaria.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

1. INTRODUCCIÓN

La presente investigación es una sistematización para reducir los paros de producción en las industrias de manufactura, debido a la alta vulnerabilidad a los ataques cibernéticos en el área de la tecnología operativa *OT* (*Operational Technology*), también denominada como el área del piso de planta. Esta investigación se trabajará bajo la línea de investigación del Área de Operaciones y el Análisis de Riesgos.

Debido al requerimiento de incrementar la productividad, muchas industrias de manufactura implementaron en sus procesos productivos la cuarta revolución industrial denominada Industria 4.0, la cual consiste en la integración de tecnologías digitales con el objetivo de obtener más información de cada uno de los diferentes procesos productivos en una industria de manufactura, sin embargo, uso de la tecnología y su conectividad para la recolección de la información, ha generado la vulnerabilidad cibernética en las áreas productivas, las cuales han sido objeto de ataques cibernéticos que han causado grandes pérdidas de la producción en muchas industrias a nivel mundial, representando una oportunidad de negocio fraudulento para los piratas cibernéticos que secuestran la información a cambio de grandes cantidades de dinero.

Esta investigación se desarrollará en un ingenio azucarero que sufrió un ataque cibernético que afectó toda el área administrativa de *IT* (*Information Technology*), lo cual generó una gran preocupación en el área productiva de fabricación y generación de energía en lo que respecta identificar el nivel de vulnerabilidad cibernética con el objetivo de reducir el riesgo de paros de

producción no programados causados por ataques cibernéticos, en base a las recomendaciones finales de la investigación que consistirán en un plan metodológico que propondrá las posibles soluciones y beneficios que se obtendrían de realizarlas, para reducir el riesgo de la ocurrencia de paros no programados en las áreas del piso de planta de fabricación y generación de energía, para no afectar la producción de los procesos productivos del ingenio azucarero.

El desarrollo de esta investigación se desarrollará en 4 fases, como se mostrará en el Esquema de Solución propuesto, que incluirá varias actividades que se desarrollarán cronológicamente para la obtención de los resultados finales. Las 4 fases son la revisión documental, la identificación de los factores y la relación entre los paros de producción y la vulnerabilidad cibernética, analizar el nivel de vulnerabilidad cibernética y, por último, identificar las posibles soluciones para reducir el nivel de vulnerabilidad cibernética y evitar los paros de producción no programados por esta causa, debido a que la afectación de los procesos de fabricación de azúcar y generación de energía de este ingenio podrían llegar a una afectación nacional e internacional.

Debido a que se contará con los recursos necesarios, la accesibilidad de la información y de las personas que trabajan en los procesos productivos de fabricación y generación de energía y la disponibilidad para realizar visitas a campo, se cuenta con la factibilidad de la realización de esta investigación.

Los capítulos del informe final de esta investigación se presentarán con la estructura del índice propuesto, con varios capítulos que contienen la siguiente información: en el primer capítulo se desarrollarán los antecedentes en los que se fundamenta esta investigación, en el segundo capítulo se desarrollará el marco teórico con información que proporcionará la estructura

conceptual requerida para entender, contextualizar y abordar eficazmente el problema de investigación. En el tercer capítulo, se desarrollará la investigación, la cual consiste en 4 fases, con el estudio de factibilidad que valida la viabilidad del desarrollo de esta investigación. En el cuarto capítulo se presentarán los resultados obtenidos conforme a los objetivos de la investigación. En el quinto capítulo y último de esta investigación se discutirán los resultados obtenidos al terminar la investigación.

2. ANTECEDENTES

A continuación, se presenta el estado de arte relacionado con el tema de alta vulnerabilidad de ataques cibernéticos en el piso de planta, habiendo considerado de importancia las siguientes investigaciones debido al desarrollo de investigación y resultados obtenidos, así como las conclusiones respecto al tema de ciberseguridad y gestión de activos.

Para REA (2020), la gestión de riesgos conlleva un análisis sistemático para determinar donde una empresa puede comprometer su operación, las consecuencias y el grado de exposición que una amenaza afecte la vulnerabilidad de uno o más activos causando daños a la organización, y las maneras de reducir la probabilidad o la gravedad de esos daños. El aporte para esta investigación dado que el enfoque es para la gestión de riesgos en el piso de planta de una industria, será el proceso simplificado que se muestra para la gestión de riesgos, pues la gestión de riesgos comienza con los activos, que es lo que se quiere proteger, considerando 4 tipos de activos de interés, personal, instalaciones, procesos e información, también se mencionan varios marcos de ciberseguridad que serán una buena referencia para este trabajo de investigación.

De acuerdo con Chun (2024), el internet de las cosas (*IoT*), es la integración entre objetos convencionales y los seres humanos, mediante su interconexión para satisfacer necesidad de comunicación e interacción en todo momento. La información que se puede obtener de los objetos requiere ser medida, procesada y almacenada de forma segura, por lo que es necesario tener una infraestructura de red capaz de conectar cada vez más dispositivos

por medio de buenas prácticas de gestión de red. El aporte para esta investigación será el modelo de arquitectura y diseño de los dispositivos *IoT* y sus características, así como los diferentes protocolos y estándares de comunicación que hay en el mercado actual sobre la capa de implementación en el modelo OSI, dado que en trabajo de investigación a desarrollar hay una gran diversidad de activos en el piso de planta que se comunican de diferente manera.

Como indica Girón (2021), es necesario que el gobierno guatemalteco se involucre en lo referente a los ataques cibernéticos, por lo que propone una política cibernética para el desarrollo de un plan nacional estratégico de ciberseguridad y así asegurar la integridad de la información. El aporte de esta investigación será que se recomienda la fundación del Instituto Nacional de Ciberseguridad, que tendrá la función de implementar las herramientas necesarias para garantizar la seguridad de la infraestructura de la información a nivel nacional creando conciencia en el territorio guatemalteco de las consecuencias que conlleva no tener una gestión de ciberseguridad en las empresas, sin descartar que las industrias puede ser afectadas indirectamente por la afectación de las instituciones del estado por temas de ataques cibernéticos.

Tal y como lo menciona Cedeño & Loor (2020) se realizó un análisis de ciberseguridad basado en las metodologías AMFE y MARISMA para identificar las variables de ciberseguridad y determinar los controles a utilizar en ciberseguridad, implementando una gestión de riesgo, logrando determinar los patrones comprendidos en seguridad de la información, seguridad de las aplicaciones de redes basados en los riesgos, direccionando a los procesos existentes de control y la actualización de mantenimientos dinámicos de gestión de riesgos para mitigar los riesgos existentes y futuros. El aporte para

este trabajo de investigación será de conocer otras metodologías para la identificación de riesgos y la implementación de la gestión de ciberseguridad para mitigar los riesgos.

De acuerdo con Giraldo (2020), es indispensable contar con un modelo cibernético que se base en la gestión de riesgos con un plan para el control de los eventos de seguridad cibernética para las entidades que brindan servicios informáticos, lo cual permitirá ofrecer mejores aspectos en los productos y servicios, relacionados con seguridad cibernética, estableciendo un camino a seguir respecto a la infraestructura a proteger ante cualquier evento de seguridad. El aporte para esta investigación se basará en el marco de ciberseguridad *NIST*, construyendo un modelo de ciberseguridad para empresas que ofrecen servicios informáticos, dado que en el piso de planta se maneja una diversidad de aplicaciones de software deben de ser protegido adecuadamente al igual que los activos del piso de planta.

3. PLANTEAMIENTO DEL PROBLEMA

En la industria de manufactura, la continuidad y eficiencia de la producción son factores críticos para la competitividad y rentabilidad de las empresas. Sin embargo, la dependencia de sistemas tecnológicos y redes interconectadas ha incrementado significativamente la vulnerabilidad de estas plantas a ataques cibernéticos. Los paros de producción causados por la falta de una gestión de ciberseguridad empresarial no solo generan pérdidas económicas directas, sino que también afectan la imagen, reputación y confiabilidad operativa de las empresas. Este planteamiento del problema se enfoca en el diseño de una metodología de investigación para identificar y mitigar las causas que contribuyen a una alta vulnerabilidad de las plantas de manufactura a ataques cibernéticos, con el objetivo final de reducir la frecuencia y el impacto de los paros de producción causados por estos eventos.

3.1. Contexto general

En enero de 2010, la planta nuclear de Natzanz fue víctima de un ciberataque por medio del gusano Stuxnet que destruyó 1000 máquinas centrifugadoras enriquecedoras de uranio, esta fue la primera vez que un ataque cibernético logró dañar la infraestructura del mundo real. A partir del 2010, los ataques cibernéticos han continuado cada año causando daño en la infraestructura de diferentes procesos industriales. A partir de la pandemia, el delito cibernético se ha incrementado hasta un 600 %. Hoy en día, existe una alta vulnerabilidad a ataques cibernéticos en la industria de manufactura en el

piso de planta que es lo que llamamos *OT* en sus siglas en inglés (*Operational Technology*).

Las empresas industriales son los principales objetivos de los ataques cibernéticos a nivel mundial. Hay varias causas de tener una vulnerabilidad en el piso de piso de planta *OT*, que deben de ser mitigadas para mitigar y/o reducir la vulnerabilidad a los ciberataques. En los últimos 3 años, el 61 % de la industria ha experimentado grandes retos en el tema de ciberseguridad y para el 2025 las empresas podrían está pagando alrededor de USD10T anualmente concerniente al cibercrimen. En términos generales, todas las organizaciones son vulnerables y la mayoría no está preparada, pues el 60 % de los ciberataques pasan desapercibidos. La gente de informática conoce muy bien el lado de *IT* (*Information Technology*) no así el lado del *OT*.

3.2. Descripción del problema

La industria de la manufactura enfrenta una alta vulnerabilidad a ataques cibernéticos, especialmente en el piso de planta (OT), lo que resulta en múltiples efectos adversos. Entre estos, se destacan la pérdida total o parcial de la producción, la pérdida de propiedad intelectual, y la afectación de la rentabilidad empresarial. Además, los ataques cibernéticos pueden llevar a la extorsión, la introducción de malware y graves consecuencias como accidentes laborales o incluso muertes humanas debido a la pérdida de seguridad de los procesos. Las principales causas de esta vulnerabilidad incluyen la falta de conciencia empresarial sobre ciberseguridad, la ausencia de estrategias empresariales adecuadas, el incumplimiento de estándares cibernéticos, la obsolescencia de equipos OT, y la falta de monitoreo y gestión de amenazas. Esta situación subraya la urgente necesidad de implementar medidas efectivas de ciberseguridad para proteger la integridad de los

procesos de manufactura y garantizar la seguridad de los empleados y la continuidad del negocio.

3.3. Formulación del problema

Paros de producción debido a la alta vulnerabilidad a ataques cibernéticos en la industria en el piso de planta (OT-Operational Technology) en 2 industrias de manufactura en Guatemala

3.3.1. Pregunta central

¿Cuál es el plan metodológico propuesto para reducir los paros de producción debido a la alta vulnerabilidad a ataques cibernéticos en el piso de planta (OT)?

3.3.2. Preguntas Auxiliares

- ¿Cuál son los factores que permiten una alta vulnerabilidad a ataques cibernéticos que afectan la producción en el piso de planta (OT) en una industria de manufactura dentro del marco de ciberseguridad NIST?
- ¿Cuál es el nivel de vulnerabilidad de amenazas y ataques cibernéticos en el piso de planta OT?
- ¿Cuáles son las posibles soluciones, beneficios e indicadores para reducir los paros de producción debido a la alta vulnerabilidad a ataques cibernéticos de los equipos en el piso de planta OT?

3.4. Delimitación del problema

La investigación comienza en mayo 2024 y terminará en diciembre 2025. El desarrollo de la investigación se llevará a cabo dentro del territorio guatemalteco.

El desarrollo de la investigación se llevará a cabo en el piso de planta de una industria de manufactura, para esta investigación un ingenio azucarero ubicado dentro del territorio guatemalteco.

3.5. Viabilidad

Esta investigación será viable realizarla ya que se contará con los recursos necesarios para su ejecución. La investigación se llevará en un ingenio azucaro en Guatemala, en las áreas de fabricación y energía. Se contará con el acceso a la información que será utilizada en el análisis de la investigación, así como también con el acceso para poder realizar visitas a campo y el contacto con el personal de las 2 áreas con la que se interactuará en entrevistas y las visitas a campo. También se cuenta con los recursos financieros necesarios para poder realizar las actividades de cada una de las fases de esta investigación.

3.6. Consecuencias realizar y no realizar la investigación

Realizar o no esta investigación conlleva beneficios o consecuencias respectivamente que estaremos detallando a continuación y que fueron enunciadas en el árbol del problema.

3.6.1. De realizar

Con esta investigación las empresas de industria se beneficiarán al tener un plan metodológico para implementar en gestión de ciberseguridad y tener una red industrial segura en el piso de planta. Esta investigación hará conciencia en los departamentos de IT y OT de las industrias, demostrando la importancia de proteger el área del piso de planta contra amenazas y ataques cibernéticos y de esta manera evitar los paros de producción en el piso de planta OT.

La obsolescencia de los equipos de control en el piso de planta representa una alta vulnerabilidad a amenazas y ataques cibernéticos, por lo que debe realizarse una evaluación sobre todos los activos de planta para conocer su vulnerabilidad y gestionar la modernización correspondiente con equipos de reciente tecnología diseñados para no ser afectados por vulnerabilidad cibernética.

La transformación digital sigue implementándose en la mayoría de la industria, buscando una mayor rentabilidad para las empresas en sus procesos productivos. El lado de IT tiene principal atención en todas las industrias, descuidando el piso de planta OT debido al desconocimiento de los riesgos que se presentan en los equipos de control, por lo que la intención de esta investigación es hacer conciencia en las diferentes industrias de implementar una gestión de ciberseguridad tanto en el lado de IT como en el de OT.

3.6.2. De no realizar

Las industrias implementan planes estratégicos empresariales buscando una mayor rentabilidad buscando una mayor eficiencia productiva en el piso de planta. De no realizarse esta investigación la falta de conciencia de implementar una gestión de ciberseguridad en el piso de planta continuaría dejando una brecha amplia de vulnerabilidad incrementándose la probabilidad de que un ataque cibernético alcance un paro de producción parcial o total en el piso de planta.

Uno de los objetivos de esta investigación es dar a conocer una guía práctica para implementar la gestión de ciberseguridad en el piso de planta, de no realizarse esta investigación esta información no estaría alcanzado a varias industrias que se beneficiarían con la información y los resultados obtenidos.

4. JUSTIFICACIÓN

La investigación se sitúa en la línea de investigación de Área de Operaciones en el área de Análisis de Riesgos de Gestión Industrial de la Universidad de San Carlos de Guatemala, ya que se enfocará en desarrollar un plan metodológico para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos de la industria de manufactura.

La necesidad de esta investigación surge de la creciente dependencia de la industria manufacturera en sistemas interconectados y tecnologías operacionales, que, aunque mejoran la eficiencia, también incrementan significativamente los riesgos de los ataques cibernéticos. Estos ataques pueden causar paros de las líneas de producción y/o de los diferentes procesos en el piso de planta, así como la pérdida de la seguridad de proceso y máquinas, teniendo como resultado grandes pérdidas económicas y accidentes de personas pudiendo llegar a la pérdida de vidas humanas, afectando de gran manera la rentabilidad y la imagen de las empresas.

La importancia de esta investigación es abordar esta problemática porque la integridad y seguridad de los sistemas tecnológicos en la manufactura son esenciales para mantener la continuidad operativa. La falta de una estrategia efectiva de ciberseguridad y el incumplimiento de estándares cibernéticos no solo ponen en riesgo la producción, sino también la seguridad de los empleados y la propiedad intelectual de la empresa.

La motivación de esta investigación es desarrollar un plan metodológico que permita a las empresas de manufactura identificar vulnerabilidades

cibernéticas específicas en los equipos y sistemas del OT, aplicando medidas preventivas y correctivas, a manera de mitigar los paros de producción causados por ataques cibernéticos, protegiendo sobre estándares de ciberseguridad el piso de planta y por ende los diferentes procesos de producción, incrementando la resiliencia y sostenibilidad de las operaciones industriales.

Los beneficios de esta investigación serán la mejora de ciberseguridad en las áreas de producción de plantas de manufactura, minimizar las pérdidas económicas por paros de producción y la protección de la propiedad intelectual. Adicionalmente se espera incrementar la conciencia y preparación de las empresas para implementar un sistema de gestión para mitigar la amenazas y ataques cibernéticos, promoviendo una cultura organizacional de seguridad cibernética.

Los beneficiarios de esta investigación serán principalmente las empresas de la industria de manufactura, teniendo una guía para implementar la gestión de ciberseguridad en el piso de planta, garantizando una productividad eficiente eliminando los riesgos de vulnerabilidad cibernética, lo cual asegura la buena rentabilidad de la empresa. De igual manera, los empleados del área productiva en general que laboran en el piso de planta se beneficiarán en un entorno de trabajo más seguro y estable. A nivel académico esta investigación aportará conocimientos valiosos en el campo de excelencia operacional, fortaleciendo la formación de profesionales en estas áreas.

5. OBJETIVOS

5.1. General

Proponer el plan metodológico para reducir los paros de producción debido a la alta vulnerabilidad a ataques cibernéticos en el piso de planta (OT).

5.2. Específicos

1. Identificar los factores que permiten una alta vulnerabilidad a ataques cibernéticos que afectan la producción en el piso de planta (OT) en una industria de manufactura dentro del marco de ciberseguridad NIST.

2. Analizar el nivel de vulnerabilidad de amenazas y ataques cibernéticos en el piso de planta (OT).

3. Identificar las posibles soluciones, beneficios e indicadores para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos de los equipos en el piso de planta (OT).

6. NECESIDADES A CUBRIR Y ESQUEMA DE SOLUCIÓN

En esta investigación se diseñará un plan metodológico para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos en plantas de la industria de manufactura. Este plan será fundamental para mejorar la seguridad cibernética en el piso de planta OT en las industrias de manufactura. A partir de esta investigación, se identificarán las debilidades en ciberseguridad, se implementarás estrategias para cumplir con los estándares cibernéticos y se fortalecerá la conciencia empresarial para tener un sistema de gestión empresarial cibernético. Se analizará cómo impacta la mejora cibernética en la reducción de la pérdida parcial y total de la producción, la propiedad intelectual y la disminución de la extorsión cibernética.

La necesidad de desarrollar este plan metodológico surge debido a los paros de producción causados por la falta de conciencia empresarial sobre ciberseguridad, la ausencia de estrategias de ciberseguridad y el incumplimiento de estándares cibernéticos. La obsolescencia de los equipos en el piso de planta OT y la vulnerabilidad cibernética en estos sistemas agravan la situación, haciendo que las empresas sean más susceptibles a ataques continuos. Estos problemas no solo afectan la rentabilidad empresarial, sino que también pueden llevar a la pérdida de datos, descontrol de procesos de manufactura y hasta accidentes laborales leves pudiendo llegar hasta la fatalidad de pérdidas humanas.

El esquema de solución muestra la secuencia de las 4 fases de la investigación. La fase 1 consistirá en la diseño y revisión de la documentación, la cual consistirá en la creación y definición de las encuestas y material para

desarrollar las entrevistas con el personal de cada uno de los procesos productivos relacionados con el nivel de vulnerabilidad cibernética en las 2 áreas del piso de planta. En la fase 2 se diagnosticarán los factores que generan la vulnerabilidad cibernética, se analizará la relación que hay entre el histórico de los paros de producción no programados y el nivel de vulnerabilidad cibernética en las 2 áreas del piso de planta, analizando las variables que podrían generar vulnerabilidad cibernética a los procesos productivos en el piso de planta.

En la fase 3 se analizará la información obtenida en la fase anterior para analizar el nivel de vulnerabilidad cibernética en las 2 áreas a investigar, para finalmente llegar a la fase 4 donde basados en el análisis de la fase 3 se propondrán las posibles soluciones de implementar las recomendaciones para reducir el nivel de vulnerabilidad cibernética en las áreas de fabricación y generación de energía.

En la figura 1 se muestra el esquema de solución con la secuencia y objetivo a cumplir de cada una de las 4 fases.

Figura 1.

Esquema de solución

Nota. Fases del Esquema de Solución. Elaboración propia, realizada con Canvas.

7. MARCO TEÓRICO

En este capítulo se desarrolla información relacionada con el ingenio azucarero donde se desarrollará la investigación, con el objetivo de entender de mejor manera sus procesos productivos y poder visualizar de mejor manera el impacto que tienen los paros no programados en el proceso productivo de este ingenio. También se incluirán temas relacionados con los paros de producción y de la infraestructura instalada en el piso de planta donde se genera la vulnerabilidad cibernética. Por último, se desarrollarán temas de los métodos utilizados para obtener las posibles soluciones y beneficios al planteamiento del problema de esta investigación.

7.1. Antecedentes de la empresa

De acuerdo con el Ingenio Palo Gordo, S.A., (s. f.) Inicialmente el ingenio azucarero inició operaciones en el año de 1930, se encuentra ubicado en el municipio de San Antonio, Suchitepéquez, iniciando con una capacidad de molienda por día de 1,000 toneladas de caña de azúcar. En la zafra 1961/1962 llegaron a moler durante la zafra 20,000 toneladas de caña de azúcar. En el año de 1962 después de haber sido adquirido por un grupo de empresarios y agricultores en una subasta pública, se logró la ampliación del ingenio para una molienda diaria con capacidad de 4,000 toneladas de caña de azúcar. En el año de 1975 se adquirió un tándem de 5 molinos ampliando su capacidad de producción de molienda por día a 7,000 t de caña de azúcar. En el año de 1,988 se implementó tecnología para control de plagas a manera de eliminar el uso de insecticidas químicos con el cultivo de caña.

En el año de 2022 se agregaron 2 molinos nuevos, llevando la capacidad de molienda diaria a un total de 10,000 toneladas de caña de azúcar. Durante la zafra 2008-2009 se logró el récord de producción de más de 2,000,000 quintales producidos de azúcar. Hoy en día el ingenio cuenta con una producción por encima de 1,680,000 toneladas caña molida y una producción de energía de 185GWh, lo cual les permite cubrir el consumo local de toda la fábrica y la mayor para para la venta de energía al sistema eléctrico del país.

7.1.1. Procesos

A continuación, se describirán los diferentes procesos productivos del ingenio azucaro donde se desarrollará la investigación con la finalidad de brindar un mejor entendimiento de los procesos productivos y el impacto que generan los paros de producción no programados.

7.1.1.1. Azúcar

Con el objetivo de explicar brevemente el proceso de fabricación de azúcar, según Instituto de Promoción del Azúcar y el Alcohol Tucumán (IPAAT, s. f.), el primer paso inicia con el proceso de Entrada que consiste en el pesaje en básculas de las toneladas de caña entregada previo a ingresar a las mesas de caña. En este proceso se toman muestras de la caña para efectos de análisis de calidad. A continuación, la caña es transportada hacia las troceadoras, picadoras y por último por las desfibradoras. El segundo paso es la Molienda, en donde la caña desfibrada pasa por un tándem de molinos de caña, que pudiera variar en su cantidad, pero regularmente son de 5 a 6 molinos, los cuales muelen la caña a través de los rodillos y masas,

resultando el producto final el jugo de caña y como subproducto el bagazo que luego será utilizando en el proceso de generación de energía.

El tercer paso es la clarificación del jugo de caña, de acuerdo con IPAAT (s. f.), el proceso de clarificación consiste en que el jugo producido en los molinos de caña es llevado a altas temperaturas para reducir el PH previo a la producción de azúcar. Luego el jugo es alimentado a baja velocidad a los clarificadores y así poder concentrar los lodos que fueron extraídos en el proceso de clarificación.

El cuarto paso es el de Evaporación, en este proceso el jugo pasa de un operador a otro, por medio de bombas de transferencia, con el objetivo de eliminar sólidos que causan turbidez. El quinto paso es el proceso de Cristalización, que consiste en hacer crecer la sacarosa contenida en el jarabe haciéndolo pasar por los tachos al vacío, este proceso se inicia agregando granos de azúcar que son llamados semilla. El sexto paso el proceso de Separación, el cual la masa proveniente de los tachos es introducida en la centrífugas que son equipos cilíndricos girando a alta velocidad.

Por último, el séptimo paso aplica solamente a la industria azucarera que comercializa el azúcar blanco refinado, según IPAAT (s. f.) el azúcar pasa por un proceso con filtros verticales hasta llegar a obtener un licor claro que luego es evaporado para finalmente general la cristalización de los granos. El octavo paso es el Secado donde simplemente se seca el producto terminado en secadoras de forma cilíndrica llamados de tambor. Por último, el noveno paso es el Envasado, donde el producto terminado es envasado regularmente en sacos jumbo para su distribución local y exportación.

7.1.1.2. Cultivo

El cultivo de la caña de azúcar es un factor determinante para lograr el nivel deseado de calidad de caña cosechada y así poder generar buenos índices de productividad de azúcar en cada zafra año con año. Se inicia con el Diseño de Fincas, basados en la topografía de los terrenos en donde se realizará el cultivo de la caña. Luego viene la Preparación de los suelos, qué básicamente consiste en crear una base adecuada para la siempre, roturando, volteando, fraccionando y puliendo el suelo. A continuación, viene la Siembra, el cual consiste en colocar la semilla vegetativa, que debe de tener característica adecuadas para el terreno donde se realizará la siembra. Es importante tener el Control de Malezas, que le restan luz, agua y nutrientes a las plantas de caña. Un factor determinante es el Riego, que debe ser suministrado con una cadencia y en cantidades determinadas para garantizar las condiciones del terreno de la siembra.

La fertilización juega un papel importante para garantizar que el terreno pueda proveer a cada planta los nutrientes necesarios para su crecimiento. Por otro lado, el Control y Manejo de Plagas garantiza el cuidado y crecimiento de las plantas, evitando su afectación por insectos y enfermedades. Por último, se debe realizar el proceso de floración de la caña, para poder obtener mejores rendimientos en la producción de azúcar.

7.1.1.3. Cosecha

La cosecha es la última etapa del cultivo de la caña de azúcar, como lo señala el Ingenio Palo Gordo, S.A. (s. f.) esta etapa consiste en quemar, cortar, alzar y trasladar la caña de su lugar de siembra al área industrial de fábrica donde será procesada para producir azúcar y sus subproductos como melaza

y alcohol, además de la generación de energía. En el proceso de la cosecha hay una Planificación que deberá ser realizada considerando la edad, madurez, variedad, estrato, condiciones climáticas y capacidad de riego, lo que permitirá una cosecha con una mayor concentración de azúcar, a manera de definir el método de cosecha que puede ser a granel, por tramos, mecanizada o por maletas.

Para esto es necesario hacer un muestreo previamente para obtener los datos de la tendencia de maduración. Existe un proceso que consiste en recolectar la caña desde el suelo por medio de alzadoras llamado Alce de Caña, que En este ingenio la cosecha se realiza de forma manual y mecanizada, seguidamente la caña es transportada en jaulas de metal hasta el área de fábrica.

7.1.2. Comercialización de azúcar

Guatemala está clasificado como el quinto exportador de producción de azúcar a nivel mundial, por lo que la comercialización de azúcar a los mercados extranjeros tiene una gran relevancia para el producto interno bruto del país.

7.1.2.1. Productos

Según Ingenio Palo Gordo, S.A. (s. f.) el 40 % del azúcar producido en Guatemala se consume localmente y el 60 % restante se exporta al mercado mundial. El ingenio azucarero comercializar 3 tipos de azúcar, blanco, crudo y moreno. El azúcar blanco es refinado y procesado para eliminar la melaza y otros compuestos, el azúcar crudo se obtiene del azúcar sin procesar ni refinar

y por último el azúcar moreno se obtiene al agregar melaza a los cristales del azúcar blanco.

7.1.3. Comercialización de electricidad

La comercialización de la venta de energía eléctrica en la industria azucarera tiene una gran relevancia debido a sus bajos costos de operación, debido a que utilizan el bagazo de la caña de azúcar denominado biomasa como combustible para para las calderas, siendo un proceso bastante eficiente.

7.1.3.1. Generación

Es importante definir la diferencia entre generación y cogeneración. De acuerdo con Appa renovables (s. f.) se definen las fuentes de energía convencionales o no renovables, las que son de cantidad limitada por la naturaleza, están clasificadas debido a su extracción en 2 categorías: los combustibles fósiles y nucleares. Según Cengicaña (2020), el ingenio azucarero generó energía utilizando combustible de carbón por un total de 7GWh, generalmente en la época de no zafra cuando ya no tienen bagazo para cogenerar.

7.1.3.2. Cogeneración

La cogeneración en la industria azucarera seguirá en aumento debido a sus bajos costos de operación y alta eficiencia, como lo indica Varón (2020):

El concepto de cogeneración (COG) define los sistemas tecnológicos que, a partir de una sola fuente de energía primaria (combustibles),

producen en forma secuencial y/o combinada, tanto energía eléctrica como térmica. En los sistemas COG, el rendimiento o eficiencia energética global, se sitúa entre el 75 al 90 % en promedio y corresponde a energía contenida en los combustibles. (p. 35)

La producción de energía por parte de los ingenios azucareros seguirá en aumento, según la Asociación de Azucareros de Guatemala (2023), la cogeneración producida por los ingenios azucareros representó el 26 % de la energía consumida durante la temporada de zafra, que inicia en noviembre y termina en mayo del siguiente año. Como se explicó en el proceso de azúcar, el bagazo es un subproducto del proceso de molienda de la caña de azúcar, que es catalogado como biomasa. Un dato importante en lo que respecta al tema de sostenibilidad, con la energía producida por los ingenios azucareros se evita que cada año la atmósfera sea afectada por más de 4 millones de toneladas CO2eq. Según Cengicaña (2020) el ingenio produjo un total de 185 GWh, siendo la generación con bagazo de 175 GWh.

7.1.4. Comercialización de alcohol

De acuerdo con la Red Latinoamericana de Investigadores de Cadenas Globales de Mercancías (REDILACG, 2015) el etanol carburante o bioetanol se aprueba en el año de 1985, con del Decreto 17-85, correspondiente a la Ley de Alcohol Carburante creándose los incentivos correspondientes para el beneficio de los productores. Este fue el único ingenio azucarero que aprovechó los incentivos fiscales, convirtiéndose en un exportador de etanol.

Para Curruchich (2021) el alcohol producido en Guatemala alcanza un 96 % de pureza. El alcohol guatemalteco se utiliza para la elaboración de bebidas, etanol (combustible renovable) y en la industria farmacéutica.

7.2. Tipos de Paros de Producción

A continuación de definirán los tipos de paros de producción y sus consecuencias en los procesos productivos de una industria de manufactura.

7.2.1. Paros de producción no programado

Cualquier tipo de paro de producción interrumpirá el proceso productivo. Según NC Tech (2021) un paro de producción es la interrupción de un proceso productivo afectando la cadena del proceso de producción y generando pérdidas en la empresa. La causa de los paros o fallas pueden ser debido a defectos en el diseño, en la fabricación, desgaste por uso, errores de cálculo, mal uso de los equipos y mala instalación, ataques cibernéticos entre otras. Para evitar los paros en el proceso productivo, es responsabilidad de las áreas correspondientes concernientes a la causa de los paros o fallas generados de tal manera implementar acciones preventivas y correctivas que reduzcan la ocurrencia de estos.

7.2.2. Paros de producción programados

Los paros de producción programados se definen como los paros de producción que son programados para efectuar regularmente tareas de mantenimiento en los diferentes equipos de las líneas de producción. Para NC Tech (2021) un paro de producción programado brindará mayo confiabilidad de los equipos, incrementará su vida útil, generarán ahorro en costos de

mantenimiento, brindarán mayor seguridad al proceso, mejorarán la eficiencia, incrementará la disponibilidad de máquina teniendo una mejor gestión sobre los activos.

7.2.3. Costos asociados en los paros de producción

Como lo menciona NC Tech (2021) los paros de producción no programados, ocurren repentinamente causando desde pequeñas hasta grandes pérdidas de la producción que dependerá del tiempo de reparación de la falla o causa que haya generado el paro. Los paros de producción no programados generan atrasos en el proceso productivo, clientes insatisfechos por falta de cumplimiento de entrega de sus pedidos, altos costos de reparación, tensión entre las áreas de operaciones y mantenimiento.

El uso de la tecnología del *IoT* se recomienda hoy en día para monitorear el estado de los procesos utilizando dispositivos inteligentes que envían información a través de una red industrial.

7.2.3.1. Costos Tangibles

Para Ferremayoreo Elizondo (2021) existen costos tangibles relacionados con los paros de producción como lo son para pérdida de producción, al tener paro en las líneas de producción y la falta de cumplimiento de entrega a los pedidos de los clientes. También se puede generar desperdicio al ser interrumpido el proceso productivo, dado que corresponde a material prima daña por la falta de continuidad de la cadena de producción. Los costos laborales se mantienen a pesar de que la producción esté detenida y luego también se podrían generar gastos adicionales de horas extras para reponer el tiempo de producción improductivo. La capacidad de producción se

ve reducida y no permitirá incrementos de la producción por ventas adicionales que se puedan registrar.

7.2.3.2. Costos Intangibles

Según Ferremayoreo Elizondo (2021) existen costos intangibles generados por los paros no programados como la generación de estrés y la desmotivación laboral debido a la alta presión generada en el proceso de reparación y resolución del paro. Por otro lado, también existe una pérdida de capacidad en tiempo de respuesta por parte del personal, debido a que están ocupados en la resolución de la causa que haya generado el paro y por último, se genera una pérdida de creatividad e innovación por parte de los equipos de mantenimiento, debido a que invierten la mayor cantidad de su tiempo en la resolución de las causas que hayan generado los paros en las diferentes áreas del proceso productivo.

7.2.4. Tecnología operativa (Operational Technology)

La Tecnología Operativa *(OT)* pareciera ser un término complejo, se trata de la tecnología interactuando con el mundo físico. De acuerdo con Bickerstaffe (2023), la tecnología operativa incluye todo el *hardware*, *software* y los sistemas que monitorean, controlan y optimizan en tiempo real los procesos en los diferentes tipos de industria como manufactura, energía, tecnología, ciencias de la vida entre otros. En el mundo de tecnología existen 2 grandes áreas definidas como *Infomation Technology (IT)* y *Operational Technolgy (OT)*, en esta investigación nos enfocaremos en la tecnología operativa *(OT)*. La tecnología operativa se preocupa por la operación de los

procesos físicos, incluyendo dispositivos inteligentes, sistemas de control y redes que para monitorear, controlar y optimizar los procesos industriales.

La tecnología operativa se encuentra ubicada en el piso de planta de las industrias, donde están ubicadas las líneas de producción y los equipos que manejan los diferentes procesos productivos de una planta de producción. Las prioridades de la tecnología operativa son confiabilidad, seguridad, ciberseguridad y la productividad de los diferentes procesos productivos, mientras que para la tecnología de información *(IT)*, las prioridades son la integridad de la información, disponibilidad, confidencialidad y ciberseguridad.

7.2.4.1. Industria 4.0

De acuerdo con Yánez (2017) en 1850, la segunda revolución implementó la electricidad lo que generó la producción en serie. A mediados del siglo XX, la tercera revolución trajo consigo la electrónica, comunicaciones e informática. La cuarta revolución es conocida como Industria 4.0 en el continente europero y como *Smart Industry* en los Estados Unidos. En este modelo de industria se utilizarán diferentes tecnologías con el uso de *IoT (Internet of Things)* en los diferentes procesos industriales con el objetivo de integrar la información de los diferentes dispositivos de cada proceso y poder así tomar decisiones en tiempo real.

Para Yánez (2017) las 4 claves para entender la cuarta revolución son las siguientes:

- El primer país en implementar la estrategia de tecnología llamada Industria 4.0 fue Alemania.

- Básicamente consiste en una combinación de sistemas de software, sensores, tecnología digital, nanotecnología y telecomunicaciones.
- Existirá un desequilibrio económico y social que los gobiernos tendrás que resolver.
- La cuarta revolución cambiará el mundo.

7.2.4.2. Redes Industriales

En la industria 4.0, las redes industriales juegan un papel primordial para el manejo de la información. A diferencia de la red tradicional de *IT (Information Technology)*, que es la red administrativa convencional que brinda los servicios de internet, correo electrónico, licenciamiento de software, en el piso de planta que es el denominado *OT (Operational Technology)*, se requieren de switches industriales con puertos de comunicación en cobre y fibra óptica que dependerán de las distancias del cableado de la red al igual que en una red convencional. Es importante aclarar que las prioridades entre ambos mundos son diferentes, debido a la funcionalidad de cada una de las redes. En el piso de planta una red industrial debe utilizar switches de grado industrial debido a que están expuestos a condiciones adversas dependiendo del tipo de procesos y manufactura de cada industria.

En el piso de planta existen varios protocolos de comunicación, según VENCO (2023), la comunicación industrial en el piso de planta incluye la comunicación de diversos dispositivos de campo como instrumentos de campo, controladores lógicos programables, sistemas *SCADA* que son sistemas de supervisión, sistemas de control distribuido y sistemas de gestión. Una red industrial debe de ser altamente confiable ya de los procesos dependen cómo maneje la información para la ejecución de los diferentes procesos. Existen varias topologías de red, punto a punto, bus, estrella y del

tipo árbol. Con respecto a los protocolos de comunicación, se manejan varios tipos de protocolo que varían según el fabricante de los equipos de control, siendo los más utilizados *Ethernet*, Modbus (RTU y TCP/IP), Profinet y Profibus.

7.2.4.3. IoT y IIoT

Los dispositivos inteligentes en el piso de planta están clasificados por el área donde se instalarán, pudiendo ser un área administrativa o un área industrial. De acuerdo con Yánez (2017) el *IoT (Internet of Things)*, es el conjunto de dispositivos comunicados entre sí a través de una red industrial con el objetivo que envíen la información automáticamente con completa independencia sin necesidad de la gestión humana. En lo que respecta al *IIoT (Industrial Internet of Things)*, utiliza dispositivos de campo con grado industrial debido a que se ubican dentro del piso de planta cerca de los procesos que generan ambientes corrosivos, de altas temperaturas y gases contaminantes. A diferencia de los dispositivos *IoT*, los dispositivos *IIoT* tiene capacidad de manejar mayo cantidad de variables de información, teniendo sus propios sistemas de seguridad, teniendo la capacidad de personalización a diferencia de los dispositivos *IoT* que no tienen esta funcionalidad.

En el 2020, según Munirathinam (2020), habrán más de 30 mil millones de dispositivos en el mundo que estarán conectados a una red enviando información. Entre las áreas emergentes de la cuarta revolución se incluye *IoT*, la robótica, inteligencia artificial, nanotecnología, biotecnología y computación cuántica. En ciudades conectadas se está implementando el *IIoT*, con el objetivo de buscar el ahorro energético buscando reducir la huella de carbono para hacer un mundo más verde. El *IIoT* revolucionará la manufactura inteligente al utilizar dispositivos más rápidos y con mayor capacidad de

manejo de información, permitiendo la captura de información, comunicación y análisis en tiempo real, con la finalidad de poder tomar decisiones en tiempo real.

7.2.4.4. Almacenamiento de información

En Industria 4.0, el proceso del almacenamiento de la información tomará una gran relevancia, como lo menciona Coppola (2023) el término de *Big Data*, está relacionado con grandes cantidades de datos que son recopilados de varias aplicaciones y usuarios, transacciones electrónicas, también incluye el manejo de diferentes fuentes de información a través de programas y herramientas. Entre las fuentes de *Big Data*, están las personas, máquinas, estadísticas biométricas, estadísticas de mercadeo digital y de estadísticas de transacciones de datos. Entre las ventajas están que ayudan a comprender el mercado, mejora la toma de decisiones, brindan una retroalimentación inmediata y tienen una versatilidad de aplicación, por otro lado, entre las desventajas están que pueden ser susceptibles a brechas de seguridad, podrían generar un exceso de datos, se requiere analizar los lineamientos de privacidad en cada diferente país y pudiera existir un recelo en los usuarios en compartir su información.

De acuerdo a Microsoft (s.f.), el almacenamiento en la nube es un servicio de almacenamiento de datos que se transfiere por internet de una red a un sistema de almacenamiento externo de un tercero. Este tipo de sistema de almacenamiento suele ser escalable. Hay 3 tipos de almacenamiento: nube pública, para datos no estructurados, nube pública, nube privada y nube híbrida.

7.2.4.5. Tipos de Activos

Los equipos de control ubicados en el piso de planta *OT*, que pueden son vulnerables a los ataques cibernéticos encontramos los Sistemas *SCADA (Supervisory Control and Data Adquisition)*, lo controladores lógicos programables *PLC (Programmable Logic Controllers)* y los Sistemas de Control Distribuido *DCS (Distributed Control Systems)*. En el área de energía encontramos los Sistemas de Gestión de Energía *EMS (Energy Management Systems)*. En ciertos tipos de industria que necesitan gestionar la climatización, iluminación y seguridad de los edificios, encontramos los Sistemas de Control de Edificios *BMS (Building Management Systems)*.

7.2.5. Vulnerabilidad cibernética en el piso de planta

La vulnerabilidad cibernética en el piso de planta genera un alto riesgo para la productividad de las organizaciones, por lo que es importante identificar el nivel de vulnerabilidad cibernética en las áreas de los procesos productivos. El impacto del potencial de daño de un ataque cibernético puede ir desde un nivel bajo afectando un área del proceso productivo hasta un nivel alto que pueda detener toda la producción de una industria de manufactura.

7.3. Gestión de Riesgo en Sistemas de Seguridad de la información

La gestión de riesgos implica un proceso continuo de identificación, evaluación y respuesta a los riesgos. Para poder gestionar los riesgos es indispensable que las organizaciones puedan entender la probabilidad de que ocurra un evento y el impacto potencial que pudiera causar. Con esta información, deberá establecer el nivel de riesgo tolerable según la estrategia cibernética, que se conoce como tolerancia al riesgo. Una vez comprendida la

tolerancia al riesgo, las organizaciones podrán realizar actividades de seguridad cibernética. La implementación de un programa de gestión de riesgos proporcionará a las organizaciones la capacidad de cuantificar y realizar ajustes necesarios en la estrategia de ciberseguridad.

El marco de gestión de riesgos utiliza estos procesos para ayudar a las organizaciones a informar y dar prioridad a las decisiones relacionadas con ciberseguridad cibernética. Este marco respalda las evaluaciones de riesgos recurrentes, ayudando a las organizaciones a realizar las actividades de seguridad cibernética que cumplan con los objetivos de la estrategia de ciberseguridad.

7.3.1. Gestión de Riesgos Lean Six Sigma

En toda industria de manufactura existen diferentes clases de riesgos asociados a las diferentes áreas del proceso. La metodología Lean Six Sigma es una metodología utilizada en varias compañías con el objetivo de lograr la mejora de los diferentes procesos asociados con la productividad. Basados en la identificación de las causas que están afectando los procesos, se busca resolver los distintos problemas de raíz y así llegar a la reducción de costos, la optimización de la calidad de los productos y servicios para lograr un aumento en la satisfacción de los clientes.

En la gestión de riesgos de *Lean Six Sigma*, el primer paso es la identificación de los riesgos asociados en los diferentes procesos. De acuerdo con Laisequilla (2023), será necesario utilizar las herramientas de *Lean Six Sigma*, como el mapa de procesos, análisis del Pareto y análisis de causa y efecto. Al utilizar el mapa de procesos podremos tener la visibilidad del proceso completo, teniendo las entradas, las salidas y los subprocesos. Por

otro lado, el Pareto identifica los problemas más comunes de cada uno de los diferentes procesos, utilizando el análisis de causa y efecto para identificar la causa raíz de los problemas. Una vez se hayan identificado los riesgos, habrá que clasificarlos de acuerdo con su ocurrencia y el impacto potencial.

Para el análisis de riesgos se utilizarán herramientas de *Lean Six Sigma*, como el análisis de *FMEA* y la matriz de riesgos. El *FMEA* analiza e identifica y evalúa el impacto potencial de las fallas en un proceso determinado, además de la probabilidad de porder detectar la falla antes de causar un daño significativo en el proceso productivo. Por otro lado, la matriz de riesgos se utiliza para identificar la probabilidad de que ocurra un riesgo y el impacto potencial que pudiera tener en el proceso de producción.

Con respecto a la gestión de riesgos, para Laisequilla (2023), *Lean Six Sigma* puede identificar las medidas necesarias para la mitigación de los riesgos identificados; luego se deberá de implementar un plan con medidas de prevención, mitigación y contingencia. En lo que respecta a las medidas preventivas, pudieran incluir capacitación del personal, la mejora de los procesos y la implementación de controles adicionales para monitoreo y control.

7.3.2. Marco de Seguridad NIST

El 12 de febrero de 2013, debido a la cantidad de ataques cibernéticos, el presidente de los Estados Unidos, Barack Obama, emitió la orden ejecutiva No. 13636, en donde delega al *NIST*, siglas que significan Instituto Nacional de Estándares y Tecnología en español, desarrollar el Marco de Ciberseguridad para proteger las áreas críticas, habiéndose identificado 16 áreas a proteger, como lo son: los sectores químico, comercios,

comunicaciones, producción esencial, hidroeléctricas, presas/represas, industrial militar, servicios públicos de emergencia, sector energético, sector financiero, alimentos y agricultura, administración pública, salud pública, sector informático, reactores nucleares, gestión de residuos, transporte y sistemas de abastecimiento y tratamiento de agua. El Marco se basó en los estándares internacionales de industria ya reconocidos en el área de ciberseguridad.

El Marco de Ciberseguridad *NIST* es un conjunto de directrices que gestiona los riesgos de ciberseguridad de manera adaptable y flexible para cualquier tamaño de organización. A pesar de que el Marco de Ciberseguridad fue una herramienta creada para poder evaluar el nivel de ciberseguridad de los sectores críticos en Estados Unidos, dado que es basado en estándares, se ha demostrado perfectamente que aplica para diferentes países y sectores a nivel mundial. El Marco de Ciberseguridad *NIST* se desarrollará basado en cinco funciones: Identificar, Proteger, Detectar, Responder y Recuperar.

7.3.2.1. Identificar

La primera función es identificar donde se desarrollará una compresión organizacional para poder administrar el nivel de riesgo para personas, datos, activos y sistemas. En esta etapa, las actividades son fundamentales, debido a que identificar los riesgos relacionados con ciberseguridad permite a las organizaciones enfocarse y darle prioridad a la estrategia de gestión de riesgos. En esta función, las categorías de resultados son la Gestión de Activos, Entorno del Negocio, Gobernanza, Evaluación y Estrategia de Riesgos.

7.3.2.2. Proteger

En esta etapa se implementan las medidas de seguridad necesarias para la reducción de los niveles de vulnerabilidad cibernética. En esta función, las categorías de resultados son Gestión de Identidad y Control de Acceso, Entrenamiento y Conciencia, Protección de la información, Procedimientos y Procesos para la protección de la información almacenada, Mantenimiento y Tecnología para la protección.

7.3.2.3. Detectar

En esta función se desarrollan actividades para poder identificar la ocurrencia de los eventos de ataques cibernéticos. La categoría de resultados de esta función es detección de Anomalías y Eventos, Monitoreo continuo de seguridad cibernética y Procedimientos de Protección.

7.3.2.4. Responder

En esta función se desarrollan actividades para tomar medidas con la ocurrencia de un evento de ataque cibernético. Con esta función se facilita la capacidad de poder mitigar el impacto de un posible ataque cibernético. Las categorías de los resultados en esta función son la Planificación de la Respuesta, Comunicaciones, Mejoras y Mitigación.

7.3.2.5. Recuperar

Esta última función desarrolla capacidades para restablecer los servicios de forma eficiente, manteniendo el plan de resiliencia empresarial. Esta función permite poder recuperar los servicios y las operaciones a la

normalidad después de un evento de ataque cibernético. Las categorías de resultados son Planificación de Respuesta, Comunicaciones y Mejora.

8. PROPUESTA DE ÍNDICE DE CONTENIDOS

9. METODOLOGÍA

La metodología para esta investigación será desarrollada con varios enfoques, como se describirá en los párrafos posteriores. Esta investigación tendrá un enfoque mixto, con el uso de variables cualitativas y cuantitativas; por otro lado, tendrá un enfoque descriptivo en el que se realizará una gestión de análisis de riesgo en 2 áreas productivas, energía y fabricación. Se analizarán las causas de paros de producción en ambas áreas y se desarrollará un plan metodológico para reducir la vulnerabilidad cibernética en el piso de la planta de energía y fabricación. El diseño será no experimental dado que no se procederá con ninguna implementación, pero sí con las recomendaciones para reducir los niveles de vulnerabilidad cibernética en las áreas a investigar. Por último, la metodología será del tipo transversal en base a la información recopilada de las variables utilizadas en esta investigación.

9.1. Características del estudio

El enfoque del estudio propuesto es mixto, debido a que se analizarán variables cualitativas y cuantitativas. El enfoque cualitativo porque se necesita analizará los procesos de automatización relacionados directamente con la producción de energía, azúcar y sus derivados. La productividad del ingenio dependerá del buen desempeño de los equipos de control por el alto grado de automatización en ambos pisos de planta. Para este fin, se entrevistará a las personas relacionadas con las áreas de automatización, fabricación, energía y de tecnología de la información, debido a que comportamientos no adecuados o malas prácticas podrían afectar directamente los procesos productivos. Por otro lado, el enfoque será cuantitativo porque se necesita

identificar las áreas, procesos, sistemas de control y equipos que estén promoviendo una vulnerabilidad cibernética en las distintas áreas de los procesos productivos.

El alcance es descriptivo, ya que se hará una evaluación de las causas de los paros de producción en las 2 áreas del ingenio a investigar, energía y fabricación, debido a que los paros de producción podrían estar relacionados con la vulnerabilidad cibernética en ambas áreas. Los equipos de control instalados en el piso de planta para identificar los equipos con alto nivel de obsolescencia, análisis del diseño de la red industrial y desarrollando un plan metodológico para poder identificar y mitigar la vulnerabilidad en el piso de planta basado en la información disponible del nivel de vulnerabilidad cibernética de los equipos instalados en el piso de planta.

El diseño adoptado será no experimental, dado que no se realizará ninguna acción de implementación de equipos o software para obtener posibles resultados, sino básicamente se identificará la relación de los paros de producción con el nivel de vulnerabilidad cibernética en el piso de planta de las áreas de energía y fabricación después de analizar el nivel de vulnerabilidad cibernética en el piso de planta de las áreas de fabricación y energía.

El diseño de esta investigación será de un enfoque transversal debido a que se realizará el análisis por una sola ocasión con el objetivo de relacionar los paros de producción no programados con el nivel de vulnerabilidad cibernética, realizando un análisis de gestión de riesgos para identificar el nivel de vulnerabilidad cibernética, ya que con esto se harán las recomendaciones posibles para reducir el nivel de vulnerabilidad cibernética en las áreas de fabricación y energía.

9.2. Unidades de análisis

Para el desarrollo de esta investigación, se trabajará con una población de 20 personas que son directamente responsables en las áreas de Fábrica (producción), Automatización (sistemas de control), Energía (cogeneración) e Informática (Information Technology). Todas estas áreas están relacionadas con los diferentes procesos productivos para la fabricación de azúcar, etanol y generación de energía, para lo cual estarán brindando información requerida para poder relacionar los paros de producción con el nivel de vulnerabilidad cibernética en las 2 áreas a investigar.

La siguiente fórmula será utilizada para determinar la muestra "n" con la que se procederá a realizar la investigación:

$$n = \frac{N\sigma^2 Z^2}{e^2(N-1) + \sigma^2\, Z^2}$$

$$n = \frac{(20) * (0.05)^2 * (1.96)^2}{(0.05)^2 * (35-1) + (0.05)^2 * \ (1.96)^2} = 19.06 \sim 19$$

n = Tamaño de la muestra

N = Tamaño de la población (20)

σ = Desviación Estándar Poblacional (0.5 por convención)

Z = Nivel de Confianza (1.96 para 95 % de confianza para este estudio)

e = error de estimación máximo esperado (5 % para este estudio)

Para la presente investigación se utilizará una muestra de población de 20 personas de las áreas de fabricación, automatización, eléctrica y de

informática, entre los que estarán los dueños de cada proceso, coordinadores y supervisores de cada una de las áreas respectivas.

9.3. Variables

Las variables en estudio se describen a continuación. Serán utilizadas para diagnosticar, analizar e identificar el nivel de vulnerabilidad a ataques cibernéticos en el piso de planta de las áreas de energía y fábrica en el ingenio azucarero, con el objetivo final de proponer las posibles soluciones que evitarán paros de producción causados por vulnerabilidad cibernética en las áreas a investigar.

Tabla 1.

Variables en estudio

Variable	Definición Teórica	Definición operativa
Paros de producción no programados	Interrupción inesperada en el proceso productivo que no fue programada. Los paros no programados se pueden presentar por fallas en equipos, cortes de energía, desastres naturales y/o errores humanos.	Paro del proceso productivo en líneas de producción en un área específica de proceso, causando pérdidas en el proceso productivo afectando la continuidad de un proceso productivo.
Respaldo de la información de los sistemas de control (Backup)	Es el proceso de la creación de una copia de seguridad del programa almacenado en un sistema de control	Recuperación rápida del programa y configuración de un sistema de control

Continuación tabla 1.

Variable	Definición Teórica	Definición operativa
Control Lógico Programable (PLC)	Es una computadora programable utilizada en la automatización industrial, se compone de CPU (Unidad de Procesamiento de Datos), que ejecuta las instrucciones del programa; módulo de memoria para almacenaje del programa; módulos de entradas y salidas para la ejecución del programa; y fuente de alimentación	Su función principal es controlar la automatización de procesos específicos, funciones de máquinas o líneas de producción, haciendo los procesos más eficientes y productivos
Sistemas *SCADA*	*SCADA (Supervisory Control and Data Acquisitition),* traducido significa Control de Supervisión y Adquisición de Datos. Es una herramienta de control industrial y automatización. Se compone de varios elementos: 1. *HMI (Human Machine Interface)*, que es la interfaz que conecta a la persona con la máquina mostrando los datos del proceso a través de una pantalla; 2. *MTU (Master Terminal Unit*, recopila datos del proceso y envía las instrucciones mediante una línea de comandos; 3. Unidades Terminales Remotas *(RTU)*, microprocesadores que recolectan señales para que sean procesadas; 4. *PLC*,	Dentro de sus funciones principales están controlar, supervisar, recopilar datos, analizar datos y generar informes para la toma de decisiones. Dentro de sus funciones principales es la evaluación de la información para mitigar errores en los procesos.

Continuación tabla 1.

Variable	Definición Teórica	Definición operativa
Sistemas *SCADA*	descritos anteriormente; 5. Red de comunicación, establece la establece la conectividad de los elementos que conforman el sistema; 6. Sensores, dispositivos de instrumentación que miden variables de proceso necesarias para el desarrollo del proceso	
Sistemas de Control Distribuido *(DCS)*	*DCS (Distributed Control System)*, un Sistema de Control Distribuido es un control automatizado formado por dispositivos de control en varias áreas de una planta para garantizar la eficiencia y calidad de los procesos productivos. Está conformado por varios elementos: 1. Controlador de Ingeniería, que es el responsable de todos los demás controladores en el proceso distribuidor; 2. Controlador de Distribución, que controlan los dispositivos de campo en varias áreas de la planta, detectan y controla entradas digitales y analógicas del proceso; *HMI*, descrito en el inciso anterior; Red de comunicación, descrito en el inciso anterior	Su función es controlar procesos automatización de gran número de entradas y salidas, ejecutando varias funciones como la presentación de datos, adquisición de datos, control de procesos, reporte de información, almacenamiento y recuperación de la información.

Nota. Variables en estudio con sus definiciones teórica y operativa para la presente investigación. Elaboración propia, realizado con *Word*.

Para esta investigación se utilizarán las variables descritas anteriormente para relacionar los paros de producción no programados con el nivel de vulnerabilidad cibernética y realizar el análisis de la gestión de riesgo para identificar el nivel de vulnerabilidad cibernética, con lo que consecuentemente, una vez identificadas las causas que podrían producir un nivel alto de vulnerabilidad cibernética, se harán las recomendaciones de las posibles soluciones para la reducción del nivel de vulnerabilidad cibernética en las 2 áreas a investigar, fabricación y energía.

Tabla 2.

Matriz de consistencia de variables e indicadores

Objetivos Específicos	**Variable**	**Tipo de Variable**	**Indicador**	**Técnica de Recolección**	**Resultados esperados por objetivo**
Identificar los factores que permiten una alta vulnerabilidad a ataques cibernéticos que afectan la producción en el piso de planta (OT) en una industria dentro del marco de ciberseguridad NIST	Paros de producción no programados	Cuantitativa	Nivel de afectación a la producción debido a impacto del paro no programado	Datos históricos SAP	Relacionar los paros de producción no programados con el nivel de vulnerabilidad cibernética
	Equipos de control en el piso de planta (Controladores Lógicos Programables, Switches de industriales)	Cuantitativa	Cantidad de equipos con posible vulnerabilidad cibernética	Observación, visita a campo	Identificar los equipos con posible vulnerabilidad cibernética
	Respaldo de la información de los sistemas de control (Backup)	Cualitativa	Red segura o no segura	Observación, revisión del diseño	Identificar redes con posible vulnerabilidad cibernética

Continuación tabla 2.

Objetivos Específicos	**Variable**	**Tipo de Variable**	**Indicador**	**Técnica de Recolección**	**Resultados esperados por objetivo**
	Red Industrial	Cualitativa	Red confiable o no confiable	Entrevista	Obtener el diseño de la red industrial para su evaluación
	Sistemas *SCADA*	Cuantitativo	Cantidad de sistemas *SCADA*	Entrevista	Identificar el o los sistemas *SCADA* de ambas áreas
	Sistemas de Control Distribuido	Cuantitativo	Cantidad de Sistemas de Control Distribuido	Entrevista	Identificar los sistemas de Control Distribuido en ambas áreas
Identificar las posibles soluciones, beneficios e indicadores para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos de los equipos en el piso de planta (OT).	Nivel de vulnerabilidad (bajo, medio, alto)	Cualitativa	Obsolescencia de equipos de control	Observación	Proponer las recomendaciones para reducir la vulnerabilidad cibernética en el piso de planta de las áreas de energía y fábrica
	Respaldo de la información de los sistemas de control (*Backup*)	Cualitativa	Red segura o no segura	Observación, revisión del diseño	Identificar redes con posible vulnerabilidad cibernética
	Red industrial	Cualitativa	Diseño basado en normas estandarizadas	Observación	Recomendaciones del diseño de la red

Continuación tabla 2.

Objetivos Específicos	Variable	Tipo de Variable	Indicador	Técnica de Recolección	Resultados esperados por objetivo
Identificar las posibles soluciones, beneficios e indicadores para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos de los equipos en el piso de planta (OT).	Nivel de vulnerabilidad (bajo, medio, alto)	Cualitativa	Obsolescencia de equipos de control	Observación	Proponer las recomendaciones para reducir la vulnerabilidad cibernética en el piso de planta de las áreas de energía y fábrica
	Red industrial	Cualitativa	Diseño basado en normas estandarizadas	Observación	Recomendaciones del diseño de la red

Nota. Matriz de consistencia con el tipo de variables, indicadores, técnicas de recolección y resultados esperados por objetivo. Elaboración propia, realizado con *Word*.

En la matriz de consistencia se describen las variables que se analizarán en cada una de las fases de la investigación, describiendo la variable, su tipo, el indicador, la técnica de recolección y el resultado esperado.

9.4. Fases de estudio

Esta investigación se realizará en 4 fases; a continuación, se describirán las fases del proceso de investigación, indicando para cada una de ellas cuáles serán las técnicas de recolección, las actividades a realizar y cuáles serán los resultados esperados, indicando el propósito de la utilización de cada técnica de recolección e identificando a las personas que facilitarán la

información en cada una de las áreas de planta donde se realizará la investigación.

9.4.1. Fase 1: revisión de la documentación

En esta fase se definirán las encuestas a realizar, así como las preguntas a realizar a las personas que proveerán la información necesaria para su recolección y posterior análisis para la presentación de los resultados finales. Las personas de contacto en esta fase serán el dueño del proceso de automatización, metrología y electricidad, dueño del proceso de fabricación, dueño del proceso de cogeneración, coordinador de TI, coordinador de área y supervisores. El resultado de esta fase es obtener toda la documentación que se utilizará para las encuestas y entrevistas con las personas involucradas directamente en los procesos de las áreas de energía y fábrica.

9.4.2. Fase 2: identificar los factores de vulnerabilidad cibernética

La técnica de recolección será la observación por medio de una visita de campo, con el propósito de hacer un levantamiento de los equipos y sistemas de control del piso de planta en el área del cuarto de control de la subestación de energía eléctrica, así como en el área de fábrica. También se realizarán encuestas y entrevistas al dueño del proceso de automatización, metrología y electricidad; dueño del proceso de fabricación, dueño del proceso de cogeneración, coordinador de TI, coordinador de automatización y coordinador de mantenimiento eléctrico, para conocer detalles de procedimientos de almacenaje de la información, diseño de la red industrial, mantenimiento de los equipos y gestión de activos en lo que respecta a su vida útil. El resultado esperado de la fase 1 es identificar los equipos con posible

vulnerabilidad previo a ser analizados basados en la información proveída por cada fabricante en lo que respecta a la vulnerabilidad de equipos.

9.4.3. Fase 3: analizar el nivel de vulnerabilidad en las áreas a investigar

Una vez definido el listado de los equipos de control con posible vulnerabilidad, diseño de la red industrial, prácticas de almacenamiento de información, mantenimiento y gestión de activos, se procederá a investigar el nivel de vulnerabilidad de los equipos para diagnosticar el nivel de vulnerabilidad cibernética en cada una de las áreas a investigar.

La técnica a utilizar en esta fase será la observación basada en la investigación de la información proveída por cada uno de los fabricantes, así como de las entrevistas realizadas al dueño del proceso de automatización, metrología y electricidad; dueño del proceso de fabricación, dueño del proceso de cogeneración, coordinador de TI, coordinador de automatización y coordinador de mantenimiento eléctrico, para identificar malas prácticas de ciberseguridad según su responsabilidad en la operación del proceso. El resultado obtenido será definir el nivel de vulnerabilidad cibernética en las 2 áreas investigadas.

9.4.4. Fase 4: identificar las posibles soluciones, beneficios e indicadores para reducir la vulnerabilidad cibernética

Una vez identificado el nivel de ciberseguridad, se harán las recomendaciones necesarias basado en el marco de seguridad NIST y de estándares internacionales de seguridad cibernética, proponiendo un plan de

mejoras en el piso de planta de ambas áreas al dueño del proceso de automatización, metrología y electricidad, dueño del proceso de fabricación, dueño del proceso de cogeneración, coordinador de TI, coordinador de automatización y coordinador de mantenimiento eléctrico, con el fin de que puedan desarrollar un plan de implementación para la reducción del nivel de vulnerabilidad cibernética en ambas áreas.

10. TÉCNICAS DE ANÁLISIS DE INFORMACIÓN

Para esta investigación se utilizará la técnica de análisis de la información de estadística descriptiva, que es una rama de la estadística que se encarga de recolectar, organizar, presentar y describir un conjunto de datos para facilitar su interpretación. Debido a que el objetivo de esta investigación es reducir los paros de producción debido al nivel de vulnerabilidad cibernética, se hará analizar la relación del histórico de los paros de producción y su posible relación con la vulnerabilidad cibernética de las 2 áreas a investigar. Es importante aclarar que para la fase 1 no se utilizarán técnicas de análisis de información.

10.1. Fase 2: identificar los factores de vulnerabilidad cibernética

En esta fase, se identificarán los factores, que pudieran ser personas, procedimientos, sistemas de control y/o equipos, que generan una vulnerabilidad cibernética en las 2 áreas a investigar que serán el área de fabricación y energía. Se analizará si existe una posible relación entre el histórico de paros de producción y el nivel de vulnerabilidad cibernética en el piso de planta. Considerando las variables de los paros de producción y los equipos de control en el piso de planta, se utilizará la moda como técnica de análisis de información para identificar las causas que generan la mayor cantidad de paros de producción, y de igual manera se hará con los equipos que generan el mayor nivel de vulnerabilidad cibernética en las 2 áreas del piso de planta a investigar.

10.2. Analizar el nivel de vulnerabilidad en las áreas a investigar

Siguiendo con el desarrollo de la investigación en el área de gestión de riesgos en el área de operaciones, es necesario analizar el nivel de vulnerabilidad cibernética relacionada con los paros de producción históricos de las 2 áreas a investigar. Para esto se utilizará la técnica de visualización de datos que se obtendrán del análisis obtenido en la fase anterior de la investigación para identificar el nivel de vulnerabilidad debido a personas, procedimientos, sistemas de control y/o equipos instalados, con lo que se identificará el nivel de vulnerabilidad bajo, medio o alto de las variables generadoras de vulnerabilidad cibernética, para lo cual se utilizará la moda como técnica de análisis de la información de estadística descriptiva.

10.3. Identificar las posibles soluciones, beneficios e indicadores para reducir la vulnerabilidad cibernética

Basado en la gestión de riesgos del área de operaciones, considerando el nivel de vulnerabilidad cibernética bajo, medio o alto, se hará la propuesta de un plan metodológico para reducir la vulnerabilidad cibernética en el piso de planta para evitar paros de producción no programados por ataques cibernéticos o malas prácticas de operación que también pudieran causar paros a la producción en el piso de planta. En esta fase no se utilizarán técnicas de análisis de información de estadística descriptiva.

11. CRONOGRAMA

A continuación, se mostrará el cronograma de actividades de las 4 fases de la metodología con el objetivo de ejecutar cronológicamente cada una de las actividades definidas en cada una de las 4 fases para garantizar el avance y cumplimiento de cada una de las 4 fases para cumplir con los objetivos de esta investigación.

Tabla 3.

Cronograma de actividades

ID	Task Mode	Task Name	Duration	Start	Finish
1		**CRONOGRAMA DE LA INVESTIGACIÓN**	37 wks?	Mon 10/7/24	Fri 6/20/25
2		**FASE 1: Revisión de la documentación**	**9 wks**	**Mon 10/7/24**	**Fri 12/6/24**
3		Definición del listado de información a solicitar	2 wks	Mon 10/7/24	Fri 10/18/24
4		Preparación y plan de encuentas	2.2 wks	Mon 10/21/2	Mon 11/4/24
5		Preparación y plan de entrevistas	2 wks	Mon 11/4/24	Fri 11/15/24
6		Calendario de visitas a campo	3 wks	Mon 11/18/2	Fri 12/6/24
7		**FASE 2: Identificar los factores de vulnerabilidad cibernética**	**11 wks?**	**Mon 12/9/24**	**Fri 2/21/25**
8		Entrevistas a los dueños del proceso	6 wks	Mon 12/9/24	Fri 1/17/25
9		Entrevistas a los coordinadores de áreas	6.2 wks	Mon 12/9/24	Thu 5/22/25
10		Recolección de información de histórico de paros de producció	6 wks	Mon 12/9/24	Fri 1/17/25
11		Recolección de información de histórico de paros de producció	6 wks?	Mon 12/9/24	Fri 1/17/25
12		Levantamiento de base instalada de PLC´s	6 wks?	Mon 1/13/25	Fri 2/21/25
13		Levantamiento de sistemas SCADA	6 wks?	Mon 1/13/25	Fri 2/21/25
14		Levantamiento de sistemas de control	6 wks?	Mon 1/13/25	Fri 2/21/25
15		Levatamiento de la topología de redes	6 wks?	Mon 1/13/25	Fri 2/21/25
16		Identificación de procesos de almacenamiento de datos Task>	6 wks?	Mon 1/13/25	Fri 2/21/25
17		**FASE 3: Analizar el nivel de vulnerabilidad en las áreas a investig**	**10 wks?**	**Mon 2/10/25**	**Fri 4/18/25**
18		Análisis estadístico de variables	2 wks?	Mon 2/10/25	Fri 2/21/25
19		Evaluación de vulnerabilidad de PLC´s	4 wks?	Mon 2/24/25	Fri 3/21/25
20		Evaluación de vulnerabilidad de sistemas SCADA	4 wks?	Mon 2/24/25	Fri 3/21/25
21		Evaluación de vulnerabilidad de sistemas de control	4 wks?	Mon 2/24/25	Fri 3/21/25
22		Evaluación de los procesos de almacenamiento de datos	4 wks?	Mon 3/24/25	Fri 4/18/25
23		Mapa de proceso Lean Six Sigma	4 wks?	Mon 3/24/25	Fri 4/18/25
24		Análisis de Pareto	4 wks?	Mon 3/24/25	Fri 4/18/25
25		Análisis de Causa Efecto	4 wks?	Mon 3/24/25	Fri 4/18/25
26		**FASE 4: Identificar las posibles soluciones, beneficios e indicadores para reducir la vulnerabilidad cibernética**	**9 wks?**	**Mon 4/21/25**	**Fri 6/20/25**
27		Análisis final de resultados	4 wks?	Mon 4/21/25	Fri 5/16/25
28		Plan metodológico de posibles soluciones	4 wks?	Mon 4/21/25	Fri 5/16/25
29		Conclusiones	5 wks?	Mon 5/19/25	Fri 6/20/25
30		Reporte final	5 wks?	Mon 5/19/25	Fri 6/20/25

Nota. Cronograma. Elaboración propia realizada en Microsoft Project.

12. FACTIBILIDAD DE ESTUDIO

El presente análisis tiene como objetivo evaluar la factibilidad de la investigación a desarrollar, la cual será financiada con recursos propios. El análisis incluye aspectos técnicos, económicos y operativos, para el aseguramiento de la ejecución de esta investigación. La investigación se basó en una metodología establecida para la recolección y análisis de datos.

Se ha elaborado un presupuesto detallado que será cubierto con recursos propios, garantizando así la disponibilidad de los recursos económicos sin dependencia de fuentes externas. La investigación contará con un plan de trabajo definido detallado en el capítulo anterior con el cronograma de actividades en cada una de las fases de la investigación; por lo tanto, el análisis de factibilidad es viable desde los puntos de vista técnico, económico y operativo.

Tabla 4.

Factibilidad del estudio

Descripción	Unidades	Costo Unitario	Costo Total
Recursos Humanos			
Honorarios del Asesor (ad honorem)	1	Q -	Q -
Honorarios estimados (aporte del estudiante)	7	Q 500.00	Q 3,500.00
Recursos Materiales			
Resma papel bond	3	Q 50.00	Q 150.00
Cartuchos impresora tinta	4	Q 100.00	Q 400.00
Bolígrafos	15	Q 5.00	Q 75.00
Folders	20	Q 3.00	Q 60.00
Ganchos para folder	20	Q 2.00	Q 40.00
Servicios			
Teléfono Celular con línea habilitada	7	Q 225.00	Q 1,575.00
Servicio de Internet	7	Q 600.00	Q 4,200.00
Gasolina	7	Q 300.00	Q 2,100.00
Alimentación	7	Q 300.00	Q 2,100.00
Computadora	7	Q -	Q -
Aplicaciones/programas celular/computadora	7	Q 300.00	Q 2,100.00
Imprevistos	7	Q 300.00	Q 2,100.00
Total			Q 18,400.00

Nota. Factibilidad del estudio. Elaboración propia realizada con Excel.

REFERENCIAS

Appa renovables (s. f.). *Diferencias entre energías renovables y convencionales*. https://www.appa.es/energias-renovables/renovables-tipos-y-ventajas/diferencias-entre-energias-renovables-y-convencionales/#

Asociación de Azucareros de Guatemala (18 de agosto de 2023). *Cogeneración de energía*. https://www.azucar.com.gt/tag/cogeneracion-de-energia/

Bickerstaffe, W. (2023). *Operational Technology: The Beginner's Guide: Everything You Need to Know About OT* [Tecnología operativa: la guía para principiantes: todo lo que saber sobre OT]. Edición Kindle.

Cedeño, K. & Loor, G. (2020). *Análisis de ciberseguridad en la SPAM MFL, utilizando las metodologías de AMFE y MARISMA*. [Tesis de maestría, Escuela Superior Politécnica de Manabí Manuel Félix López]. Archivo digital. https://repositorio.espam.edu.ec/bitstream/42000/1338/1/TTMTI01D.pdf

Cengicaña (2020). *Boletín Estadístico Generación de Energía, Recopilación de la información del proceso de generación de energía presentada en los simposios de análisis de las zafras de 1997 al 2020.* https://cengicana.org/files/20201204105723 42.pdf

Coppola, M. (20 de enero de 2023). *Qué es el big data, para qué sirve, características y herramientas*. Hubspot, Inc. https://blog.hubspot.es/website/que-es-big-data

Chun, Y. (2024). *Creación de un sistema embebido para la interconexión de un refrigerador convencional a internet y la automatización de sus funciones mediante comandos de voz a través de AWS*. [Tesis de maestría, Universidad de San Carlos de Guatemala]. Archivo digital. https://drive.google.com/file/d/1zJPLDpuV1wLd6lnsH3QBbdEhtxkDys3/view

Curruchich, S. (24 de mayo de 2021). País produce alcohol con 96 % de pureza. *Diario de Centro América*. https://dca.gob.gt/noticias-guatemala-diario-centro-america/pais-produce-alcohol-con-96-de-pureza/

Ferromayoreo Elizondo (septiembre de 2021). *3 estrategias para Evitar Paros Técnicos en Planta.* https://blog.fmelizondo.com/estrategias-evitar-paros-tecnicos-planta.

Giraldo, Y. (2020). *Construcción de un modelo de ciberseguridad para empresas de servicios informáticos que fortalezca un adecuado manejo de incidentes de seguridad.* [Tesis de maestría, Instituto Tecnológico Metropolitano, Medellín, Colombia]. Archivo digital. http://biblioteca.usac.edu.gt/tesis/04/04_15455.pdf

Girón, W. (2021). *Necesidad de una política nacional de ciberseguridad para infraestructuras críticas en Guatemala.* [Tesis de doctorado,

Universidad de San Carlos de Guatemala]. Archivo digital. http://biblioteca.usac.edu.gt/tesis/04/04_15455.pdf

Instituto de Promoción del Azúcar y el Alcohol Tucumán, IPAAT (s. f.). *Proceso de fabricación del azúcar*. Proceso de fabricación de azúcar (ipaat.gov.ar)

Ingenio Palo Gordo S.A. (s.f.). *Reseña histórica.* https://ipg.com.gt/

Laisequilla, I. (2023). *Todo sobre Lean Six Sigma.* Edición Kindle.

Munirathinam, S. (2020). Industria 4.0: Internet industrial de las cosas (IIoT). *Anvances en las computadoras*, *117*(1), 129-164. https://doi.org/10.1016/bs.adcom.2019.10.010

Microsoft (s.f.). *¿Qué es el almacenamiento en la nube?* https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-cloud-storage

NC Tech (6 de diciembre de 2021). *¿Cómo evitar eventos de paro en industrias de producción continua?* ¿Cómo evitar eventos de paro en industrias de producción continua? - NC Tech

Rea, A. (2020). *Madurez en la Identificación y Evaluación de Riesgos en Ciberseguridad*. [Tesis de doctorado, Universidad Politécnica de Madrid]. Archivo digital. https://oa.upm.es/65871/1/ANGEL_MARCELO_REA_GUAMAN.pdf

Red Latinoamericana de Investigadores de Cadenas Globales de Mercancías REDILACG. (2015). *Sector de biocombustibles de Guatemala.* http://www.redilacg.org/etanol-gm

Varón, R. (2020). *Contextualización de la generación distribuida de energía eléctrica por sistemas de cogeneración y energías alternativas en Colombia*. [Tesis de maestría, Universidad EAN Facultad de ingeniería Bogotá, Colombia]. Archivo digital. https://repository.universidadean.edu.co/server/api/core/bitstreams/d72f0838-7ca8-4909-b341-0348da370af9/content

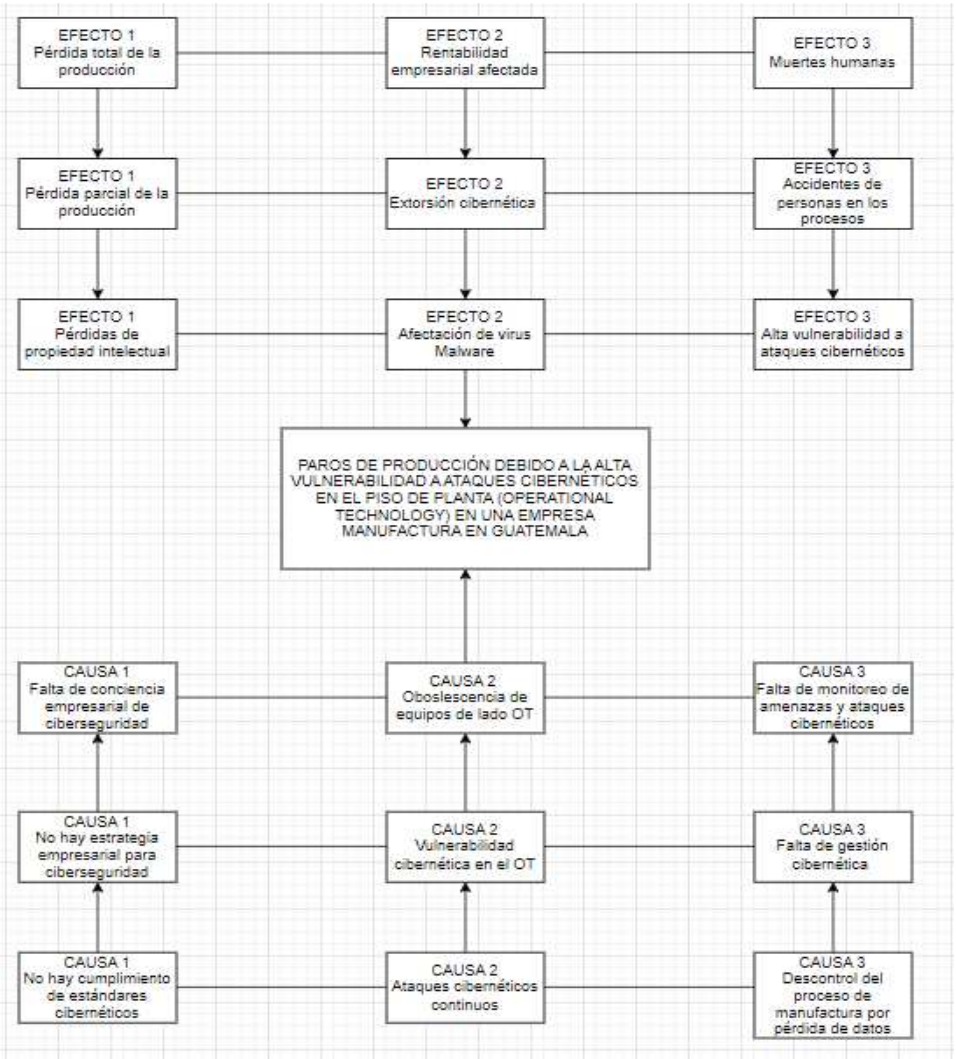
VENCO (5 de octubre de 2023). *Comunicaciones industriales: una guía completa de aplicaciones y usos.* Venco Electrónica. https://www.vencoel.com/comunicaciones-industriales-una-guia-completa-de-aplicaciones-y-usos/

Yánez, F. (2017). *La Meta es la Industria 4.0: Descubre la tecnología que hace posible la nueva Revolución Industrial.* Edición *Kindle*.

APÉNDICES

Apéndice 1.

Árbol de problema



Nota. Diagrama de árbol del problema del trabajo de investigación desarrollado. Elaboración propia realizado con Word.

Apéndice 2.

Matriz de Coherencia

TEMA	TÍTULO	PROBLEMA	PREGUTNA CENTRAL	PREGUNTAS SECUNDARIAS	OBJETIVO CENTRAL	OBJETIVOS SECUNDARIOS
ÁREA DE OPERACIONES: Análisis de riesgos	Diseño de investigación del plan metodológico para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos en una empresa de manufactura en Guatemala, utilizando la metodología de Six Sigma	Paros de producción debido a la alta vulnerabilidad a ataques cibernéticos en la industria en el piso de planta (OT-Operational Technology) en una empresa de manufactura en Guatemala	¿Cuál es el plan metodológico propuesto para reducir los paros de producción debido a la alta vulnerabilidad a ataques cibernéticos en el piso de planta (OT) en una industria de manufactura?	¿Cuáles son los factores que permiten una alta vulnerabilidad a ataques cibernéticos que afectan la producción en el piso de planta (OT) en una industria de manufactura	Proponer el plan metodológico para reducir los paros de producción debido a la alta vulnerabilidad a ataques cibernéticos en el piso de planta (OT) en una industria de manufactua	Identificar los factores que permiten una alta vulnerabilidad a ataques cibernéticos que afectan la producción en el piso de planta (OT) en una industria dentro del marco de
				¿Cuál es el nivel de vulnerabilidad de amenazas y ataques cibernéticos en el piso de planta OT?		Analizar el nivel de vulnerabilidad de amenazas y ataques cibernéticos en el piso de planta OT
				¿Cuáles son las posibles soluciones, beneficios e indicadores para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos de los equipos en el piso de planta (OT)?		Identificar las posibles soluciones, beneficios e indicadores para reducir los paros de producción debido a la alta vulnerabilidad de ataques cibernéticos de los equipos en el piso de planta (OT).

Nota. Matriz de Coherencia realizada en base al planteamiento del problema de investigación. Elaboración propia, realizado con Word.